



الجمهورية العربية السورية

جامعة دمشق

كلية الاقتصاد

قسم المحاسبة

**« تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة
لدى البنوك التجارية في الجمهورية اليمنية »
"دراسة تطبيقية"**

*« Evaluating the Risks of the Security Computerized Accounting Information
Systems at the Commercial Banks in Republic of Yemen »
" An Applied Study "*

أطروحة مقدمة لنيل درجة الدكتوراه في المحاسبة

إعداد الباحث:

عبدالكريم محمد يحيى فاضل

المشرف العلمي الرئيسي:

الأستاذ الدكتور/ عطا الله وراد خليل

أستاذ المحاسبة في كلية الاقتصاد بجامعة دمشق

المشرف العلمي المشارك:

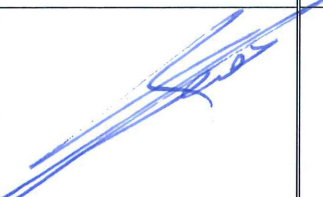
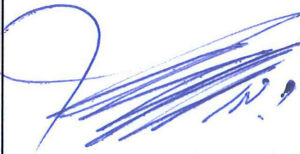
الأستاذ الدكتور/ عبدالمك إسماعيل حجر

أستاذ المحاسبة في كلية التجارة والاقتصاد بجامعة صنعاء

2018 م

قرار لجنة المناقشة والحكم

استناداً إلى قرار مجلس البحث العلمي والدراسات العليا رقم (1279) المتخذ بالجلسة رقم (13) بتاريخ: 2018/3/12 م، بالموافقة على تأليف لجنة المناقشة والحكم على أطروحة الدكتوراه في قسم المحاسبة في كلية الاقتصاد بجامعة دمشق التي أعدها الطالب: **عبدالكريم محمد يحيى فاضل** بعنوان: ((تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية - دراسة تطبيقية))، فقد قررت اللجنة في جلستها العلنية المنعقدة في تمام الساعة الثانية عشر ظهراً من يوم الاثنين الموافق 7 أيار (مايو) 2018م، في مبنى كلية الاقتصاد منح الطالب: **عبدالكريم محمد يحيى فاضل** درجة الدكتوراه في المحاسبة بتقدير "إمتياز"، وبعلامة قدرها (91) درجة، واللجنة مؤلفة من السادة الأساتذة:

م	الاسم والمرتبة العلمية	الصفة	التوقيع
1	د. حسين دحدوح الأستاذ في قسم المحاسبة بكلية الاقتصاد - جامعة دمشق	عضواً	
2	د. عطا الله خليل الأستاذ في قسم المحاسبة بكلية الاقتصاد - جامعة دمشق	عضواً مشرفاً	
3	د. عقبة الرضا الأستاذ المساعد في قسم المحاسبة بكلية الاقتصاد - جامعة دمشق	عضواً	
4	د. علي يوسف الأستاذ المساعد في قسم المحاسبة بكلية الاقتصاد - جامعة دمشق	عضواً	
5	د. مدين الضابط الأستاذ المساعد في قسم المحاسبة بكلية الاقتصاد جامعة طرطوس	عضواً	

مناقشة أطروحة دكتوراه

د.عبدالكريم فاضل



جامعة دمشق - كلية الاقتصاد
7 أيار (مايو) 2018 م

مناقشة أطروحة دكتوراه
د.عبدالكريم فاضل



جامعة دمشق - كلية الاقتصاد
7 أيار (مايو) 2018 م

مناقشة أطروحة دكتوراه
د.عبدالكريم فاضل



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

”يُرَافِقُ اللَّهَ الْتَائِبُ الْمُتَوَلِّئُ الْمُتَنَبِّئُ وَالْزَائِرُ الْوَالِدُ الْعَلِيمُ“

وَالْحَمْدُ لِلَّهِ نَمَا نَعْلَمُ الْخَبِيرُ“

حُزْنُكَ اللَّهُ الْعَظِيمُ

سورة المجادلة، الآية (11).

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

الحمد لله ربّ العالمين، أولاً وأخيراً، الذي بنعمته تتم الصالحات، الحمد لله حمداً كثيراً طيباً مباركاً فيه، والشكر له سبحانه وتعالى على نعمته وتوفيقه، والذي بفضلہ وعونه وتوفيقه منحني العزيمة والقدرة على السير في طريق البحث العلمي، والصلاة والسلام على سيدنا محمد عليه وعلى آله أفضل الصلاة وأتم التسليم القائل "لا يشكر الله من لا يشكر الناس"، أما بعد:

لا يسعني في هذا المقام إلا أن أتقدم بجزيل شكري وامتناني إلى أستاذي العزيز المشرف على هذه الأطروحة، الأستاذ الدكتور عطا الله ورّاد خليل لتحمله عناء الإشراف على هذه الأطروحة، ولسعة صدره وعظيم فضله، والذي قدم لي النصّح والتوجيه والمساعدة والنقد البناء والذي كان له الأثر الكبير في إنجاز هذه الدراسة والوصول بها إلى ما وصلت إليه الآن، وكان مثلاً يُحتذى، فله منى عظيم الشكر والتقدير والعرفان. وهي موصولة كذلك لأستاذي الفاضل الأستاذ الدكتور عبد الملك حجر على تفضله لي بالمشاركة في الإشراف على إجراء الدراسة التطبيقية في اليمن، وعلى ما فاض به عليا من واسع علمه وكريم خلقه، ومتابعته المستمرة وتوجيهاته المفيدة في الجانب العملي، والتي عززت من منهجية هذه الدراسة، فجزاه الله عني خير الجزاء، ومتعته بالصحة والعافية.

كما أتقدم بالشكر والامتنان للأساتذة الأجلاء أعضاء لجنة المناقشة والحكم لتكرمهم بقراءة وتقييم ومناقشة هذه الأطروحة وإبداء ملاحظاتهم وآرائهم وحكمهم عليها، وهي فرصة طيبة للباحث للاستفادة من توجيهاتهم العلمية القيمة دعماً وإثراء لهذه الدراسة.

وأتوجه بالشكر الجزيل لكل أستاذ علّمني ولو حرفاً واحداً عبر سني عمري الدراسية، كما أتوجه بالشكر والعرفان إلى هذا الصرح العلمي الشامخ، جامعة دمشق العريقة التي منحتني شرف الانتساب العلمي إليها في مرحلة الدكتوراه، وإلى جميع أعضاء هيئة التدريس بكلية الاقتصاد الذين كانوا مثلاً للأخوة العربية الصادقة، وعنواناً مشرفاً للتعامل الطيب، وإلى كافة الأشقاء أبناء الشعب السوري الأصيل.

ويقتضي العرفان بالجميل أن أتقدم بالشكر لجميع العاملين في سفارة الجمهورية اليمنية في دمشق، وأخص بالذكر الرفيق نائف القانص سعادة سفير الجمهورية اليمنية بدمشق وكافة الأخوة العاملين في الملحقة الثقافية بالسفارة، على تعاونهم معي وتذليلهم معظم الصعاب خلال فترة البحث والدراسة في دمشق.

والشكر والتقدير لرئاسة جامعة عمران وللزملاء الأعزاء أعضاء هيئة التدريس بكليتي التجارة والاقتصاد بجامعتي صنعاء وعمران، وجميع العاملين فيهما لدعمهم المعنوي لي أثناء فترة البحث.

وفي الختام اللهم إني أسألك السداد والفلاح، وأن يكون عملي هذا خالصاً لوجهك الكريم ومسخرّاً لرفعة شأن اليمن وأمتنا العربية والإسلامية، وفي ميزان حسناتنا يوم القيامة.

بسم الله

والله ولي التوفيق والسداد،،

قائمة المحتويات

رقم الصفحة	الموضوع	التسلسل
....	عنوان الدراسة	...
....	قرار لجنة المناقشة والحكم.	...
...	تفويض.	...
أ	توطئة.	...
ب	الإهداء.	...
ج	الشكر والتقدير.	...
د	قائمة المحتويات.	...
ط	قائمة الجداول.	...
م	قائمة الأشكال.	...
م	قائمة الملاحق.	...
ن	قائمة الرموز المختصرة المستخدمة في الدراسة.	...
ع	ملخص الدراسة باللغة العربية.	...
1	الإطار العام للدراسة	
1	مقدمة.	1
2	مشكلة الدراسة.	2
3	أهمية الدراسة.	3
4	أهداف الدراسة.	4
5	الدراسات السابقة.	5
12	ما يميز هذه الدراسة عن الدراسات السابقة.	6
14	فرضيات الدراسة.	7
15	أنموذج الدراسة.	8
16	حدود ومحددات الدراسة.	9
17	خطة الدراسة.	10
18	الفصل الأول: مخاطر أمن نظم المعلومات المحاسبية	1
18	المبحث الأول: أمن نظم المعلومات المحاسبية.	1-1
19	ماهية نظم المعلومات المحاسبية (CAIS).	:1-1-1
21	مكونات نظم المعلومات المحاسبية.	:2-1-1
22	أنواع نظم المعلومات المحاسبية المحوسبة على أساس بيئة التشغيل البيانات.	:3-1-1
23	دورة تجهيز البيانات في نظم المعلومات المحاسبية المحوسبة ووظائفه المختلفة.	:4-1-1
26	تعريف أمن نظم المعلومات المحاسبية المحوسبة.	:5-1-1
29	المبادئ والأهداف الأساسية لأمن نظم المعلومات المحاسبية المحوسبة.	:6-1-1
33	مكونات أمن نظم المعلومات المحاسبية المحوسبة.	:7-1-1
35	المحاور الأساسية لأمن نظم المعلومات المحاسبية المحوسبة.	:8-1-1

رقم الصفحة	الموضوع	التسلسل
40	المبحث الثاني: طبيعة وأنواع مخاطر أمن نظم المعلومات المحاسبية المحوسبة:	2-1
41	تعريفات ومفاهيم مخاطر أمن نظم المعلومات المحاسبية المحوسبة.	1-2-1
48	المخاطر التي تهدد أمن الأفراد العاملين في نظم المعلومات المحاسبية المحوسبة.	2-2-1
49	المخاطر التي تهدد الأمن المادي لنظم المعلومات المحاسبية المحوسبة.	3-2-1
51	المخاطر التي تهدد أمن الوصول البرمجي لنظم المعلومات المحاسبية المحوسبة.	4-2-1
53	المخاطر التي تهدد أمن التخزين غير المتصل بقاعدة بيانات نظم المعلومات المحاسبية المحوسبة.	5-2-1
54	المخاطر التي تهدد أمن مدخلات نظم المعلومات المحاسبية المحوسبة.	6-2-1
54	المخاطر التي تهدد أمن عمليات تشغيل نظم المعلومات المحاسبية المحوسبة.	7-2-1
55	المخاطر التي تهدد أمن مخرجات نظم المعلومات المحاسبية المحوسبة.	8-2-1
56	المخاطر التي تهدد أمن تبادل البيانات عبر شبكات نظم المعلومات المحاسبية المحوسبة.	9-2-1
60	المخاطر التي تهدد أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة.	10-2-1
62	المبحث الثالث: التهديدات الداخلية المسببة لمخاطر أمن نظم المعلومات المحاسبية المحوسبة:	3-1
65	التهديدات الأمنية المتعلقة بفلسفة الإدارة العليا للمنشأة.	1-3-1
69	التهديدات الأمنية المتعلقة بالعوامل التنظيمية للمنشأة.	2-3-1
72	التهديدات الأمنية المتعلقة بالتكنولوجيا المستخدمة في المنشأة.	3-3-1
76	التهديدات الأمنية المتعلقة بالأفراد العاملين في المنشأة.	4-3-1
81	التهديدات الأمنية المتعلقة بضعف إجراءات الرقابة الداخلية في المنشأة.	5-3-1
85	التهديدات الأمنية المتعلقة بحدوث الكوارث غير الطبيعية في المنشأة.	6-3-1
86	المبحث الرابع: التهديدات الخارجية المسببة لمخاطر أمن نظم المعلومات المحاسبية المحوسبة:	4-1
86	التهديدات الأمنية المتعلقة بالتغيرات والتطورات التكنولوجية المتسارعة.	1-4-1
90	التهديدات الأمنية المتعلقة بالكوارث الطبيعية والسياسية.	2-4-1
92	التهديدات الأمنية المتعلقة بالمخترقين والقراصنة.	3-4-1
94	التهديدات الأمنية المتعلقة بالبرمجيات الخبيثة.	4-4-1
99	التهديدات الأمنية المتعلقة بالمنافسة الاقتصادية بين المنشآت.	5-4-1
100	التهديدات الأمنية المتعلقة بضعف الرقابة الخارجية.	6-4-1
104	التهديدات الأمنية المتعلقة بضعف التشريعات والقوانين المحلية المتعلقة بتكنولوجيا المعلومات.	7-4-1
107	التهديدات الأمنية المتعلقة بنقص الوعي الإلكتروني لدى العملاء.	8-4-1
110	الفصل الثاني: تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة	2
111	المبحث الأول: أهم المعايير والأطر الدولية المستخدمة في تقييم مخاطر أمن نظم المعلومات:	1-2
112	مفهوم معايير أمن نظم المعلومات.	1-1-2

رقم الصفحة	الموضوع	التسلسل
113	أهمية استخدام المعايير لتقييم وإدارة مخاطر أمن نظم المعلومات الحاسوبية.	2-1-2
115	الإطار المستند إلى أهداف الرقابة على المعلومات والتكنولوجيا ذات العلاقة (COBIT).	3-1-2
119	المبادئ العامة لأمن نظم المعلومات الصادرة عن منظمة التعاون الاقتصادي والتنمية (OECD).	4-1-2
122	المعايير الصادرة عن المنظمة الدولية لتوحيد المعايير (ISO).	5-1-2
129	الأدلة الصادرة عن المعهد الوطني للمعايير والتكنولوجيا (NIST).	6-1-2
131	أهم التشريعات والقوانين والتعليمات المحلية الصادرة في الجمهورية اليمنية والمتعلقة بأمن نظم المعلومات.	7-1-2
132	المبحث الثاني: طبيعة ومنهجية تقييم مخاطر أمن نظم المعلومات الحاسوبية:	2-2
133	مفهوم تقييم مخاطر أمن نظم المعلومات الحاسوبية.	1-2-2
136	أهمية تقييم مخاطر أمن نظم المعلومات الحاسوبية.	2-2-2
138	خطوات عملية تقييم مخاطر أمن نظم المعلومات الحاسوبية.	3-2-2
148	أدوات تقييم مخاطر أمن نظم المعلومات الحاسوبية.	4-2-2
151	المبحث الثالث: تأثيرات حدوث المخاطر على أمن نظم المعلومات الحاسوبية:	3-2
153	تأثير حدوث المخاطر على إتاحة نظم المعلومات الحاسوبية.	1-3-2
156	تأثير حدوث المخاطر على سلامة وتكامل تجهيز البيانات في نظم المعلومات الحاسوبية.	2-3-2
159	تأثير حدوث المخاطر على سرية المعلومات الناتجة عن نظم المعلومات الحاسوبية.	3-3-2
161	تأثير حدوث المخاطر على خصوصية بيانات الأطراف المتعاملة مع المنشأة والمخزنة في نظم المعلومات الحاسوبية.	4-3-2
164	تأثير حدوث المخاطر على إثبات تصرفات الأطراف المتعاملة مع المنشأة.	5-3-2
167	المبحث الرابع: إجراءات ووسائل الحماية الداخلية في نظم المعلومات الحاسوبية المصممة لمواجهة المخاطر الأمنية:	4-2
169	طبيعة الرقابة الداخلية لنظم المعلومات الحاسوبية وأنواعها.	1-4-2
169	أهمية وأهداف نظم الرقابة الداخلية في نظم المعلومات الحاسوبية.	2-4-2
171	أنواع إجراءات ووسائل الحماية الداخلية في نظم المعلومات الحاسوبية.	3-4-2
177	حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات الحاسوبية.	4-4-2
178	حماية الأمن المادي لنظم المعلومات الحاسوبية.	5-4-2
179	حماية أمن الوصول البرمجي لقاعدة بيانات نظم المعلومات الحاسوبية.	6-4-2
180	حماية أمن التخزين غير المتصل بقاعدة البيانات في نظم المعلومات الحاسوبية.	7-4-2
180	حماية أمن مدخلات نظم المعلومات الحاسوبية.	8-4-2
181	حماية أمن عمليات التشغيل البرمجي لنظم المعلومات الحاسوبية.	9-4-2
181	حماية أمن مخرجات نظم المعلومات الحاسوبية.	10-4-2
182	حماية أمن البيانات والمعلومات المنقولة عبر شبكات نظم المعلومات الحاسوبية.	11-4-2
184	حماية أمن تعديل وتطوير نظم المعلومات الحاسوبية.	12-4-2

رقم الصفحة	الموضوع	التسلسل
186	الفصل الثالث: الدراسة التطبيقية:	3
186	المبحث الأول: منهج وأساليب جمع وتحليل البيانات والاختبارات التمهيدية:	1-3
187	منهجية الدراسة والإجراءات المتبعة.	1-1-3
188	مجتمع الدراسة وعينتها.	2-1-3
189	مصادر جمع البيانات والمعلومات.	3-1-3
190	آلية وإجراءات تحليل ومعالجة بيانات الاستبيان.	4-1-3
192	أداة الدراسة - مكوناتها وآلية توزيعها واستردادها.	5-1-3
194	آلية وإجراءات تحليل ومعالجة بيانات الاستقصاء	6-1-3
195	المقاييس والأساليب التحليلية الإحصائية المستخدمة في معالجة البيانات:	7-1-3
197	التحقق من صدق أداة الدراسة واختبار موثوقيتها وثباتها.	8-1-3
198	اختبار التوزيع الطبيعي لبيانات متغيرات الدراسة.	9-1-3
199	اختبار قوة نموذج الدراسة.	10-1-3
201	المبحث الثاني: دراسة الحالة العملية لتقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى بعض البنوك التجارية في الجمهورية اليمنية:	2-3
201	هيكل البنوك التجارية في الجمهورية اليمنية.	1-2-3
203	الخدمات المصرفية التقليدية للبنوك التجارية في الجمهورية اليمنية.	2-2-3
204	تطور الخدمات المصرفية الإلكترونية في البنوك التجارية في الجمهورية اليمنية.	3-2-3
209	معلومات أساسية عن البنوك التجارية محل الدراسة العملية.	4-2-3
212	تقييم مخاطر أمن نظم المعلومات المحاسبية لدى البنوك التجارية محل الدراسة العملية.	5-2-3
220	تقييم التهديدات الداخلية لأمن نظم المعلومات المحاسبية لدى البنوك محل الدراسة العملية.	6-2-3
226	تقييم التهديدات الخارجية لأمن نظم المعلومات المحاسبية لدى البنوك محل الدراسة العملية.	7-2-3
233	تقييم تأثير المخاطر المختلفة على أمن نظم المعلومات المحاسبية لدى البنوك محل الدراسة العملية.	8-2-3
237	تقييم إجراءات ووسائل الحماية لأمن نظم المعلومات المحاسبية لدى البنوك محل الدراسة العملية.	9-2-3
246	جوانب أخرى متعلقة بتقييم مخاطر أمن نظم المعلومات المحاسبية لدى البنوك محل الدراسة العملية.	10-2-3
247	أهم ملاحظات ومقترحات الباحث من واقع قيامه بدراسة الحالة العملية.	11-2-3
258	المبحث الثالث: عرض وتحليل ومناقشة البيانات:	3-3
258	تحليل البيانات المتعلقة بالخصائص الشخصية والوظيفية للأفراد الممثلين لعينة الدراسة.	1-3-3
261	تحليل البيانات المتعلقة بخصائص البنوك التجارية في الجمهورية اليمنية وطبيعة نظم المعلومات المحاسبية في تلك البنوك.	2-3-3
267	تحليل البيانات المتعلقة بالمخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة.	3-3-3

رقم الصفحة	الموضوع	التسلسل
275	تحليل البيانات المتعلقة بالتهديدات الداخلية التي تسبب مخاطر أمن نظم المعلومات المحاسبية المحوسبة	4-3-3:
282	تحليل البيانات المتعلقة بالتهديدات الخارجية التي تسبب مخاطر أمن نظم المعلومات المحاسبية المحوسبة	5-3-3:
288	تحليل البيانات المتعلقة بمدى تأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة.	6-3-3:
294	تحليل البيانات المتعلقة بحماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية المحوسبة.	7-3-3:
298	تحليل البيانات المتعلقة بحماية الأمن المادي لنظم المعلومات المحاسبية المحوسبة.	8-3-3:
302	تحليل البيانات المتعلقة بحماية أمن الوصول البرمجي لقاعدة البيانات المتصلة بنظم المعلومات المحاسبية المحوسبة.	9-3-3:
306	تحليل البيانات المتعلقة بحماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية المحوسبة.	10-3-3:
308	تحليل البيانات المتعلقة بحماية أمن مدخلات نظم المعلومات المحاسبية المحوسبة.	11-3-3:
311	تحليل البيانات المتعلقة بحماية أمن عمليات التشغيل البرمجي لنظم المعلومات المحاسبية المحوسبة.	12-3-3:
315	تحليل البيانات المتعلقة بحماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة.	13-3-3:
317	تحليل البيانات المتعلقة بحماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية المحوسبة.	14-3-3:
321	تحليل البيانات المتعلقة بحماية أمن تعديل تطوير نظم المعلومات المحاسبية المحوسبة.	15-3-3:
324	تحليل البيانات المتعلقة بإجراءات ووسائل حماية أمن نظم المعلومات المحاسبية المحوسبة ككل.	16-3-3:
327	المبحث الرابع: التحليل الاستدلالي للبيانات لاختبار فرضيات الدراسة:	4-3
327	نتيجة اختبار الفرضية الأولى.	1-4-3:
332	نتيجة اختبار الفرضية الثانية.	2-4-3:
335	نتيجة اختبار الفرضية الثالثة.	3-4-3:
338	نتيجة اختبار الفرضية الرابعة.	4-4-3:
341	نتيجة اختبار الفرضية الخامسة.	5-4-3:
358	نتيجة اختبار الفرضية السادسة.	6-4-3:
360	نتيجة اختبار الفرضية السابعة.	7-4-3:
361	نتيجة اختبار الفرضية الثامنة.	8-4-3:
362	نتيجة اختبار الفرضية التاسعة.	9-4-3:
363	نتيجة اختبار الفرضية العاشرة.	10-4-3:
364	المبحث الخامس: النتائج والتوصيات والمقترحات:	5-3
364	نتائج الدراسة.	1-5-3:
368	توصيات ومقترحات الدراسة.	2-5-3:

الترتيب	الموضوع	الصفحة
	- قائمة المصادر والمراجع:	375
أولاً:	المراجع باللغة العربية.	375
ثانياً:	المراجع باللغة الإنجليزية.	385
	- الملاحق:	
1	قائمة الاستقصاء.	1
2	قائمة بأسماء الأساتذة المحكمين الذين قاموا بالتأكد من صدق وصلاحية قائمة الاستقصاء.	17
3	عينة الدراسة لدى البنوك التجارية في الجمهورية اليمنية.	18
4	آلية توزيع قائمة الاستقصاء.	19
5	مخرجات ونتائج التحليل بواسطة برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS).	20
...	تعريف بالباحث.	...
...	الملخص باللغة الانجليزية.	...
...	عنوان الدراسة باللغة الانجليزية.	...

قائمة الجداول

الترتيب	عنوان الجدول	الصفحة
1-1-3	البنوك التجارية في الجمهورية اليمنية مرتبة وفقاً لسنة التأسيس موضحاً فيها مجتمع الدراسة والعينة المختارة.	191
2-1-3	الاستقصاءات الموزعة والمستردة والمستبعدة والخاضعة للتحليل مصنفة وفقاً لاسم البنك	193
3-1-3	مستويات الأهمية النسبية لإجابات عينة الدراسة وفقاً للمتوسط الحسابي	194
4-1-3	درجات الموافقة والنسب المئوية المقابلة لها والصيغة الكمية المقابلة لها.	194
5-1-3	اختبار معامل ألفا كرونباخ للتحقق من درجة ثبات البيانات الواردة في الاستقصاء.	198
6-1-3	يبيّن نتيجة اختبار (K-S) حول إتباع بيانات الدراسة للتوزيع الطبيعي (توزيع غوس)	199
7-1-3	مصفوفة معاملات ارتباط (بيرسون) بين متغيرات الدراسة	200
1-2-3	البنوك التجارية في الجمهورية اليمنية مرتبة وفقاً لسنة التأسيس.	202
2-2-3	الخدمات المصرفية الإلكترونية في البنوك التجارية في الجمهورية اليمنية	207
3-2-3	مصفوفة تقييم مخاطر أمن الأفراد العاملين في نظم المعلومات المحاسبية.	212
4-2-3	مصفوفة تقييم مخاطر الأمن المادي لنظم المعلومات المحاسبية.	213
5-2-3	مصفوفة تقييم مخاطر الوصول البرمجي لقواعد نظم المعلومات المحاسبية.	214
6-2-3	مصفوفة تقييم مخاطر أمن النسخ في وسائط غير متصلة بقواعد بيانات نظم المعلومات المحاسبية.	214
7-2-3	مصفوفة تقييم مخاطر أمن عمليات مدخلات نظم المعلومات المحاسبية.	215
8-2-3	مصفوفة تقييم مخاطر أمن عمليات تشغيل نظم المعلومات المحاسبية.	216
9-2-3	مصفوفة تقييم مخاطر أمن مخرجات نظم المعلومات المحاسبية.	217
10-2-3	مصفوفة تقييم مخاطر أمن تبادل البيانات عبر شبكات نظم المعلومات المحاسبية	218
11-2-3	مصفوفة تقييم مخاطر أمن تعديل وتطوير نظم المعلومات المحاسبية	219
12-2-3	مصفوفة تقييم المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة.	219
13-2-3	مصفوفة تقييم التهديدات الداخلية المسببة للمخاطر نتيجة فلسفة الإدارة العليا للبنك.	221

الصفحة	عنوان الجدول	التسلسل
221	مصفوفة تقييم التهديدات الداخلية المسببة للمخاطر نتيجة التهديدات التنظيمية للبنك.	14-2-3
222	مصفوفة تقييم التهديدات الداخلية المسببة للمخاطر نتيجة إمكانات البنك التكنولوجية.	15-2-3
223	مصفوفة تقييم التهديدات الداخلية المسببة للمخاطر نتيجة الأفراد العاملين.	16-2-3
224	مصفوفة تقييم التهديدات الداخلية المسببة للمخاطر نتيجة ضعف نظم الرقابة الداخلية للبنك.	17-2-3
225	مصفوفة تقييم التهديدات الداخلية المسببة للمخاطر نتيجة الكوارث الداخلية للبنك.	18-2-3
225	مصفوفة تقييم التهديدات الداخلية المسببة لحدوث مخاطر أمن نظم المعلومات المحاسبية.	19-2-3
227	مصفوفة تقييم التهديدات الخارجية المسببة للمخاطر نتيجة التغير التكنولوجي.	20-2-3
227	مصفوفة تقييم التهديدات الخارجية المسببة للمخاطر نتيجة الكوارث الطبيعية.	21-2-3
228	مصفوفة تقييم التهديدات الخارجية المسببة للمخاطر نتيجة المخترقون والقراصنة.	22-2-3
229	مصفوفة تقييم التهديدات الخارجية المسببة للمخاطر نتيجة فيروسات الحاسوب.	23-2-3
229	مصفوفة تقييم التهديدات الخارجية المسببة للمخاطر نتيجة المنافسة الاقتصادية.	24-2-3
230	مصفوفة تقييم التهديدات الخارجية المسببة للمخاطر نتيجة ضعف الرقابة الخارجية.	25-2-3
231	مصفوفة تقييم التهديدات الخارجية المسببة للمخاطر نتيجة ضعف التشريعات والقوانين.	26-2-3
231	مصفوفة تقييم التهديدات الخارجية المسببة للمخاطر نتيجة ضعف الوعي الإلكتروني للعملاء.	27-2-3
232	مصفوفة تقييم التهديدات الخارجية المسببة لحدوث مخاطر أمن نظم المعلومات المحاسبية.	28-2-3
233	مصفوفة تقييم تأثير حدوث المخاطر على إتاحة نظم المعلومات المحاسبية.	29-2-3
234	مصفوفة تقييم تأثير حدوث المخاطر على سلامة وتكامل نظم المعلومات المحاسبية.	30-2-3
234	مصفوفة تقييم تأثير حدوث المخاطر على سرية المعلومات المحاسبية.	31-2-3
235	مصفوفة تقييم تأثير حدوث المخاطر على خصوصية بيانات الأطراف المتعاملة مع البنك.	32-2-3
236	مصفوفة تقييم تأثير حدوث المخاطر على إثبات تصرفات الأطراف المتعاملة خلال تبادل البيانات إلكترونياً.	33-2-3
236	مصفوفة تقييم تأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية.	34-2-3
238	مصفوفة تقييم حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية.	35-2-3
239	مصفوفة تقييم حماية أمن الوصول المادي لنظم المعلومات المحاسبية.	36-2-3
240	مصفوفة تقييم حماية أمن الوصول البرمجي لنظم المعلومات المحاسبية.	37-2-3
241	مصفوفة تقييم حماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية.	38-2-3
242	مصفوفة تقييم حماية أمن مدخلات نظم المعلومات المحاسبية.	39-2-3
242	مصفوفة تقييم حماية أمن عمليات تشغيل نظم المعلومات المحاسبية.	40-2-3
243	مصفوفة تقييم حماية أمن مخرجات نظم المعلومات المحاسبية.	41-2-3
244	مصفوفة تقييم حماية أمن تبادل البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية.	42-2-3
245	مصفوفة تقييم حماية أمن عمليات تعديل وتطوير نظم المعلومات المحاسبية.	43-2-3
245	مصفوفة تقييم إجراءات ووسائل حماية أمن نظم المعلومات المحاسبية المحوسبة.	44-2-3
246	مصفوفة تقييم الجوانب الأخرى الخاصة المتعلقة بإدارة وتقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة.	45-2-3
247	ملخص لملاحظات وتوصيات الباحث الخاصة بدراسة الحالة العملية.	46-2-3
258	الخصائص الشخصية والوظيفية للأفراد الممثلين لعينة الدراسة.	1-3-3
261	خصائص البنوك التجارية في الجمهورية اليمنية وطبيعة نظم المعلومات المحاسبية المستخدمة في تلك البنوك حسب آراء أفراد العينة.	2-3-3
267	الإحصاءات الوصفية على مستوى الفقرات والمتغيرات الرئيسية المتعلقة بحدوث المخاطر التي	3-3-3

الصفحة	عنوان الجدول	التسلسل
	تهدد أمن نظم المعلومات المحاسبية المحوسبة.	
273	الإحصاءات الوصفية للمتغيرات الرئيسية المتعلقة بحدوث المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة مرتبة تنازلياً حسب الأهمية النسبية.	4-3-3
275	الإحصاءات الوصفية على مستوى الفقرات والمتغيرات الرئيسية المتعلقة بالتهديدات الداخلية التي تسبب مخاطر أمن نظم المعلومات المحاسبية المحوسبة.	5-3-3
280	الإحصاءات الوصفية للمتغيرات الرئيسية المتعلقة بالتهديدات الداخلية المسببة لحدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة مرتبة تنازلياً حسب الأهمية النسبية.	6-3-3
282	الإحصاءات الوصفية على مستوى الفقرات والمتغيرات الرئيسية المتعلقة بالتهديدات الخارجية التي تسبب مخاطر أمن نظم المعلومات المحاسبية المحوسبة.	7-3-3
286	الإحصاءات الوصفية للمتغيرات الرئيسية المتعلقة بالتهديدات الخارجية التي قد تسبب حدوث مخاطر أمن نظم المعلومات المحاسبية مرتبة تنازلياً حسب الأهمية النسبية.	8-3-3
288	الإحصاءات الوصفية على مستوى الفقرات والمتغيرات الرئيسية المتعلقة بمدى تأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة.	9-3-3
292	الإحصاءات الوصفية للمتغيرات الرئيسية المتعلقة بتأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة مرتبة تنازلياً حسب الأهمية النسبية.	10-3-3
294	الإحصاءات الوصفية على مستوى الفقرات المتعلقة بمدى تطبيق إجراءات ووسائل حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية المحوسبة.	11-3-3
298	الإحصاءات الوصفية على مستوى الفقرات المتعلقة بمدى تطبيق إجراءات ووسائل حماية الأمن المادي لنظم المعلومات المحاسبية المحوسبة.	12-3-3
302	الإحصاءات الوصفية على مستوى الفقرات المتعلقة بمدى تطبيق إجراءات ووسائل حماية أمن الوصول البرمجي لقاعدة البيانات المتصلة بنظم المعلومات المحاسبية.	13-3-3
306	الإحصاءات الوصفية على مستوى الفقرات المتعلقة بمدى تطبيق إجراءات ووسائل حماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية المحوسبة.	14-3-3
309	الإحصاءات الوصفية على مستوى الفقرات المتعلقة بمدى تطبيق إجراءات ووسائل حماية أمن مدخلات نظم المعلومات المحاسبية المحوسبة.	15-3-3
312	الإحصاءات الوصفية على مستوى الفقرات المتعلقة بمدى تطبيق إجراءات ووسائل حماية أمن عمليات التشغيل البرمجي لنظم المعلومات المحاسبية المحوسبة.	16-3-3
315	الإحصاءات الوصفية على مستوى الفقرات المتعلقة بمدى تطبيق إجراءات ووسائل حماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة.	17-3-3
318	الإحصاءات الوصفية على مستوى الفقرات المتعلقة بمدى تطبيق إجراءات ووسائل حماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية المحوسبة.	18-3-3
321	الإحصاءات الوصفية على مستوى الفقرات المتعلقة بمدى تطبيق إجراءات ووسائل حماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة.	19-3-3
324	الإحصاءات الوصفية للمتغيرات الرئيسية المتعلقة بإجراءات ووسائل حماية أمن نظم المعلومات المحاسبية المحوسبة مرتبة تنازلياً حسب الأهمية النسبية.	20-3-3
328	نتيجة اختبار (T) لعينة الدراسة بشأن الفقرات الرئيسية والفرعية للفرضية الأولى المتعلقة بحدوث المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة	1-4-3
332	نتيجة اختبار (T) لعينة الدراسة بشأن الفقرات الرئيسية والفرعية للفرضية الثانية والمتعلقة بالتهديدات الداخلية المسببة لحدوث مخاطر أمن نظم المعلومات المحاسبية.	2-4-3
336	نتيجة اختبار (T) لعينة الدراسة بشأن الفقرات الرئيسية والفرعية للفرضية الثالثة والمتعلقة	3-4-3

الصفحة	عنوان الجدول	التسلسل
	بالتحديات الخارجية المسببة لحدوث مخاطر أمن نظم المعلومات المحاسبية.	
339	نتيجة اختبار (T) لعينة الدراسة بشأن الفقرات الرئيسية والفرعية للفرضية الرابعة والمتعلقة بتأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة	4-4-3
342	نتيجة اختبار (T) لعينة الدراسة على مستوى الفقرات المتعلقة بحماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية المحوسبة	5-4-3
344	نتيجة اختبار (T) لعينة الدراسة على مستوى الفقرات المتعلقة بحماية الأمن المادي لنظم المعلومات المحاسبية المحوسبة	6-4-3
346	نتيجة اختبار (T) لعينة الدراسة على مستوى الفقرات المتعلقة بحماية أمن الوصول البرمجي لقواعد بيانات نظم المعلومات المحاسبية المحوسبة.	7-4-3
348	نتيجة اختبار (T) لعينة الدراسة على مستوى الفقرات المتعلقة بحماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية.	8-4-3
349	نتيجة اختبار (T) لعينة الدراسة على مستوى الفقرات المتعلقة بحماية أمن مدخلات نظم المعلومات المحاسبية المحوسبة	9-4-3
351	نتيجة اختبار (T) لعينة الدراسة على مستوى الفقرات المتعلقة بحماية أمن عمليات التشغيل البرمجي لنظم المعلومات المحاسبية المحوسبة	10-4-3
352	نتيجة اختبار (T) لعينة الدراسة على مستوى الفقرات المتعلقة بحماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة	11-4-3
354	نتيجة اختبار (T) لعينة الدراسة على مستوى الفقرات المتعلقة بحماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية المحوسبة	12-4-3
355	نتيجة اختبار (T) لعينة الدراسة على مستوى الفقرات المتعلقة بحماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة	13-4-3
357	نتيجة اختبار (T) لعينة الدراسة على مستوى الأبعاد الكلية المتعلقة بأساليب وإجراءات حماية أمن نظم المعلومات المحاسبية المحوسبة	14-4-3
359	نتائج اختبار تحليل الانحدار البسيط لبيان مدى تأثير أساليب وإجراءات الحماية المطبقة في البنوك التجارية في الجمهورية اليمنية على المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة	15-4-3
360	نتائج اختبار تحليل التباين الأحادي (ANOVA) للفروق بين إجابات أفراد العينة حول مخاطر أمن نظم المعلومات المحاسبية المحوسبة حسب المسمى الوظيفي.	16-4-3
361	نتائج اختبار تحليل التباين الأحادي (ANOVA) للفروق بين إجابات أفراد العينة حول مخاطر أمن نظم المعلومات المحاسبية المحوسبة حسب ملكية البنك.	17-4-3
362	نتائج اختبار تحليل التباين الأحادي (ANOVA) للفروق بين إجابات أفراد العينة حول مخاطر أمن نظم المعلومات المحاسبية المحوسبة حسب نوعية تشغيل النظام	18-4-3
363	نتائج اختبار تحليل التباين الأحادي (ANOVA) للفروق بين إجابات أفراد العينة حول مخاطر أمن نظم المعلومات المحاسبية المحوسبة حسب مستوى ارتباط النظم التي يعملون بها بشبكات الاتصال	19-4-3

قائمة الأشكال

رقم الصفحة	عنوان الشكل	التسلسل
15	أنموذج الدراسة يوضح المتغيرات المستقلة والمتغير التابع.	1
22	مكونات نظم المعلومات المحاسبية المحوسبة.	1-1-1
26	دورة تجهيز البيانات في نظام المعلومات المحاسبي.	2-1-1
30	المبادئ والأهداف الثلاثة الهامة لأمن نظم المعلومات.	3-1-1
34	مكونات أمن نظم المعلومات المحاسبية المحوسبة.	4-1-1
42	سياق نشوء الخطر.	1-2-1
43	الترباط المنطقي لمكونات مخاطر أمن نظم المعلومات المحاسبية المحوسبة.	2-2-1
50	مواطن الخطر الرئيسية في بيئة نظم المعلومات المحوسبة.	3-2-1
124	مجموعة معايير ISO 27K.	1-1-2
141	تحليل أثر حدوث المخاطر.	1-2-2
143	العلاقة بين مدى قابلية المنشأة للتعرض للمخاطر والأثر الناتج عن التهديدات.	2-2-2
147	مراحل تقييم وإدارة مخاطر أمن نظم المعلومات المحاسبية المحوسبة.	3-2-2
149	مصفوفة تقييم شدة المخاطر.	4-2-2
158	المخاطر المرتفعة تؤدي إلى قرارات منخفضة القيمة.	1-3-2
170	دور الرقابة الداخلية في تحقيق أهداف المنشأة.	1-4-2
204	وظائف البنوك التجارية المعاصرة.	1-2-3

قائمة الملاحق

رقم	عنوان الملحق	التسلسل
1	قائمة الاستقصاء الخاصة بالدراسة.	1
17	كشف بأسماء الأساتذة المحكمين لصدق وصلاحيّة قائمة الاستقصاء.	2
18	البنوك التجارية في الجمهورية اليمنية مرتبة وفقاً لسنة التأسيس موضحاً فيه مجتمع الدراسة وحجم العينة المختارة.	3
19	توزيع أفراد مجتمع وعينة الدراسة على البنوك التجارية في الجمهورية اليمنية موضحاً فيه قوائم الاستقصاء الموزعة والمستردة والمستبعدة والخاضعة للتحليل مصنفة وفقاً لاسم البنك.	4
20	مخرجات ونتائج التحليل بواسطة برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS).	5

قائمة الرموز المختصرة المستخدمة في الدراسة

م	الرمز المختصر	مضمونه باللغة الإنجليزية	مضمونه باللغة العربية
1	AISA	<i>American Information Systems Association</i>	جمعية نظم المعلومات الأمريكية
2	ATMs	<i>Automated Teller Machines</i>	ماكينات الصراف الآلية
3	CERT	<i>Computer Emergency Response Team</i>	فريق الاستجابة لطوارئ الحاسوب
4	CISO	<i>Chief Information Security Officer</i>	المدير التنفيذي لأمن المعلومات
5	CISSP	<i>Certified Information Systems Security</i>	شهادة خبير أمن المعلومات
6	COBIT	<i>Control Objectives for Information and Related Technology</i>	أهداف الرقابة على المعلومات والتكنولوجيا ذات العلاقة
7	COSO	<i>Committee of Sponsoring Organization</i>	لجنة رعاية المنظمات
8	CPS	<i>Computerized Banking Systems.</i>	النظم المصرفية المحوسبة
9	CPU	<i>Central Processing Unit</i>	وحدة التشغيل المركزية
10	CRISC	<i>Certified in Risk and Information Systems Control</i>	شهادة في المخاطر ورقابة نظم المعلومات.
11	CRSA	<i>Control & Risk self-Assessment</i>	نظام التقييم الذاتي للرقابة والمخاطر
12	DRP	<i>Disaster Recovery Planning</i>	التخطيط لمواجهة الكوارث
13	EDI	<i>Electronic Data Interchange</i>	التبادل الإلكتروني للبيانات
14	ERPS	<i>Enterprise Resource Planning Systems</i>	نظم تخطيط موارد المشروع
15	FBI	<i>Federal Bureau of Investigation</i>	مكتب التحقيقات الفيدرالي
16	FTP	<i>Files Transfer Protocol</i>	بروتوكول نقل الملفات
17	ICT	<i>Information and Communication Technologies</i>	تكنولوجيا الاتصالات والمعلومات
18	IEC	<i>International Electro-technical Commission</i>	اللجنة الكهروتقنية الدولية
19	IFAC	<i>International Federation of Accountant</i>	الاتحاد الدولي للمحاسبين.
20	ISRM	<i>Information Security Risk Management</i>	إدارة مخاطر أمن المعلومات

م	الرمز المختصر	مضمونه باللغة الإنجليزية	مضمونه باللغة العربية
21	ISACA	Information Systems Audit and Control Association	جمعية التدقيق والرقابة على نظم المعلومات
22	ISMS	Information Security Management System	نظام إدارة أمن المعلومات
23	ISO	International Organization for Standardization	المنظمة الدولية لتوحيد المعايير
24	ISRA	Information Security Risk Assessment	تقييم مخاطر أمن المعلومات
25	ITSEC	Information Technology Security Evaluation Criteria	معايير تقييم أمن تكنولوجيا المعلومات
26	IDS	Intrusion Detection Systems	نظم كشف اقتحام الشبكة
27	NIST	National Institute of Standards and Technology	المعهد الوطني للمعايير والتكنولوجيا
28	OECD	The Organization for Economic Co-operation and Development	منظمة التعاون الاقتصادي والتنمية
29	PIN	Personal Identification Number	رقم التعريف الشخصي
30	PKE	Public Key Encryption	المفتاح العام للتشفير
31	QRM	Qualitative Research Methods	مناهج البحث النوعي
32	RSA	Risk Security Assessment	تقييم مخاطر الأمن
33	RMF	Risk Management Framework	إطار إدارة المخاطر
34	PPS	Physical Protection Systems	نظم الحماية المادية
35	SET	Secure Electronic Transaction	التداول الإلكتروني الآمن
36	SPSS	Statistical Package of Social Sciences	الحزمة الإحصائية للعلوم الاجتماعية
36	SRA	Security Risks Analysis	تحليل المخاطر الأمنية
37	SWIFT	Society for World-wide Inter-bank Financial Telecommunication	جمعية الاتصالات المالية العالمية بين البنوك.
38	UPS	Uninterruptible Power Supply	تغذية مستمرة بالتيار الكهربائي
39	VA	Vulnerability Assessment	تقييم نقاط الضعف (الثغرات)

ملخص الدراسة

« تَقْيِيمُ مَخَاطِرِ أَمْنِ نُظْمِ الْمَعْلُومَاتِ الْمَحَاسِبِيَّةِ الْمَحُوسَبَةِ لدى البنوك التجارية في الجمهورية اليمنية » - "دراسة تطبيقية"

أطروحة مُقدِّمة لنيل دَرَجَةِ الدُّكُورَاهِ فِي الْمَحَاسِبَةِ

إعداد الباحث:

عبدالكريم محمد يحيى فاضل

هدفت هذه الدراسة إلى تقييم مَخَاطِرِ أَمْنِ نُظْمِ الْمَعْلُومَاتِ الْمَحَاسِبِيَّةِ الْمَحُوسَبَةِ لدى البنوك التجارية في الجمهورية اليمنية، من خلال التعرف على أهم المخاطر الجوهرية التي تحدث وتهدد أمن تلك النظم، وتحديد التهديدات الداخلية والخارجية المسببة لحدوث مخاطر أمن تلك النظم، وقياس مدى تأثير تلك المخاطر على العناصر الرئيسية المكونة لأمن تلك النظم الممثلة بـ (إتاحة النظم، وصحة وسلامة وتكامل التشغيل، وسرية وخصوصية مخرجات تلك النظم، وعدم إنكار حدوث العمليات من الأطراف المتعاملة)، والتحقق من مدى تطبيق البنوك التجارية في الجمهورية اليمنية لأساليب وإجراءات الحماية وفق القواعد المحلية والأسس والمعايير الدولية لأمن نظم المعلومات، وقياس تأثير تلك الأساليب والإجراءات على المخاطر الأمنية في تلك البنوك، بهدف تشخيص نقاط القوة والضعف في أمن نظم المعلومات المحاسبية المحوسبة، بالإضافة إلى بيان مدى اختلاف تلك المخاطر بين البنوك التجارية في اليمن باختلاف ملكية البنك ونوعية النظام المستخدم ومستوى ارتباط نظم المعلومات المحاسبية بشبكة الاتصالات.

ولتحقيق تلك الأهداف فقد اعتمدت الدراسة على المنهج الوصفي التحليلي، فبعد أن قام الباحث بالاطلاع على الدراسات السابقة، وعلى الخلفية النظرية للدراسة، قام بإجراء دراسة حالة عملية تطبيقية لدى ثلاثة بنوك تجارية تمثل القطاعات الاقتصادية المختلفة (العامة والخاصة والمختلطة)، من خلال بيانات عملية، وتم تعزيز ذلك بدراسة مسحية شاملة لجميع البنوك التجارية العاملة في الجمهورية اليمنية، من خلال تصميم وتطوير قائمة استقصاء محكمة، وقد تم تحليل البيانات واختبار الفرضيات باستخدام الأساليب الوصفية والتحليلية المناسبة، اعتماداً على الحزمة الإحصائية للعلوم الاجتماعية (SPSS).

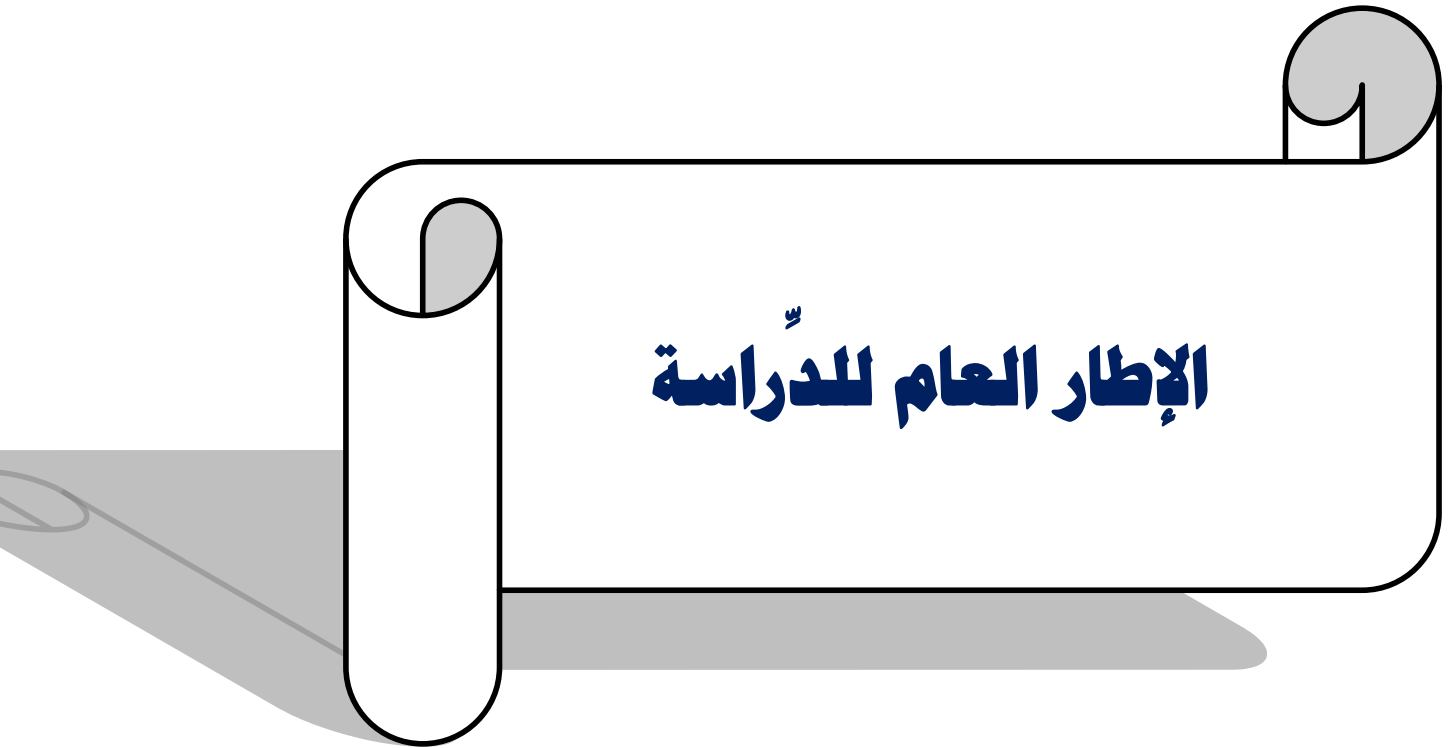
واستناداً للدراسة التطبيقية - بشقيها الاستكشافية والميدانية - فقد توصلت الدراسة إلى الكثير من النتائج كان من أبرزها ما يلي:

1. بالرغم من وجود العديد من المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية إلا أنه لا تحدث مخاطر جوهرية ذات أهمية نسبية تهدد أمن تلك النظم بل كانت محدودة نتيجة محدودية التقنية المستخدمة في البيئة اليمنية، ولأن البنوك التجارية في الجمهورية اليمنية تمتلك وسائل وتستخدم مجموعة من إجراءات الحماية المختلفة بشكل أو بآخر للسيطرة على تلك المخاطر.
2. يؤثر حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية على العناصر المكونة لأمن تلك النظم المتمثلة ب (إتاحة النظم، وصحة وسلامة وتكامل التشغيل، وسرية وخصوصية المعلومات المحاسبية، وعدم إنكار العمليات) لدى تلك البنوك، حيث وجد أن تلك التأثيرات مرتفعة بشكل عام وتتسبب في تأثيرات سلبية على أمن تلك النظم.
3. يوجد اختلاف في حجم المخاطر التي تتعرض لها البنوك التجارية في الجمهورية اليمنية باختلاف شكل ملكية البنك للقطاعات المختلفة التي تنتمي لها تلك البنوك، حيث وجد أن المخاطر تزداد بشكل تصاعدي لدى كلاً من (بنوك القطاع الخاص ثم بنوك القطاع المختلط ثم بنوك القطاع العام) على الترتيب، ولكن بالرغم من ذلك لا يوجد فرق جوهري دال إحصائياً بين تلك البنوك بشكل عام فيما يتعلق بحجم المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة يُعزى لملكية تلك البنوك.

وفي ضوء النتائج التي توصلت لها الدراسة قدم الباحث مجموعة من التوصيات والمقترحات، فيما يلي أهمها:

1. ضرورة التزام الإدارات التنفيذية والإدارة العليا لدى البنوك التجارية في الجمهورية اليمنية بالتقييم الدوري والمستمر لمخاطر أمن نظم المعلومات والاهتمام بتأثير تلك المخاطر وضرورة توقعها قبل حدوثها وإيجاد الحلول المناسبة لها في حال وقوعها، وإيجاد السبل الكفيلة باستعادة العمل ووضع خطط الطوارئ اللازمة لضمان أمن نظم المعلومات المحاسبية المحوسبة.
2. ينبغي وجود إستراتيجية شاملة ومتكاملة وواضحة ومكتوبة وقابلة للتطبيق لتقييم وإدارة مخاطر أمن نظم المعلومات المحاسبية، وأن تحدد بوضوح مصادر تلك المخاطر، كما يجب أن تشمل الإستراتيجية مستوى المخاطر التي يتقبلها البنك والذي يعكس تحديد أولويات البنك في إدارته للمخاطر، وفق منهجية علمية تستند إلى معايير وقواعد علمية واضحة في مجال تقييم عمليات إدارة المخاطر.

■ **كلمات مفتاحية:** تقييم مخاطر، أمن نظم المعلومات، نظم المعلومات المحاسبية المحوسبة، البنوك التجارية، الجمهورية اليمنية.



الإطار العام للدراسة

الإطار العام للدراسة

أولاً: مقدمة الدراسة:

نعيش في وقتنا الحاضر عصر ثورة المعلومات وتسارع موجات توالدها وتراكمها بوحداث زمنية تعجز كل القدرات الإنسانية المتاحة على ضبطها والإلمام بها، حتى أصبح بإمكاننا القول أن العالم بفضل التغيرات التكنولوجية الهائلة قد أصبح بحق قرية كونية صغيرة، حيث انبثق مجتمع المعلومات والمعرفة وانتقلت مفاتيح الحضارة ومكامن القوة من المادة إلى المعلومة ومن الآلة إلى المعرفة، فالمعلومات لا تقل أهمية عن الموارد المادية والبشرية في تسيير الأعمال وبناء المنظمات والحفاظ على الموارد المتاحة ولهذا فتوفير المعلومات يعد أحد المجالات الحيوية التي تلقى اهتماماً بالغاً بصورة لم يسبق لها مثيل من قبل.

وقد أدى التطور والانتشار الواسع لتكنولوجيا المعلومات والاتصالات إلى حدوث تغيرات كبيرة في الكثير من المجالات ومنها المجال المحاسبي، ومما لا شك فيه أن وجود نظام معلومات محاسبي كفوء وفَعَال يعتبر بمثابة أحد العوامل الأساسية المحددة لمدى نجاح أو فشل أي إدارة في تحقيق المستهدف منها بكفاءة وفعالية.

كل ذلك أدى إلى رغبة الكثير من المنشآت التجارية في إدخال نظم المعلومات المحاسبية المحوسبة في مجال أعمالها وذلك لما توفره تلك النظم من دقة في العمل وسرعة في الإنجاز وزيادة في كفاءة أداء المحاسبين ودقتهم في العمل والحصول على المعلومات المحاسبية المطلوبة بأسرع وقت وبأقل تكلفة ممكنة، فأتت الخدمات المالية أدت إلى سرعة التعامل والحفاظ على الوقت ودقة الأداء، وكلها أمور ومتطلبات لازمة لما يسمى بعصر العولمة المالية. وتتعرض نظم المعلومات المحاسبية المحوسبة في المنشآت الاقتصادية المختلفة كغيرها من النظم في عصر التطور التكنولوجي الحالي للعديد من المخاطر، فبقدر ما يحمل استخدام تكنولوجيا الحاسوب وأنظمة المعلومات من فوائد جمة لا تحصى، ولكنه على الجانب الآخر قد يحمل بين طياته العديد من المخاطر الهامة التي تهدد أمن وسلامة وتكامل وتوافر نظم المعلومات المحاسبية المحوسبة.

فتطور نظم المعلومات المحاسبية في القطاع المصرفي كان يرافقه التعرض لعدة مخاطر متعلقة بموثوقية وأمن وصحة وسلامة محتوى وتكامل وسرية نظم المعلومات المحاسبية، والتي قد ينجم عنها أضرار قد تؤدي إلى توقف المنشأة عن العمل لفترات، وقد تؤدي إلى ضياع البيانات والمعلومات المخزنة بها، وتؤدي بعض المخاطر إلى تلف البنية التحتية لنظم المعلومات المحاسبية، وهذا من شأنه أن يؤدي إلى تعطيل أو توقف المنشآت عن القيام بأعمالها، لفترة طويلة مما سينتج عنه خسائر جوهريّة للمنشأة قد تؤدي أحياناً إلى خروجها من السوق والإعلان عن إفلاسها. والعمل المصرفي يعتمد أساساً على الثقة والتي تنبع أساساً من السرية والأمانة التي تتعامل بها البنوك التجارية مع حسابات ومعلومات العملاء ودقتها وسلامتها، فحدوث المخاطر يؤدي حتماً إلى فقدان الثقة في تلك البنوك على المدى الطويل، وبالتالي فإن أهمية وحساسية المعلومات المحاسبية المحوسبة في البنوك التجارية تتطلب الحذر واليقظة المستمرة لتأمينها من خلال سياسات حريصة ومحددة وموثقة لحماية أمن نظم المعلومات بما يضمن المحافظة على سريتها وتكاملها وإتاحتها عند الحاجة لإدارة العمل المالي والمصرفي.

فالمخاطر التي تواجه أمن نظم المعلومات المحاسبية المحوسبة في إدارة واعية قادرة على مواجهتها حتى لا تؤثر تأثيراً سلبياً على قدرة نظم المعلومات المحاسبية في المنشأة على تحقيق أهدافها بكفاءة وفعالية، وعلى

بقاء المنشأة واستمرارها في مزاولة النشاط، حيث أضحت إجراءات ووسائل الحماية التقليدية عاجزة عن جعل المنشآت المختلفة ونظمها قادرة على البقاء أمام تلك المخاطر.

الأمر الذي يُحتم علينا تقييم تلك المخاطر وأسبابها وإجراءات الحماية المرتبطة بها، من منظور متكامل لمحاولة إدارتها والتقليل من أثارها السلبية، ولا بد لتلك المنشآت من تقييم تلك المخاطر من خلال اكتشافها وتحديد درجة تأثيرها ومدى استخدام وسائل وإجراءات الحماية، ومن هنا غدت دراسة مخاطر أمن نظم المعلومات المحاسبية المحسوبة مطلباً ملحاً وحاجةً أساسية.

إن معرفة نقاط القوة ونقاط الضعف في نظم المعلومات المحاسبية يقود إلى تقديم المقترحات والتوصيات اللازمة لتطوير نظم المعلومات المحاسبية، وذلك يعد من العوامل الرئيسية في نجاح المنشآت وازدهارها وتحقيقها لأهدافها. وبناءً عليه تأتي هذه الدراسة لتجري تقييماً لمخاطر أمن نظم المعلومات المحاسبية المحسوبة من خلال تسليط الضوء على أهم المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحسوبة لدى البنوك التجارية في الجمهورية اليمنية، وتحديد التهديدات التي أدت لحدوث تلك المخاطر، وبيان مدى تأثير تلك المخاطر على عناصر ومكونات أمن نظم المعلومات المحاسبية، مستعرضاً الأساليب والإجراءات المطبقة لدى تلك البنوك لمواجهة تلك المخاطر، وعلاقتها بحجم تلك المخاطر مستهدفاً في هذه الدراسة الوصول إلى نتائج تفيد إدارات البنوك التجارية لما من شأنه تطوير نظم المعلومات المحاسبية المحسوبة وتحديثها، لتكون نظم معلومات إستراتيجية، تتلاءم والتطورات التكنولوجية الحديثة والمتسارعة في البيئة المصرفية المتطورة إقليمياً ودولياً، لضمان استمرار وبقاء تلك البنوك في عالم الأعمال في ظل الأزمات الاقتصادية المتتالية.

ويتناول هذا الإطار العام وصفاً تمهيدياً ومنهجياً لهذه الدراسة من خلال تحديد مشكلة الدراسة وأهميتها وأهدافها والدراسات السابقة ذات العلاقة، وبيان فرضياتها المتبناة لدراسة المشكلة، و تصميم أنموذج الدراسة وإبراز حدود ومحددات الدراسة، وبيان خطتها.

ثانياً: مشكلة الدراسة:

لا شك في أن استخدام وسائل تكنولوجيا الاتصالات والمعلومات في العمل المحاسبي يتيح إمكانات وفرصاً كبيرة لخدمة المنشآت الاقتصادية المختلفة ولكن يُرافق ذلك الاستخدام تعرض أمن نظم المعلومات المحاسبية المحسوبة للعديد من المخاطر، وتشدد حدتها كلما أوغلنا في تبني التقنيات والحوسبة الحديثة وذلك يشكل تحدياً كبيراً لأي منشأة، فمشكلات أمن نظم المعلومات المحاسبية المحسوبة تحمل الكثير من التعقيدات التي تشمل في طياتها الجوانب التقنية والتنظيمية والبشرية، لأن تلك النظم تعمل في بيئة سريعة التغير تتسم بالدينامكية، والتحكم في كل متغيرات هذه البيئة صعب إن لم يكن مستحيلاً، ولعل الحل يكمن في القيام بتقييم المخاطر الأمنية لنظم المعلومات المحاسبية للوقوف على جوانب الخلل ومعالجة أو إيجاد حلول لقضايا أمن نظم المعلومات المحاسبية، ومن هنا تأتي مشكلة الدراسة في دراسة تلك المخاطر، والبحث عن تقييم لها من خلال التعرف عليها وتحديد أهم أنواعها، وتحليل درجة خطورتها أثناء المراحل المختلفة لعمل النظم، ومعرفة

التحديات المسببة لتلك المخاطر ومصادرها، ومعرفة مدى تأثير تلك المخاطر على العناصر المختلفة لأمن نظم المعلومات المحاسبية المحوسبة، وتحديد مدى كفاية الأساليب والإجراءات التي تقوم بها البنوك التجارية في اليمن للحد من تلك المخاطر أو تقليلها وبما يسهم في حماية أمن تلك النظم ومنح مخرجاتها درجة عالية من الموثوقية من خلال إتاحة وسلامة وتكامل المحتوى، والمحافظة على سرية وخصوصية بيانات تلك البنوك والأطراف المتعاملة معها، وبالتالي فإن هذه الدراسة تسعى إلى الإجابة عن التساؤلات التالية:

1. ما المخاطر الجوهرية التي تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، وما درجة خطورة ومعدل حدوث تلك المخاطر؟
2. ما التهديدات الداخلية الهامة والجوهرية التي تؤدي إلى حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية؟
3. ما التهديدات الخارجية الهامة والجوهرية التي تؤدي إلى حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية؟
4. ما مدى تأثير مخاطر أمن نظم المعلومات المحاسبية المحوسبة على العناصر الرئيسية المكونة لأمن تلك النظم الممثلة ب (إتاحة النظم، وصحة وسلامة وتكامل التشغيل، وسرية وخصوصية مخرجات تلك النظم، وعدم إنكار حدوث العمليات من الأطراف المتعاملة) لدى البنوك التجارية في الجمهورية اليمنية؟
5. ما مدى تطبيق الوسائل والإجراءات الرقابية الأمنية لدى البنوك التجارية في الجمهورية بشكل كافٍ وصحيح وفق التشريعات والقوانين والسياسات والمبادئ التوجيهية المحلية والأسس والمعايير الدولية لحماية أمن نظم المعلومات المحاسبية المحوسبة من المخاطر التي تتهددها؟
6. ما مدى تأثير أساليب وإجراءات الحماية المطبقة في البنوك التجارية في الجمهورية اليمنية على مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى تلك البنوك؟
7. هل توجد فروق بين مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية تُعزى لملكية البنك، أو لنوع النظام المعلومات المحاسبي المستخدم، أو لمدى ارتباط النظام بشبكة الانترنت؟

ثالثاً: أهمية الدراسة:

تتبع أهمية هذه الدراسة من أهمية المواضيع الحديثة التي تبحثها والتي من المتوقع أن تتعاظم في القرن الحالي، وتتمثل في أهمية إدراك ووعي المعنيين بالمخاطر التي تهدد أمن نظم المعلومات المحاسبية، وأهمية البحث عن أفضل السبل الملائمة للحماية من تلك المخاطر وبما ينعكس على سلامة ونزاهة وموثوقية وسرية

تلك النظم ومخرجاتها، وتكتسب أهمية هذه الدراسة من أهمية النتائج المتوقعة منها، وقد أقدم الباحث على إجراء هذه الدراسة من منطلق القنوات التالية:

1. الرغبة والميول في البحث في هذا الموضوع كونه يتسم بالحدثة ويمس قضايا معاصرة.
2. أهمية الدور الذي تلعبه البنوك التجارية العاملة في الجمهورية اليمنية في دعم الاقتصاد الوطني، ودفع عجلة تقدمه، الأمر الذي يتطلب تبصير إدارات تلك البنوك بالمخاطر المحيطة بأمن نظم المعلومات المحاسبية لديها، ولا نبالغ إذا قلنا إن حماية أمن نظم المعلومات المحاسبية المصرفية هي حاجة ماسة وضرورية ليس فقط للبنوك وعمالها وإنما حماية للأمن الاقتصادي والاجتماعي والسياسي على الصعيدين الوطني والقومي.
3. تعتبر هذه الدراسة محاولة جادة لمعرفة أهم المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، واقتراح أساليب حماية ورقابة أكثر كفاءة وفاعلية تسهم في الحد أو التقليل من تلك المخاطر وبالتالي تجنب الخسائر المحتملة المترتبة على تلك المخاطر.
4. تزداد أهمية هذه الدراسة كونها تعتبر من أوائل الدراسات التي تعرضت للمخاطر والتهديدات التي تواجه أمن نظم المعلومات المحاسبية المحوسبة بهذا التفصيل والتخصص في بيئة الأعمال المصرفية اليمنية، وبمنظرة أكثر شمولية، ولذلك فإن هذه الدراسة قد تسهم بشكل متواضع في سد الفجوة المعرفية في هذا الميدان.
5. تتطرق هذه الدراسة إلى أحد الموضوعات التي تمثل تحدياً أساسياً لمهنة المحاسبة والمراجعة في مطلع القرن الحادي والعشرين، فهناك فجوة توقعات بين الدور المنتظر من المحاسبين والمراجعين والدور الفعلي الذي يقومون به حالياً في مجال تأمين نظم المعلومات المحاسبية، ويتوقع أن يكون لهذه الدراسة مردود مهم على كل من عمل المراجعين الداخليين والخارجيين، بمساعدتهم في وضع رؤاهم وتصوراتهم وخططهم على أسس سليمة عند القيام بمهامهم.
6. إن هذا التقييم والدراسة يسهم في تسليط الضوء على جوانب القوة والضعف في أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في اليمن، وبالتالي تقديم المقترحات الملائمة لتعزيز جوانب القوة ومعالجة جوانب الضعف التي تحتاج إلى الاهتمام والعناية، وبالتالي منح مخرجات تلك النظم درجة عالية من المصداقية، وبما يجعلها نظم عصرية تلبي كافة الاحتياجات من المعلومات الملائمة والموثوقة.
7. تخدم هذه الدراسة البنوك التجارية في الجمهورية اليمنية، وجميع الأطراف ذات العلاقة بأمن نظم المعلومات المحاسبية المحوسبة، بما تقدمه من نتائج وتوصيات، الأمر الذي يمكن الاستفادة منها في بلورة أسس سليمة عند تطبيق الممارسات السليمة لإدارة وضبط المخاطر، وبالتالي ضمان اتخاذ البنوك الإجراءات والضوابط التي تساعد في تخفيض المخاطر والخسائر التي قد تنشأ بسببها.

رابعاً: أهداف الدراسة:

في سياق التساؤلات المطروحة في مشكلة الدراسة، يتمثل الهدف الرئيسي للدراسة في وضع تصور يساعد في تقييم المخاطر التي تهدد أمن نظم المعلومات المحاسبية لدى البنوك التجارية في الجمهورية اليمنية وسبل الحماية

من تلك المخاطر، من خلال تحديد أهم تلك المخاطر وأسباب حدوثها، وتحديد مدى كفاية وسائل الحماية والإجراءات المتبعة لتخفيض تلك المخاطر أو الحد منها، وتقديم التوصيات المناسبة بهذا الخصوص، ولذلك فإن هذه الدراسة تسعى لتحقيق عدد من الأهداف الفرعية المتكاملة والتي تتمثل في الأهداف التالية:

1. التعرف على أهم المخاطر الجوهرية التي تحدث وتهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، ودرجة خطورة ومعدل حدوث تلك المخاطر.
2. تحديد التهديدات الداخلية والخارجية لحدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية.
3. قياس مدى تأثير مخاطر أمن نظم المعلومات المحاسبية المحوسبة على العناصر الرئيسية المكونة لأمن تلك النظم الممثلة ب (إتاحة النظم، وصحة وسلامة وتكامل التشغيل، وسرية وخصوصية مخرجات تلك النظم، وعدم إنكار حدوث العمليات من الأطراف المتعاملة) لدى البنوك التجارية في الجمهورية اليمنية؟
4. التحقق من مدى تطبيق البنوك التجارية في الجمهورية اليمنية للأساليب والإجراءات الرقابية والأمنية الكافية وفق الأسس والمعايير الدولية لحماية أمن نظم المعلومات المحاسبية المحوسبة من المخاطر التي تتهددها؟
5. قياس تأثير أساليب وإجراءات الحماية المطبقة في البنوك التجارية في الجمهورية اليمنية على مخاطر أمن نظم المعلومات المحاسبية المحوسبة في تلك البنوك.
6. توضيح العلاقة بين مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية وكل من ملكية البنك، ونوع نظام التشغيل المستخدم، ومستوى ارتباط النظام بشبكات الاتصالات؟
7. تشخيص نقاط القوة ونقاط الضعف لنظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية من خلال دراسة استكشافية تطبيقية لتقييم المخاطر الأمنية داخل عدة بنوك تمثل القطاعات المختلفة، ومعرفة إجراءات ووسائل الحماية الأمنية المتبعة.

خامساً: الدراسات السابقة: قبل صياغة فرضيات الدراسة لا بد من التطرق لبعض الدراسات الحديثة

التي تناولت موضوع هذه الدراسة بشكل مباشر أو غير مباشر، وقد تفاوتت هذه الدراسات في أهدافها ومتغيراتها والبيئات التي أجريت فيها، وفيما يلي عرض لبعض هذه الدراسات:

أ- الدراسات باللغة العربية:

1. **دراسة (حسين & ودياب 2018):**⁽¹⁾ هدفت هذه الدراسة للتعرف على مخاطر استخدام نظم المعلومات المحاسبية الإلكترونية وعلاقتها بجودة المعلومات، والتعرف على أثر تلك المخاطر على الخصائص النوعية للمعلومات المحاسبية.

(1) حسين، وسام نعمة & ودياب، محمد أحمد، (2018)، " مخاطر استخدام نظم المعلومات المحاسبية الإلكترونية وأثرها على خصائص جودة المعلومات المحاسبية - دراسة استطلاعية"، مجلة تكريت للعلوم الإدارية والاقتصادية، المجلد (3)، العدد (43)، كلية الإدارة والاقتصاد، جامعة تكريت، العراق، ص ص: 45-65.

وقد تناولت الدراسة تحديد هذه المخاطر وأسبابها ومدى تأثيرها على خصائص جودة المعلومات المحاسبية حيث تم اختيار شركة كورك لتكون عينة البحث واعتمد الباحثان على قائمة الاستقصاء في الجانب العملي من أجل تحقيق أهداف الدراسة وفرضياتها، وتم وضع نموذج البحث الافتراضي والذي يوضح تأثير هذه المخاطر على خصائص جودة المعلومات المحاسبية، وبناءً على ذلك تم التوصل إلى مجموعة من الاستنتاجات ومن أهمها إن المنشأة عينة البحث تتعرض إلى هذه المخاطر بالإضافة إلى وجود ارتباط وتأثير بين متغيري الدراسة وتم توضيح أسباب هذا التأثير والارتباط في الجانب العملي.

2. **دراسة (أبو شيبية والفطيمي، 2017):**⁽¹⁾ هدفت هذه الدراسة إلى التعرف على مخاطر استخدام نظم المعلومات المحاسبية الإلكترونية في البنوك العاملة في بلدية مصراتة الليبية، والتعرف على أهم الأسباب التي تؤدي إلى حدوث تلك المخاطر والإجراءات التي تحول دون وقوع تلك المخاطر. واتبعت الدراسة المنهج الوصفي التحليلي وتكون مجتمع الدراسة من موظفي تلك البنوك أما عينة الدراسة فبلغت (39) فرداً وتم استعمال عدد من الأساليب الإحصائية لتحليل البيانات مثل المتوسطات والانحراف المعياري واعتمدت قائمة الاستقصاء مصدراً رئيسياً لجمع البيانات وتم تحليلها باستخدام حزمة البرنامج الإحصائي للعلوم الاجتماعية (SPSS).

وتوصلت الدراسة إلى عدة نتائج ساهمت في التعرف على تلك المخاطر محل الدراسة ومدى إدراك البنوك لها، وأن أهم سبب لحدوثها يرجع لموظفي البنوك كنفق الخبرة وقلة الوعي، وأسباب تتعلق بالإدارة كعدم وجود سياسات واضحة ومكتوبة وضعف الإجراءات والأدوات الرقابية المطبقة لدى تلك البنوك.

3. **دراسة (محمد، 2017):**⁽²⁾ هدفت الدراسة إلى التعرف على مخاطر نظم المعلومات المحاسبية الإلكترونية وتأثيرها على فاعلية أداء المراجعة الداخلية بهيئة الموانئ البحرية السودانية، واتبعت الدراسة المنهج الوصفي التحليلي وتكون مجتمع الدراسة من المراجعين الداخليين والخارجيين والمحاسبين والمديرين والمبرمجين، وتم استعمال عدد من الأساليب الإحصائية لتحليل البيانات مثل المتوسطات والانحراف المعياري وتم تطبيق الدراسة في إدارة المراجعة الداخلية بهيئة الموانئ البحرية، واعتمدت قائمة الاستقصاء مصدراً رئيسياً لجمع البيانات.

وتوصلت الدراسة إلى عدة نتائج أبرزها: تعدد الآثار على المراجعة الداخلية نتيجة لوجود أنواع مختلفة من المخاطر، وإن وجود الضوابط والإجراءات يحد ويقلل من المخاطر وتأثيرها، وأن للمخاطر أثر واضح على أعمال المراجعة الداخلية في الكشف عن الأخطاء في عمليات مراجعة الترصيد والتسويات وتقييد الحسابات، وقامت الدراسة بتقديم توصيات أبرزها الانتباه للمخاطر المصاحبة لتطبيق نظام المعلومات المحاسبي

(1) أبوشيبية، إبراهيم علي & الفطيمي، محمد مفتاح، (2017)، "مخاطر استخدام نظم المعلومات المحاسبية الإلكترونية - دراسة ميدانية على المصارف التجارية في بلدية مصراتة"،

مجلة دراسات الاقتصاد والأعمال، المجلد (5)، عدد خاص، كلية الاقتصاد والعلوم السياسية، جامعة مصراتة، ليبيا، ص: 80-97.

(2) محمد، عصام الدين، (2017)، "مخاطر نظم المعلومات المحاسبية الإلكترونية وأثرها على المراجعة الداخلية - دراسة حالة هيئة الموانئ البحرية"، رسالة ماجستير غير منشورة، كلية الاقتصاد والعلوم الإدارية، جامعة البحر الأحمر، السودان.

الالكتروني والعمل علي كشفها وتفعيل وإيجاد وسائل للحد من المخاطر وآثارها وتحديث اللوائح والإجراءات وتغييرها لمواكبة العمل في البيئة الالكترونية، وتدريب العاملين بالمراجعة الداخلية علي العمل الالكتروني.

4. دراسة (الداهمة، 2013):⁽¹⁾ هدفت هذه الدراسة إلى تقصي أثر مخاطر استخدام تكنولوجيا المعلومات على

أداء نظم المعلومات المحاسبية من وجهة نظر مراجعي الحسابات في السعودية.

ولتحقيق أهداف الدراسة استخدم الباحث استقصاء خاص لجمع البيانات من عينة الدراسة لتحليل البيانات واختبار الفرضيات باستخدام المنهج الإحصائي، اعتماداً على برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS).

وقد أظهرت نتائج الدراسة أن مخاطر استخدام تكنولوجيا المعلومات تؤثر على أداء نظم المعلومات المحاسبية بدرجة كبيرة بنسبة مئوية (75.6 %)، وخلصت الدراسة إلى توصيات تساعد على الحد من مخاطر استخدام تكنولوجيا المعلومات على أداء نظم المعلومات المحاسبية.

5. دراسة (فاضل، 2012):⁽²⁾ هدفت هذه الدراسة إلى معرفة مدى تأثير استخدام الصيرفة الإلكترونية على

فاعلية الرقابة التطبيقية لنظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية اليمنية.

ولتحقيق أهداف الدراسة استخدم الباحث قائمة استقصاء خاصة لجمع البيانات من عينة الدراسة، حيث تم إخضاع (57) قائمة استقصاء لتحليل البيانات واختبار الفرضيات باستخدام المنهج الوصفي التحليلي، اعتماداً على برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS).

ووصلت الدراسة إلى عدة نتائج، أهمها أن هنالك تأثيرات إيجابية واضحة لاستخدام الصيرفة الإلكترونية على فاعلية الرقابية التطبيقية في نظم المعلومات المحاسبية المحوسبة، تسهم في تفسير التغيرات الحاصلة في سلوك تلك الفاعلية لدى تلك البنوك، مما يستوجب على الإدارة زيادة الدورات التدريبية للمحاسبين والمدققين الداخليين فيها، وتزويدها بكوادر متخصصة، ومؤهلة لمواجهة التحديات والمشاكل، التي فرضتها الصيرفة الإلكترونية، وبما ينعكس إيجاباً على فاعلية الرقابة التطبيقية لنظم المعلومات المحاسبية.

6. دراسة (البحيصي، 2011):⁽³⁾ هدفت هذه الدراسة إلى استكشاف المخاطر التي تواجه نظم المعلومات

المحاسبية الإلكترونية في البنوك العاملة في قطاع غزة، ومعرفة أهم الأسباب التي تؤدي إلى حدوثها والإجراءات التي تحول دون وقوعها، ومن أجل تحقيق هذا الهدف تم تنفيذ واستخدام استقصاء أعد خصيصاً لهذا الغرض، وقد تم توزيع الاستقصاء على عينة من البنوك الفلسطينية.

(1) الداهمة ، سليمان مصطفى، (2013)، "أثر مخاطر استخدام تكنولوجيا المعلومات على أداء نظم المعلومات المحاسبية من وجهة نظر مراجعي الحسابات في المملكة العربية السعودية"، مجلة جامعة القدس المفتوحة للأبحاث والدراسات، العدد(30)، فلسطين، ص ص: 11-36.

(2) فاضل، عبدالكريم محمد يحيى، (2012)، "مدى تأثير استخدام الصيرفة الإلكترونية على فاعلية الرقابية التطبيقية لنظم المعلومات المحاسبية المحوسبة - دراسة ميدانية لدى البنوك التجارية اليمنية"، بحث مقبول للنشر، مجلة الباحث الجامعي، جامعة إب، اليمن.

(3) البحيصي، عصام محمد، (2011)، "استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة في الشركات الفلسطينية العامة في قطاع غزة : دراسة تطبيقية"، مجلة الجامعة الإسلامية، سلسلة الدراسات الإنسانية، المجلد (19)، العدد (1)، غزة، فلسطين، ص ص: 1147-1177.

وقد أظهرت النتائج الإحصائية أن من أهم مخاطر نظم المعلومات: الإدخال المتعمد للبيانات الخاطئة عن طريق المستخدمين، وانقطاع التيار الكهربائي والإتلاف غير المقصود للبيانات من قبل المستخدمين واشتراك العاملين في كلمات الدخول للحاسوب، ودخول الفيروسات إلى الأنظمة، إضافة إلى ذلك فقد أظهر البحث أن البنوك الفلسطينية تختلف فيما بينها في درجة تكرار وأهمية المخاطر حسب نوعية نظام المعلومات المستخدم وحسب مدى الارتباط بشبكة الانترنت، إلا أنه ليس هناك ارتباط بين نوع القطاع الذي ينتمي إليه البنك ودرجة تكرار وأهمية المخاطر التي تتعرض لها البنوك الفلسطينية، وأظهرت هذه الدراسة أن من أسباب حدوث تلك المخاطر، قلة الخبرة لموظفي البنوك، وعدم وجود سياسات واضحة ومكتوبة، وضعف الإجراءات والأدوات الرقابية المطبقة، ومن أهم توصيات الدراسة ضرورة دعم الإدارة العليا لأمن نظم المعلومات، وضرورة وضع إجراءات تضمن استمرارية عمل نظم المعلومات المحاسبية للعمل في حالة الأزمات.

7. **(دراسة القاسم والردايدة، 2010):⁽¹⁾** هدفت هذه الدراسة إلى معرفة مدى اهتمام البنوك الأردنية بتطبيق إجراءات أمن البيانات ونظم المعلومات المحاسبية، باستخدام استقصاء مكون من ثلاثين فقرة، وزع على موظفي البنوك من مستوى مدير في المجال التقني أو المجال المحاسبي في البنوك المشمولة. وتبين من النتائج أن نسبة الاهتمام بالأمن المادي للمعلومات المحاسبية ووسائل التخزين عالي، حيث بلغت (87.33%)، كما بلغت نسبة الاهتمام بأمن الأفراد (91.73%) ونسبة الاهتمام بأمن النظم والتطبيقات والبرمجيات (90.68%)، ونسبة الاهتمام بأمن الأجهزة والمعدات (90.94%)، ونسبة الاهتمام بأمن طرق الحفظ السليمة وتبادل المعلومات وتخزينها (92.53%)، وهذا يدل على أن الإجراءات المتبعة في تلك البنوك لحماية البيانات والمعلومات المحاسبية كافية وشاملة. وتم اختتام الدراسة بمجموعة توصيات تؤكد على ضرورة الاستمرار بتطوير وتحديث وسائل حماية البيانات ونظم المعلومات المحاسبية المحوسبة، وأماكن ووسائل التخزين الآلية في البنوك الأردنية.

ب- الدراسات باللغة الإنجليزية:

1. **دراسة (Kasasbeh, Thuneibat, 2018)⁽²⁾** بعنوان: " قدرة نظم المعلومات المحاسبية المحوسبة في الجامعات السعودية لمواجهة التهديدات السيبرانية". هدفت الدراسة إلى توضيح الهجمات السيبرانية التي تشهدها نظم المعلومات المحاسبية المحوسبة لدى الجامعات الخاصة والعامة السعودية، حيث شملت الدراسة على (486) مستجيباً من ثلاث جامعات مختلفة

(1) قاسم، عبدالرزاق & الردايدة، مراد، (2010)، " أمن البيانات ونظم المعلومات المحاسبية في بيئة تكنولوجيا المعلومات في البنوك الأردنية - دراسة ميدانية "، **المجلة العربية للعلوم الاقتصادية والإدارية**، العدد (5)، كلية إدارة الأعمال والعلوم التجارية، جامعة الروح القدس، الكسليك، بيروت، لبنان، تشرين الأول (أكتوبر)، ص ص: 91-111.

(2) Kasasbeh, F. I. O., & Thuneibat, N. S. M., (2018), *The Ability of Computerized Accounting Information Systems in Saudi Public Universities to Face Cyber Threats. International Review of Management and Marketing*, Vol. (8), No. (3), 19.

في السعودية، تم إجراء المسح من خلال قوائم من الاستقصاء وتم تحليل البيانات التي تم جمعها باستخدام البرنامجين الإحصائيين: (IBM-SPSS) و (AMOS).

أظهرت نتائج الدراسة أن رأي المشاركين فيما يتعلق بقدرة نظم المعلومات المحاسبية المحوسبة (CAIS) على الحماية ومواجهة التهديد السيبراني يعتمد على الوعي بأحداث الهجمات الأخيرة، وأن التحكم في الوصول له علاقة متوسطة بين هجمات البرامج الخبيثة وقدرة النظام على صد تلك الهجمات، ويؤثر التحكم في الوصول بشكل أفضل وإيجابي على قدرة نظم المعلومات المحوسبة في مواجهة التهديدات، ولم يجد الباحث أي اختلاف كبير في إدراك الأفراد فيما يتعلق بقدرة نظم المعلومات المحاسبية المحوسبة على مواجهة التهديد السيبراني، تتعلق باختلاف الصفات الشخصية والوظيفية المختلفة للمستجوبين.

2. دراسة (Hossin, A. M. & Avedh, A. M., 2016):⁽¹⁾ بعنوان مخاطر نظام المعلومات المحاسبية الإلكترونية في البنك المركزي الليبي.

هدفت هذه الدراسة لتحديد المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية في البيئة الليبية داخل البنك المركزي الليبي، والتحقق ومعرفة أهم الأسباب التي تؤدي إلى حدوث تلك المخاطر، والتحقق في الإجراءات التي تمنع حدوث هذه المخاطر.

ويتكون مجتمع الدراسة من البنك المركزي الليبي، وعينة الدراسة هم الأفراد العاملين في البنك والذين طبيعة عملهم لها علاقة بموضوع الدراسة، واستخدمت الدراسة قائمة الاستقصاء كأداة لجمع البيانات واعتمدت منهجية هذه الدراسة على الدراسة التطبيقية لتحديد مخاطر نظم المعلومات المحاسبية المحوسبة، وأسباب هذه المخاطر والإجراءات التي يمكن اتخاذها لمواجهة تلك المخاطر لدى بنك ليبيا المركزي، من خلال مصادر الكتب والمقالات والأوراق المنشورة في المجلات العلمية والرسائل العلمية المتخصصة والتقارير الصادرة عن البنك المركزي الليبي في السنوات الماضية وأيضاً عن طريق توزيع الاستقصاء المصمم للتوزيع على عينة الدراسة في مجتمع الدراسة ومن ثم سيحلل الباحث هذه البيانات باستخدام برنامج الحزمة الإحصائية (SPSS).

وتوصلت الدراسة إلى حدوث المخاطر التالية بشكل متكرر في البنك المركزي الليبي، المخاطر المتعلقة بإدخال البيانات، المخاطر المتعلقة بالعملية، المخاطر المتعلقة بالمخرجات، المخاطر المتعلقة بالبيئة، ومن أهم أسباب حدوث المخاطر التي تهدد أنظمة المعلومات المحاسبية الإلكترونية في البنك نقص الخبرة والتوعية والتدريب لدى موظفي البنك، وعدم وجود سياسات واضحة ومكتوبة وضعف الإجراءات والأدوات التنظيمية المعمول بها، بالرغم من وجود تدابير حماية مناسبة لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية في البنك.

(1) Hossin, A. M. & Avedh, A. M., (2016), "The Risks of Electronic Accounting Information System in The Central Bank of Libya", *South East Asia Journal of Contemporary Business, Economics and Law*, Vol. 10, Issue 1 (Aug.2016), ISSN: 2289-1560, PP:74-79.

3. دراسة (Tarmidi, M., et al., 2013):⁽¹⁾ بعنوان: تهديدات نظم المعلومات المحاسبية المحوسبة للخدمات العامة الماليزية.

هدفت هذه الدراسة في التحقق من وجود تهديدات لنظم المحاسبية المحوسبة في قطاع الخدمات العامة الماليزية، وقد استخدمت الدراسة أداة الاستبيان حيث تم توزيع (500) قائمة استقصاء تم توزيعها على مستخدمي تلك النظم في الإدارات العامة للحسابات في ولاية نيجارا، وأظهرت نتائج الدراسة تصور المستخدمين للحالة الراهنة من التهديدات التي يواجهها النظام وكان أهمها أخطاء في إدخال البيانات، وخرق النظام، وانتهاك الرقابة الداخلية والتلاعب بالمعلومات المالية التي تثير انتباه وقلق المنشأة ولذلك أوصت الدراسة باتخاذ الإجراءات المناسبة.

وقد كشفت نتائج الدراسة أن معظم التهديدات الأمنية نشأت من مصدر داخلي والذي هو الموظف العام في تلك النظم، والذي يسلط الضوء عن نقص التدريب لدى الموظفين قد يؤدي إلى سوء فهم وسوء استغلال النظام، ووجدت هذه الدراسة أن الكوارث الطبيعية، وسرقة البيانات بالدخول المتعمد للبيانات من قبل الموظفين كانت أقل تهديد متصور بين المستخدمين، وعلى الرغم من أن معظم التهديدات المدرجة ينظر إليها على أنها نادراً ما تحدث، ولكن هناك مجموعة من الأفراد أشاروا إلى أنها لا تزال قائمة الحدوث، وبالتالي، قد يشكل هذا الدليل التجريبي أداة هامة يمكن من خلاله إدارة المنشآت تقييم أمن النظم المحاسبية المحوسبة ومتابعته بشكل صحيح كاستراتيجيات فعالة لتحسين الجودة وانخفاض مخاطر الحوادث الأمنية.

4. دراسة (Al Hanini, Eman, 2012)⁽²⁾ بعنوان: "مخاطر استخدام نظم المعلومات المحاسبية المحوسبة في البنوك الأردنية".

هدفت هذه الدراسة إلى التعرف على مخاطر نظم المعلومات المحاسبية المحوسبة في البنوك الأردنية، وأسبابها وسبل الوقاية منها، ولتحقيق ذلك تم تصميم قائمة استقصاء تم توزيعها على عينة تتكون من (63) مستجيب من الأفراد الذين يعملون كمدرء الإدارات ومدرء الفروع ومساعدتهم من موظفي البنوك الأردنية، لتحليل البيانات باستخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية SPSS .

وتوصلت الدراسة إلى أن هناك مخاطر تهدد أمن نظم المعلومات المحاسبية في البنوك الأردنية، كإدخال الموظفين للبيانات السيئة عن عمد، ودخول الفيروسات إلى تلك النظم، المخاطر المتعلقة بالرقابة الداخلية على أنها غير مصرح بها لرؤية المخرجات والمخاطر المتعلقة بالطبيعة و غير الطبيعية، والكوارث التي قام بها البشر. وخلصت الدراسة إلى أن أحد أهم هذه المخاطر هو عدم خبرة الموظفين في الحفاظ على أمن

(1) Tarmidi, M., et al., (2013), Computerized Accounting Systems Threats in Malaysian Public Services", *International Journal of Finance and Accounting*, Vol. 2, No.2, PP: 109-113.

(2) Al Hanini, Eman, (2012), "The Risks of Using Computerized Accounting Information Systems in the Jordanian Banks: Their Reasons and Ways of Prevention", *European Journal of Business and Management*, Vol. 4, No.20, PP: 53-63, www.iiste.org

المعلومات الممثلة ونقص الموظفين في التدريب على استخدام وسائل حماية النظم المحاسبية قبل البدء بعملها وعدم توفر نظام التوظيف الذي يعين الشخص المناسب في المكان المناسب.

5. دراسة (Zainol et al, 2012)⁽¹⁾ بعنوان: "التحديات الداخلية القائمة على الموارد البشرية والرقابة الأمنية: أدلة من ماليزيا".

استهدفت هذه الدراسة فحص احتمالية وجود تهديدات داخلية من الأفراد العاملين والتي قد تسبب مخاطر أمنية للنظم المصرفية المحوسبة (CBS) في ماليزيا، من خلال رأي مدراء البنوك في تلك التهديدات، ومدى وجود الضوابط الأمنية في تلك النظم، وهل تختلف من بنك لآخر.

وبما أن معظم المنشآت المالية الماليزية الكبرى تعمل في العاصمة كوالالمبور، فقد أرسلت قوائم الاستقصاء للبنوك المختارة في كوالالمبور، وكشفت نتائج هذه الدراسة وجود انخفاض لتلك التهديدات في جميع البنوك في ماليزيا لوجود إجراءات وسياسات داخلية لتوظيف الأفراد العاملين، وفصل الواجبات والتحكم في الوصول المادي كسبل للتخفيف من المخاطر الناتجة عن تهديدات أمن الأفراد.

وبالتالي وفرت هذه الدراسة رؤية لكيفية إمكانية تحسين نظام الرقابة الداخلية للمنشآت المالية كوسيلة للحد من التهديدات الأمنية التي تترتب عليها آثار مالية، وقدمت آلية للرقابة الداخلية بكفاءة وفعالية بين المنشآت المالية في ماليزيا، من شأنها أن توفر تأكيد معقول لتحقيق رسالة المنشأة الدولية.

6. دراسة (Sharairi & Lababidi, 2011)⁽²⁾ بعنوان: "العوامل التي تؤثر على دور المدقق الداخلي للحسابات في حماية نظم المعلومات المحاسبية المحوسبة من الاختراق - دراسة ميدانية على البنوك العاملة في الأردن".

هدفت هذه الدراسة إلى التعرف على العوامل التي تؤثر على دور المدقق الداخلي في حماية نظم المعلومات المحاسبية المحوسبة من الاختراق الالكتروني، ولتحقيق أهداف الدراسة تم توزيع قائمة استقصاء على المدققين الداخليين المتخصصين في مجال المحاسبة وتدقيق نظم المعلومات وموظفي تكنولوجيا المعلومات في البنوك العاملة في الأردن، وأظهرت نتائج الدراسة أن المدقق الداخلي لديه دور هام في حماية نظم المعلومات المحاسبية المحوسبة من الاختراق الالكتروني، ممثلة في اختبار أمن ضوابط ضد المعلومات الواردة مع مصدر غير معروف، و أن المراجع يقوم بالاختبار التجريبي من خلال محاولة اختراق المعلومات من أجل تقييم فعالية الضوابط الموجودة، وأظهر الاستطلاع أيضا أن هناك تأثير المعرفة والمهارة

(1) Zainol, Zaini & Nelson, Sherliza & Malami, AbuBakar,(2012),"Internal Human Based Threats and Security Controls in Computerized Banking Systems: Evidence from Malaysia", *Procedia - Social and Behavioral Sciences*, No. 65, 2012, PP: 199 – 204, Available Online at: www.sciencedirect.com

(2) Sharairi, Jamal & Lababidi, Mohammad,(2011),"Factors Affecting the Role of Internal Auditor in the Protection of Computerized Accounting Information Systems from Electronic Penetration-A Field Study on Banks Operating in Jordan", *International Research Journal of Finance and Economics*, Issue 68, Euro Journals Publishing, Inc. 2011, PP:140-161.

للمدقق الداخلي لدوره في حماية نظم المعلومات المحاسبية المحوسبة، وهذا يدل على المدقق الداخلي الذي لديه المعرفة والمهارة سيكون له دور أكثر فعالية في حماية نظم المعلومات المحاسبية المحوسبة.

7. **دراسة (NITS, 2010):⁽¹⁾** بعنوان: "معايير تصنيف أمن المعلومات الاتحادية ونظم المعلومات".

هدفت هذه الدراسة إلى تطوير المعايير المستخدمة من قبل الوكالة الاتحادية الأمريكية للمعايير والتكنولوجيا (NIST)، لحماية أمن نظم المعلومات المحوسبة، من حيث استخدام وتصنيف أمن نظم المعلومات المنشورة على الشبكات الإلكترونية الاتحادية، بما يتفق والإدارة الفعالة، والإشراف الأمن على نظم المعلومات، والتي تم اعتمادها من قبل وزارة التجارة الأمريكية، بغرض تطبيقها في منشآت القطاع الخاص الأمريكي، ونتيجة لهذه الدراسة تم وضع ثلاث درجات لقياس أمن نظم المعلومات (مرتفع – متوسط – منخفض)، لتحقيق أهداف أمن نظم المعلومات (السرية، التكامل، ومدى إتاحة المعلومات عند الحاجة)، وأشارت الدراسة إلى أن أي ضعف في تحقيق هذه الأهداف سيؤدي حتماً إلى خسائر كبيرة تنتج عن فقدان أو تلف أو اختراق أو تسريب معلومات حساسة تضر بالمصلحة العامة، وقامت فيها بتحليل أهم المبادئ والممارسات التي يمكن إتباعها بغرض تحقيق أعلى درجة من التكامل والإتاحة والسرية لأمن نظم المعلومات المحوسبة، وبعد البحث والمشاهدة تم وضع مجموعة من المبادئ والممارسات والسياسات وبرامج تتماشى وأهداف أمن نظم المعلومات المحاسبية المحوسبة وتحد من أثر المخاطر التي تهدد تلك النظم.

سادساً: ما يميز هذه الدراسة عن الدراسات السابقة: تبين من الدراسات السابقة اختلاف البيانات

التي أجريت فيها، واختلاف طبيعة نشاط المنشآت التي طبقت عليها، وتنوع المتغيرات التي تناولتها، وتأتي هذه الدراسة امتداداً ومتابعة للجهود الكبيرة للدراسات التي تطرقت لمواضيع المعالجة المحاسبية الآلية وأمن نظم المعلومات المحاسبية، والتهديدات والمخاطر المختلفة التي يواجهها، ولعل ما يميز هذه الدراسة بشكل جوهري عن الدراسات السابقة ويبرز القيمة المضافة لها هي الجوانب المختلفة المتميزة بها، ومن أهمها ما يلي:

1. من حيث بيئة الدراسة وقطاع التطبيق: تبين من الدراسات السابقة أنها أجريت في بيئات مختلفة مع اختلاف

الأنشطة التي طبقت عليها أيضاً، حيث أجريت على المنشآت الأمريكية والأوروبية وبعض المنشآت العربية في حين تم تطبيق هذه الدراسة في البيئة اليمنية خاصة لدى البنوك التجارية في الجمهورية اليمنية، وما يتبع ذلك من متغيرات اقتصادية واجتماعية وقانونية وإمكانيات تكنولوجية مختلفة عن بيئات الدراسات السابقة، وعلى حد علم الباحث لا توجد دراسة بهذا الخصوص في البيئة اليمنية.

2. من حيث هدف الدراسة: تنوعت الاتجاهات البحثية للدراسات السابقة والتي هدفت إلى قياس التأثير والعلاقة ووضع

مجموعة من معايير أمن نظم المعلومات، أما الدراسة الحالية فقد هدفت بشكل أساسي إلى تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة من خلال تحديد أهم المخاطر التي قد تتعرض لها نظم المعلومات المحاسبية

(1) National Institute of Standards and Technology (NIST), *Standards for Security Categorization of Federal Information and Information Systems*, February Available at <http://www.Nist.Gov> as 19/2/ 2010 at 08:15:00 PM GMT, PDF Copy.

وأسبابها وتأثيراتها، وما هي إجراءات الحماية المطبقة لدى البنوك التجارية في الجمهورية اليمنية لمواجهة المخاطر المهددة لها.

3. **من حيث المنهجية:** كانت غالبية الدراسات السابقة دراسات نظرية وميدانية، وتعد الدراسة الحالية دراسة تطبيقية بالإضافة إلى استخدام الباحث لأسلوب الدراسة الميدانية من وجهة نظر مدراء ورؤساء الأقسام وكافة العاملين في نظم وتكنولوجيا المعلومات، وكذلك المدققين الداخليين والخارجيين لتلك النظم، فقد أجرى قبل ذلك دراسة حالة عملية استكشافية في ثلاثة بنوك تجارية معتمداً على بيانات من واقع مقابلات الباحث وملاحظاته للسجلات والتقارير لتعزيز الجانب التطبيقي، حيث لم تتطرق أية دراسة سابقة لتناول وجهات نظر هذه الأطراف مجتمعة وبنفس أدوات هذه الدراسة.

4. **من حيث وضوح وتمييز المتغيرات البحثية:** قليل من الدراسات السابقة تناولت مخاطر أمن نظم المعلومات المحاسبية على استحياء ولم تميز أو تفرق بين تلك المخاطر والتهديدات المختلفة المسببة لها، كضعف أو عدم كفاية إجراءات الحماية، بالإضافة إلى أن العديد من الدراسات السابقة اعتبرت عدم فعالية آليات إدارة المخاطر على أنها تمثل مخاطر لنظم المعلومات المحاسبية المحوسبة، وهذا ما تلافته هذه الدراسة حيث أبرزت تلك المخاطر بشكل شمولي تحليلي، ودرست متغيرات ومفاهيم مختلفة من حيث المضمون مع ما جاء في بعض تلك الدراسات، وسلطت الضوء على التهديدات المسببة للمخاطر، وأبرزت العلاقة بين المخاطر وإجراءات الحماية المطبقة، وهذا ما لم تتناوله أي دراسة سابقة.

5. **من حيث تصنيف متغيرات الدراسة وفق أسس علمية:** لم تصنف العديد من الدراسات السابقة المخاطر التي تتعرض لها نظم المعلومات أو إجراءات الحماية بحسب مدى ارتباطها بالجوانب المادية أو غير المادية لنظام المعلومات أو بحسب طبيعية أصول نظم المعلومات أو بحسب المراحل المختلفة لعملها وهذا ما تلافته هذه الدراسة.

6. **من حيث نطاق ومجال الدراسة:** يوجد عدد كبير من المخاطر لم يتم تقييمها بصورة كافية في الدراسات السابقة، وهو ما تلافته هذه الدراسة، كما أن هذه الدراسة اقترحت عدد من الإجراءات التي يجب تطبيقها لتجنب العديد من المخاطر وكيفية التعامل معها من خلال إستراتيجية تأخذ في الاعتبار المعايير الدولية المتعارف عليها، والبيئة اليمنية، وبشكل عام فإن هناك فترة زمنية كافية ومتغيرات تكنولوجية متعددة ومتسارعة في مجال نظم المعلومات المحاسبية تدعو لضرورة الاستمرار في مثل هذه الدراسات لمواكبة التطور التكنولوجي الديناميكي، كما أنها فترة كافية لتغيير قنوات المحاسبين وكذا رجال إدارة المال والأعمال نحو مواكبة هذا التطور.

سابعاً: فرضيات الدراسة: من خلال التساؤلات المطروحة في مشكلة الدراسة ومن خلال الدراسات السابقة فإن هذه الدراسة تسعى إلى اختبار الفرضيات التالية:

الفرضية الأولى: H⁰¹: "لا تحدث مخاطر جوهرية وملموسة تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية".

الفرضية الثانية: H⁰²: "لا يُعزى حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية إلى مجموعة من التهديدات الداخلية".

الفرضية الثالثة: H⁰³: "لا يُعزى حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية إلى مجموعة من التهديدات الخارجية".

الفرضية الرابعة: H⁰⁴: "لا يؤثر حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية على العناصر المكونة لأمن تلك النظم المتمثلة ب(إتاحة النظم، وصحة وسلامة وتكامل التشغيل، وسرية وخصوصية المخرجات، وعدم إنكار العمليات) لدى تلك البنوك".

الفرضية الخامسة: H⁰⁵: "لا تُطبق البنوك التجارية في الجمهورية اليمنية أساليب وإجراءات رقابية وأمنية كافية وفعالة لحماية أمن نظم المعلومات المحاسبية المحوسبة من المخاطر التي تتهددها وفق القواعد المحلية والأسس والمعايير الدولية".

الفرضية السادسة: H⁰⁶: "لا تؤثر أساليب وإجراءات الحماية المطبقة في البنوك التجارية في الجمهورية اليمنية على المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى تلك البنوك".

الفرضية السابعة: H⁰⁷: "لا توجد فروق جوهرية بين آراء أفراد عينة الدراسة فيما يتعلق بالمخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية تُعزى للمسمى الوظيفي لهم".

الفرضية الثامنة: H⁰⁸: "لا يوجد اختلاف جوهري بين البنوك التجارية في الجمهورية اليمنية فيما يتعلق بحجم المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة يُعزى لملكية تلك البنوك".

الفرضية التاسعة: H⁰⁹: "لا يوجد اختلاف جوهري بين نظم المعلومات المحاسبية المحوسبة المستخدمة لدى البنوك التجارية في الجمهورية اليمنية فيما يتعلق بحجم المخاطر التي تهدد أمن تلك النظم يُعزى لنوعية تشغيل تلك النظم".

الفرضية العاشرة: H⁰¹⁰: لا يوجد اختلاف جوهري بين نظم المعلومات المحاسبية المحوسبة المستخدمة لدى البنوك التجارية في الجمهورية اليمنية فيما يتعلق بحجم المخاطر التي تهدد أمن تلك النظم يُعزى لمستوى ارتباط تلك النظم بشبكات الاتصال".

ثامناً: أنموذج الدراسة: بناءً على أهداف الدراسة وعلى ضوء فرضياتها فإن أنموذج الدراسة يتكون من متغيرات مستقلة (التهديدات الداخلية والخارجية المسببة للمخاطر وأساليب وإجراءات الحماية من تلك المخاطر)، وهي محددات يتم على أساسها التقييم، ومتغير تابع يتمثل في (مخاطر أمن نظم المعلومات المحاسبية المحوسبة المباشرة وغير المباشرة) وهذا الأنموذج عبارة عن تصور يستخدم لتعزيز الدراسة التطبيقية:

الشكل رقم (1) أنموذج الدراسة يوضح المتغيرات المستقلة والمتغير التابع والغاية من الدراسة. (1)

المتغيرات المستقلة

(Independents Variables)

التهديدات الداخلية لأمن نظم المعلومات:

1. فلسفة الإدارة العليا للبنك.
2. العوامل التنظيمية.
3. إمكانات البنك التكنولوجية.
4. الأفراد العاملين في النظام.
5. ضعف الرقابة الداخلية.
6. الكوارث الداخلية.

التهديدات الخارجية لأمن نظم المعلومات:

1. التغيير التكنولوجي غير المتوازن.
2. الكوارث الطبيعية والسياسية.
3. المخترقون والقرصنة.
4. الفيروسات وبرمجيات الحاسوب الخبيثة.
5. المنافسة الاقتصادية بين البنوك.
6. ضعف الرقابة الخارجية على النظام.
7. ضعف التشريعات والقوانين المحلية.
8. نقص الوعي الإلكتروني لدى العملاء.

أساليب وإجراءات حماية أمن نظم المعلومات:

1. حماية الأمن التنظيمي للعاملين.
2. حماية الأمن المادي للنظم.
3. حماية أمن الوصول البرمجي للبيانات.
4. حماية أمن وسائط التخزين غير المتصلة.
5. حماية أمن مدخلات النظم.
6. حماية أمن عمليات تشغيل النظم.
7. حماية أمن مخرجات النظم.
8. حماية أمن البيانات المنقولة عبر الشبكات.
9. حماية أمن تطوير وتعديل النظم.

المتغير التابع

(Dependent Variable)

المخاطر المباشرة التي تهدد أمن نظم المعلومات المحاسبية المحوسبة:

1. مخاطر أمن الأفراد.
2. مخاطر الأمن المادي للنظم.
3. مخاطر أمن الوصول البرمجي للبيانات.
4. مخاطر أمن وسائط التخزين غير المتصلة.
5. مخاطر أمن مدخلات النظم.
6. مخاطر أمن عمليات تشغيل النظم.
7. مخاطر أمن مخرجات النظم.
8. مخاطر أمن البيانات المنقولة عبر الشبكات.
9. مخاطر أمن تطوير وتعديل النظم.

المخاطر غير المباشرة التي تهدد أمن نظم المعلومات المحاسبية المحوسبة:

تأثيرات المخاطر المباشرة

1. مخاطر تهدد إتاحة نظم المعلومات.
2. مخاطر تهدد سلامة وتكامل تجهيز البيانات.
3. مخاطر تهدد سرية المعلومات.
4. مخاطر تهدد خصوصية بيانات الأطراف المتعاملة مع البنك.
5. مخاطر إنكار الأطراف المتعاملة للعمليات خلال تبادل البيانات إلكترونياً.

الغاية:

تقييم ومعالجة المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة بهدف رفع كفاءة وفاعلية أمن تلك النظم لدى البنوك التجارية في الجمهورية اليمنية

تاسعاً: حدود الدراسة ومحدداتها: تتمثل حدود هذه الدراسة في النقاط الآتية:

1. **الحدود المكانية والمؤسسية:**

- الدراسة العملية التطبيقية تمت بالتطبيق على البنوك التجارية في الجمهورية اليمنية، حيث تم اختيار ثلاثة بنوك رئيسية تمثل كلاً من القطاع العام والخاص والمختلط لإجراء دراسة الحالة العملية.
- وتم اختيار البنوك التجارية في الجمهورية اليمنية والبالغ عددها (16) بنكاً⁽¹⁾ (بما فيها فروع البنوك التجارية العربية والأجنبية في اليمن)، كونها أكثر المنشآت مواكبة لتكنولوجيا المعلومات، وقد اكتفى الباحث بالمراكز الرئيسة لتلك البنوك وفروعها الهامة في العاصمة صنعاء لتمرکز معظم النشاط المصرفي لتلك البنوك هناك، ولأن الإجراءات المستخدمة في الفروع هي تطبيق للإجراءات المستخدمة في الإدارات والمراكز الرئيسية.
- 2. **الحدود الموضوعية لمتغيرات الدراسة:** هناك مخاطر كثيرة تهدد أمن نظم المعلومات المحاسبية وأسباب متعددة لحدوثها ولكن يعتقد الباحث أن المخاطر والتهديدات المسببة لها والتي تناولتها الدراسة هي الأكثر شيوعاً وتحتاج إلى دراسة في البيئة اليمنية ولذلك اقتصرت الدراسة عليها، وبالمثل هناك إجراءات وضوابط رقابية كثيرة ومتعددة لحماية أمن نظم المعلومات ولكن هذه الدراسة ركزت على أهم تلك الإجراءات.

وتتمثل محددات الدراسة في بعض الصعوبات والمعوقات التي واجهت الباحث أثناء إنجاز هذا العمل ومن أهمها:

1. صعوبة الحصول على بعض البيانات التفصيلية المتعلقة بالدراسة لعدم تعاون بعض الإدارات لدى البنوك التجارية محل الدراسة، في تزويد الباحث ببعض البيانات التفصيلية المتعلقة بهذه الدراسة بسبب ادعائها أنها تتعلق بمعلومات حساسة وسرية لا يجوز الإفصاح عنها، وعدم إدراك القائمين على البنوك التجارية عن أهمية الإداء بالمعلومات التي تساهم في مساعدة الباحثين في تحقيق الهدف من البحث العملي، وعدم المخاطرة بالاعتراف بضعف نظامها المحاسبي، خوفاً من فقدان الثقة بها من قبل المتعاملين معها، وعدم تعاون بعض المختصين في تعبئة قوائم الاستقصاء بحجة ضغوط العمل لديهم، فإلى جانب انعدام الشفافية فيما يتعلق بهذه البيانات، فالعديد من التقديرات المستخدمة هي نتاج تحليل الخبراء وحسب الباحث وملاحظاته.
2. كانت هناك عدة مفاهيم تقنية حديثة صعب فهمها بشكل جيد من قبل عينة الدراسة، وبناءً فقد تم رجوع الباحث إلى المستهدفين أكثر من مرة وتم شرح بعض تلك المفاهيم في الاستقصاء على شكل تعريف مختصر لكل منها.
3. لم تركز الدراسة كثيراً على الجوانب الفنية المتخصصة إلا بما تقتضيه طبيعة وترتيب عناصر الموضوع.
4. عدم وجود قوانين محلية واضحة في الجمهورية اليمنية تحكم وتضبط جرائم الحاسوب.
5. الأحداث السياسية والأمنية التي شهدتها الجمهورية اليمنية خلال فترة إعداد الدراسة وانعكاساتها على الباحث.

(1) البنك المركزي اليمني، الإدارة العامة للبحوث والإحصاء، مجموعة تقارير ربع سنوية عن الأعوام : 2012-2016م، مطابع اليمن العصرية، صنعاء، اليمن.

عاشرًا: خطة الدراسة: لحل مشكلة الدراسة وتحقيقاً لهدفها واختبار فرضياتها قام الباحث بتقسيم هذه الدراسة إلى إطار عام وثلاثة فصول رئيسية وذلك على النحو التالي:

1. **الإطار العام للدراسة:** ويتناول الباحث من خلاله بيان مشكلة الدراسة، وأهميتها، وأهدافها، والدراسات السابقة لها، وما تتميز به هذه الدراسة عن الدراسات السابقة، وفرضيات الدراسة، وأنموذج الدراسة، وحدود الدراسة ومحدداتها، وخطة هذه الدراسة.

2. **الفصل الأول:** يتطرق إلى مخاطر أمن نظم المعلومات المحاسبية المحوسبة: وقد تم تقسيمه لأربعة مباحث: يتناول **المبحث الأول:** أمن نظم المعلومات المحاسبية المحوسبة، تمهيداً **للمبحث الثاني:** الذي ركز على طبيعة مخاطر أمن نظم المعلومات المحاسبية المحوسبة من حيث تعريفها وتصنيفاتها وأنواعها المختلفة، وجاء **المبحث الثالث:** ليوضح التهديدات الداخلية المسببة لحدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة، وأخيراً **المبحث الرابع:** الذي سلط الضوء على التهديدات الخارجية المسببة لحدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة.

3. **الفصل الثاني:** يتناول تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة: وقد تم تقسيمه لأربعة مباحث حيث تناول **المبحث الأول:** المعايير والأطر الدولية والتشريعات المنظمة لتقييم وإدارة مخاطر أمن نظم المعلومات، تمهيداً **للمبحث الثاني:** الذي تناول طبيعة وأدوات ومناهج تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة، أما **المبحث الثالث:** فقد ركز على مدى تأثير حدوث المخاطر على أمن نظم المعلومات المحاسبية المحوسبة، وأخيراً **المبحث الرابع:** تناول إجراءات ووسائل وأساليب الحماية والرقابة الداخلية المطبقة لمواجهة تلك المخاطر.

4. **الفصل الثالث:** الدراسة التطبيقية لدى البنوك التجارية في الجمهورية اليمنية: وقد تم تقسيمه إلى خمسة مباحث، **المبحث الأول:** تطرق إلى بيان منهج الدراسة ومجتمعها وعينتها، وآلية تحليل البيانات والاختبارات التمهيدية، أما **المبحث الثاني:** فقد تطرق لدراسة حالة عملية لواقع أمن نظم المعلومات المحاسبية المحوسبة والمخاطر التي تتهددها لدى ثلاثة بنوك تجارية رائدة في الجمهورية اليمنية كنموذج تطبيقي لهذه الدراسة، و**المبحث الثالث:** تناول تحليل البيانات الذي تم الحصول عليها بواسطة الاستقصاء الموزع على المراكز الرئيسية لجميع البنوك التجارية في الجمهورية اليمنية، بينما جاء **المبحث الرابع:** لاختبار الفرضيات باستخدام الانحدار البسيط وتحليل التباين الأحادي، وغيرها من الأساليب الإحصائية المناسبة، وأخيراً جاء **المبحث الخامس:** ليقدم الباحث فيه نتائج هذه الدراسة التطبيقية التي تم التوصل إليها، وكذلك التوصيات والمقترحات المنبثقة عنها لتطوير وتعزيز أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية ورفع كفاءته وفاعليته، والحد من المخاطر التي تتهدده، وعلى ضوء ما توصل إليه بالجانب النظري، فضلاً عن ما حققه من إثباتات تطبيقية باستخدام الأدوات الإحصائية المناسبة.

الخاتمة:

تضمن هذا الإطار العام وصفاً منهجياً لهذه الدراسة حيث تم بيان مشكلة الدراسة وفرضياتها والأنموذج الذي يوضح متغيراتها والغاية منها، مع بيان هيكل الدراسة، وحدودها ومحدداتها، وبذلك يمثل هذا الإطار العام أساساً هاماً لإجراء الدراسة النظرية في الفصلين الأول والثاني ثم القيام بالدراسة التطبيقية وتحليل نتائجها واقتراح التوصيات والمقترحات المنبثقة عنها، والتي يشملها الفصل الثالث من هذه الدراسة.

الفصل الأول

مخاطر أمن نظم المعلومات المحاسبية المحوسبة

الفصل الأول: مخاطر أمن نظم المعلومات المحاسبية

مقدمة: شهد الفكر المحاسبي بوجه عام ونظم المعلومات المحاسبية بوجه خاص تطوراً سريعاً وملحوظاً أظهرته العديد من الأبحاث المنشورة في هذا المجال، وبدأ يظهر ملامحها في الواقع العملي بالمنشآت التي تريد البقاء والاستمرار والتنافس في السوق وخاصة المنشآت الصناعية بدول اليابان والولايات المتحدة الأمريكية ومعظم دول أوروبا وجنوب شرق آسيا. وذلك التطور أحدث اتجاهات جديدة وتغييرات محورية في أساليب تعامل البنوك التجارية مع المعلومات الناتجة عن هذه التطبيقات الحديثة والأساليب الالكترونية التي غيرت من أسلوب وشكل وتقديم الخدمات المصرفية للزبائن والعملاء.

وإذا كانت نظم المعلومات المحاسبية المحوسبة قد ساهمت في سرعة وسهولة أداء الأنشطة المالية والمصرفية المختلفة إلا أنها قد واجهت العديد من المخاطر التي أثرت على إتاحة ودقة وسلامة وسرية هذه النظم وما ينتج عنها من معلومات، وهذا قد يعرض أي منشأة تجارية تعتمد على تلك النظم للانحيار والتوقف.

ولاشك أن نجاح تلك المنشآت في البقاء واستمرار احتفاظها بثقة الأطراف المتعاملة معها يتوقف على جودة وموثوقية معلوماتها والنظم الآلية التي تتعامل بها لتقديم خدماتها المختلفة، لذلك يرى الباحث أن مخاطر أمن نظم المعلومات المحاسبية المحوسبة، من أهم القضايا التي تشغل بال الفكر الاقتصادي الحديث.

ومن هذا المنطلق جاء هذا الفصل ليتناول مخاطر أمن نظم المعلومات المحاسبية المحوسبة سواء من حيث طبيعتها أو أنواعها المختلفة، وقد تم تقسيمه لأربعة مباحث، يتناول المبحث الأول أمن نظم المعلومات المحاسبية المحوسبة، وتناول للمبحث الثاني طبيعة مخاطر أمن نظم المعلومات المحاسبية المحوسبة من حيث تعريفها وتصنيفاتها المختلفة، أما المبحث الثالث فقد ركز على التهديدات الداخلية المسببة لتلك المخاطر، وأخيراً جاء المبحث الرابع ليوضح التهديدات الخارجية المسببة لتلك المخاطر، وسيتم استعراض تلك المباحث على النحو التالي:

1-1: المبحث الأول: أمن نظم المعلومات المحاسبية المحوسبة

إن انتشار نظم المعلومات المحوسبة أدى إلى أن تكون عرضة للكثير من المخاطر لذلك أصبحت هذه التقنية سلاحاً ذو حدين، حيث تحرص المنشآت على اقتناءها مع توفير سبل الحماية لها، ولذلك أصبحت قضية أمن نظم المعلومات المحاسبية المحوسبة من القضايا التجارية الأكثر أهمية، ومن المسائل الحاسمة والساخنة والمتجددة التي تواجه المنشآت بمختلف أنواعها، وأحد الهواجس التي توترق كل من لديه معلومات محوسبة سواء كان فرداً أو منشأة وبفس الوقت تهتم رجال الأمن والتشريع والمتخصصين في الاتصالات بل تهتم المجتمع بأكمله، ومن أهم المنشآت التي تسعى جاهدة للتعامل معها البنوك التجارية.⁽¹⁾

(1) زويلف، إنعام، (2009)، " طبيعة تهديدات أمن نظم المعلومات المحاسبية الإلكترونية - دراسة تطبيقية على شركات التأمين الأردنية، المجلة العربية للمحاسبة، العدد (12)، جامعة البحرين، المنامة، البحرين، ص ص: 46-77.

وقد أكد المعهد الأمريكي للمحاسبين القانونيين أن أهم أمرين في التكنولوجيا سيواجهان مهنة المحاسبة في السنوات الأولى من القرن الحادي والعشرين هما: التجارة الإلكترونية وأمن نظم المعلومات،⁽¹⁾ فالبيئة الاقتصادية التي يعمل فيها المحاسب اليوم أصبحت متغيرة بطريقة غير متوقعة، حيث أصبح معدل التطور الحاصل في تكنولوجيا المعلومات متزايداً بشكل كبير، كما أن المنشآت التجارية أصبحت تقوم بتغيير بنية إدارتها وإدارة أعمالها لكي تستطيع الاستمرار في بيئة يتزايد فيها التنافس، وفي ضوء ما تتعرض له الأسواق العالمية والاقتصاد العالمي من انكماش وتدهور وتعرض العديد من المنشآت العالمية الكبرى للإفلاس، كان لزاماً على الإدارة توجيه الاهتمام بعمليات جمع المعلومات وتصنيفها وتبويبها وتخزينها بطرق آمنة.

وأصبح أمن المعلومات التي تحتويها النظم الإلكترونية، وخاصة المالية والمحاسبية، موضع اهتمام وقلق لإدارات المنشآت التي تستخدم هذه النظم، ولمدققي الحسابات الذين يقومون بفحص وتدقيق البيانات المالية المستخرجة منها لإبداء الرأي في مدى سلامتها، ويرجع هذا القلق إلى تزايد أنواع واحتمالات المخاطر المحيطة بهذه النظم والتي تهدد صحة وموثوقية وسرية وتكامل البيانات المالية والمحاسبية فيها.⁽²⁾

ويتضمن هذا المبحث مفهوم أمن نظم المعلومات المحاسبية المحوسبة، والمبادئ الرئيسية لأمن تلك النظم، وأهمية وأهداف أمن نظم المعلومات المحاسبية المحوسبة كعنصر هام للمنشأة، وأنماط أو مجالات وأبعاد أمن نظم المعلومات المحاسبية، وسيتم تسليط الضوء على أهم عناصر النظام التي يجب أن تكون محل الحماية وأخيراً سيتم توضيح أهم العوامل التي يجب أن تؤخذ في الاعتبار عند وضع أي إستراتيجية أو سياسة لأمن نظم المعلومات المحاسبية المحوسبة.

1-1-1: ماهية نظم المعلومات المحاسبية المحوسبة: (CAIS):

1-1-1-1: ماهية نظم المعلومات المحاسبية (AIS): ينظر إلى نظام المعلومات المحاسبي من جانبين، الجانب الأول ينظر له بأنه مجموعة الوظائف التي تقوم بعملية تجميع البيانات وتسجيلها وتخزينها ومعالجتها وإنتاج المعلومات المحاسبية وتقديمها إلى الأطراف ذات المصلحة لاستخدامها في اتخاذ القرارات الاقتصادية المختلفة⁽³⁾، وهذا ما يراه (شحادة)، بأنه "ذلك الجزء من نظام المعلومات الكلي الذي يختص بتجميع وتشغيل وتخزين واسترجاع البيانات الكمية النقدية وغير النقدية لأغراض توفير المعلومات لمتخذي القرارات بالمنشأة،⁽⁴⁾ فهو نظام يختص بجمع البيانات ويتم فيه مجموعة من الإجراءات لمعالجتها لإنتاج المعلومات المحاسبية المطلوبة لمستخدميه.⁽⁵⁾

أما الجانب الثاني فينظر إلى نظام المعلومات المحاسبي على أنه مجموعة من الأنظمة الفرعية المتخصصة والتي تعالج العمليات المالية وغير المالية لنشاطات المنشأة ومن أهم مكوناته نظام (أو دورة) الإيرادات والمصروفات والتمويل

(1) Romney, Marshall B. & Steinbart, Paul J., (2015), "Accounting Information Systems", 13th Edition, England: Pearson Education (Pearson International Edition), Prentice Hall, New Jersey, USA., PP: 18-20.

(2) خطاب، محمد & أبو موسى، أحمد (2012)، "عوامل نجاح برامج أمن نظم المعلومات المحاسبية ودورها في تفعيل حوكمة الشركات: دراسة ميدانية على الشركات السعودية، مجلة كلية التجارة للبحوث العلمية، العدد (1) - المجلد (49)، جامعة الإسكندرية، مصر.

(3) Romney, M. B. & Steinbart, P. J., (2015), "Accounting Information Systems", OP. Cit., P.6.

(4) شحادة، حسين خليل، (2012)، "مذكرات في اقتصاديات البيانات والمعلومات المحاسبية"، كلية الإدارة والاقتصاد، الأكاديمية العربية المفتوحة في الدنمارك، فرع الموصل، العراق، ص300.

(5) Bagranof, Nancy A. & Simkin, Mark G. & Norman, Carolyn S. (2010). Accounting Information Systems. Eleventh Edition: South-Western, USA, P. 4.

والإنتاج والموارد البشرية،⁽¹⁾ وهذا ما يراه (السقا)، بأنه أحد النظم الفرعية في المنشأة، يتكون من عدة نظم فرعية تعمل مع بعضها البعض بصورة مترابطة ومتناسقة ومتبادلة، بهدف توفير المعلومات التاريخية والحالية والمستقبلية، المالية وغير المالية، لجميع الجهات التي يهتمها أمر المنشأة وبما يخدم تحقيق أهدافها".⁽²⁾

ومن خلال ما تقدم فإن نظام المعلومات المحاسبية يعتبر نظاماً رئيسياً ينطوي على العديد من النظم الفرعية (Subsystems) والتي يتم تطبيقها عند كافة مستويات الهيكل الإداري في المنشأة، (مثل نظام المحاسبة المالية، ونظام المحاسبة الإدارية)، والتي تعمل مع بعضها بصورة مترابطة ومتناسقة لتوفير المعلومات للجهات المختلفة لمساعدتها في التخطيط والرقابة وترشيد اتخاذ القرار.

كما يمكن النظر إلى نظام المعلومات المحاسبية بوصفه نظاماً فرعياً يدخل في إطار مكونات نظم المعلومات الإدارية الكلي في المنشأة، ولذلك يرى الباحث بأن النظرة الحديثة لدراسة نظم المعلومات التي يمكن أن تتواجد في أي منشأة يجب أن لا تكون نظرة جزئية، وإنما يجب الأخذ بنظر الاعتبار النظرة الكلية التي تنظر إلى ضرورة التكامل والتنسيق والترابط بين كل نظم المعلومات التي يمكن أن تتواجد ضمن إطار المنشأة وصولاً إلى تحقيق أهدافها العامة للمنشأة.

ويرى الباحث إن كلا المفهومين لنظام المعلومات المحاسبي المحسوب متداخلان فيما بينهما، فمفهوم مجموعة الوظائف يعتمد بالأساس على عدد من الأنشطة الفرعية التي تقوم بتجميع البيانات المتعلقة بأنشطتها المختلفة، وفي الوقت نفسه فإن مفهوم مجموعة الأنظمة الفرعية يعتمد على تجميع البيانات لكل نشاط أو نظام فرعي ومن ثم تجميع بيانات الأنظمة الفرعية لتصب في وعاء أكبر للبيانات تخص كل نظام المعلومات المحاسبي، وهذا الأمر يعكس الترابط بين مكونات نظام المعلومات المحاسبي في المنشأة.

1-1-2: ماهية نظم المعلومات المحاسبية المحوسبة (CAIS): نظام المعلومات المحاسبي يمكن أن يكون نظاماً يدوياً أو شبه يدوي أو نظاماً محسوباً، حسب طريقة تشغيل البيانات التي يمكن أن تتبعها المنشأة ومدى استخدامها للحاسوب، ويعرف نظام المعلومات المحسوب بأنه عبارة عن توليفة من البرامج والمعدات والمكونات البشرية يتم تصميمها من أجل تجميع البيانات وتجهيزها وإدارتها وحفظها وتوفير المخرجات التي تفيد متخذي القرارات في مختلف الوظائف.⁽³⁾

- هو استخدام أجهزة الحاسوب لإدخال البيانات والتعامل مع نظم المعلومات في المنشآت المختلفة على نحو يمكن تلك المنشآت من الحصول على البيانات والمعلومات وحفظها وتحويلها بمساعدة أجهزة الحاسوب.⁽⁴⁾

(1) Hall, James A., (2013), *Accounting Information Systems*, 8th Edition, CENGAGE Learning, Lehigh University, Thomson, South-Western, Mason, Ohio, USA, THOMSON, South-Western, USA, P.9.

(2) السقا، زياد هاشم، (2011)، *نظام المعلومات المحاسبية*، الطبعة الثانية، دار الطارق للنشر والتوزيع، الموصل، العراق، ص 41.

(3) حجر، عبد الملك إسماعيل، (2009) " *نظم المعلومات المحاسبية* "، الطبعة الثانية، الأمين للنشر والتوزيع، صنعاء، اليمن، ص 29.

(4) Dalci, I. & Tanis, V. (2009), "Benefits of Computerized Accounting Information Systems on the JIT Production Systems", *Review of Social Economic & Business Studies*, Vol.2, PP: 45-64.

- هو استخدام الموارد المادية والبشرية والبرمجية والمعلوماتية لإدخال البيانات وتخزينها ومعالجتها واسترجاعها وإخراج المعلومات وتوصيلها إلى الجهات المستخدمة والمستفيدة منها لمساعدتها في ممارسة أنشطتها الرئيسية (وظائف المنشأة ووظائف الإدارة) واتخاذ القرارات وتقييم الأداء.⁽¹⁾
- وتأسيساً على ما تقدم يمكن للباحث تعريف نظم المعلومات المحاسبية المحوسبة بأنها مجموعة من النظم الالكترونية التي تعتمد على الحاسوب والتقنيات الحديثة وباستخدام مجموعة من الأدوات المادية والبشرية والتي تعمل بصورة مترابطة ومتناسقة ومتكاملة ومتبادلة، لتنفيذ مجموعة من الإجراءات والعمليات وفق المبادئ والقواعد المحاسبية المتعارف عليها بهدف توفير المعلومات التي تساعد الإدارة والجهات ذات العلاقة بالمنشأة على القيام بالمهام واتخاذ القرارات وبما يخدم تحقيق أهداف المنشأة.

1-1-2: مكونات نظم المعلومات المحاسبية المحوسبة (The Components of CAIS):

يتطلب الكشف عن الأبعاد المختلفة لمخاطر نظم المعلومات تناول المقومات الأساسية لأي نظام معلومات، وقد سبق أن ذكرنا بأن النظام هو مجموعة من العناصر أو الأجزاء المتداخلة والمترابطة والتي تعمل كوحدة واحدة وتتفاعل مع بعضها البعض لتحقيق الأهداف المرسومة، ويتكون أي نظام معلومات بشكل عام من أصول متعددة تشكل بنيته التحتية، وأهمها الأفراد العاملين والمستخدمين، والأجهزة، والبرمجيات، وشبكات الاتصال وقواعد البيانات، وكذلك الإجراءات والتعليمات والضوابط التي تحكم العمل،⁽²⁾ فنظام المعلومات الفعال يشمل الأجهزة والبرامج وقواعد البيانات و المعلومات وغيرها من الأصول، كما يشمل الموارد البشرية، والسياسات والإجراءات المرتبطة بجمع وتوزيع واستخدام وصيانة هذه النظم،⁽³⁾ وتتكامل هذه المكونات مع بعضها البعض من أجل تحقيق أهداف تلك النظم.⁽⁴⁾

ولذلك فإن نظام المعلومات المحاسبي المحوسب في أي منشأة يشمل مزيج أو خليط من تلك المكونات المذكورة والتي تتفاعل مع بعضها البعض لتوفير المعلومات المفيدة لدعم ترشيد اتخاذ القرارات الصائبة،⁽⁵⁾ ويوضح الشكل التالي أهم تلك المكونات:

(1) Romney, M. B. & Steinbart, P. J., (2015), "Accounting Information Systems", OP. Cit., P.7.

(2) Sun, L. & Srivastava, R. & Mock, T.J., (2015), "An Information Systems Security Risk Assessment Model Under Dempster-Shafer Theory Of Belief Functions", *Journal of Management Information systems*, Vol. 22, No.4, PP:109-142.

(3) Parakkattu, Sindhuja & Kunnathur, Anand. S., (2010), "A Framework for Research in Information Security Management", *Northeast Decision Sciences Institute Proceedings (NEDSI)*, March 2010, PP: 318-323.

(4) الرضا، عقبة كامل، (2008)، "تدقيق الحسابات في ظل نظم المعلومات المحاسبية"، ورقة بحث ضمن *الفعاليات العلمية*، جمعية المحاسبين القانونيين السوريين، دمشق، سوريا، أيار (مايو) 2008، ص: 1-13.

(5) Shamala, Palaniappan & Ahmad, Rabiah & Yusoff, Mariana, (2013), "A conceptual Framework of Info Structure for Information Security Risk Assessment (ISRA)", *Information Security and Applications*, Vol. 18, No. 1, PP: 45-52.

شكل رقم (1-1-1) مكونات نظم المعلومات المحاسبية المحوسبة (1)



وعليه يستطيع الباحث القول أن نظام المعلومات المحاسبي يتكون من مجموعة من الأجزاء البشرية ممثلة بكافة العاملين في دائرة نظم المعلومات الذين يستخدمون مجموعة من الأجزاء المادية ممثلة بكافة لوازم أداء العمل المحاسبي من معدات وبرامج وسجلات... الخ وفق إجراءات وقواعد محاسبية معينة للقيام بتسجيل البيانات وتشغيلها وتوصيل نتائجها لكافة الجهات التي يمكن أن تستفيد منها، والجدير بالذكر أن المكونات قد تكون في صورة مادية ملموسة (الأفراد، الآلات، المجموعة المستندية والدفترية)، وقد تكون في صورة غير مادية (البرامج والقواعد والإجراءات والمبادئ) وهذين المكونين متلازمين لا يمكن الفصل بينهما.

3-1-1: أنواع نظم المعلومات المحاسبية المحوسبة على أساس بيئة التشغيل البيانات:

من المعروف بأن كل منشأة تحتاج إلى نظام محاسبي محوسب خاص بها، فكل منشأة لها طبيعة عمل تختلف عن الأخرى وبالتالي تحتاج إلى نظام يتماشى معها، فنظام المحاسبة المحوسب للبنوك لا يصلح لشركات التأمين، وبالمثل للمنشآت الصناعية، كما إن التطور السريع والمستمر في تكنولوجيا الحاسب الإلكتروني، واستخدامها في تطوير نظم المعلومات المحاسبية، نتج عنه أنواعاً مختلفة من نظم المعلومات المحاسبية المحوسبة، ومن أهم هذه النظم ما يلي:

1. **نظام التشغيل على أساس الدفعات:** هو النظام الذي يتم فيه تشغيل البيانات بالدفعات بعد استكمال تجميع البيانات ذات العلاقة خلال فترة محددة، ويعرف باسم التغذية البعيدة، حيث يتم تجميع مجموعات من البيانات وتحويلها إلى وسط إدخال ما، في مواقع بعيدة عن الحاسوب، وأجهزة الإدخال والإخراج بهذه المواقع تسمى محطات الإدخال والإخراج البعيدة، ويتم تحديث الملف الرئيسي بعد أن يتم جمع البيانات وترتيبها في مجموعات ومعالجتها جميعاً في وقت واحد على دفعة واحدة، أي لا يتم تحديث الملف الرئيسي إلا عندما يتوفر قدر كاف من البيانات،⁽²⁾ وبالتالي في إطار هذا النهج هناك دائماً فجوة زمنية بين النقطة التي يحدث فيها الحدث الاقتصادي، والنقطة التي ينعكس ذلك الحدث في حسابات المنشأة.

(1) O'Brien, J. A., (2010), "Management Information systems: Managing Information Technology in the E-Business Enterprise", 15th Ed., Boston: Irwin: Mc Graw-Hill Companies, Inc., USA, P.8.

(2) الجزراوي، إبراهيم & سعيد، لقمان، (2009)، "أدوات تكنولوجيا المعلومات ودورها في كفاءة وفاعلية المعلومات المحاسبية"، مجلة الإدارة والاقتصاد، العدد (75)، الجامعة المستنصرية، بغداد، العراق، ص: 1-36.

2. **نظم تشغيل البيانات المباشرة:** هي تلك النظم التي تتعامل مع كميات كبيرة من المعاملات حيث تقوم بإدخال ومعالجة وتحديث بيانات العمليات فور حدوثها وفي الوقت الحقيقي (*On-Line Real-Time*) من خلال أجهزة طرفية أو فرعية في بيئة شبكية، حيث تتيح هذه النظم للمستخدمين البدء مباشرة بتأدية مهام مختلفة كإدخال المعاملات، وعمل الاستفسارات، وطلب تقارير عند الحاجة، ومن ثم الحصول على معلومات محدثة بآخر عملية،⁽¹⁾ وبعض تلك النظم تكون متاحة (24) ساعة في اليوم، الأمر الذي ساعد المحاسب في تنفيذ جميع أو بعض أجزاء العمل الخاص به دون ضرورة التنقل إلى مكان العمل، وقد منح ذلك مواصفات جديدة وإعادة النظر في المواصفات التقليدية السائدة وهي: مكان العمل ووسائل العمل وتحسين أفضل لوقت العمل، والحفاظ على الموظفين، وتحسين إنتاج الموظفين، وتخفيض تكاليف المهام، وتوسيع مهام الوظيفة المحاسبية،⁽²⁾ كما أدى إلى تطوير ممارسة مهنة مراقبي الحسابات وذلك باستخدام التدقيق المستمر الفوري والمباشر.⁽³⁾

3. **نظم تشغيل البيانات الموزعة:** هي تلك النظم التي تربط عدة مواقع بشبكة اتصالات، وتعمل هذه المواقع معاً وتكون متصلة بقاعدة بيانات واحدة ولكن قد لا يكون كل مستعمل مطلعاً بالضرورة على جميع البيانات المستعملة في تلك القاعدة أو الطرق التي تستعمل بها هذه البيانات لأغراض متعددة، وتعني أن هناك عدة نظم متصلة معاً بقاعدة بيانات واحدة من خلال شبكة اتصال، ويتم توزيع مهام تشغيل البيانات على نظم الشبكة، ويمكن هذا التوزيع من معالجة البيانات والاتصال عن بعد بسرعة أكبر حسب المهام الموكلة سواء من داخل المنشأة أو خارجها، كما في البنوك والفنادق وشركات التأمين والمستشفيات وشركات الطيران والجامعات وغيرها من المؤسسات التي تتعامل مع حجم كبير من البيانات، وتتميز نظم قواعد البيانات بأنها متكاملة ومتاحة للاستخدام، وهي تتصف باستقلالية بياناتها، وبالأمان، وقلة احتمال وقوع الأخطاء، وإمكانية استخدامها مع أنظمة أخرى.

4. **نظم التشغيل المستقلة:** لا تخلو أي بيئة أعمال من وجود حاسبات شخصية أو ما تعرف بالمايكرو كومبيوتر (*PCs*) وهي حاسبات اقتصادية قوية وتامة ذاتياً (*Self Contained*) وتستعمل لأغراض عامه وقد تمثل كامل النظام المحاسبي الإلكتروني أو جزءاً منه فقط.

1-1-4: دورة تجهيز البيانات في نظم المعلومات المحاسبية المحوسبة ووظائفه المختلفة:

تعتبر نظم المعلومات المحاسبية نظاماً مفتوحاً تتأثر بالبيئة التي تعمل في محيطها وتؤثر عليها، وقد قام أحد الباحثين باستخدام عمل الخلية الحيوية في جسم الإنسان لوصف وتفسير عمل النظام المحاسبي، فكل خلية حيوية وظيفية محددة تقوم بها لكنها تتفق عموماً بالقيام باستقبال المدخل وتحويله ومن ثم تكوين المخرج والاستفادة منه وتكمن أهمية نجاح الخلية في أداء هذه الدورة الوظيفية في تأثيرها على جسم الإنسان ككل باعتباره البيئة الأوسع مجاًلاً والتي تعمل في محيطها وليس العضو الذي يعمل فيه فقط وهذا بالضبط ما يمثل نظام المعلومات المحاسبية للمنشأة التجارية، وأياً كان

(1) Hall, James A., (2013), *Accounting Information Systems*, OP. Cit., P.80.

(2) حوري، زينب & وخضراوي، ساسية، (2013)، "معالجة مخاطر التكنولوجيا في أعمال المحاسبة والتدقيق"، *مجلة العلوم الإنسانية*، العدد (30-31)، جامعة محمد خيضر، بسكرة، الجزائر، مايو 2013، ص ص: 396-379.

(3) الدوغوي، علي حسين، (2008)، " دور مراقبي الحسابات في ظل تكنولوجيا المعلومات المعقدة ومخاطر التدقيق"، *مجلة العلوم الاقتصادية والإدارية*، المجلد (14)، العدد (52)، كلية الإدارة والاقتصاد، جامعة بغداد، العراق، ص ص: 304-285.

نوعية نظم المعلومات المحاسبية المستخدمة وطبيعة عمل المنشأة فقد اتجهت معظم المنشآت إلى تصميم وبناء نظم معلومات محاسبية من أجل السيطرة على الكم الهائل من المعلومات الضرورية لإدارة المنشأة ولضمان وصول تلك المعلومات موثوقة وصحيحة ودقيقة ذات جودة عالية لكافة مستويات الإدارة بالشكل الملائم والوقت المناسب وبأقل تكلفة لاستخدامها في اتخاذ قرارات رشيدة تحقيقاً لأهداف المنشأة، فالهدف من نظم المعلومات المحاسبية هو توفير المعلومات المحاسبية الموثوق بها وفي الوقت المناسب،⁽¹⁾ وبشكل عام فإن نظام المعلومات المحاسبي في أي منشأة أياً كان نوعه يهدف إلى تحقيق ثلاث مهمات رئيسية وهي:⁽²⁾

1. تجميع وتخزين البيانات والمعلومات عن أنشطة وعمليات المنشأة وذلك لاسترجاعها عند الحاجة.
 2. تحويل تلك البيانات إلى معلومات ذات قيمة لغايات اتخاذ القرارات والتي تمكن الإدارة من التخطيط والتنفيذ، والرقابة على الأنشطة المختلفة.
 3. توفير ضمانات معقولة بأن إجراءات الرقابة الداخلية سوف تحمي أصول المنشأة بما فيها المعلومات المتعلقة بتلك الأصول للتأكد من توفرها عند الحاجة وأنها دقيقة وموثوقة يمكن الاعتماد عليها.
- وتقوم حركة العمل في نظام المعلومات من خلال مجموعة محددة ومنظمة من المراحل تنتهي بتحقيق تلك الأهداف التي من أجلها وُجِدَ النظام، حيث يقوم نظام المعلومات المحاسبي باستخدام مكوناته المادية من الأجهزة (أجهزة و سائل الإعلام) ، والبرمجية (برامج)، و البشرية (الأفراد المتخصصين والمستخدمين) لتنفيذ أنشطة الإدخال والمعالجة والإخراج والتخزين و الرقابة التي تحول موارد البيانات إلى منتجات (المعلومات)، حيث يتم جمع البيانات الأولية وتحويلها إلى شكل يمكن أن يكون مناسب للتجهيز (المدخلات)، ثم يتم تشغيل البيانات وتحويلها إلى معلومات (معالجة)، وتخزينها لاستخدامها في المستقبل (التخزين) ، أو نقلها إلى المستخدم النهائي لها (مخرجات) وفقاً لإجراءات معالجة صحيحة (الأمن والتحكم)،⁽³⁾ ولذلك تتكون دورة تجهيز البيانات في أي منشأة من خمس مراحل أساسية هي:
1. **مرحلة إدخال البيانات (Data Input Cycle):** تعتبر من أهم مراحل المعالجة في النظم المحوسبة، لأنها تؤثر على السجلات وقواعد بيانات المنشأة والتقارير المستخرجة منها، حيث أن حدوث خطأ في عملية الإدخال قد يترتب عليه وقوع سلسلة من الأخطاء وهي نقطة بداية عمل النظام، حيث يتم تجميع البيانات التي تصف الأحداث التي تدخل النظام من الأدلة الموضوعية المؤيدة للأحداث المالية نتيجة عمليات المنشأة المختلفة،⁽⁴⁾ ويجب أن تكون متعلقة بالموضوع المراد حله وإلا فهي بمثابة تشويش لمتخذ القرار، كما أن البيانات المكررة والزائدة عن الحاجة يمكنها أن تؤدي إلى إجراءات غير ملائمة وقرارات سيئة وغير صائبة.⁽⁵⁾

(1) Fardinal,(2013), "The Quality of Accounting Information and The Accounting Information System through The Internal Control Systems: A Study on Ministry and State Agencies of The Republic of Indonesia", Research Journal of Finance and Accounting, Vol.4, No.6, PP: 156-161.

(2) Romney, M. B. & Steinbart, P. J.,(2015), " Accounting Information Systems", OP. Cit., P.8.

(3) Abdelhak, Djenane & Dalel, Hammoudi (2010), "Evaluation of The Performance of The Financial and Accounting Computerized Information Systems In The Jordanian Banking Sector: An Empirical Study", Laboratoire Finances, Banques Et Management, No. 26, Université de Biskra, Algeria, PP: 1-17.

(4) الحميد، محمد دباس & ونيو، ماركو إبراهيم، (2007)، " حماية أنظمة المعلومات "، الطبعة الأولى، دار الحامد للنشر والتوزيع، عَمَّان، الأردن، ص15.

(5) Hall, James A., (2013), Accounting Information Systems, OP. Cit., P. 9.

2. **مرحلة تشغيل البيانات (Data Processing Cycle):** وهي تركز على الجانب الفني للنظام ممثلة بالعمليات التشغيلية للبيانات المدخلة بغرض تحويلها إلى صورة جديدة ذات معنى وقيمة ممثلة بالمعلومات،⁽¹⁾ ويتم ذلك وفق أحكام ومبادئ وقواعد علمية، ومع استخدام النظم المحاسبية المحوسبة يتم إثبات وإدخال كافة المعاملات مباشرة من قبل الأفراد كلاً فيما يخصه، ليتم معالجتها وترحيلها بشكل آلي وفوري إلى قاعدة البيانات للحصول على العديد من التقارير، فالمعالجة الفورية، تعني أن كل معاملة تدخل للحاسوب عند حدوثها ويجري عليها اختبارات للتأكد من خلوها من الأخطاء ويتم تحديث كل ملفات قاعدة البيانات المتأثرة بهذه المعاملة فوراً، وبالتالي يتم الحصول على تقارير محدثة وسهلة الوصول إليها من كل الأطراف الداخلية والخارجية.⁽²⁾
 3. **مرحلة إخراج المعلومات (Information Output Cycle):** ويتم فيها إخراج وتوصيل المعلومات المحاسبية إلى المستفيدين منها، وفق أشكال متعددة كالتقارير، والجداول، والقوائم، والأشكال البيانية وهذه المعلومات يطلق عليها مخرجات نظام المعلومات، حيث أن الهدف الرئيسي لأي نظام معلومات هو إنتاج المعلومات المناسبة للمستفيدين.⁽³⁾
 4. **مرحلة الرقابة والأمن وتخزين البيانات (Controlling & Security & Storage Cycle):** تتم إجراءات التحكم والسيطرة والرقابة وتخزين البيانات أثناء المراحل الثلاث السابقة، وهناك إجراءات أمن لحماية البيانات واكتشاف أي فقد أو تزوير أو تغيير فيها أثناء كافة مراحل النظام ووظائفه المختلفة من بداية تجميع البيانات إلى توصيل المعلومات للمستخدم.⁽⁴⁾ ويتم تخزين البيانات من خلال ترميزها وحمايتها واستعادتها في الوقت المناسب من قاعدة البيانات، ومختلف التقنيات والإجراءات توظف لفاعلية نظام المعلومات للمحافظة على وجود رقابة وأمن كافيين،⁽⁵⁾ فتكامل النظم الفرعية للنظام يؤدي إلى إن توقف أي نظام فرعي عن العمل لأي سبب قد يؤدي إلى توقف بقية النظم نظراً للاعتماد المتبادل للنظم على بعضها مما يتطلب ضرورة وجود إجراءات رقابية مستمرة لدقة وصلاحية البرامج حيث أن انهيار البرنامج يعني انهيار العمل في المنشأة وعدم استمرارها.
 5. **مرحلة التغذية العكسية "المرتدة" (Feedback):** وأخيراً تأتي مرحلة التغذية العكسية (المرتدة) حيث تمثل العمليات الارتدادية للنظام المحاسبي والتي يستفاد منها في قياس مدى استجابة النظام وتحقيقه للأهداف المرغوبة،⁽⁶⁾ وكما يستخدم مفهوم التغذية العكسية في أنظمة التحكم والسيطرة بهدف تحقيق الأمن والحماية وتحديد الإجراءات اللازم اتباعها للكشف عن الأخطاء ومعالجتها لضمان تصحيح العمليات الخاطئة ولضمان الوصول لمخرجات ملائمة، وعادة ما تنتج التغذية المرتدة مدخلات جديدة، أو معدلة للنظام.
- وعليه يمكن للباحث القول بأن المراحل الرئيسية لنظام المعلومات المحاسبية هي المدخلات (الممثلة بالبيانات التي يتم تغذية النظام بها) والعمليات التشغيلية والمخرجات (الممثلة بالمعلومات الناتجة) بالإضافة إلى حفظ وتخزين البيانات والمعلومات**

(1) Gelinas, Ulric J. & Sutton, Steven G. & Hunton, James E., (2012), *Accounting Information Systems*, 9th Edition, Thomson South-Western, Mason, Ohio, USA., P17.

(2) شحادة، حسين خليل، (2012)، "مذكرات في اقتصاديات البيانات والمعلومات المحاسبية"، مرجع سابق، ص157.

(3) شحادة، حسين خليل، (2012)، "نفس المرجع السابق"، ص157.

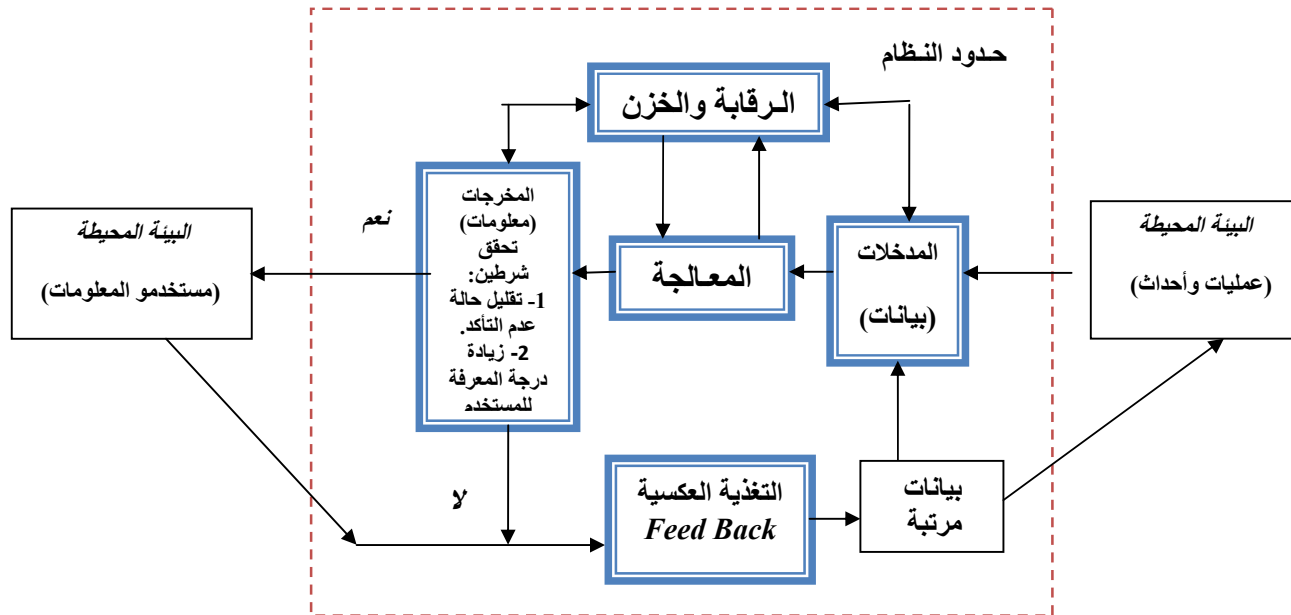
(4) Bodnar, George H. & Hoop-wood, William S., (2010), *Accounting Information Systems*, 10th Ed. NJ: Prentice Hall, PP:10-12.

(5) شحادة، حسين خليل، (2012)، "مذكرات في اقتصاديات البيانات والمعلومات المحاسبية"، مرجع سابق، ص166.

(6) الحميد، محمد دباس & ونيو، ماركو إبراهيم، (2007)، "حماية أنظمة المعلومات"، مرجع سابق، ص15.

ومراقبتها (قاعدة بيانات وإجراءات الأمن والرقابة)، وأخيراً عملية التغذية العكسية المرتبطة بالهدف المراد تحقيقه من النظام، والشكل التالي يوضح دورة تجهيز البيانات في النظام وفقاً للمراحل المختلفة.

الشكل رقم (2-1-1) دورة تجهيز البيانات في نظام المعلومات المحاسبي (i)



وبناءً على ما سبق توجد خمس وظائف أساسية لنظم المعلومات المحاسبية وهي: تجميع البيانات من مصادرها المتعددة، وتشغيلها، وتخزينها وإدارتها، وراقبتها وأخيراً استخراج المعلومات.

ويرى الباحث أنه يجب أن تحوز تلك الوظائف على الاهتمام عند دراسة وتقييم مخاطر أمن نظم المعلومات المحاسبية بهدف الوصول إلى أفضل مستوى ممكن من الكفاءة والفاعلية الأمنية لتلك النظم.

5-1-1: تعريف أمن نظم المعلومات المحاسبية المحوسبة:

احتل مصطلح "أمن نظم المعلومات" (*Information Systems Security*)، مكانة خاصة منذ القدم وحتى قبل نشأة الوسائل الحديثة لتكنولوجيا المعلومات، فمشكلة أمن المعلومات في المنشآت ليست جديدة فقد حرصت المنشآت في مختلف الأزمان على حماية أسرارها من مخاطر الوصول إلى أيدي منافسيها للحفاظ على استمراريتها، إلا أن استخدامه شاع وازداد انتشاراً مع استبدال الطرق التقليدية لحفظ وتخزين ومعالجة وتبادل المعلومات بالطرق الالكترونية، وتجاوز هذا المصطلح استخدامه التقليدي وظهرت تعبيرات جديدة تتصل بحماية وأمن المعلومات.⁽²⁾

(1) الشكل من إعداد الباحث.

(2) القرني، ميسون محمد، (2007)، "أمن المعلومات المحاسبية"، كلية الحاسبات وتقنية المعلومات، جامعة الملك عبد العزيز، الرياض، السعودية، من الموقع: www.maysoon.ws/archives/420، بتاريخ 2014-2-1، س: 6:06 صباحاً.

يعتبر مصطلح أمن المعلومات " بأنه " مزيج من السرية ، وسلامة و توافر المعلومات، فوفقاً للمعيار الدولي لإدارة أمن المعلومات (ISO 27002) الصادر عن المنظمة الدولية للمعايير يعرف أمن المعلومات بأنه "مجموعة من التدابير الشاملة التي تضمن الحفاظ على توافر وسرية ونزاهة المعلومات، بالإضافة إلى خصائص أخرى مثل : الأصالة، والمساءلة، وعدم التنصل، والموثوقية،⁽¹⁾ وعرفه مجموعة من الباحثين بأنه "حماية المعلومات من مجموعة واسعة من المخاطر التي تتهددها، من أجل ضمان وتأكيد استمرارية الأعمال، وتقليل خسائر ومخاطر الأعمال ، وتعظيم العائد على الاستثمارات و رفع فرص النجاح والأرباح"،⁽²⁾ فأمن المعلومات يعبر عن التدابير التقنية والتدابير الإدارية التي تستخدم لحماية أصول المعلومات ضد الاستحواذ غير المصرح به، أو الضرر، أو الكشف، أو التلاعب، أو تغيير أو فقدان أو إساءة استخدام المعلومات.⁽³⁾

ويمكن تعريف أمن المعلومات من عدة زوايا علمية وعملية وقانونية، فمن الزاوية العلمية أو الأكاديمية يعرف أمن المعلومات بأنه العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها،⁽⁴⁾ وأما من الزاوية العملية أو التطبيقية أو التقنية أو الفنية فأمن المعلومات هو مجموعة الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من المخاطر والتهديدات المتأتية سواء من داخل بيئة المعلومات محل الحماية أو من خارجها⁽⁵⁾، أما من الزاوية القانونية أو التشريعية فإن أمن المعلومات هو محل دراسات وتدابير قانونية وتشريعية لحماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب جرائم الاعتداء على المعلومات ومعاينة مرتكبي الاعتداء وذلك بهدف توفير الردع.⁽⁶⁾

وفي رأي الباحث يُعدّ التعريف السابق تعريفاً شاملاً لمصطلح "أمن المعلومات" ومن شتى النواحي العلمية والعملية والقانونية.

لكن مصطلح "أمن نظم المعلومات" جاء أوسع من مصطلح "أمن المعلومات" وذلك لأنه يتناول جميع الأمور الأمنية المتعلقة بحماية عناصر ومكونات النظم المستخدمة في التعامل مع المعلومات، وبما فيها حماية المعلومات التي تمت معالجتها بواسطة تلك النظم، حيث تم تعريف أمن نظم المعلومات بأنها مجموعة العمليات والإجراءات والأدوات التي تتخذها المنشآت لتأمين وحماية معلوماتها وأنظمتها من الوصول غير المصرح به

(1) ISO/IEC 27002, (2005), **Information Technology – Security Techniques - Code of Practice for Information Security Management International**, International Standards Organization and International Electro technical Commission (ISO/IEC), Geneva, Switzerland.

(2) Maram, Venkata et al., (2012), "A Study of Risk Management of an Information System by Assessing Threat, Vulnerability and Countermeasure", **International Journal of Advanced Research in Computer Science and Software Engineering**, Vol. 2, No. 12, December 2012, PP: 51-53,

http://www.ijarcsse.com/docs/papers/12_December2012/Volume_2_issue_12_December2012/V2I12-0122.pdf

(3) Kazemi, Mehdi et al., (2012), "Evaluation of Information Security Management System Success Factors: Case Study of Municipal Organization", **African Journal of Business Management**, Vol. 6, No. 14, April 2012, PP: 4982-4989, Available online at <http://www.academicjournals.org/AJBM>

(4) O'Brien. J. A., (2010), "**Management Information systems: Managing Information Technology in the E-Business Enterprise**", OP. Cit., P. 448.

(5) السانكي، سعد & العواد، حنان، (2012)، "مخاطر استخدام تكنولوجيا المعلومات وأثرها على أداء نظم المعلومات المحاسبية – دراسة تطبيقية لعينة من الشركات المساهمة المدرجة في بورصة عمان للأوراق المالية"، **دراسات المعلومات**، العدد (14)، جامعة الإمام محمد بن سعود، الرياض، السعودية، أيار (مايو) 2012، ص ص: 207-257.

(6) الخطيب، محمد، (2012)، **أمن المعلومات**، الاجتماع الثاني لرؤساء الإدارات المختصة بتقنية المعلومات بالنيابات العامة العربية، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، بيروت، لبنان، 5-7 أيار مايو 2012.

سواء من داخل المنشأة أو من خارجها،⁽¹⁾ وهناك من يرى أن أمن نظم المعلومات يشير إلى كل ما اتخذ من خطوات لحماية المعلومات ونظم المعلومات من الدخول غير المصرح به أو الاستخدام أو الإفصاح أو الخلل أو التغيير، أو الدمار.⁽²⁾

ويمكن تعريف أمن نظم المعلومات بأنه حماية جميع أنواع المعلومات ومصادر الأدوات التي تتعامل معها وتعالجها من منشأة وغرفة تشغيل الأجهزة والأجهزة ووسائط التخزين والأفراد من السرقة والتزوير والتلف والضياع والاختراق وذلك بإتباع إجراءات وقائية وضوابط واضحة،⁽³⁾ وهناك من يرى بأن أمن نظم المعلومات يتمثل في أخذ التدابير الوقائية للإبقاء على كافة مكونات نظم المعلومات المادية والبرمجية وغيرها محمية من الدخول أو الاستخدام غير المصرح،⁽⁴⁾ بينما توسع آخرون وذكروا بأن أمن نظم المعلومات هو مجموعة من العمليات والإجراءات، والموظفين، والتكنولوجيا تستخدم لحماية أصول المعلومات في المنشأة،⁽⁵⁾ وبالتالي فإن أمن نظم المعلومات المحاسبية هو حماية كافة الموارد المستخدمة في معالجة المعلومات المحاسبية، حيث يتم تأمين المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسبات المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات المنشأة ويتم ذلك عن طريق إتباع إجراءات ووسائل الحماية.

ويرى الباحث أنه بالرغم من تنوع التعريفات لأمن نظم المعلومات، إلا أنها جميعاً تدور حول حماية عناصر نظام المعلومات المحوسب، من أي اعتداء أو تهديد يخل بسلامتها وتوافرها وسرية معلوماتها، من خلال الالتزام بإجراءات الحماية ووسائلها المختلفة، وبالتالي فإن أمن نظم المعلومات المحاسبية المحوسبة هو العلم الذي يهتم بدراسة النظريات (الأفكار)، والاستراتيجيات والمعايير والمقاييس والقواعد والقوانين والسياسات التي تهتم بتوفير الحماية لأمن نظم المعلومات من المخاطر التي قد تواجهها ومن ثم العمل على تطبيق الأساليب والوسائل والإجراءات التي يجب تطبيقها من قبل إدارة المنشأة بمختلف مستوياتها وفق الصلاحيات المتعارف عليها، وذلك لمواجهة التهديدات والمخاطر الداخلية والخارجية التي يمكن أن تحدث والتغلب عليها ومنع حدوثها مستقبلاً، ومعاينة مرتكبيها، وكل ذلك بهدف ضمان حماية تلك النظم بكافة مكوناتها، والتأكد من توافر وسلامة وسرية المعلومات الناتجة عنها بمختلف أشكالها، وتحديد مسؤولية المتصرف بها ولما من شأنه زيادة الثقة في تلك النظم.

وبذلك فإنه يوجد فرقاً جوهرياً بين أمن المعلومات المحاسبية وأمن نظم المعلومات المحاسبية حيث يركز المفهوم الأول على تعريف الأمن من منظور حماية المعلومات دون ذكر لنظام المعلومات بما يشمل من تقنيات واستراتيجيات لإدارة تلك النظم، وهنا قد يتساءل البعض ما بال الباحث في عنوان هذه الأطروحة قد اختار "أمن

(1) Kritzing, E & Smith, E., (2008), "Information security management: An information security retrieval and awareness model for industry", *Computer & Security*, Vol.27, No.5-6,2008, PP.:224 – 231.P225

(2) Wallace, Linda et al., (Spring 2011), Information Security and Sarbanes-Oxley Compliance :An Exploratory Study, *Journal of Information System*, Vol. 25, No. 1, American Accounting Association, USA, PP: 185–211.

(3) الحميد، محمد دباس & ونيو، ماركو إبراهيم، (2007)، "حماية أنظمة المعلومات"، مرجع سابق، ص34.

(4) Jessup, Leonard and Valanch, Joseph, (2008), "Information Systems Today- Managing the Digital World", Pearson Prentice Hall, Inc, New Jersey, USA, P. 232.

(5) Shamala, Palaniappan & Ahmad, Rabiah & Yusoff, Mariana, (2013), "A conceptual Framework of Info Structure for Information Security Risk Assessment (ISRA)", *OP. Cit.*, PP: 45-52.

نظم المعلومات المحاسبية" ولم يختَر "أمن المعلومات المحاسبية"؟، الإجابة هنا تكمن في أن الباحث رأى بعد بحثه الموسع، في مشكلة الدراسة أنها بحاجة إلى تفصيل في جوانبها المختلفة وبمنظور أوسع، بمعنى أننا أمام حالة تتجاوز الهدف من حماية المعلومات، لتشمل حماية الأوعية والموارد التي تحقق وتعزز هذه الحماية.

1-1-6: المبادئ والأهداف الأساسية لأمن نظم المعلومات المحاسبية المحوسبة:

يعد أمن نظم المعلومات المحاسبية حجر الأساس للمبادئ التي تشكل المرتكزات الأساسية لملائمة وموثوقية نظم المعلومات المحاسبية،⁽¹⁾ وقد تضمن الإطار العام لخدمات الثقة (Sys Trust) والذي أُعدّ من قبل معهدي المحاسبين الأمريكي والكندي (CICA & AICPA) خمسة مبادئ وأهداف أساسية لتحقيق أمن وموثوقية نظام المعلومات لمواجهة مختلف المخاطر الأمنية في ظل استخدام تكنولوجيا المعلومات.⁽²⁾

إن تلك المبادئ الخمسة تتمثل في (السرية، تكاملية وسلامة التجهيز، والتوفر والإتاحة، والخصوصية، وإثبات عدم الإنكار التصرف) تعتبر هي الأهداف الجوهرية والغاية التي تسعى إليها معظم أبحاث واستراتيجيات ووسائل أمن نظم المعلومات المحاسبية المحوسبة سواء من الناحية العلمية أو التقنية أو التدابير الرقابية والتشريعية، وبالتالي فإن الغرض من أمن نظم المعلومات المحاسبية المحوسبة هو ضمان توفير تلك المبادئ، وذلك جوهر العمل الرقابي والأمني للنظام، وبالتالي لا بد من وجودها في نظم المعلومات المحاسبية، والسعي إلى تطبيقها من قبل المنشآت الكبيرة على وجه الخصوص، وربط عمل النظم بتلك المبادئ حتى تكون جديرة بالثقة.

وعليه فإن هناك ثلاثة مبادئ وأهداف رئيسية تُستخدم على نطاق واسع في مجال الدراسات الأمنية لنظم المعلومات المحاسبية المحوسبة لبيان مدى توفر الحماية الكافية والمطلوبة لتلك النظم من المخاطر التي تتهددها، وتلك المبادئ والأهداف هي سرية النظام (Confidentiality)، وسلامة وتكامل التجهيز (Integrity)، وإتاحة وتوفر النظام (Availability)، وهي معروفة باسم الثلاث (CIA Triangle)⁽³⁾، وذلك لا يشير إلى وكالة الاستخبارات الأمريكية، إنما يشير إلى أهداف أمن نظم المعلومات التي لا بد من السعي إلى تطبيقها بشكل جيد، لأن الفشل في حماية المعلومات وسلامة التعاملات وانتهاك السرية، يبدأ بانتهاك أي من هذه المبادئ الثلاثة، وهي على نفس الدرجة من الأهمية حيث يتم استعمالها من قبل معايير آيزو (ISO - 27001) كدليل خلال تطبيق نظم إدارة حماية وتطوير أمن نظم المعلومات المحاسبية⁽⁴⁾، وقد وصفت بأحجار الزاوية لأمن نظم المعلومات كما في الشكل الآتي:

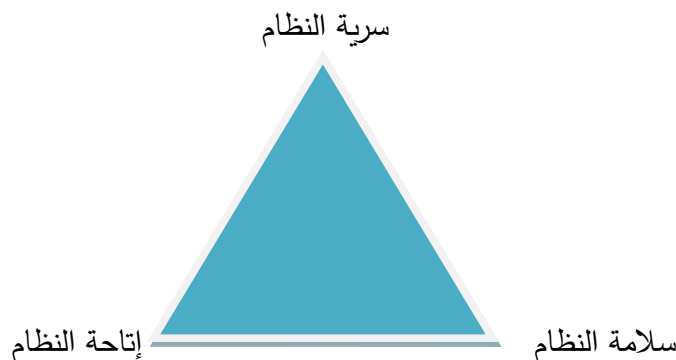
(1) مشتهى، صبري & وحمدان، علاء و شكر، طلال، "مدى موثوقية نظم المعلومات المحاسبية وأثرها في تحسين مؤشرات الأداء المصرفي - دراسة مقارنة على المصارف الأردنية والفلسطينية المدرجة ببورصتي عمان ونابلس"، دراسات - العلوم الإدارية، المجلد 38، العدد1، الجامعة الأردنية، عمان، الأردن، 2011، ص: 46-21.

(2) حجر، عبد الملك إسماعيل، "نظم المعلومات المحاسبية"، مرجع سابق، ص 394.

(3) Shamala, Palaniappan & Ahmad, Rabiah & Yusoff, Mariana, (2013), "A conceptual Framework of Info Structure for Information Security Risk Assessment (ISRA)", OP. Cit., PP: 45-52.

(4) Von Solms, Rossouw & Niekerk, Johan van, (2013), "From information security to cyber security", Computers & Security, No. 38, Elsevier Ltd. All rights reserved, PP: 97-102.

الشكل (3-1-1) المبادئ والأهداف الثلاثة الهامة لأمن نظم المعلومات (1)



ويتم تناول تلك المبادئ والأهداف على النحو التالي:

1. السرية (Confidentiality): هي خاصية عدم إتاحة المعلومات للأفراد أو الكشف عنها لغير المصرح لهم

بذلك من الأشخاص أو الكيانات أو العمليات،⁽²⁾ وتعني أن النظام يجب أن يكون محمياً ومؤمناً ضد أي دخول مادي أو منطقي غير مصرح به، من خلال منع الاطلاع أو الاستخدام السيئ وتبديل أو تدمير المعلومات والبرمجيات أو سرقة مواد النظام،⁽³⁾ ويشمل كل التدابير اللازمة لمنع إطلاع غير المصرح لهم على المعلومات الحساسة أو السرية، أو استخدامها سواء كان ذلك أثناء عملية جمعها، أو معالجتها، أو تخزينها أو نقلها عبر الشبكات وهو ما يتبادر إلى ذهن السامع عند الحديث عن أمن المعلومات،⁽⁴⁾ وذلك يعني أن المعلومات لا يمكن الكشف عنها لغير الكيانات أو الأفراد المعنيين بها، مع الأخذ في الاعتبار أن درجة هذه السرية ونوع المعلومات يختلف من مكان لآخر وفق السياسة المتبعة في المنشأة،⁽⁵⁾ حيث تصنف المعلومات إلى معلومات متاحة يمكن الوصول إليها لكل الأطراف المتعاملة، وسرية، وسرية للغاية لا يمكن الوصول إليها لغير المخولين.⁽⁶⁾

2. سلامة وتكامل التجهيز (Integrity): وتعني أن تكون معالجة النظام مكتملة ولأحداث حقيقية وقعت فعلاً

وغير وهمية⁽⁷⁾، أي أن النظام قد تم تشغيله بشكل متكامل وتام ودقيق وفي الوقت الملائم وفي ضوء السلطة المصرح بها، ويتضمن مبدأ السلامة خاصية الاعتمادية (Reliability)، من خلال التأكد من أن محتوى المعلومات لم يتم تعديله أو تدميره أو العبث به في أي مرحلة من مراحل عمل النظام (مبدأ الصحة)، سواء من

(1) الشكل من إعداد الباحث.

(2) ISO/IEC 27000, (2012), "Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary", ISO /IEC, Available at: <http://www.27000.org> (Accessed July 14, 2013).

(3) Romney, Marshall B. & Steinbart, Paul J., (2015), "Accounting Information Systems", OP. Cit., P. 225.

(4) الغثير، خالد سليمان، & القحطاني، محمد عبدالله، أمن المعلومات بلغة مبسطة، ط1، مركز التميز لأمن المعلومات، جامعة الملك سعود، الرياض، السعودية، 2009، ص23.

(5) حسنين، رجب عبد الحميد، (2012)، "أمن شبكات المعلومات الإلكترونية: المخاطر والحلول"، *Cybrarians Journal*، ع 30 (ديسمبر 2012)، تاريخ الاطلاع 30 - 7 2013 م، متاح في: http://www.journal.cybrarians.org/index.php?option=com_content&view=article&id=629:networks&catid=257:studies

(6) Al-Awadi, Maryam, (2009), "A Study of Employees' Attitudes Towards Organizational Information Security Policies in the UK and Oman", *PhD thesis*, Glasgow University, Glasgow, UK, PP: 11-13.

(7) الحكيم، سليم، (2010)، "إمكانية الرقابة على نظم المعلومات المحاسبية المؤتمتة للمؤسسات العامة ذات الطابع الاقتصادي من قبل مفتشي الجهاز المركزي للرقابة المالية"، *مجلة جامعة دمشق للعلوم الاقتصادية والقانونية*، مجلد (26)، العدد(1)، جامعة دمشق، دمشق، سوريا، 2010م، ص ص: 563 - 592، ص573.

مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع، فوجود أي ثغرة رقابية سيؤدي إلى عدم دقة وصحة المعلومات، وذلك سيؤثر سلباً على قرارات المنشأة، وبالتالي فمستقبلها مرهون بأمن النظام،⁽¹⁾ ويطلق أحياناً على هذا المبدأ بمبدأ النزاهة لأنه يرتبط بالمحافظة على البيانات والمعلومات دون أي تعديل أو تحريف غير مشروع، وهذا ما يؤدي إلى صحة وسلامة ونزاهة عمليات النظام وما ينتج عنها،⁽²⁾ فالنزاهة تعني أنه ينبغي أن يظل محتوى النظام من البيانات والمعلومات - في جميع مراحل عمل النظام- بشكله الأصلي دون تغيير أو تعديل أو اعتراض أو حذف من قبل أشخاص غير مخولين بذلك،⁽³⁾ ويتضمن هذا المبدأ عدم تعديل أو تحديث وتطوير النظام دون موافقة المخولين بذلك وفق الضوابط المقررة والمعمول بها.⁽⁴⁾

3. **إتاحة وتوفر النظام (Availability):** وتعني التأكد من أن نظم المعلومات متاحة للاستخدام في الوقت المناسب للأفراد المرخص لهم، لضمان استمرار المنشأة في ممارسة نشاطها كلما دعت الحاجة⁽⁵⁾، وضمان استمرار تلك النظم في العمل دون توقف أو تقطع، أو أي عمليات تمنع المستخدمين المخولين باستخدامها أو الدخول إليها عند الاقتضاء وكل ذلك ضمن منظومة الوقت المناسب لتنفيذ متطلبات عمل المنشأة (مبدأ الوجود)، ونعني باستمرارية النظم التأكد من استمرار عمل نظم المعلومات بكل مكوناتها من حاسبات وبرمجيات وأجهزة اتصال أو غيرها، وقدرتها على تقديم الخدمات المطلوبة منها لمستخدميها عند الطلب، ويعد عدم استمرارية الخدمة من أسوأ ما يحدث لمستخدمي نظم المعلومات،⁽⁶⁾ ولعله من المنطقي أن نعرف أن غالبية إجراءات وصناعة أمن نظم المعلومات في الأساس تهدف إلى هدف واحد وهو إيصال المعلومات والبيانات إلى الأشخاص المناسبين في الوقت المناسب، وبالتالي فإن الحفاظ على سرية المعلومات وضمان سلامتها وعدم التغيير فيها لا يعني شيئاً إذا لم يستطع الأشخاص المخولين أو المصرح لهم الوصول إليها،⁽⁷⁾ ومبدأ التوافر مصطلح واسع لما تنطوي عليه من جوانب كثيرة ويرتبط ذلك بمبدأ قابلية التطوير فالنظام من الممكن تحديثه عند الحاجة ليكون مرناً وسهل الاستعمال وبالشكل الذي يسمح بتوفير مبادئ الحماية والسرية والدقة.

وفي الوقت الحاضر، تشكل نظم المعلومات جزءاً أساسياً من المنشآت، ضمان أمن المعلومات ينطوي على تنفيذ خمسة أهداف هي: السرية، والسلامة، والتوفر إلى جانب مراعاة الخصوصية، وعدم الاتصال.⁽⁸⁾

(1) Lendle, Klaus, (2008), "Performance Management in Internal Audit: Implementation, Merits and Challenges in A Medium-Sized Audit Department", *Journal of Securities Law, Regulation & Compliance*, Nov, Vol. 2 Issue 1, 2008, PP: 62-67.

(2) Rafique, Rajia & Mehmood, Furhan (2010), "Management of Operational Risks Related to Information Security in Financial Organizations", *Master Thesis in IT Management*, School of Sustainable Development of Society and Technology (HST), P.6.

(3) Zimucha, Tafadzwa et. al, (2012), "An Evaluation of the Effectiveness of E-banking Security Strategies in Zimbabwe: A Case Study of Zimbabwean Commercial Banks", *Journal of Internet Banking and Commerce*, Vol. 17, No.3, December 2012, PP: 1-16.

(4) Vacca, John R., (2009), *Computer and Information Security Handbook*, 3rd Edition, Morgan Kaufmann Publishers is An Imprint of Elsevier, USA, P.256, <http://www.elsevierdirect.com>

(5) National Institute of Standards and Technology: NIST, (March 2011), "*Managing Information Security Risk-Organization, Mission, and Information System View*", Special Publication (SP) 800-39, 2011, Available at <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>

(6) Eloff, J. H. P. & Eloff M. M., (2005), "Information Security Architecture", *Computer Fraud & Security*, Vol. 22, No.4, November 2005, PP: 308-313.

(7) حسنين، رجب عبد الحميد، "أمن شبكات المعلومات الإلكترونية: المخاطر والحلول"، *Cybrarians Journal*، ع 30 (ديسمبر 2012). تاريخ الاطلاع 30 - 7 - 2013 م، متاح في:

http://www.journal.cybrarians.org/index.php?option=com_content&view=article&id=629:networks&catid=257:studies

(8) Mihalache, Arsenie, (2011), "Security of the Accounting Information System Infrastructure", *Annals of the "Ovidius" University, Economic Sciences Series*, Volume XI, No.1, PP: 1339-1345, <http://ideas.repec.org/a/ovi/oviste/v11y2011p1339-1345.html>

4. **مراعاة الخصوصية (Privacy):** وتتمثل بحسن الاستخدام والإفصاح عن المعلومات الشخصية التي يتم جمعها عن العملاء، بحيث تكون بعيدة عن الوصول غير المخول به، فمثلاً يتم استخدام التشفير لتوفير مستوى عالي من الأمن للمعلومات مع مرونة في تداول تلك البيانات،⁽¹⁾ فالمعلومات الشخصية التي تم الحصول عليها نتيجة التعاملات الالكترونية يجب أن يتم تجميعها واستخدامها والإفصاح عنها والإبقاء عليها كما تم التعهد به والاتفاق عليه،⁽²⁾ والجدير بالذكر هنا أن مصطلحات الأمن والسرية والخصوصية كثيراً ما يجري الخلط بينها، فالخصوصية تركز على فرض قواعد السرية على استخدام البيانات الشخصية التي يتم حمايتها من خلال اتخاذ إجراءات الأمانة، والسرية يتم تطبيقها على البيانات بشكل عام حسب متطلبات المنشأة ووفق السياسة المتبعة، وكلا المبدأين السرية والخصوصية تقعان تحت مبدأ الأمن، الذي هو مفهوم واسع يشمل أيضاً مبدأ السلامة والإتاحة وكذلك إثبات عدم إنكار التصرفات، وهنا تجدر الإشارة إلى أمر بالغ الأهمية وهو أن على المستخدم اتباع إجراءات الأمانة بشكل عام، وإجراءات السرية بشكل خاص لضمان المحافظة على خصوصية المعلومات الخاصة بعملاء المنشأة، خلال مراحل جمع المعلومات وتصنيفها وتخزينها، من خلال تحديد المسؤولين عن توفير هذه الخصوصية، مع التوثيق الدقيق لذلك، ووضع الإجراءات التي من شأنها تلبية النظام لحاجات العملاء المتجددة.⁽³⁾

5. **عدم إنكار التصرف أو عدم التنصل (Non-Repudiation):** ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بنظام المعلومات إنكار أنه هو الذي قام بهذا التصرف بحيث تتوفر قدرة إثبات أن تصرفاً ما قد تم من شخص ما في وقت معين⁽⁴⁾، وذلك أمر هام مع استخدام شبكات تبادل البيانات المحوسبة (EDI)، فلا يمكن للمرسل أو المستقبل تكذيب رسالة محددة أثناء مزاولة العمليات التجارية، فمثلاً يكون لمنشأة معينة ولتكن بنك باثبات أن مستخدماً معيناً قد أجرى معاملات معينة في حالة نفي ذلك المستخدم إجراءات تلك المعاملات،⁽⁵⁾ ويرتبط هذا المفهوم بمفهوم المحاسبة والملاحقة والتدقيق، حيث تستوجب بعض الحالات التأكد من حدوث مداولة أو حدث معين عبر الشبكة الإلكترونية، فتحديد المسؤولية يفترض مسبقاً وجود آليات تسمح بالتعرف على هوية الأفراد وعلى أعمالهم، وتتيح تسجيل مجريات الأحداث بطرق سليمة،⁽⁶⁾ وإن أي طرف من طرفي المعاملة المعاملة المالية الالكترونية يريد أن يضمن أن الطرف الآخر أو أي طرف ثالث لن ينكر تنفيذه وإجرائه للعملية، ولذلك لا بد من معرفة هوية الأطراف المتعاملة ومن أكثر التقنيات الأمنية شيوعاً المفتاح العام للتشفير، وكذلك التوقيعات الرقمية (Digital Signatures)، والشهادات الرقمية (Digital Certificates).⁽⁷⁾

(1) Ashenden, Debi, (2008), "Information Security management: A human challenge?", *Information Security Technical Report*, Vol.13, No.4, PP: 195 – 201, P.197.

(2) حجر، عبد الملك إسماعيل، (2009)، "نظم المعلومات المحاسبية"، مرجع سابق، ص 307.

(3) مشتهى، صبري & وحمدان، علاء & شكر، طلال، (2011)، "مدى موثوقية نظم المعلومات المحاسبية وأثرها في تحسين مؤشرات الأداء المصرفي - دراسة مقارنة على المصارف الأردنية والفلسطينية المدرجة ببورصة عمان ونابلس"، مرجع سابق، ص: 21-46.

(4) الخطيب، محمد، (2012)، *أمن المعلومات*، مرجع سابق.

(5) Lin, Fengyi & Sheng, Olivia R.L. & Wu, Soushan, (2005), "An integrated Frame-work For E-Chain Bank Accounting Systems", *Industrial Management & Data Systems*, Vol. 105, No. 3, Emerald Group Publishing Limited, PP:291-306

(6) الأمم المتحدة، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الاسكوا)، ESCWA، (2009)، "بناء الثقة بالخدمات الالكترونية في منطقة الإسكوا"، 10 آذار (مارس)، ص: 74.

(7) Darragh, Warren J., (2009), "An Analysis of Information Security in Selected Australian Organizations", *Master of Information Technology (Research)*, University of Southern Queensland, Australia, P. 10.

ونخلص من ذلك إلى أن نظم المعلومات المحاسبية المحوسبة يجب أن تحتوي معلومات دقيقة وتمثل الواقع وتحظى بحماية وتوفر وسرية تجعلها محمية من الكشف والتغيير والسرقة وتكون دائماً متوفرة لذوي الصلاحية عند حاجتهم لها، وتلك الغايات المرجو تحقيقها، إنما هي الصفات التي يجب توافرها في المعلومات كصفات تؤهلها لتصبح ذات قيمة، ولكي تكون المنشأة آمنة فلا بد لها من تحقيق تلك الأهداف الجوهرية لأمن نظم المعلومات، وذلك لن يتم في ظل نظم المعلومات المحاسبية المحوسبة إلا بإعادة تصميم الإجراءات والضوابط الرقابية لتلك النظم، لكي تكون آمنة وفعالة، مع الأخذ في الاعتبار أن تحقيق مبادئ وأهداف أمن نظم المعلومات كلها أو بعضها يعتمد على طبيعة المعلومات محل الحماية واستخدامها وعلى الخدمات المتصلة بها، فليس كل المعلومات داخل نظام المعلومات تتطلب السرية ولكن هناك مستويات لأمن المعلومات تبعاً لكل حالة على حدة، فمن المعلومات ما يتطلب حماية بقدر متوسط ومنها ما يتطلب حماية قصوى، فمستوى الأمن المطلوب لتحقيق هذه المبادئ يختلف في المنشأة، وذلك لأن لكل منها تركيبة فريدة من نوعها للأهداف ومتطلبات العمل والأمن، ويتم قياس جميع المخاطر والتهديدات، ونقاط الضعف لقدرتها المحتملة لتقديم تنازلات عن واحدة أو أكثر من تلك المبادئ، كما يتم تنفيذ جميع الضوابط الأمنية، والآليات، والضمانات لتقديم واحدة أو أكثر من هذه المبادئ.⁽¹⁾

ويخلص الباحث إلى أن أمن نظم المعلومات المحاسبية المحوسبة من القضايا الحيوية والهامة في الوقت الحاضر، وأصبح من متطلبات الرقابة على تلك النظم وذلك لضمان سلامة وصحة عمل النظام بشكل عام، للمحافظة على البيانات والمعلومات ودقتها وسلامتها بشكل خاص، حيث يؤدي غياب أو نقص الأمن لنظم المعلومات المحاسبية إلى فقدان الثقة في النظم وبالتالي توقفها أو عدم الاستفادة القصوى منها مما يجعلها عبئاً على المنشأة، ومن هنا تظهر مهمة جديدة ومسؤولية كبيرة أمام إدارة نظم المعلومات المحاسبية في المنشأة، وهي ضرورة توفير الوسائل والأساليب اللازمة لضمان استمرارية عمل هذه النظم بشكل صحيح، والتخطيط الدقيق لمواجهة جميع المخاطر التي يمكن أن تؤدي إلى تعطيلها أو توقفها عن العمل .

1-1-7: مكونات أمن نظم المعلومات المحاسبية المحوسبة:

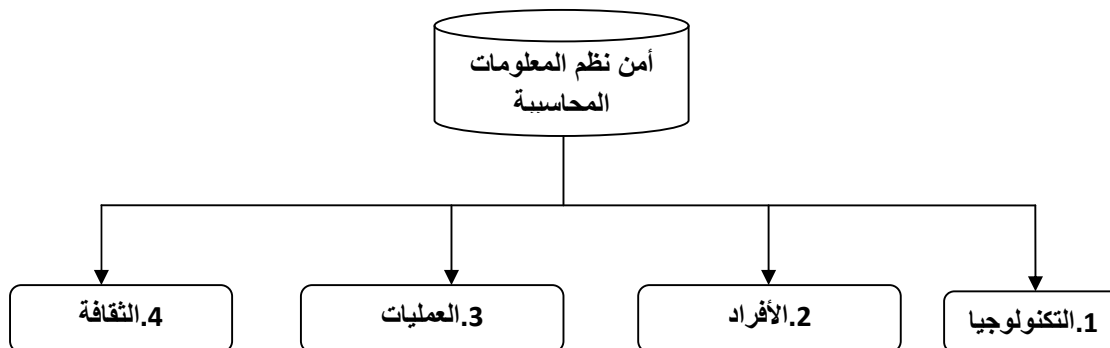
إن إدارة أمن نظم المعلومات المحاسبية تعتمد على التكنولوجيا والناس والعمليات، وينبغي أن ننظر إلى المهارات التي يجب توافرها في العنصر البشري وتغيير الثقافة وبناء الاتصال الفعال بين جميع أعضاء المنشأة فيما يتعلق بأمن نظم المعلومات،⁽²⁾ وبالتالي فإن بيئة أمن نظم المعلومات المحاسبية المحوسبة تتكون من أربع مكونات أساسية وهي التكنولوجيا والأفراد، والعمليات، والثقافة، حيث يمثل تنفيذ وتشغيل نظم أمن المعلومات

(1)Wikipedia,(2014),http://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Information_Security_and_Risk_Management, Accessed 26/02/2014, in 08:33 GMT.

(2) Parakkattu, Sindhuja & Kunnathur, Anand. S.,(2010), "A Framework for Research in Information Security Management", **OP. Cit.**, PP: 318-323.

طريقة حياة تعتمد علي تكامل تلك المكونات فكل منها مهم ولا يُمكن التعامل مع أي منها بصفة فردية مستقلة، ولا يتحقق أمن نظم المعلومات دون توفير الحماية المتكاملة لتلك المكونات عبر معايير أمنية تكفل توفير هذه الحماية، ومن خلال مستويات أمن متعددة ومختلفة من حيث الطبيعة،⁽¹⁾ ويحدد الشكل التالي مكونات أمن نظم المعلومات المحاسبية المحوسبة:

شكل رقم (4-1-1) مكونات أمن نظم المعلومات المحاسبية المحوسبة⁽²⁾



وفيما يلي توضيح موجز لتلك المكونات:

1. **التكنولوجيا (Technology):** وهي الأجهزة والبرامج المتوفرة في المنشأة، وتشكل جزءاً أساسياً من البنية التحتية للمنشأة وعنصر حاسم في إنجاز مهمتها، وتتكون من جميع الأدوات والتطبيقات والبنية التحتية التي تجعل عمليات الأمن أكثر كفاءة، وبالنظر إلى نموذجية اعتماد المنشأة على التكنولوجيا فهي من العناصر المتطورة وتواجه تغييرات متكررة، ولها مخاطر الديناميكية الخاصة،⁽³⁾ حيث تعتبر سوق التكنولوجيا ذات طبيعة تنافسية، يتوافر لها عدد كبير من المنتجين والبائعين والموزعين، وذلك يجعل عملية تقييم التكنولوجيا أصعب مما كانت عليه في الماضي.
2. **الأفراد أو العناصر البشرية (People):** وهي العناصر العاملة المتخصصة داخل نظام المعلومات المحاسبية في بيئة الحاسب الالكتروني، وتعتبر العناصر البشرية أهم عناصر المنظومة، وهم الأشخاص الذين يطبقون أمن المعلومات وتقنياته أو مستخدمو الأنظمة ممثلين كمحلي ومصممي نظم المعلومات ومخططي البرامج ومشغلي الحاسب ومستخدمي النظم وهم ينجزوا كل العمليات والخدمات ويحتاج إلى تواجدهم بأعداد وتخصصات ملائمة وبمهارات وخبرات مناسبة، فلكي يتم بناء نظام معلومات محاسبي آمن وفقاً للأسس العلمية في ظل بيئة الحاسبات الالكترونية فإنه من الضروري أن يكون ضمن مجموعة العناصر البشرية المتخصصة خبراء في

(1) المري، عايض، (2011)، "أمن المعلومات ماهيتها وعناصرها واستراتيجياتها"، الدراسات والاستشارات القانونية، 6 تشرين الثاني (نوفمبر) 2011،

http://www.dralmarri.com/show.asp?field=res_a&id=205 في 3 تشرين الأول (أكتوبر) 2013، 5:18 صباحاً.

(2) Wood, C.C. & Banks, W.W., (2003), "Human error: an overlooked but significant information security problem", Computers & Security, Vol.12, No.1, 2003, PP: 51-60.

(3) Information Systems Audit and Control Association (ISACA), (2009), An Introduction to the Business Model for Information Security, Printed in the United States of America, USA, Available at: <http://www.isaca.org> Accessed on 8-12-2012.

مجال أمن المعلومات حتى يمكن تحقيق الكفاءة والفعالية في إنتاج نظام معلومات محاسبي يتفق مع الأسس المحاسبية المتعارف عليها، ولا بد من اكتسابهم المهارات والدافعية والتدريب.⁽¹⁾

3. **العمليات (Possesses):** ويقصد بالعمليات كل الإجراءات الواجب إتباعها لتحسين المعلومات وأنظمتها، بعمل الشيء الصحيح في الوقت الصحيح، تعتبر العمليات لا غني عنها لأي نظام أمن، فهي جوهرية وذات طبيعة مستمرة، ويحكم إدارة عمليات أمن المعلومات مجموعة من المعايير كتلك التي قررتها المنظمة الدولية للتوحيد القياسي (ISO) التي تعتبر ذات قيمة كبيرة لأي نظام أمن معلومات، وتطبق العمليات بطريقة منظمة يعمل على دعم القدرة لتعزيز الأمن وخفض المخاطر بطريقة منظمة، كما تراجع باستمرار في إطار الخبرة المتراكمة بغية استبعاد المخاطر المختلفة.⁽²⁾

4. **الثقافة (Culture):** وتركز على حاجات العمل والمستخدمين، كما ترتبط بتفسير بيئة الأعمال وتتعلق بأخلاقيات المنشأة تجاه المجتمع، حيث يكون لإدارة المنشأة دور رئيسي تؤديه في حفظ ثقافة المنشأة المتوافقة مع ثقافة مجتمعها، ولقد أشار المعهد القومي للمعايير والتكنولوجيا الأمريكي إلى أن حجم الخسائر المتعلقة بأمن المعلومات معظمها يرجع إلى عدم وجود ثقافة كافية لدى المنشآت، ومن أمثلة الثقافات الناجحة في إدارة أمن المعلومات التي يمكن تتبعها في مجالات الاستخبارات في الأمن والدفاع، والصرافة الإلكترونية والتبادل الخارجي والتأمين.

1-1-8: المحاور الأساسية لأمن نظم المعلومات المحاسبية المحوسبة وفقاً لمستويات الحماية:

أمن المعلومات وفقاً للمنظمة الدولية للتوحيد القياسي (ISO 17799) تشمل على سياسة الأمن وتنظيم الأمن وتصنيف الأصول ورقابتها وأمن الأفراد والأمن الطبيعي والبيئي والرقابة على الوصول وتطوير النظم وصيانتها وإدارة استمرارية الأعمال والتوافق.⁽³⁾

أمن نظم المعلومات لا يعني أمن المعلومات فقط ولكن يشتمل أيضاً على كامل البنية التحتية التي تسهل استخدامه، وهو يغطي التهديدات الأمنية المادية للأجهزة والبرامج، وأمن العناصر البشرية، حيث كل من هذه المكونات لديها خصائص خاصة، حيث تشمل إستراتيجية أمن نظم المعلومات عناصر مهمة يجب الاهتمام بها وهي المكونات المادية والبرمجيات والبيانات نفسها والطرق والعمليات وكذلك العنصر البشري ونلاحظ أن هذه العناصر تتراوح بين الفنية وغير الفنية والتقنية وغير التقنية.⁽⁴⁾

(1) المري، عايض، (2011)، "أمن المعلومات ماهيتها وعناصرها واستراتيجياتها"، **الدراسات والاستشارات القانونية**، 6 تشرين الثاني (نوفمبر) 2011، http://www.dralmarri.com/show.asp?field=res_a&id=205 في 3 تشرين الأول (أكتوبر) 2013، 5:18 صباحاً.

(2) الهادي، محمد، (2006)، "توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية"، **cybrarians journal**، العدد (9)، أكاديمية السادات للعلوم الإدارية، القاهرة، مصر، حزيران (يونيو) 2006، <http://www.journal.cybrarians.org>.

(3) ISO/IEC 27001:2005, (2013), **Information Technology - Security Techniques - Information Security Management Systems - Requirements**, 2nd Ed., International Standards Organization and International Electro technical Commission (ISO/IEC), Geneva, Switzerland.

(4) أبو شنب، عماد، (2009)، "إدارة وتحليل مخاطر أمن المعلومات"، **مؤتمر أمن المعلومات والحكومة الإلكترونية**، كوالالمبور، ماليزيا، 12 - 16 أبريل (نيسان) 2009.

ويمثل أمن نظم المعلومات أحد عناصر البنية الأساسية التي يجب توافرها في نظام المعلومات، من خلال وجود إطار سياسات أمن يختص بكل أوجه الأمن الطبيعي وأمن الأفراد وأمن المعلومات، بالإضافة إلى وجود أدوار ومسؤوليات واضحة للمستخدمين وأفراد الأمن وأعضاء لجنة إدارة نظم المعلومات.⁽¹⁾

ويشير التطور السريع والمذهل لتكنولوجيا المعلومات إلى ضرورة التعرف على أهم محاور أمن نظم المعلومات المحاسبية - والذي يتضمن أمن الأفراد والأمن المادي لمراكز تجهيز المعلومات، والأمن البرمجي وأمن وسائط التخزين وأمن تبادل البيانات عبر الشبكات.⁽²⁾

إن أمن وسلامة البيانات في نظم المعلومات المحاسبية المحوسبة التي تتميز بأنها معقدة البنية ومتعددة الطبقات يتطلب أن يؤخذ بعين الاعتبار مستوى كل طبقة من هذه الطبقات وكذلك مستوى قنوات الاتصال ما بين هذه الطبقات، وأيضاً مستوى كل من البرمجيات الأساسية والتطبيقية الخاصة بكل طبقة.⁽³⁾

وللوصول إلى نظام معلوماتي آمن يضمن سلامتها وسريتها وتوافرها بما فيها البيانات المتضمنة فيه فلا بد من تصنيف ومعالجة القضايا الأمنية المتعلقة بذلك النظام من خلال عدد من المحاور أهمها:⁽⁴⁾

1. **محور أمن الأفراد العاملين في نظام المعلومات:** وهي تتعلق بالموظفين العاملين على النظام التقني المعني من حيث توفير وسائل التعريف الخاصة بكل منهم وتحقيق التدريب والتأهيل للمتعاملين بوسائل الأمن إلى جانب الوعي بمسائل الأمن ومخاطر الاعتداء على المعلومات،⁽⁵⁾ والحفاظ على سلامة الأفراد أولى الأولويات في أي منشأة وتختلف أدوار هؤلاء الأشخاص: فمنهم مديرو الأنظمة، ومديرو الشبكات، والمشغلون والمديرون والمستخدمون والشركاء التجاريون، وهم بحاجة ماسة إلى التدريب ليتمكنوا من القيام بمسؤولياتهم تجاه هذه الأنظمة، فمحور الخطر الإنسان سواء المستخدم أو الشخص المناط به مهام تقنية معينة تتصل بالنظام، فإدراك هذا الشخص حدود صلاحياته، وإدراكه آليات التعامل مع الخطر وسلامة الرقابة على أنشطته في حدود احترام حقوقه القانونية تعد مسائل رئيسية يعنى بها نظام الأمن الشامل وتحديداً في بيئة العمل المرتكزة على نظام الحاسوب وقواعد البيانات، حيث يلعب الفرد دوراً أساسياً ومهماً في مجال أمن نظم المعلومات المحوسبة وله تأثير فعال في أداء عمل الحواسيب بجانبه الإيجابي و السلبي، فهو عامل مؤثر في حمايتها و لكن في الوقت نفسه فإنه عامل سلبي في مجال تخريب الأجهزة و سرقة المعلومات سواء لمصالح ذاتية أو لمصالح الغير.

إن من متطلبات أمن الحواسيب تحديد مواصفات محددة للعاملين ووضع تعليمات واضحة لاختيارهم ووضع الخطط لزيادة الحس الأمني والحصانة من التخريب، كما يتطلب الأمر المراجعة الدورية للتدقيق في شخصية وسلوك الأفراد العاملين من وقت لآخر وربما يتم تغيير مواقع عملهم ومحاولة عدم احتكار المهام على موظفين محددين.⁽⁶⁾

ويجب أن يؤخذ في الاعتبار القيم والسلوكيات الإنسانية داخل المنشأة وخارجها، فمن الناحية الداخلية من المهم بمكان بالنسبة لمدير أمن المعلومات العمل مع الموارد البشرية والإدارات القانونية لمعالجة قضايا مثل:

(1) الهادي، محمد، (2006)، " توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية"، مرجع سابق، <http://www.journal.cybrarians.org>

(2) الحميد، محمد دباس & ونينو، ماركو إبراهيم، (2007)، " حماية أنظمة المعلومات"، مرجع سابق، ص55.

(3) الخطيب، محمد، (2012)، أمن المعلومات، مرجع سابق.

(4) الخطيب، محمد، (2012)، المرجع السابق ذاته.

(5) النجار، فايز جمعه، (2010)، "نظم المعلومات الإدارية: منظور إداري"، الطبعة الثالثة، دار الحامد للنشر والتوزيع، عثان، الأردن، 2010، ص271.

(6) الحاج علي، عوض & وحسين، عبد الأمير، (2005)، أمنية نظم المعلومات وتقنيات التشفير، ط (2)، مطبعة جامعة النيلين، الخرطوم، السودان، ص 138.

إستراتيجيات التوظيف (التحريات، والمقابلات، والأدوار والمسؤوليات)، وكذلك قضايا العمالة (الحصول على الأدوات والبيانات والتدريب والوعي داخل المنشأة)، وإنهاء الخدمة (أسباب مغادرة، توقيت الخروج، والأدوار والمسؤوليات، والوصول إلى النظام، والوصول إلى الموظفين الآخرين)، أما خارجياً فيمكن للعملاء والموردين ووسائل الإعلام وأصحاب المصلحة وبعض القوى الأخرى التأثير على المنشأة وتحتاج إلى النظر فيها ضمن الوضع الأمني.⁽¹⁾

2. **محور الأمن المادي والبيئي للنظام:** وتشمل كافة الوسائل التي تمنع الوصول إلى الكيان المادي لنظم المعلومات من مباني وأجهزة وملحقاتها وقواعدها، كالأقفال والحواجز والغرف المحصنة وغيرها من وسائل الحماية المادية التي تمنع الوصول إلى الأجهزة الحساسة،⁽²⁾ فيجب أن يمنع الأشخاص غير المصرح لهم من الوصول إلى أجهزة النظام المختلفة، كالخدمات المركزية وأجهزة التخزين، ومنعهم من دخول المرافق والمباني المهمة، حيث يجب أن تعطى أهمية للمواقع والأبنية التي يحوي أجهزة الحواسيب وملحقاتها، وحسب طبيعة المنظومات والتطبيقات المستخدمة يتم اتخاذ الإجراءات الاحترازية لحماية الموقع وتحصينه من أي تخريب أو سطو وحمايته من الحريق أو تسرب المياه والفيضانات، ومحاولة إدامة مصدر القدرة الكهربائية وانتظامها وتحديد أساليب وإجراءات التفتيش والتحقق من هوية الأفراد الداخلين والخارجين من الموقع وعمل سجل لذلك.

3. **محور أمن الوصول البرمجي لقاعدة البيانات المتصلة:** ويراد به حماية المعلومات داخل النظام بكافة أنواعها وأنماطها كحماية نظم التشغيل، وحماية برامج التطبيقات، وحماية برامج إدارة البيانات، وحماية قواعد البيانات بأنواعها المختلفة،⁽³⁾ وتعتبر البرمجيات من المكونات غير المادية وعنصر أساسي في نجاح استخدام النظام، لذلك من الأفضل اختيار حواسيب ذات أنظمة تشغيل لها خصائص أمنية ويمكن أن تحقق حماية للبرامج وطرق حفظ كلمات السر وطريقة إدارة نظام التشغيل وأنظمة الاتصالات، إن أمن البرمجيات يتطلب أن يؤخذ هذا الأمر بعين الاعتبار عند تصميم النظام وكتابة برامجه من خلال وضع عدد من الإجراءات كالمفاتيح والعوائق التي تضمن عدم تمكن المستفيد من التصرف خارج الحدود المخول بها وتمنع أي شخص من إمكانية التلاعب والدخول إلى النظام وذلك من خلال أيضا تحديد الصلاحيات في مجال قراءة الملفات أو الكتابة فيها، ومحاولة التمييز بين اللذين يحق لهم الاطلاع وحسب كلمات السر الموضوعية.

4. **محور أمن تخزين البيانات في وسائط غير متصلة:** وهي تلك الوسائط التي تمكن المستخدم من التعامل مع بيئة تكنولوجيا المعلومات، وهي بحاجة إلى المراجعة لضمان تحقيق المتطلبات الأمنية فيها.

5. **محور أمن المدخلات (البيانات):** وهي الإجراءات المبرمجة (الروتينية) والتي تقوم بإجراء الاختبارات على البيانات للتأكد من خلوها من الأخطاء،⁽⁴⁾ وهو يهدف إلى توفير درجة تأكد معقولة من صحة اعتماد البيانات التي يتسلمها قسم معالجة البيانات ومن سلامة تحويلها بصورة تساعد الحاسوب على التعرف عليها، وعدم فقدانها أو الإضافة إليها أو حذف جزء منها أو طبع صورة منها أو عمل أي تعديلات غير مصرح بها، كما تشمل رفض

(1) Information Systems Audit and Control Association (ISACA), (2009), *OP. Cit.*, Available at: <http://www.isaca.org> Accessed on 8-12-2012.

(2) النجار، فايز جمعه، (2010)، "نظم المعلومات الإدارية: منظور إداري"، مرجع سابق، ص 271.

(3) النجار، فايز جمعه، *نفس المرجع السابق*، ص 271.

(4) Hall, James A., (2013), *Accounting Information Systems*, OP. Cit., P. 741.

وتصحيح وإعادة إدخال البيانات السابقة رفضها،⁽¹⁾ وتعد هذه الرقابة هامة جداً لأن الجزء الأكبر من الخطأ في نظم الحاسوب ينتج عن أخطاء المدخلات، ويرى الباحث أن إعداد المدخلات مرحلة هامة وتمثل أساساً لما بعدها من المراحل، ويعتبر التحقق من دقة وسلامة المدخلات عنصراً حيوياً للوقاية من حدوث الأخطاء ومنع الوقوع في المشكلات ومواجهة الصعوبات.

6. **محور أمن عمليات التشغيل:** ويقصد بها الرقابة على كل العمليات المتصلة بتشغيل البيانات أي عملية اختيار الحاسوب وإعداده للتشغيل واختيار برامج التشغيل والرقابة على الملفات وذلك بغرض التأكد من ضمان صحة عمليات المعالجة التي تقوم بها نظم المعلومات المحاسبية المحوسبة، ويتم تضمين هذه الوسائل خلال كتابة برامج النظم،⁽²⁾ ويهدف إلى توفير درجة تأكد معقولة حول تنفيذ عمليات معالجة البيانات إلكترونياً طبقاً للتطبيقات المحددة، من خلال معالجة كافة العمليات كما صرح بها وعدم إغفال معالجة عمليات مصرح بها،⁽³⁾ والتأكد من أن البرنامج المطلوب لعملية المعالجة هو البرنامج الذي تم استدعائه، وأن الملفات التي يجب معالجتها هي الملفات التي تمت عليها عملية المعالجة، ووجود ضوابط رقابية في برنامج المعالجة لمنع حدوث الأخطاء أثناء عمليات المعالجة، وتشمل حماية نظم التشغيل وهي بحاجة ماسة لحمايتها من المخاطر الداخلية والخارجية سواء كانت نظم يونيكس أم ويندوز وهذه الأنظمة بحاجة إلى التحسين والتدقيق بصورة مستمرة.

7. **محور أمن المخرجات (المعلومات):** ويتمثل في السيطرة على إعادة إنتاج المعلومات وعلى عملية إتلاف مصادر المعلومات عند القرار بعدم استخدامها،⁽⁴⁾ والتي تشمل وثائق الفاكس، والبيانات المنقولة عبر الشبكات، والعمليات التجارية، وقواعد بيانات العملاء، وغير ذلك، فهناك سرقة معلومات آلاف البطاقات الائتمانية الخاصة بعملاء بعض المنشآت التي فرطت كثيراً في معلوماتها ولذلك فإن العملاء سيبحثون عن بديل تجاري يحظى بالثقة.

8. **محور أمن البيانات المنقولة عبر قنوات الاتصال:** هو حماية المعلومات خلال عملية تبادل البيانات من نظام إلى آخر، وذلك من خلال توفير درجة تأكيد معقولة من أن البيانات المنقولة عبر شبكات النظام محمية من كافة المخاطر التي قد تتعرض لها، فالرقابة على إرسال البيانات تصبح أكثر أهمية في المنشآت التي تستخدم تبادل البيانات الإلكترونية أو الإرسال الإلكتروني للأموال، ويمكن الوصول إلى رقابة داخلية عالية في بيئة كذلك باستخدام كلمات المرور، والجدران النارية، وتشفير البيانات، والتوقيع الرقمي، والشهادات الرقمية، وبروتوكولات التبادل الآمن للبيانات، ونظم الكشف عن الدخلاء، حيث تتعرض الشبكات لعدة مخاطر داخلية وخارجية ويجب على مدير الشبكة أن يحمي الشبكة من الاختراقات سواء كانت من داخل المنشأة أو من خارجها، ومما يساعد على ذلك استخدام البرامج الخدمية المتخصصة في إدارة الشبكات وحمايتها.

وتعتبر شبكة تنقل المعلومات المحلية أو الدولية ثمرة من ثمرات التطورات في مجالات الاتصالات كما أنها سهلت عملية التراسل بين الحواسيب و تبادل و استخدام الملفات، و لكن من جهة أخرى أتاحت عملية سرقة المعلومات أو تدميرها سواء من الداخل كاستخدام الفيروسات أو من خلال الدخول عبر منظومات الاتصال

(1) صيام، وليد زكريا، (2010)، "الرقابة الداخلية على تطبيقات نظم المعلومات المحاسبية الإلكترونية"، مجلة المدقق، العدد 85-86، جمعية المحاسبين القانونيين الأردنيين، عمان، الأردن، أغسطس 2010، ص: 17-19.

(2) رملي، فياض حمزة، (2011)، نظم المعلومات المحاسبية المحوسبة - مدخل معاصر لأغراض ترشيد القرارات الإدارية، شركة مطابع السودان للعملة المحدودة، الأباي للنشر والتوزيع، الخرطوم، السودان، 2011، ص 117.

(3) Romney, Marshal B. & Steinbart, Paul John, (2015), Accounting Information Systems, OP. Cit., P. 286.

(4) النجار، فايز جمعه، (2010)، نظم المعلومات الإدارية: منظور إداري، مرجع سابق، ص 271.

المختلفة ، لذلك لا بد من وضع إجراءات حماية و ضمان أمن الشبكات من خلال إجراء الفحوصات المستمرة لهذه المنظومات وتوفير الأجهزة الخاصة بالفحص، كما أن نظم التشغيل المستخدمة والمسؤولة عن إدارة الحواسيب يجب أن تتمتع بكفاءة وقدرة عالية على الكشف عن التسلل إلى الشبكة وذلك من خلال تصميم نظم محمية بإقفال معقدة أو عن طريق التشفير وربطها بخطوط الاتصال والتي هي عبارة عن استخدام الخوارزميات الرياضية أو أجهزة ومعدات لغرض تشفير تناقل المعلومات أو الملفات.

9. **محور أمن تعديل وتطوير النظام:** وهي مصممة لتوفير ثقة معقولة بأن برمجيات النظام قد تم اكتسابها أو تطويرها بطريقة مرخصة وكفؤة، وتتضمن المصادقة والموافقة والاختبار والتطبيق والتوثيق لبرمجيات الأنظمة الجديدة، وللتعديلات على برمجيات الأنظمة الحالية، وتقييد الوصول إلى برمجيات الأنظمة والتوثيق للموظفين المرخصين فقط، فعند تطوير أو تصميم أي نظام يجب إتباع الطرق العلمية الصحيحة في التصميم كم يجب مراجعته جيداً واختباره والتأكد من خلوه من الأخطاء قبل بدء التنفيذ وكذلك يجب التأكد من تدريب موظفي التشغيل والاستخدام تدريباً جيداً يضمن تشغيلهم واستخدامهم للنظام بطريقة آمنة ومتدرجة قبل الاعتماد كلياً عليه، ويجب استخدام الإجراءات والأساليب المعيارية للتعامل بفاعلية وحسم مع التغييرات والتحكم بالتعديلات، يجب توثيق كل التغييرات، والحصول على موافقة مسبقة لكل التغييرات المطبقة على أنظمة المعلومات.⁽¹⁾

وسوف تتناول الدراسة تلك المحاور بشكل موسع في المبحث الرابع من الفصل الثاني.

الخاتمة:

في ضوء ما سبق تناولت الدراسة في هذا المبحث لمحة عامة عن أمن نظم المعلومات المحاسبية المحوسبة لدى المنشأة، حيث تم تناول مراحل تطور مفهوم الأمن المعلوماتي، تعريف أمن نظم المعلومات المحاسبية المحوسبة حيث تم مناقشة مفهوم "الأمن" و"أمن المعلومات" و"أمن نظم المعلومات"، والمبادئ والأهداف الأساسية لأمن نظم المعلومات المحاسبية المحوسبة والتي أهمها السرية والسلامة والتوافر ومن ثم الخصوصية وعدم انكار التصرف، وتم بيان أهمية أمن نظم المعلومات المحاسبية المحوسبة، والعناصر الرئيسية التي يتكون منها أمن تلك النظم، وكذلك تم تسليط الضوء على محاور وأنماط أمن نظم المعلومات المحاسبية المحوسبة، وأخيراً تم توضيح الاعتبارات التي يجب مراعاتها لضمان فعالية وكفاءة أمن نظم المعلومات المحاسبية المحوسبة، وسوف نناقش في المبحث التالي طبيعة مخاطر أمن نظم المعلومات المحاسبية المحوسبة.

(1) خالد، أبو ذر عثمان، (2011)، "سياسات أمن المعلومات"، الطبعة الأولى، المركز القومي للمعلومات، الخرطوم، السودان، 2011، ص 77.

2-1: المبحث الثاني

طبيعة المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة

يحيط الخطر بالإنسان من كل جانب، ويستمر معه في حركاته وسكناته منذ ولادته وحتى وفاته، والخطر ليس وليد اليوم وإنما هو قديم قدم التاريخ نفسه، ومع التقدم العلمي والتكنولوجي ظهرت مخاطر لم تكن معروفة من قبل مثل مخاطر الطيران ومخاطر الفضاء، ومخاطر الاتصالات وتكنولوجيا المعلومات، فالخطر ظاهرة عالمية تتغير تبعاً لتقدم المدنية وتطور الحياة الإنسانية، وتختلف المخاطر التي تتعرض لها المنشآت باختلاف طبيعة نشاط المنشأة واختلاف السياسات والاستراتيجيات التي تنتهجها إدارات المنشآت لتحقيق أهدافها.

وتعتبر دراسة المخاطر أحد الموضوعات الهامة في عدد من العلوم الاجتماعية كعلم الإحصاء، وعلم الاقتصاد، وعلم الإدارة المالية، والتأمين، ولا شك أن نظرة كل علم من هذه العلوم إلى المخاطر له خصوصياته التي ينفرد بها عن الآخر، إلا أن مضمونها لا يختلف في جميع تلك العلوم،⁽¹⁾ وغالباً ما توصف مخاطر أمن المعلومات فقط دون الاهتمام بالمخاطر المرتبطة بأمن نظم المعلومات ككل رغم أن المخاطر الأخيرة تمثل قضية أوسع مع عدد من وجهات النظر المختلفة، فمن الممكن أن تجتمع هنا المفاهيم والمعارف من التخصصات العلمية الأخرى، كإدارة الموارد البشرية، وإدارة المشاريع، وإدارة المخاطر، وهندسة البرمجيات، وإدارة العمل الجماعي، وإدارة التغيير ... الخ.⁽²⁾

ويواجه أمن نظم المعلومات المحاسبية المحوسبة العديد من المخاطر على تهدد ملائمة وموثوقية وسلامة محتوى وتكامل وسرية المعلومات المحاسبية والتي قد ينجم عنها أضرار تتسبب في خسائر جوهريّة وهامة، وبالتالي أصبحت قضية أمن نظم المعلومات المحاسبية المحوسبة أحد الهواجس التي تؤرق مختلف المنشآت⁽³⁾، حيث تزامن التطور الكبير لنظم المعلومات مع تطور تكنولوجيا المعلومات وسرعة انتشارها، وصاحب هذا التطور العديد من المخاطر التي تؤثر على أمن نظم المعلومات سواء كانت تلك المخاطر مقصودة أو غير مقصودة وإن كانت المخاطر المقصودة أشد خطراً من المخاطر غير المقصودة،⁽⁴⁾ ومن المتوقع أن تزداد تلك المخاطر وتتنوع بشكل واسع خلال الفترة المقبلة خاصة في ظل التطور المتنامي في مجال التقنية، وأيضاً مع تزايد أعداد المنشآت المستخدمة للنظم المحاسبية المحوسبة.

ويتطلب تقييم المخاطر تحديد المخاطر ومعرفة التهديدات المسببة لها وكذلك بيان تأثيراتها، واختبار التقنيات اللازمة لمواجهتها وإدارتها، وقبل التطرق لتقييم مخاطر أمن نظم المعلومات المحاسبية، لا بد من التطرق لمفهوم المخاطر الأمنية وأنواعها، وعلى ذلك فإن هذا المبحث يتضمن تحليل لطبيعة المخاطر التي تهدد أمن نظم

(1) بن علي، بلعزوز، (2010)، "استراتيجيات إدارة المخاطر في المعاملات المالية"، مجلة الباحث، العدد (7)، جامعة الشلف، الجزائر، 2010، ص: 331-344.

(2) Černá, Marie, (2012), "Information Risks and Their Connection With Accounting", 6th European Conference on Information Management and Evaluation, Faculty of Economics - University of West Bohemia, Pilsen, Czech Republic, 2012, PP: 375-382.

(3) زويلف، إنعام، (2009)، "طبيعة تهديدات أمن نظم المعلومات المحاسبية الإلكترونية - دراسة تطبيقية على شركات التأمين الأردنية"، مرجع سابق، ص: 46-77.

(4) الذبيبة، زياد & الرمحي، نضال & الجعدي، عمر، (2011)، "نظم المعلومات في الرقابة والتدقيق"، الطبعة الأولى، دار المسيرة للنشر والتوزيع والطباعة، عمان، الأردن، ص: 64.

المعلومات المحاسبية المحوسبة والمفاهيم المرتبطة بها من منظور متكامل، ويلقي الضوء على التصنيفات والتقسيمات المختلفة لتلك المخاطر وفقاً لأسس ومعايير معينة، كما يتناول هذا المبحث الأنواع المختلفة لتلك المخاطر محل هذه الدراسة.

1-2-1: تعريفات ومفاهيم مخاطر أمن نظم المعلومات المحاسبية المحوسبة:

مصطلح "الخطر" كثيراً ما يرتبط مع مصطلح "الأمن"، فالخطر في جوهره احتمال حدوث شيء ينتج عنه أضرار،⁽¹⁾ وعندما نتحدث عن الخطر فنحن نتحدث عن شيء غير مؤكد بل مجرد احتمال، فإذا لم يكن هناك شك فليس هناك خطر، فنتيجة القفز من طائرة بدون مظلة لا يعتبر خطر لأنه لا يوجد شك في النتيجة ولا يوجد احتمال بل هي نتيجة حتمية وواحدة، أما نتيجة القفز باستخدام مظلة فهو خطر لوجود احتمال محدود في تحقيقه، ومن المفيد التمييز بين المشكلة (*Problem*) والخطر (*Risk*)، فالمشكلة تمثل حالة من التوتر وعدم الرضا نتيجة وجود بعض الصعوبات التي قد تعيق تحقيق الأهداف المتوقعة من أنشطة المنشأة، فالمشكلة تكون سبباً في وجود حالة غير مرغوب فيها، وعليه فإنها تكون بمثابة تهديد للخطر، ومتى ما تعقدت واتخذت مساراً حاداً يصعب توقع نتائجه بصورة دقيقة يمكن القول أن الخطر تحول إلى أزمة وهي حالة من عدم التوازن أو الاتساق بين ما هو كائن، وما يجب أن يكون أو هي انحراف الأداء المخطط له عن الأداء الفعلي.

وهناك علاقة بين مصطلحات المخاطر والأزمات والكوارث، فهذه المصطلحات تربطها علاقة تتابع، حيث تبدأ العملية بالتعرض للمخاطر، والتي قد تتحول - في حالة عدم السيطرة عليها - إلى أزمة، والتي قد تتحول هي الأخرى - في حالة عدم السيطرة عليها - إلى كارثة، والجدير بالذكر أن الباحث قد ركز على استخدام مصطلح المخاطر (*Risks*) بدلاً من مصطلح الأزمات أو مصطلح الكوارث لعدة أسباب أهمها رغبة الباحث في السيطرة على مخاطر - أمن نظم المعلومات المحاسبية - قبل استفحالها وتحولها إلى أزمات، أو كوارث.

وتشير بعض الأدبيات إلى وجود خلط بين مفهوم الخطر وغيره من المفاهيم، وكثيراً ما تستخدم دون تحديد منضبط لتلك المفاهيم، لذلك كان من الأهمية إلقاء الضوء على بعض المفاهيم التي يجري الخلط بينها، فثمة فرق بين المخاطر، والتهديدات، والثغرات أو نقاط الضعف، والتي تستخدم للتعبير عن نفس الشيء رغم أنها حقيقة لها معاني مختلفة تربطها مع بعض علاقات منطقية،⁽²⁾ ولا بد من التمييز بين تلك المفاهيم والمصطلحات على النحو التالي:

(1) Vacca, John R., (2009), *Computer and Information Security Handbook*, OP. Cit., P.231 , <http://www.elsevierdirect.com>

(2) Dahbur, Kamal & Mohammad, Bassil & Tarakji, Ahmad, (2011), "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing", *International Conference on Intelligent Semantic Web-Services and Applications*, New York, USA.

- تعرف المخاطر بصفة عامة بأنها احتمال وقوع حدث ما أو تصرف ما من شأنه أن يؤدي إلى فشل المنشأة في تحقيق أهدافها. (1)
- فالخطر هو احتمالية إن يكون هناك ضعف في أصل أو مجموعة من الأصول يمكن استغلاله من قبل تهديد معين وينتج عنه خسارة أو ضرر في تلك الموارد، ويكون تأثيره سلبي على المنشأة. (2)
- الخطر في أمن نظم المعلومات المحاسبية هو إمكانية وقوع أضرار لنظم المعلومات أو بعض أصولها نتيجة تلاقي كل من أصل من أصول نظم المعلومات له قيمة معينة، ومواطن للضعف في ذلك الأصل، وأحد التهديدات الذي يمكن أن يستغل موطن الضعف لإلحاق الضرر بالأصل، فوجود أي تهديد يمكن استغلاله وبالتالي إذا استغل ذلك التهديد يمكن أن يطلق عليه ثغرة أمنية في تلك المنشأة تؤدي إلى وقوع الخطر (3)، كما بالشكل الآتي الذي يوضح سياق نشوء الخطر.

الشكل رقم (1-2-1) سياق نشوء الخطر (4)



فالخطر يشير إلى احتمال وجود تهديد يمكن استغلاله، وبالتالي إذا استغل ذلك التهديد يمكن أن نطلق عليه ثغرة أمنية في تلك المنشأة.

ولفهم طبيعة مفهوم مخاطر أمن نظم المعلومات المحاسبية المحوسبة لابد من معرفة العلاقة بين العناصر المكونة لتلك المخاطر والمتمثلة في التهديدات الأمنية ونقاط الضعف في نظم المعلومات المحاسبية وحوادث المخاطر وتأثير تلك المخاطر وإجراءات ووسائل الحماية المطبقة والملائمة لمواجهة تلك التهديدات، (5) وإن تحليل المخاطر هي عملية تبدأ من التساؤل حول التهديدات ثم نقاط الضعف وأخيراً وسائل الوقاية المناسبة للتعامل مع التهديدات ومنع نقاط الضعف، (6) والشكل الآتي يوضح الترابط المنطقي بين تلك المكونات:

(1) عيسى، علا & عاشور، عصاف، (2010)، "مخاطر نظم المعلومات المحاسبية وحوكمة الشركات ومواجهة الأزمة المالية العالمية"، مجلة الفكر المحاسبي، المجلد 14، العدد 2، كلية التجارة، جامعه عين شمس، القاهرة، مصر، ص: 408-434.

(2) Khambhammettu, Hemanth, et al., (2013), "A Framework for Risk Assessment in Access Control Systems", computers & Security, Vol. xxx, 27 February 2013, PP: 1-18.

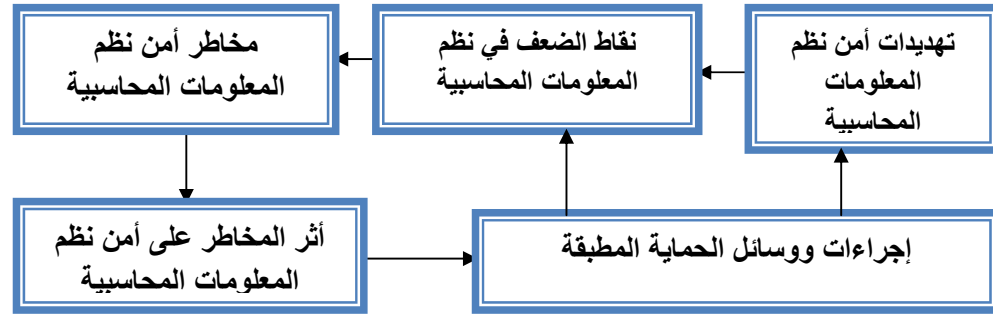
(3) Mihalache, Arsenie, (2011), "Security of the Accounting Information System Infrastructure", OP. Cit., PP: 1339-1345, <http://ideas.repec.org/a/ovi/oviste/v11y2011i1p1339-1345.html>

(4) الشكل من إعداد الباحث.

(5) Wikipedia, (2014), OP. Cit., Accessed 26/02/2014, in 08:33 GMT.

(6) المري، عريض، (2011)، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها، مرجع سابق، http://www.dralmarri.com/show.asp?field=res_a&id=205

الشكل رقم (1-2-2) الترابط المنطقي لمكونات مخاطر أمن نظم المعلومات المحاسبية المحوسبة⁽¹⁾



يتضح من هذا الشكل أن وجود أي تهديد من تهديدات نظم المعلومات المحاسبية (كعامل من عوامل الخطر)، يستغل نقاط ضعف في العناصر المكونة للنظام، ويؤدي إلى حدوث المخاطر يمكن أن تلحق ضرراً بتلك الأصول وتسبب تأثيرات سلبية على أهداف ومبادئ أمن نظم المعلومات المحاسبية وبالتالي يؤثر ذلك على أهداف المنشأة، مما يستدعي من إدارة المنشأة اتخاذ وتطبيق إجراءات الحماية الملائمة لتخفيف تأثير تلك المخاطر ومن ثم تحسين أداء تلك النظم.⁽²⁾

على سبيل المثال: إذا كانت المنشأة لديها برامج مكافحة الفيروسات ولكن لا تقوم بتحديثه عند انتهاء فترة صلاحيته، فتلك نقطة ضعف سيؤدي حتماً إلى أن التهديد المتمثل هجوم ووجود الفيروسات وانتشارها في بيئة نظم المعلومات المحاسبية المحوسبة، وتسبب ضرر (خطر)، مما يؤثر على أمن تلك النظم، وبالتالي يعرض المنشأة التي تمتلك تلك النظم لخسائر، وذلك يستوجب من تلك المنشأة أخذ التدابير المضادة في هذه الحالة وهي القيام بتنشيط وتحديث برامج مكافحة الفيروسات على كافة أجهزة الحاسوب الخاصة بتلك النظم.

ولتحديد احتمالات وجود حدث سلبي في المستقبل لتكنولوجيا المعلومات (مخاطر أمن نظم المعلومات)، فيجب تحليل التهديدات التي يتعرض لها نظام تكنولوجيا المعلومات بالتزامن مع نقاط الضعف المحتملة ووسائل وإجراءات التحكم لنظام تكنولوجيا المعلومات⁽³⁾ وعليه لابد من معرفة كلاً من التهديدات والثغرات على النحو التالي:

1-1-2-1 مفهوم التهديدات (Threats): هي الأسباب المحتملة لوقوع أحداث غير مرغوب فيها، مما قد يتسبب في ضرر للنظام أو للمنشأة، فالتهديد هو حدث محتمل غير مرغوب قد يؤدي إلى خسارة أو ضرر " فالتهديد هو أي شيء قادر على التصرف بطريقة ينجم عنه إلحاق أضرار بأحد أصول المنشأة،⁽⁴⁾ وبالتالي فإن فإن التهديدات هي مجموعة من الأعمال التي يقوم بها فرد أو مجموعة أفراد من داخل المنشأة أو من خارجها

(1) الشكل من إعداد الباحث.

(2) Wikipedia, (2014), **OP. Cit.**, Accessed 26/02/2014, in 08:33 GMT.

(3) National Institute of Standards and Technology: NIST, (July 2012), **"Guide for Conducting Risk Assessments"**, OP. Cit.

(4) ISO/IEC 27005, (2008), **Information Technology - Security Techniques -Information Security Risk Management**, International Standards Organization and International Electro technical Commission (ISO/IEC), Geneva, Switzerland.

بقصد أو بدون قصد، أو بفعل عوامل الطبيعة والتي تؤدي إلى تعطيل وظائف المنشأة أو تلف مواردها من خلال التأثير المباشر على أصول المنشأة ومن تلك الأصول نظم المعلومات المحاسبية بكل مكوناتها. وتستخدم المخاطر بشكل مترادف مع تعبير التهديدات، حيث توصف المخاطر بأنها مجموعة من التهديدات، مع أنها حقيقة تتصل بأثر التهديدات عند حصولها، فالتهديد هو مؤشر على خطر وشيك أو ضرر، والتهديد الأمني هو حالة من الضعف التي قد يؤدي إلى حدوث خطر لأمن المعلومات،⁽¹⁾ وعرفه باحث آخر بأنه حدوث مؤثر لحدث غير مرغوب فيه مما يترتب عليه أذى للنظام أو المنشأة، مثل: نقص في الكفاءات والخبرات، وعرف بأنه مصدر من مصادر الضرر المحتمل الذي قد ينشأ عنه حوادث أمنية تؤثر تأثيراً سلبياً على أصول نظم المعلومات،⁽²⁾ والتهديد هو مصدر الخطر المحتمل الذي يمكن أن يتعرض له نظام المعلومات، وقد يكون شخصاً كالجاسوس أو المخترق أو شيئاً يهدد الأجهزة أو البرامج أو البيانات والمعطيات أو حدثاً كالحريق وانقطاع التيار الكهربائي والكوارث الطبيعية، بينما يرى آخر بأن التهديدات هي استغلال نقاط الضعف الموجودة في محاولة لإحداث الضرر أو تدمير المورد،⁽³⁾ والتهديدات الأمنية للمعلومات وفق رأي إحدى الباحثات هي الظروف التي لديها القدرة على أن تسبب ضرراً ومخاطر على المعلومات.⁽⁴⁾ وعليه فإن تهديدات أمن نظم المعلومات المحاسبية هي الأحداث والأشخاص والتصرفات التي يمكن أن تؤدي إلى حدوث مخاطر تحمل تأثيراً سلبياً ومضراً على عناصر ومكونات تلك النظم، وبالتالي تؤثر سلباً على أهداف أمن نظم المعلومات المحاسبية، وبذلك تعتبر التهديدات مؤشراً لحدوث المخاطر وهي بمثابة منبهات أو نظام إنذار مبكر (*Earl Warning System*)، يساعد المنشأة في تحديد مصادر حدوث المخاطر، وتحسين قدرتها على التنبؤ بالمخاطر المحتملة، ومن تلك التهديدات تقادم الأجهزة والمعدات، وعدم كفاءة العاملين، وازدياد معدل دوران العمالة، وضعف كفاءة وأساليب الأداء، وسيتم تناولها بتفصيل أكثر في الفصل الثاني من هذه الدراسة.

1-2-1- مفهوم نقاط الضعف أو الثغرات أو القابلية للتعرض للمخاطر (*Vulnerabilities*): وهي وجود

مواطن ضعف في أصول المنشأة والتي من خلالها يستطيع المهاجم تدمير أو تخريب أو عرقلة المحل الذي هاجم من أجله، وتعني عنصر أو نقطة أو موقع في النظام يحتمل أن ينفذ من خلاله المعتدي أو يتحقق بسببه الاختراق فمثلاً يعد الأشخاص الذين يستخدمون النظام نقطة ضعف إذا لم يكن تدريبهم كافياً لاستخدام النظام وحمايته، وقد يكون الاتصال بالإنترنت نقطة ضعف مثلاً إذا لم يكن مشفراً، وقد يكون الموقع المكاني للنظام

(1) Maram, Venkata et al.,(2012), "A Study of Risk Management of an Information System by Assessing Threat, Vulnerability and Countermeasure", *International Journal of Advanced Research in Computer Science and Software Engineering*, OP. Cit. , PP: 51-53, http://www.ijarcsse.com/docs/papers/12_December2012/Volume_2_issue_12_December2012/V2I12-0122.pdf

(2) Sumner, Mary,(2008), "Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness", *OP. Cit.*, PP: 2-12.

(3) Dahbur, Kamal & Mohammad, Bassil & Tarakji, Ahmad,(2011), "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing", *OP. Cit.*

(4) Al-Awadi, Maryam, (2009), "A Study of Employees' Attitudes Towards Organizational Information Security Policies in the UK and Oman", *PhD thesis*, Glasgow University, Glasgow, UK, P. 15.

نقطة ضعف كأن يكون غير مجهز بوسائل الوقاية والحماية ، وعموماً فإن نقاط الضعف هي الأسباب المحركة لتحقيق التهديدات أو المخاطر،⁽¹⁾ فنقاط الضعف أو الثغرات وفقاً للمنظمة الوطنية للمعايير والتكنولوجيا "الأمريكية": هي خصائص أحد الأصول التي يمكن استغلالها من قبل تهديداً معين، وتمثل أحد العوامل التي تمثل عدم اليقين فليس من الممكن أن تعرف كل شيء عن كل نقاط الضعف، ويجب أن يضاف دائماً إلى عملية تقييم المخاطر، باستخدام الحكم الجيد والخبرة لمدراء أمن نظم المعلومات والأفراد ذات العلاقة،⁽²⁾ ونقاط الضعف في نظم المعلومات: هي احتمال أن أحد أصول نظم المعلومات أو مجموعة من الأصول لن تكون قادرة على مقاومة التهديد فهناك ضعف في الأصل أو مجموعة من الأصول والتي يمكن استغلالها من قبل تهديد واحد أو أكثر.⁽³⁾ ونقصد في دراستنا هذه بالثغرات أي نقاط الضعف الموجودة في نظام المعلومات ككل أو في شبكة المعلومات أو الأجهزة التي تعمل ضمن الشبكة أو حتى البرمجيات التي يتم إتاحتها على شبكة المعلومات، ويمكن أن تكون هذه الثغرات في تصميم شبكة المعلومات أو في تهيئة الشبكة أو البرمجيات أو قواعد البيانات التي تحتويها الشبكة، ومن خلال هذه الثغرات أو نقاط الضعف يمكن للمهاجمين أن يخترقوا شبكات المعلومات ويحدثوا فيها الأضرار أو حتى الاستيلاء على ما يريدوا منها،⁽⁴⁾ ونقاط الضعف يمكن أن تكون في أي جانب من جوانب النظام، وليست مجرد عيوب في الحماية التقنية المقدمة من قبل النظام، وغالباً ما ترد نقاط ضعف كبيرة في إجراءات التشغيل القياسية لأداء الأفراد، ويمكن تحديد مواطن الضعف على مستوى السياسات، مثل عدم وجود سياسة محددة بوضوح لاختبار الأمن، عدم وجود خطة واضحة للطوارئ.

ويرى الباحث أن نقاط الضعف أو الثغرات في نظم المعلومات هي أي عنصر أو نقطة أو موقع في تلك النظم قد تستغل في اختراقها، ويحتمل أن ينفذ من خلاله المعتدي أو يتحقق بسببها الاختراق وعموماً فإن نقاط الضعف هي الأسباب المحركة لتحقيق التهديدات أو المخاطر وذلك لضعف الإجراءات الوقائية والحماية الكافية، فليس هناك نظام تشغيل آمن ضد الهجوم حيث أن إغلاق ثغرة أمن لا ينفي حدوث ثغرة أخرى فيما بعد، ويرتبط ذلك بإجراءات ووسائل الحماية وهي التكنيك المتبع لحماية النظام ككلمات السر والأقفال ووسائل الرقابة والجدران النارية وغيرها، وعلى الأفراد المختصين بأمن نظم المعلومات أن يقوموا بعمليات فحص باستمرار لشبكة المعلومات وقواعدها لكي يقفوا على أي نقاط ضعف أو ثغرات يمكن أن تحدث ويعملوا على الفور على معالجتها وسد هذه الثغرات تجنباً لاكتشافها من قبل بعض العابثين.

3-1-2-1: مفهوم المخاطر (Risks): يتم استخدام مصطلح المخاطر عالمياً، ويختلف مفهوم المخاطر حسب

مجالات استخدامه، فقد تناول الكثير من الباحثين مفهوم "الخطر" حيث أخذ عدة تعريفات واختلف الكتاب

(1) الشبلي، هيثم حمود، "إدارة مخاطر الاحتيال في قطاع الاتصالات"، الطبعة الأولى، دار صفاء للنشر والتوزيع، عمان، الأردن، 2009، ص 284.

(2) National Institute of Standards and Technology: NIST, (July 2012), "Guide for Conducting Risk Assessments", OP. Cit.

(3) ISO/IEC 27005, (2008), Information Technology - Security Techniques -Information Security Risk Management, OP. Cit.

(4) حسنين، رجب عبد الحميد، (2012)، "أمن شبكات المعلومات الإلكترونية: المخاطر والحلول"، مرجع سابق، متاح في:

http://www.journal.cybrarians.org/index.php?option=com_content&view=article&id=629:networks&catid=257:studies

وبالباحثون في وضع مفهوم موحد للخطر نتيجة اختلاف وجهات نظرهم طبقاً للبيئة التي ينتمي إليها كل باحث، والهدف الذي يسعى إلى تحقيقه، والزاوية التي ينظر منها إلى الظاهرة محل الدراسة، فالخطر يعني أشياء مختلفة لأناس مختلفين، وعلى الرغم من اختلاف الآراء الرامية لتحديد مفهوم المخاطر فإننا سنتعرض لبعض هذه التعاريف كما يلي:

- الخطر هو حدث غير مؤكد، ويكون له تأثير سلبي على أهداف المنشأة، وعادة ما يتم التعبير عنه من حيث التأثير، معبرا عنه بوحدات نقدية، أو بنسبة مئوية لاحتمال الحدوث في فترة زمنية.⁽¹⁾
- يعرف الخطر بأنه حدث محتمل الوقوع تتعرض له المنشأة مما يعرضها إلى خسائر غير متوقعة في المستقبل، وهو مزيج مركب من احتمال وقوع الحدث ونتائجه،⁽²⁾ فهو مزيج من احتمال وقوع حدث مفاجئ وغير مرغوب فيه والآثار السلبية المترتبة عليه، والمتعلقة بتحقيق أهداف المنشأة.
- وفي ضوء المفاهيم السابقة فإنه يمكن للباحث تعريف المخاطر بوجه عام بأنها حالة احتمالية لعدم التأكد من وقوع أحداث معينة في الوقت الحاضر، أو قد تقع في المستقبل، ولها آثار مادية أو معنوية سلبية تؤدي إلى نتائج غير مرضية وغير متوقعة على عمليات المنشأة وأصولها بكافة أنواعها، وتؤثر سلباً في تحقيق المنشأة لأهدافها سواء القصيرة المرتبطة بتقديم السلع أو الخدمات لتحقيق الأرباح أو الطويلة الأجل متمثلة في البقاء والاستمرار.
- وتم تعريف مخاطر تكنولوجيا المعلومات من خلال جمعية تدقيق ورقابة نظم المعلومات (ISACA) بأنها احتمال تعرض المنشأة إلى تأثير سلبي شديد نتيجة تملك ونشر واستخدام وتشغيل، ومشاركة وتنفيذ واعتماد تكنولوجيا المعلومات داخل أو خارج المنشأة.⁽³⁾
- خطر أمن نظم المعلومات هو احتمال وجود تهديد معين (عامل أو مصدر الخطر) لديه إمكانات خاصة للاستفادة من الضعف مما قد يعرض أمن المعلومات لذلك التهديد وبالتالي يؤثر على الأعمال التجارية المقابلة.⁽⁴⁾
- فارتباط التهديدات الأمنية بتلك المخاطر وثيق جداً، حيث يمكن استغلال نقاط الضعف المعروفة وغير المعروفة على حد سواء للتأثير على سرية، وسلامة، وتوافر المعلومات المستخدمة من قبل المنظمة.⁽⁵⁾
- ويمكن تعريف مخاطر أمن نظم المعلومات بوصفها أحداث سلبية (كإمكانية الوصول غير المصرح به أو الاستخدام أو الإفصاح أو الخلل أو التغيير، أو تدمير نظم المعلومات... الخ) تمت تلك الأحداث نتيجة

(1) Černá, Marie, (2012), "Information Risks and Their Connection With Accounting", 6th European Conference on Information Management and Evaluation, OP. Cit., PP: 375-382.

(2) ISO/IEC 27005, (2008), Information Technology - Security Techniques -Information Security Risk Management, OP. Cit.

(3) ISACA (Information Systems Audit and Control Association) (2009) "The Risk IT Practitioner Guide", Printed in the United States of America.

(4) Dahbur, Kamal & Mohammad, Bassil & Tarakji, Ahmad, (2011), "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing", OP. Cit.

(5) Breier, Jakub & Hudec, Ladislav, (2012), "Towards a Security Evaluation Model Based on Security Metrics", International Conference on Computer Systems and Technologies, CompSysTech'12, 22-23 June 2012, Ruse, Bulgaria.

ممارسة نشاط من مصدر تهديد مستغلاً وجود ضعف خاص في مكونات النظام ويكون الأثر الناتج من هذا الحدث سلبي على المنشأة.⁽¹⁾

ويمكن للباحث صياغة تعريف لمخاطر أمن نظم المعلومات المحاسبية المحوسبة على أنها احتمال حدوث ضرر الكشف أو التعديل أو التدمير لمدخلات أو محتويات قاعدة بيانات النظام أو مخرجاته، بسبب وجود تهديدات من مصادر خارجية أو داخلية للمنشأة استغلت وجود نقاط ضعف معينة في نظم المعلومات المحاسبية المحوسبة، مما أدى إلى حدوث تأثير سلبي على أمن تلك النظم من حيث السرية والسلامة والتوافر والخصوصية وعدم الإنكار، مما يعرض المنشأة إلى خسائر مالية أو إساءة سمعتها، وقد يصل الأمر إلى توقف المنشأة وعدم استمرارها.

توجد المخاطر التي قد تتعرض لها أمن نظم المعلومات في كل أجزاء ومراحل النظام ويجب أن تقيم بشكل منفرد أو على مستوى المنشأة ككل، وتبدأ عملية تحديد المخاطر بتصور كل خطر قد يهدد أمن نظم المعلومات المحاسبية محل الحماية، ابتداء من قطع مصدر الكهرباء عن الحاسوب وحتى مخاطر اختراق النظام من الخارج بواحد أو أكثر من وسائل الاختراق عبر نقاط الضعف، مروراً بإساءة الموظفين استخدام كلمات السر العائدة لهم، ومع تعدد صور وأشكال المخاطر التي يمكن أن تواجه نظم المعلومات المحاسبية المحوسبة فإنه يمكن تصنيف أو تقسيم أو تبويب تلك المخاطر ضمن قوائم إلى عدة فئات تبعا لعدة أسس ومعايير للتصنيف وضمنها تختلف أوصاف المخاطر وطبيعتها، ووفقا لذلك يمكن أن تصنف تلك المخاطر من حيث مصدرها (إما داخلية ضمن نطاق المنظمة، أو خارجية)، أو من حيث وسائل تنفيذها، أو من حيث علاقتها مع مراحل النظام (الإدخال والمعالجة والإخراج)، أو من حيث نية المتسببين بهذه المخاطر (مقصودة أو "عرضية")⁽²⁾، أو من حيث الجاني (بشرية أم غير بشرية "بيئية")، أو من حيث أثرها على نظام الحماية وعلى المعلومات محل الحماية، وهو ما سنقف عليه بشكل تفصيلي، وهناك وجهة نظر في تصنيف تلك المخاطر إلى مخاطر تنظيمية ومخاطر تقنية ومخاطر قانونية، وعليه فإن تصنيف وتحديد المخاطر يتباين من وجهات نظر مختلفة، بحسب النظريات والمعايير المختلفة، وتختلف تبعا لذلك قائمة المخاطر ضيقاً واتساعاً وأحياناً تختلف من حيث التسميات فقط مع تغطيتها لذات المخاطر.

(1) Rees, Jackie & Allen, Jonathan, (2008), "The State of Risk Assessment Practices in Information Security: An Exploratory Investigation, *Journal of Organizational Computing and Electronic Commerce*, No. 18, USA, PP: 255-277.

(2) Kritzing, E & Smith, E. (2008), "Information security management: An information security retrieval and awareness model for industry", *OP. Cit.*, PP: 224 - 231.

مما تقدم يرى الباحث أن مخاطر أمن نظم المعلومات المحاسبية المحوسبة كثيرة ومتعددة وتستحق الانتباه من قبل الإدارة العليا لأي منشأة أعمال لضمان استمرارية نشاطها، وتعتبر التصنيفات السابقة شاملة لجميع تلك المخاطر، ومن خلال هذه الدراسة قام الباحث بتصنيف المخاطر التي تواجه نظم المعلومات المحاسبية المحوسبة بشكل عام إلى تسعة أصناف رئيسية هي:

1. المخاطر التي تهدد أمن الأفراد العاملين في نظم المعلومات المحاسبية المحوسبة.
 2. المخاطر التي تهدد الأمن المادي لنظم المعلومات المحاسبية المحوسبة.
 3. المخاطر التي تهدد أمن الوصول البرمجي لنظم المعلومات المحاسبية المحوسبة.
 4. المخاطر التي تهدد أمن التخزين غير المتصل بقاعدة بيانات نظم المعلومات المحاسبية المحوسبة.
 5. المخاطر التي تهدد أمن مدخلات نظم المعلومات المحاسبية المحوسبة.
 6. المخاطر التي تهدد أمن عمليات تشغيل نظم المعلومات المحاسبية المحوسبة.
 7. المخاطر التي تهدد أمن مخرجات نظم المعلومات المحاسبية المحوسبة.
 8. المخاطر التي تهدد أمن تبادل البيانات عبر شبكات نظم المعلومات المحاسبية المحوسبة.
 9. المخاطر التي تهدد أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة.
- وسوف يتم تناول تلك المخاطر بالتفصيل في النقاط اللاحقة من هذا المبحث وهي كثيرة ومتعددة وتتسم بالتداخل فيما بينها وليس من السهل التطرق لكل تلك المخاطر، فمحاولة إحصاء تلك المخاطر قد تكون شبة مستحيلة وذلك لتغير أسباب تلك المخاطر بشكل سريع ومستمر، فكل تغير أو تطور يواكبه مخاطر جديدة،⁽¹⁾ ولذلك فإن المخاطر عديدة في مجال أمن نظم المعلومات المحاسبية المحوسبة، ولكن يمكن تصنيف المخاطر لمجموعات رئيسية على النحو التالي:

2-2-1: المخاطر التي تهدد أمن الأفراد العاملين في نظم المعلومات المحاسبية المحوسبة:

يقصد بالمخاطر التي تهدد أمن الأفراد العاملين في نظم المعلومات هي تلك المخاطر التي محورها مستخدم نظام المعلومات المحاسبي، وقد تكون مخاطر غير مقصودة نتيجة ضعف التدريب والتأهيل، أو مقصودة نتيجة ضعف الولاء الوظيفي والنزاهة الأخلاقية عند بعض الأفراد المستخدمين لنظام المعلومات المحاسبي، حيث تحتل هذه النوعية من المخاطر المكانة الأولى نظراً لكفاءة وفعالية الموارد البشرية فهي تعكس مدى نجاح المنشأة حيث هناك مجموعة من المخاطر المتعلقة بالموارد البشرية داخل المنشأة والتي لها علاقة بالمخاطر العش والتلاعب وزيادة حالات فيروسات الحاسب والطمس المتعمد للبيانات والمعلومات والدخول غير المصرح به للنظام من قبل موظفي المنشأة.

وتعد تلك المخاطر التي تواجه الأفراد العاملين في نظم المعلومات واحدة من أهم المشاكل لدى جهات أمن نظم المعلومات المحاسبية، إذ ثمة فرصة لأن يحقق أشخاص من الداخل ما لا يمكن نظرياً أن يحققه أحد من

(1) Arens, Alvin A., Elder, Randal J., & Beasley, Mark S., (2014). *Auditing & Assurance Services: An Integrated Approach*, 15th Edition, International Edition, Inc, Pearson Education, Inc. Prentice Hall, Upper Saddle Rivers: New Jersey, USA., PP: 740-742.

الخارج، وتصل مشكلة صعوبات كشف هؤلاء قائمة إن لم يكن ثمة نظام أداء وصلاحيات يتيح ذلك، وثمة مسميات وطوائف عديدة لهذه المخاطر نتناول تالياً أبرزها، على أن يكون مدركاً أنها تتعلق بالمخاطر الداخلية والخارجية معاً.⁽¹⁾

1-2-3: المخاطر التي تهدد الأمن المادي:

تتعرض نظم المعلومات المحاسبية المحوسبة لمخاطر أمن مادية وهي مجموعة مخاطر يوجهها مرتكبوها نحو المعدات المستخدمة في بناء شبكة نظم المعلومات، ومن تلك المخاطر سرقة الأجهزة والمعدات أو إتلافها، والأضرار الكبيرة في تجهيزات الشبكة والمباني،⁽²⁾ وبالتالي فإن مخاطر الأمن المادي تعني إلحاق الضرر بالمنشأة كاملة من مبان وغرف وأجهزة ووسائط معلومات، ومحطات طرفية، وأفراد، ومن تلك المخاطر السرقة والتخريب، بسبب الحريق وانقطاع الكهرباء والاتصالات، والفيضانات.

والاختراق المادي – أو حتى البرمجي - هو محاولة لتدمير أو كشف أو تغيير أو تعطيل، أو سرقة أو الحصول على وصول غير مصرح به أو استخدام غير مصرح به لأي أصل من أصول المنشأة وهو أي شيء له قيمة للمنشأة، وتعتبر نظم المعلومات المحاسبية أحد الأصول الهامة للمنشأة، حيث تتضمن: الأصول المادية، مثل الحواسيب وما إليها من عتاد، والكوادر البشرية بمؤهلاتها، وما تملكه من مهارات وخبرات، والأصول الفكرية كاليانات والمعلومات وبرامج الحاسبات، وكذلك الأصول غير الملموسة مثل السمعة والصورة الذهنية.⁽³⁾

وتعتبر نقاط الضعف الرئيسية في البنية التحتية المادية لنظم المعلومات المحاسبية، هي الأجهزة والبرمجيات، ووسائط تخزين البيانات والمعلومات، وشبكات الاتصالات، والعنصر البشري،⁽⁴⁾ حيث تطل مخاطر الأمن المادي في بيئة نظم المعلومات المحوسبة مواطن أساسية هي مكونات تلك النظم في أحدث تجلياتها، وتتمثل في:

1. **الأجهزة:** وهي كافة المعدات والأدوات المادية التي تتكون منها النظم كالشاشات والطابعات ومكوناتها الداخلية ووسائط التخزين المادية وغيرها.⁽⁵⁾

2. **البرامج:** حيث تمثل البرامج المستخدمة في تشغيل النظام عُنصر أساسي في نجاح النظام، لذلك لا بد من اختيار البرامج الحديثة صعبة الاختراق، سواء كانت مستقلة عن النظام أو مخزنة فيه.⁽⁶⁾

3. **المعطيات:** وتشمل كافة البيانات المُدخلة والمعلومات المُستخرجة عقب معالجتها، وتمتد بمعناها الواسع للبرمجيات المُخزنة داخل النظام، والمُعطيات قد تكون في طور الإدخال أو الإخراج أو التخزين أو التبادل بين النظم عبر الشبكات.

(1) المري، عليز، (2011)، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها، مرجع سابق، http://www.dralmarri.com/show.asp?field=res_a&id=205

(2) الحميد، محمد دباس & ونيو، ماركو إبراهيم، (2007)، "حماية أنظمة المعلومات"، مرجع سابق، ص 152.

(3) ISO/IEC 27000, (2012), "Information technology - Security techniques - Information security management systems - Overview and vocabulary", OP. Cit., Available at: <http://www.27000.org> (Accessed July 14, 2013).

(4) Mihalache, Arsenie, (2011), "Security of the Accounting Information System Infrastructure", OP. Cit., PP:1339-1345.

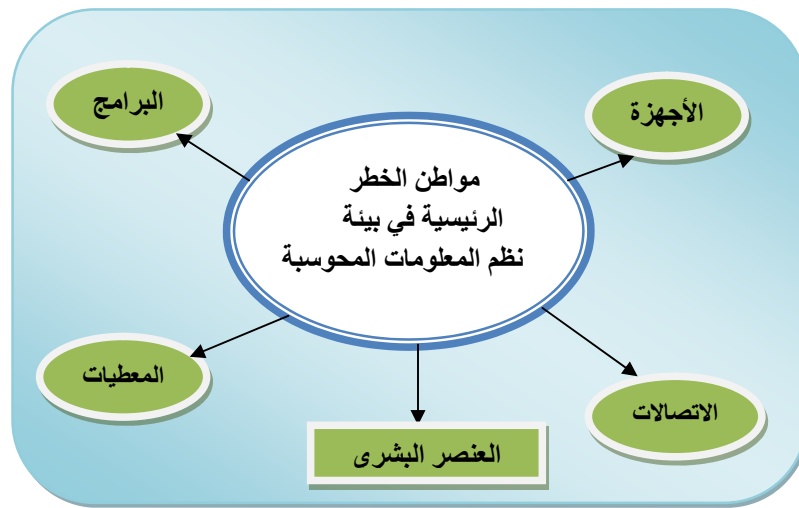
(5) الشبلي، هيثم حمود، (2009)، "إدارة مخاطر الاحتيال في قطاع الاتصالات"، مرجع سابق، ص 212.

(6) النجار، فايز جمعه، (2010)، "نظم المعلومات الإدارية : منظور إداري"، مرجع سابق، ص ص: 264-265.

4. **الاتصالات:** تشمل شبكات الاتصال التي تربط أجهزة ومعدات النظام بعضها ببعضاً محلياً ودولياً، ويمكن اختراق النظم عبرها وهي بذاتها محل للاعتداء وموطن من مواطن الخطر الحقيقي، لذلك لا بد من أن تتمتع الشبكة بكفاءة عالية في الكشف عن وسائل الاختراق المختلفة.⁽¹⁾

5. **الأفراد:** يمثل الإنسان محور الخطر سواء المستخدم أو الشخص المناط به مهام تقنية معينة تتصل بالنظام، فإدراكه لحدود صلاحياته وسلامة الرقابة على أنشطته في حدود احترام حقوقه القانونية، مسائل رئيسية يُعني بها نظام الأمن الشامل في بيئة نظم المعلومات، ويبين الشكل التالي مواطن الخطر الرئيسية في بيئة نظم المعلومات المحوسبة:

شكل رقم (1-2-3) مواطن الخطر الرئيسية في بيئة نظم المعلومات المحوسبة.⁽²⁾



وتحدث مخاطر الأمن المادي للنظم نتيجة حدوث الكوارث الطبيعية كالزلازل والعواصف والفيضانات والأعاصير بالإضافة إلى المشاكل المتعلقة بأعطال نظم التكييف والتبريد والحرائق وغيرها،⁽³⁾ أو نتيجة حدوث أعطال في المعدات وأخطاء المشغلين والتخريب المادي المتعمد، أو عدم توافر الظروف البيئية الملائمة كتعطل الكهرباء، أو تعطل الأجهزة بسبب الرطوبة، والحرارة، والمياه.⁽⁴⁾

ومن أهم أسباب المخاطر التي تهدد الأمن المادي للنظم النار والدخان، وارتفاع أو انخفاض مستوى المياه، حركة الأرض (الزلازل والانهدامات الأرضية والبراكين)، والعواصف (الرياح والبرق والمطر والثلج والصقيع والجليد)، والتخريب، والتفجيرات، وانهدام المباني، وفقدان المرافق (الكهرباء والتدفئة والتبريد

(1) صقر، ممدوح الشحات، (2007)، "أمن المعلومات"، ندوة أمن وحماية نظم المعلومات في المؤسسات العربية، القاهرة، جمهورية مصر العربية، 3-7 يونيو 2007، ص7.

(2) النجار، فايز جمعه، "نظم المعلومات الإدارية: منظور إداري"، مرجع سابق، ص265.

(3) رملي، فياض حمزة، نظم المعلومات المحاسبية المحوسبة - مدخل معاصر لأغراض ترشيده القرارات الإدارية، مرجع سابق، ص110.

(4) الجوهر، كريمة & والعقدة، صالح & أبو سردانة، جمال، (2010)، "أثر مخاطر استخدام التكنولوجيا في جودة عمل المدقق الخارجي دراسة ميدانية في بعض مكاتب التدقيق الأردنية"، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد (10)، العدد (2)، جامعة الزرقاء، الأردن، 2010، ص: 32-14.

والهواء والماء)، وفشل المعدات، وانتشار المواد السامة للأفراد، وفقدان الموظفين ذوي الخبرة والمهارة (المرض، الموت).⁽¹⁾

ومما تقدم يرى الباحث بأن مخاطر الأمن المادي للنظام هي تلك المخاطر التي قد تحدث بسبب الكوارث (الطبيعية أو غير الطبيعية) أو إهمال مستخدمي النظام (بقصد أو بدون قصد) والتي تؤدي إلى سرقة أو تدمير البنية التحتية لنظم المعلومات المحاسبية من أجهزة حاسوب وشبكات اتصال، وبرامج، وملفات بيانات، وأفراد، وتوقفها عن العمل أو تلفها جزئياً أو كلياً، وقد تؤدي إلى تعطل عمل التجهيزات وتوقفها لفترات طويلة، وبالتالي فإنها تؤثر على أمن وسلامة نظم المعلومات المحاسبية المحوسبة، وقد ينتج عنها فشل المنشأة في تقديم الخدمة للعملاء وعدم جاهزية وتوفير الخدمة مما يؤثر سلباً على صورة المنشأة لدى الجهات ذات العلاقة.

1-2-4: المخاطر التي تهدد أمن الوصول البرمجي لقاعدة بيانات نظم المعلومات:

إن التطور التكنولوجي في الاتصال عن بعد سهل عملية الاتصال بنظم المعلومات من أي مكان في العالم وبالتالي أمكن الدخول على البيانات من خلال استخدام أجهزة الحاسوب الموجودة في مواقع بعيدة عن المنشأة، فقد أدى استخدام تكنولوجيا المعلومات إلى تطور نظم المعلومات المحوسبة التي مكنت المستخدمين من الوصول للبيانات من خلال وسائط طرفية، وأصبحت النظم فورية ومباشرة (*On-Line Systems*)، ويمكن الوصول لنظم المعلومات المحاسبية المرتبطة بالإنترنت من أي مكان وفي أي وقت، وتحديث البيانات والتقارير المحاسبية عبر الإدارات الرئيسية وفروعها بشكل فوري في الوقت الحقيقي، ويتم تخزين كافة بيانات المنشأة التي تستخدم تلك النظم في قاعدة بيانات مركزية ويقوم موفر خدمة التشغيل والصيانة بإجراء عمليات النسخ الاحتياطي، وإجراء عمليات التحديث التلقائي لأحدث الإصدارات من تلك النظم.⁽²⁾

ورغم أن الوصول المباشر للبيانات من قبل المستخدمين (موظفين وعملاء)، يحسن من خدمة العملاء ويحسن العمليات الداخلية، وبالرغم من مزايا تلك النظم وإيجابيات العمل المصرفي عبر الإنترنت، إلا أنه يشتمل على مخاطر وسلبات الاستخدام السيئ لمعلومات المنشأة، وعدم توفر عنصر الأمن (الحماية والضمان)، حيث ظهرت أنماطاً جديدة من المخاطر لم تكن موجودة من قبل كمخاطر اختراق نظم المعلومات من قبل أشخاص لا يملكون صلاحية الاطلاع وتعديلها من خلال الوصول غير المصرح به.

ويقصد بالوصول المادي للنظام: القدرة على الوصول إلى المكونات المادية للنظام من أجهزة ومعدات، بينما يقصد بالوصول البرمجي إلى قاعدة البيانات: دخول شخص غير مصرح له (*Unauthorized Access*)

(1) Tayeh, A., (2008), "Effectiveness of Information Security Management at the Palestinian Information Technology Companies", *Master Thesis*, Islamic University of Gaza, Palestinian, P.56.

(2) Greenberg, Robert & Li, Wei & Wong-On-Wing, Bernard, (2012), "The effect of trust in system reliability on the intention to adopt online accounting systems", *International Journal of Accounting and Information Management*, Vol. 20, No. 4, PP: 363-376.

إلى نظام الحاسوب والقيام بأنشطة غير مشروعة كتعديل البرمجيات التطبيقية وسرقة البيانات السرية أو تدمير الملفات أو البرمجيات أو استخدامها بطريقة غير مشروعة.⁽¹⁾

وتعرف نظم قواعد البيانات بأنها مجموعة ملفات مترابطة وظيفياً تدار بصورة مركزية ويؤدي استخدامها إلى تخفيض تكرار البيانات إلى أدنى حد ممكن وتحديث البيانات أولاً بأول، والتي يمكن الوصول إليها بواسطة برنامج أو أكثر من برامج التطبيقات بهدف معالجة البيانات، ويلاحظ أنه في نظام قاعدة البيانات يكون هناك مصدر واحد لإدخال البيانات ومكان وحيد لتخزين كل بند من بنود البيانات وهذا يؤدي إلى تقليل ازدواجية البيانات وكذلك يقضي على عدم التوافق بينها، إن هناك العديد من الأفراد القادرين على اتخاذ قرارات تؤثر في دقة وسلامة البيانات المعطاة وهذا سيزيد من احتمال أن تصبح البيانات غير سليمة أو تستخدم بشكل غير مباشر.

فالحاسوب ليس لديه قدرة على التمييز بين من له الحق في استعماله وتزويده بالمعلومات ومن ليس له الحق بذلك، فهو يستجيب للأوامر الواردة إليه فقط، وبأي وسيلة مرتبطة بالنظام الذي يعمل به، إذ أنه بمجرد أن يتم التعريف على هوية الحاسب الآلي من خلال فك شفرة الدخول أو الاتصال تحت أمر من اتصل به وتنفيذه أو أمره طالما كانت ضمن نطاق مهمته لذلك استطاع المخترقون أن يستخدموا الحاسب لأغراض غير مشروعة فكانت عمليات التلاعب والحصول على البيانات غير المشروعة.⁽²⁾

ومن أهم المخاطر المرتبطة بنظم المعلومات المحوسبة: الوصول غير المرخص إلى قواعد البيانات التي تعمل على تشغيل نظم المعلومات المحاسبية سواء من داخل أو من خارج المنشأة، ودخول غير مصرح به لتسهيلات الحاسوب وبرامجه، واختراق النظام المحاسبي من خلال قنوات الاتصال، وضياع أو تحريف قاعدة البيانات المحاسبية، ووجود بعض المحطات الطرفية في أماكن غير آمنة مما يجعل سرقة المعلومات أو البيانات المالية أمراً سهلاً.⁽³⁾

وتنشأ مخاطر أمن الوصول البرمجي غير المصرح به من إمكانية قيام بعض الأفراد من العاملين الحاليين والسابقين بالمنشأة أو من قرصنة المعلومات المحترفين ولديهم نوايا عدوانية ويمتلكون مهارات خاصة في مجال الحاسوب تمكنهم من إجراء عمليات تلاعب أو تخريب للنظم المستخدمة في المنشأة المستهدفة،⁽⁴⁾ حيث يقوم المخترق بقراءة ملفات التحكم بالنظم ومعرفة نقاط الضعف الموجودة في تلك النظم واستغلالها، للحصول على صلاحيات بطريقة غير مشروعة وهنا يمكن أن يقوم بتنفيذ القيود المالية على حسابات العملاء و/أو الحسابات الوسيطة بتبديل وتعديل المعلومات سواء بالإضافة أو الحذف أو التعديل ودون ترك أي آثار لجريمته

(1) النجار، فايز جمعه، "نظم المعلومات الإدارية: منظور إداري"، مرجع سابق، ص 272.

(2) العبيدي، أسامة، (2012)، "جريمة الدخول غير المشروع إلى النظام المعلوماتي - دراسة قانونية في ضوء القوانين المقارنة"، دراسات المعلومات، العدد (14)، جامعة الإمام محمد بن سعود، الرياض، السعودية، أيار (مايو) 2012، ص: 9-68.

(3) الذبيبة، زياد & الرمحي، نضال & العبيدي، عمر، (2011)، "نظم المعلومات في الرقابة والتدقيق"، مرجع سابق، ص 63.

(4) Jessup, Leonard and Valanch, Joseph, (2008), "Information Systems Today- Managing the Digital World", OP. Cit., P. 232.

كما يمكنه تخريب النظام وإلغاء ملفاته وإتلاف أو سرقة بيانات ومعلومات هامة مثل أرقام بطاقات الائتمان الخاصة بالعملاء، ليحقق منها مكاسب شخصية.⁽¹⁾

1-2-5: المخاطر التي تهدد أمن التخزين غير المتصل بقاعدة بيانات نظم المعلومات المحاسبية:

مخاطر أمن النسخ في وسائط غير متصلة بقاعدة بيانات النظام: هي المخاطر التي تتعرض لها المعلومات في مرحلة التخزين على وسائط خارج النظام، فنظم المعلومات المحوسبة تتضمن كم هائل من البيانات ولذلك فإنه يصعب عمل نسخ ورقية لها، ومن ضمن وسائل حماية البيانات من التلف أو التغيير، القيام بتخزين البيانات أو المعلومات المحاسبية على وسائط تخزين خارجية غير متصلة بنظام المعلومات، وتتأثر تلك الوسائط بعدة عوامل منها:⁽²⁾

1. **الكثافة التخزينية:** وهي عبارة عن عدد الوحدة الرقمية من المعلومات - "البايتات" (Bytes) - الممكن تخزينها على مساحة معينة، وزيادة هذه الكثافة تعني إمكانية تخزين بيانات أكثر.
2. **معدل نقل البيانات:** وهي كمية البيانات التي يمكن نقلها إلى بيئة النظام في الثانية الواحدة.
3. **سرعة الدوران:** كلما كانت سرعة دوران الوحدات أكبر هناك سرعة أكبر في الوصول للبيانات.
4. **السعة التخزينية:** والتي تتمثل في كمية البيانات التي يمكن تخزينها.

وقد جرت دراسة مسحية خلال شهري فبراير ومارس من العام 2013 م بجهد مشترك بين جمعية المحاسبين القانونيين الأمريكيين ونظيرتها الكندية، تبين فيها بأن إدارة البيانات والمعلومات والمحافظة عليها، وكذلك تأمين بيئة تقنية المعلومات من أهم تلك الأولويات حسب شهادة من شملهم الاستطلاع، وذلك يشير إلى جزء من المخاوف والقلق لدى أولئك المحاسبين بشأن زيادة وتعقيد المخاطر الأمنية على تلك البيانات الناجمة عن النمو الهائل في كمية البيانات والمعلومات في جميع أنحاء العالم، وانتشار الأجهزة والوسائط النقالة أو المتحركة وبالتالي إمكانية أكبر لانتهاك سرية تلك البيانات والمعلومات.⁽³⁾

ويرى الباحث بأن مخاطر أمن النسخ في وسائط غير متصلة بقاعدة بيانات النظام هي المخاطر التي تحدث نتيجة عمل نسخ احتياطية من البيانات والبرامج دون حمايتها، وتتمثل أهم تلك المخاطر في:

1. الوصول غير المصرح به للبيانات والبرامج المخزنة في وسائط غير متصلة بنظام المعلومات المحاسبي.
2. ضياع أو سرقة وسائط تخزين البيانات والبرامج الاحتياطية غير المتصلة بقاعدة بيانات نظام المعلومات.

(1) Arens, Alvin A., Elder, Randal J., & Beasley, Mark S., (2014), *Auditing and Assurance Services: An Integrated Approach*, OP. Cit., PP: 740-742.

(2) Deborah & Wen, H. Joseph, (2007), " Reducing the threat levels for Accounting Information Systems Challenges for Management , Accountants, Auditors, and Academicians", *The CPA Journal Publication of the New York state society of CPA*, online , online , May 2007, PP: 34-42.

(3) Drew, Jeef, (2013), Data, security take top two spots in AICPA technology priorities survey: Organizations must know where their critical information is stored, moved, and processed, *journal of accountancy*, AICPA, USA, <http://www.journalofaccountancy.com/News/20137879> (accessed on 13 September 2013).

1-2-6: المخاطر التي تهدد أمن مدخلات نظم المعلومات المحاسبية المحوسبة:

مخاطر تهدد أمن عمليات مدخلات نظم المعلومات المحاسبية: وهي المخاطر التي تتعلق بأول مرحلة من مراحل النظام، وهي مرحلة إدخال البيانات إلى النظام المحاسبي⁽¹⁾، ولا يحتاج مرتكبها إلى مهارات عالية أو معرفة متطورة في الحاسوب، وهي مخاطر يصعب اكتشافها إلا من خلال الفحص المتعمق. ويحدث التلاعب بالمعلومات في أي مرحلة من مراحل تشغيل المعلومات بداية من مرحلة المدخلات وحتى مرحلة المخرجات، ويعد التلاعب في مرحلة المدخلات هو الأكثر شيوعاً نظراً لسهولة إنجازه فهو لا يتطلب مهارات عالية في الكمبيوتر، كما أنه من الصعب اكتشافه⁽²⁾. وبالرغم من استخدام مصطلح الغش أكثر من مصطلح الاحتيال (*Fraud*) في الأدبيات المالية والمحاسبية إلا أن معناهما يكاد يكون واحداً، وتتم في الحقيقة بعشرات الأنماط والأساليب التقنية، الجامع المشترك لهما هو المساس بأمن وحماية مرحلة إدخال البيانات، بهدف الخداع واختلاس الأصول⁽³⁾. وفي هذا الصدد يجب أن نميز بين الأخطاء والغش في ظل النظم المحوسبة، فقد يتفق الخطأ مع الغش في أن كل منهما يؤدي إلى تحريف أو حذف ولكن الخطأ يختلف عن الغش فالخطأ تحريف أو حذف غير متعمد بينما الغش تحريف أو حذف متعمد فمعياري التمييز هنا هي نية المرتكب أو إرادته، وهذا صعب معرفته في معظم الأحوال. وترجع الأخطاء في مرحلة المدخلات بشكل عام إلى عدم تغذية الحاسوب بشكل سليم، وتزيد احتمالات حدوث الخطأ في حالة تطبيق نظم التشغيل الفورية المباشرة، حيث أن تسجيل البيانات وتشغيلها يتم بشكل متزامن، وما لم يكن هناك برامج كافية وفعالة للتحقق من المدخلات (البيانات) لتحديد صلاحيتها قبل تشغيلها فإن احتمالات الخطأ تتزايد نتيجة لقبول النظام لبيانات باعتبارها مدخلات صحيحة بينما هي عكس ذلك، ومن ثم خضوعها للتشغيل لحين اكتشاف الخطأ فيما بعد وتصحيحه.

1-2-7: المخاطر التي تهدد أمن عمليات تشغيل نظم المعلومات المحاسبية المحوسبة:

وتتعلق هذه المخاطر بالمرحلة الثانية من مراحل عمل النظام وهي مرحلة تشغيل ومعالجة البيانات المخزنة في ذاكرة الحاسوب⁽⁴⁾، ويشير مفهوم المخاطر التشغيلية (*Operational Risks*) بشكل عام إلى مخاطر الناتجة عن العمليات الداخلية الخاطئة أو الفاشلة وكذلك مخاطر الأفراد والنظم إلى جانب الحوادث الخارجية والتي تؤدي في مجملها إلى وقوع خسائر للمنشأة⁽⁵⁾، وهي المخاطر التي تنتج من احتمالات الخسارة الناتجة عن

(1) الذبيبة، زياد & الرمحي، نضال & الجعدي، عمر، "نظم المعلومات في الرقابة والتدقيق"، مرجع سابق، ص 65.
 (2) عيسى، علا & وعاشور، عصافيت، (2010)، "مخاطر نظم المعلومات المحاسبية وحوكمة المنشآت ومواجهة الأزمة المالية العالمية"، مرجع سابق، ص: 408-434.
 (3) Hall, James A., (2013), *Accounting Information Systems*, OP. Cit., P.97.
 (4) الذبيبة، زياد & الرمحي، نضال & الجعدي، عمر، "نظم المعلومات في الرقابة والتدقيق"، مرجع سابق، ص 65.
 (5) القطناني، خالد محمود، "أثر خصائص البيئة التقنية وتكنولوجيا المعلومات في مخاطر الرقابة التشغيلية- دراسة تحليلية في المصارف الأردنية"، *مجلة المنارة*، المجلد (13)، العدد (2)، جامعة آل البيت، المفرق، الأردن، 2007، ص: 39-9.

خلل في شمولية النظام أو من أخطاء العملاء أو من برنامج إلكتروني غير ملائم للصيرفة والأموال الإلكترونية،⁽¹⁾ أفضل تعريف للمخاطر التشغيلية في رأي الباحث هو التعريف الصادر عن لجنة بازل للرقابة المصرفية ضمن اتفاق بازل II الذي عرفها على أنها "مخاطر تحمل خسائر ناجمة عن فشل العمليات الداخلية، والموارد البشرية العاملة في المنشأة، وضعف نظم الرقابة الداخلية وكذلك الأحداث الخارجية."⁽²⁾

من هنا يرى الباحث أن مخاطر أمن عمليات تشغيل نظم المعلومات المحاسبية المحوسبة: هي المخاطر التي تتعلق بمرحلة تشغيل ومعالجة البيانات المخزنة في ذاكرة النظام، ومن تلك المخاطر:

1. إهدار وسرقة وقت تشغيل بعض أجهزة الحاسوب المستخدمة في نظام المعلومات المحاسبي من خلال استغلالها في الأغراض الشخصية.
2. تعديل أو حذف البيانات بطريقة مقصودة نتيجة حدوث احتيال وغش من قبل مستخدم نظام المعلومات المحاسبي أثناء عمليات التشغيل.
3. تعديل أو حذف البيانات بطريقة غير مقصودة نتيجة حدوث أخطاء من قبل مستخدم نظام المعلومات المحاسبي أثناء عمليات التشغيل.
4. حدوث عمليات تشغيلية غير مكتملة لبيانات محاسبية تم إدخالها.

1-2-8: المخاطر التي تهدد أمن مخرجات نظم المعلومات المحاسبية المحوسبة:

وتتعلق تلك المخاطر بمرحلة مخرجات نظام المعلومات المحاسبية المحوسبة - سواء عند إخراجها أو بعد ظهورها واستلامها - وما يصدر عنها من قوائم وتقارير وأشرطة ملفات ممغنطة وكيفية استلام تلك المخرجات.⁽³⁾

وتتمثل في سرقة مخرجات الحاسوب أو إساءة استخدامها أو توجيهها إلى أشخاص غير مصرح لهم باستلامها أو الاطلاع عليها نظراً لسريتها أو لأن هؤلاء الأشخاص غير مخولين بالاطلاع عليها أو استلام نسخة منها،⁽⁴⁾ كما تتمثل تلك المخاطر في طمس أو تدمير بنود معينة من المخرجات، وإنتاج مخرجات زائفة أو غير صحيحة، وعمل نسخ غير مصرح بها من المخرجات، والكشف غير المصرح به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق، وتسليم المستندات الحساسة إلى أشخاص لا تتوفر فيهم الناحية الأمنية بغرض تمزيقها أو التلخيص منها.⁽⁵⁾

(1) وادي، رشدي عبد اللطيف، (2008)، "أهمية ومزايا البنوك الإلكترونية في قطاع غزة بفلسطين ومعوقات انتشارها"، مجلة الجامعة الإسلامية - سلسلة الدراسات الإنسانية، مجلد (16)، العدد (2)، غزة، فلسطين، يونيو 2008، ص ص: 855-893.

(2) NĂSTASE, Pavel & UNCHIAȘU, Simona, (2013), "Implications of the Operational Risk Practices Applied in the Banking Sector on the Information Systems Area", Accounting and Management Information Systems, Vol. 12, No. 1, 2013, PP: 101-117.

(3) الذبيبة، زياد & الرمحي، نضال & الجعدي، عمر، (2011)، "نظم المعلومات في الرقابة والتدقيق"، مرجع سابق، ص 66.

(4) Abu-Musa, Ahmad A., (2006), "Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations", King Saud University Journal, Vol. 18, Computer and Information Science, Riyadh, Saudi Arabia, 2006, PP: 1-26.

(5) الذبيبة، زياد & الرمحي، نضال & الجعدي، عمر، (2011)، "نظم المعلومات في الرقابة والتدقيق"، مرجع سابق، ص 66.

من هنا يرى الباحث بأن المخاطر التي تهدد أمن مخرجات نظم المعلومات المحاسبية المحوسبة هي المخاطر التي تتعلق بمرحلة مخرجات النظام، وما يصدر عنها من قوائم مالية وتقارير، وكيفية استلام تلك المخرجات، وتتمثل أهم تلك المخاطر في البنود التالية:

1. حذف وإخفاء بنود معينة من مخرجات نظام المعلومات المحاسبي وإنتاج مخرجات مظلمة غير سليمة.
 2. الكشف غير المخول به للمعلومات المحاسبية أثناء عرضها على الشاشات أو طباعتها على الورق أو أثناء التخلص منها بعد استخدامها.
 3. توجيه وتوزيع وتسليم بعض البيانات والمعلومات المحاسبية لأشخاص غير مخولين باستلام نسخة منها أو لا تتوفر فيهم الأمانة.
 4. سرقة وسوء استخدام مخرجات النظام (المعلومات المحاسبية) من قبل القائمين على النظام واستغلالها في أغراض شخصية.
- وتنتج تلك المخاطر من خلال قيام بعض الأفراد من داخل أو خارج المنشأة بالكشف عن المعلومات السرية للمنشأة لجهات منافسة، إما بشكل مطبوع ورقياً، أو منسوخ إلكترونياً على وسائط الكترونية، وذلك بدون التحويل الشرعي من إدارة المنشأة، أو القائمين على نظم المعلومات المحوسبة، والهدف من ذلك التهرب تحقيق أغراض شخصية،⁽¹⁾ والسطو على المعلومات المخزنة قد ينجم عنه حرمان مالك المعلومات من الوصول إليها إذا كانت النسخة المسروقة هي النسخة الوحيدة.⁽²⁾

1-2-9: المخاطر التي تهدد أمن تبادل البيانات عبر شبكات الاتصال في نظم المعلومات المحاسبية:

شهدت الفترة الأخيرة تحولاً سريعاً من الشكل التقليدي للعمليات التجارية إلى الشكل الإلكتروني، حيث تلعب نظم المعلومات المحاسبية الإلكترونية دوراً رئيسياً في تنفيذ أعمال التجارة بشكلها المعاصر، واتجهت العديد من المنشآت التجارية في بيئة الأعمال اليمينية لاستخدام نظم المعلومات المحاسبية المحوسبة وأيضاً إنشاء مواقع لها على شبكة الانترنت لعدة أهداف أهمها مباشرة التجارة الإلكترونية العادية (سلعية أو خدمية) والتحاسب عنها إلكترونياً.

يعرف الاتصال في مجال نظم المعلومات بأنها كافة الأنشطة والوسائل المتعلقة بنقل وتبادل البيانات والمعلومات إلكترونياً من خلال الأجهزة والبرامج والوسائط والتقنيات التي تربط بين الحاسبات وبعضها، وتتخذ عملية الربط شكل شبكة يطلق عليها شبكات الحاسوب، والهدف الرئيسي من شبكات المعلومات هو عمليات تبادل المعلومات والبيانات بين الأطراف المختلفة في سهولة ويسر وفي أسرع وقت ممكن،⁽³⁾ وشبكة الحاسوب هي مجموعة من الحواسيب (اثنتان أو أكثر) لها القدرة على تبادل البيانات فيما بينها

(1) Abu-Musa, Ahmad A., (2006), "Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations", *OP. Cit.*, PP: 1-26.

(2) الغنير، خالد سليمان، & القحطاني، محمد عبدالله، (2009)، أمن المعلومات بلغة ميسرة، مرجع سابق، ص13.

(3) حسنين، رجب عبد الحميد، (2012)، "أمن شبكات المعلومات الإلكترونية: المخاطر والحلول"، مرجع سابق، متاح في:

http://www.journal.cybrarians.org/index.php?option=com_content&view=article&id=629:networks&catid=257:studies

بواسطة خطوط اتصال تربطها مع بعضها البعض أو من خلال ربط عدد من الوحدات الطرفية مع حاسوب مركزي.⁽¹⁾

ويقصد بالتبادل الإلكتروني للبيانات (EDI) تبادل البيانات من مستندات وغيرها من حاسوب إلى حاسوب في صورة بنىوية منظمة وبما يكفل التجهيز المباشر لتلك الوثائق الالكترونية من قبل نظام الحاسوب المستقبل لها، ويعتبر التبادل الإلكتروني للبيانات أحد أهم التطورات التكنولوجية التي حدثت في مجال الحاسوب والاتصالات والتي أدت إلى السرعة والدقة في نقل البيانات والرقابة عليها، واستبعاد الاعتماد على الأوراق في مختلف تطبيقات نظم المعلومات.⁽²⁾

لقد كان المبدأ السائد في توزيع وظائف نظم المعلومات المحاسبية هو النظر إلى كل وظيفة من وظائف النظام على أساس أنها وحدة عمل مستقلة ويتم إسنادها إلى حاسوب محدد ضمن الشبكة، أما اليوم فقد تطورت أساليب التوزيع والربط حتى تم الوصول إلى ربط حواسيب الشبكة ببعضها وظهرت بالنسبة للمستخدم وكأنها حاسب واحد، وأصبحت الآن في الأنظمة المترابطة والمتمثلة في نظم تخطيط موارد المنشأة تقوم على تكنولوجيا متقدمة جداً متمثلة في التبادل الإلكتروني للبيانات بما فيها شبكة الانترنت، وعليه أصبحت الشبكات الإلكترونية جزءاً من مكونات نظم المعلومات المحاسبية وبالتالي فإن دراسة شبكة الاتصالات وكيفية عملها والمخاطر التي تتعرض لها وكيفية مواجهة تلك المخاطر تعتبر من الجوانب الأساسية التي على المحاسبين والمراجعين معرفتها.⁽³⁾

والإنترنت هي عبارة عن شبكة دولية واسعة النطاق مؤلفة من مئات الملايين من أجهزة الحاسوب المتصلة مع بعضها البعض والمنتشرة في جميع أنحاء العالم عن طريق خطوط الاتصال و الأقمار الصناعية وخطوط الهاتف حيث تشكل هذه الأجهزة شبكة ضخمة (شبكة الشبكات) من الأجهزة المتصلة معاً لتبادل المعلومات فيما بينها، وتضم بداخلها مجموعة شبكات خاصة وعامة،⁽⁴⁾ وهذه الشبكة تقدم البنية الأساسية للربط والتواصل بين الحواسيب في مختلف المجالات على مستوى العالم، والإنترنت تزداد وتكبر يوماً بعد يوم حيث نرى الآن أغلبية المنشآت والأفراد على مستوى العالم متصل بالإنترنت ويقوم جزئياً أو كلياً بإعماله التجارية وإدارتها عبر الانترنت.

وأصبحت التكنولوجيا المرتبطة بالإنترنت مثار إعجاب من قبل العديد من المنشآت، والتي قامت بتبنيها لأغراض التواصل الداخلي عبر شبكاتها المحلية الخاصة، وأدى ذلك إلى ظهور انترنت داخلي وهو ما يعرف بالإنترانت (Intranet)، وهي شبكة تستخدم في ربط قواعد البيانات الداخلية للمنشأة بنظام لا يتم الدخول إليه إلا من خلال المتصفح أو من برنامج يصمم داخلياً، والانترانت غير متاحة للأطراف الخارجية

(1) الشبلي، هيثم حمود، (2009)، "إدارة مخاطر الاحتيال في قطاع الاتصالات"، مرجع سابق، ص 91.

(2) حجر، عبد الملك إسماعيل، (2009)، "نظم المعلومات المحاسبية"، مرجع سابق، ص 292.

(3) حجر، عبد الملك إسماعيل، (2009)، "نفس المرجع السابق"، ص 18.

(4) طه، طارق، (2007)، "نظم المعلومات والحاسبات الآلية والانترنت"، دار الفكر الجامعي، الإسكندرية، مصر، 2007، ص 462.

إلا إذا تم منحهم صلاحية بذلك، ونتيجة ظهور الإنترنت والإنترنت بدأت الكثير من المنشآت السماح لأنظمة عملاتها وغيرهم من الدخول أو الوصول إلى الإنترنت الخاص بالمنشأة، وهذا ما يسمى بالإكسترنانت (*Extranet*) والذي يظهر عندما يتم ربط الشبكات المحلية لجهتين أو أكثر معاً،⁽¹⁾ حيث أن شبكة الإكسترنانت هي شبكة محلية تربط المنشأة مع الأطراف الخارجية لتبادل المعلومات من خلال استخدام الإنترنت، فهي شبكة حاسوب تستخدم تقنيات الإنترنت في ربط المسؤولين داخل المنشأة بأطراف خارجية مثل كبار العملاء ومسؤولي المنظمات الأخرى، ويعتبر التطور في الإنترنت والإنترنت والإكسترنانت بمثابة الأداة الرئيسية للأعمال الإلكترونية (*E-Business*) والتي تتطلب التبادل الإلكتروني للبيانات.

وباستخدام الحاسوب وشبكة الاتصالات الحديثة يتم تجهيز البيانات إما وفقاً لنظام المجموعات أو وفقاً لطريقة التجهيز المباشر على أساس الوقت الحقيقي، وبالتالي يجب معرفة كيفية تجهيز البيانات في هذه البيئة الحديثة التي تعتمد على التبادل الإلكتروني للبيانات.⁽²⁾

ويعد نظم الاتصال الفوري المباشر في معالجة البيانات إلكترونياً من أحدث النظم المستخدمة في نظم المعلومات المحاسبية، ويتكون نظام الاتصال الفوري المباشر من محطات الاتصال الفرعية المنتشرة في أنحاء المنشأة المختلفة الموصلة مباشرة بالوحدة المركزية لمعالجة البيانات، ومن هذه النظم محطات الاتصال المختلفة التي تستخدمها البنوك، ونظام حجز مقاعد الطائرات في شركات الطيران، ويعني الاتصال المباشر (*On Line*) تكامل شبكة الاتصال بين كافة أجهزة ومعدات الحاسوب واتصالها مباشرة بالوحدة المركزية لمعالجة البيانات (*CPU*)، أما صفة الفورية (*Real Time*) فتعني أنه يتم معالجة البيانات في نفس وقت إدخالها، ونتيجة لذلك يمكن لمستخدم النظام الحصول على المخرجات فور الانتهاء من إدخال البيانات مباشرة.

ومع التطور التقني الذي نعيشه وتسارعه، أصبح الأمر أكثر إلحاحاً من أي وقت مضى لاستخدام الأجهزة التقنية وتبادل المعلومات عن طريق الإنترنت واللجوء إلى حفظ هذه البيانات و تخزينها إلكترونياً، وبذلك يكون هذا التطور سبباً مهماً في تسهيل الحاجة لحفظ هذه المعلومات وإمكانية استردادها، كما أصبح ذات السبب يشكل خطراً حقيقياً في وجه أمن وسلامة تلك المعلومات،⁽³⁾ وقد أدركت المنشآت المالية - بما فيها البنوك - بأن هذه الفوائد والخدمات التي تتيحها الإنترنت يقابلها سلبيات ومخاطر عديدة أنجر عنها ظهور جرائم جديدة، تحول دون تحقيق الفوائد والمقاصد التي من أجلها تم تطوير تلك التقنيات

(1) حجر، عبد الملك إسماعيل، (2009)، "نظم المعلومات المحاسبية"، مرجع سابق، ص 283.

(2) حجر، عبد الملك إسماعيل، (2009)، "نفس المرجع السابق"، ص 19.

(3) بن يحيى، عماد، (2012)، الهجمات الإلكترونية كأكبر المخاطر التي تهدد قطاع الأعمال، عالم التقنية، من الموقع :

<http://www.tech-wd.com/wd/2012/09/08/kaspersky-global-it-security-risks-survey-report/>

ونظم المعلومات،⁽¹⁾ حيث أدى التطور والتوسع في استخدام شبكة المعلومات الدولية (الانترنت) وتقنياتها الحديثة في مجال تبادل السلع والخدمات إلى خلق المزيد من التحديات والمخاطر التي تواجه نظم الرقابة على نظم المعلومات،⁽²⁾ حيث تعتبر أنظمة تبادل المعلومات الكترونياً والمعتمدة على الانترنت أكثر سهولة في الاستخدام وأكثر قدرة على التفاعل مع المستخدم وتتاح لمدى واسع من المستخدمين وتوفر فرص كبيرة للمنشآت لزيادة قاعدة عملائها وبيع خدماتها عالمياً وبتكلفة أقل، إلا أنها من ناحية أخرى تتصف بأنها أقل أمناً من الشبكات الخاصة،⁽³⁾ فكل تكنولوجيا حديثة ورغم إيجابياتها الكثيرة إلا أن سلبياتها كثيرة كذلك، وفي حالة عدم التمكن من تحجيم تلك السلبيات والسيطرة عليها، ستكون النتائج مخيبة للآمال وقد يتم الإحجام عن هذه التكنولوجيا الحديثة وبالتالي تضيق أرباح وفوائد جمة.

ومن المخاطر التي تتعرض لها أمن شبكات نظام المعلومات خطر الدبلجة (*Fabrication*) ويحدث عندما يقوم مرسل ثالث بفبركة رسالة ثم يقوم بإرسالها بحيث يُنظر إليها وكأنها من المصدر الشرعي،⁽⁴⁾ ووصول المعلومات مبدلة أو مغيرة بسبب فعل فاعل (ثغرة في التوقيعات الإلكترونية أو نظام التوثيق) أو اختراق في الشبكة (ثغرة في الدخول للنظام).⁽⁵⁾

ويرى الباحث أنه طالما وجدت معلومات مخزنة في أجهزة الحاسوب وهناك شبكة معلومات، فلا بد من وجود مخاطر ومهددات، وتتفاقم حجم هذه المخاطر وتتنوع مصادرها بدرجة الاعتماد على التقنية وعلى مدى انفتاح المنشأة على العالم الخارجي أو انغلاقها، حيث تتدرج المخاطر والمشاكل التي تتعرض لها نظم المعلومات المحاسبية، تبعاً للتطور التقني فإذا تطورت نظم العمل والشبكات المستخدمة سواء كانت شبكات محلية أو إقليمية أو عالمية يزيد وينقص تبعاً لذلك نوع وطريقة ونسبة المخاطر، فالنظم التي تستخدم فيها الشبكات العالمية الإنترنت تتعرض لمخاطر الاختراق بصورة كبيرة وجوهرية، وهكذا نجد أن العلاقة طردية بين المخاطر والانتشار الشبكي للنظام المعني.

ومن الأمثلة العملية لحدوث ذلك الخطر قام موظف بإحدى المنشآت الروسية باختراق شبكة المعلومات الخاصة بالمنشأة، وقام بتعديل راتبه الشهري ومجموعة من زملائه بزيادة الرواتب بنسبة معينة مما أدى بخسائر مالية للمنشأة لعدة شهور لعدم اكتشاف هذا الاختراق،⁽⁶⁾ وهناك العديد من الحالات الأخرى مثل اختراق شبكة معلومات وزارة الدفاع الأمريكي الذي حدث مرات عديدة في السنوات الأخيرة، ويمكن أن نرى مدى الخسائر التي تمثلها مثل هذه الاختراقات الأمنية لشبكات المعلومات، سواء كانت هذه الخسائر

(1) زيدان، محمد & حمود، محمد، (2010)، "متطلبات أمن المعلومات المصرفية في بيئة الانترنت"، المؤتمر السادس لجمعية المكتبات السعودية "البيئة المعلوماتية"

الأمن: المفاهيم والتشريعات والتطبيقات"، عمان، الرياض، السعودية، 6-7 نيسان (أبريل) 2010 م.

(2) Arens, Alvin A., Elder, Randal J., & Beasley, Mark S., (2014), *Auditing and Assurance Services: An Integrated Approach*, OP. Cit., PP: 740-742.

(3) Koskosas, Ioannis & Koskosa, Maria-Mirela, (2011), "Internet Banking Security Management through Trust Management", *World of Computer Science and Information Technology Journal (WCSIT)*, Vol. 1, No. 3, 79-87.

(4) النجار، فايز جمعه، (2010)، "نظم المعلومات الإدارية: منظور إداري"، مرجع سابق، ص 273.

(5) الحاج علي، عوض & وحسين، عبد الأمير، (2005)، أمنية نظم المعلومات وتقنيات التشفير، مرجع سابق، ص 69.

(6) حسنين، رجب عبد الحميد، (2012)، "أمن شبكات المعلومات الإلكترونية: المخاطر والحلول"، مرجع سابق، متاح في:

http://www.journal.cybrarians.org/index.php?option=com_content&view=article&id=629:networks&catid=257:studies

مالية كما في حالة المنشآت التجارية والخدمية، أو خسائر معلوماتية واستخباراتية لا تقدر بمال ويمكن أن تمس باستقلال بلدان كبيرة مثل أمريكا، ومن هنا يتضح الأهمية القصوى لعمليات تأمين شبكات المعلومات. **وعليه فإن الباحث يرى أن المخاطر التي تهدد أمن تبادل البيانات عبر شبكات الاتصال هي تلك المخاطر التي تحدث أثناء إرسال واستلام البيانات المنقولة عبر الشبكات الداخلية (كالإنترنت، والإكسترنات)، أو عبر الشبكات الخارجية (مثل شبكة الإنترنت)، وتتمثل تلك المخاطر في:**

1. انقطاع وتوقف تدفق البيانات والمعلومات المحولة إلكترونياً عبر شبكات الحاسوب من المركز الرئيسي للبنك إلى الفروع أو العكس.
2. اعتراض وصول البيانات المرسله عبر الشبكات من أجهزة الخوادم لأجهزة المستخدمين، وتعرضها أحياناً للكشف أو التعديل، أو السرقة.
3. اختراق مواقع الويب الخاص ببيانات البنك والتجسس على خطوط الاتصالات الخاصة بنقل البيانات.
4. إنكار بعض الأطراف المتعاملة مع البنك للبيانات والمعلومات المحاسبية المتبادلة إلكترونياً.
5. حدوث أخطاء غير مقصودة أثناء نقل البيانات كإرسال بيانات أو معلومات عن طريق الخطأ إلى موقع آخر.

10-5-1: المخاطر التي تهدد أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة:

وتتمثل مراحل تطور نظم المعلومات في خمسة مراحل هي التخطيط والتحليل والتصميم والتنفيذ والدعم، وتخضع نظم المعلومات المحاسبية للتطوير بشكل دائم ودوري ابتداءً من التغيرات الهامشية وانتهاءً بالتغيرات الأساسية، وإذا كانت هذه التغيرات كبيرة تقوم المنشأة باستبدال نظامها القديم بنظام جديد.

وتتجه بعض المنشآت إلى اقتناء برمجيات نظم المعلومات عبر تطوير نظمها من خلال حزم برامج التطبيقات التي تقدمها شركات البرمجيات الكبرى والمتخصصة في إيجاد الحلول لتطوير نظم المعلومات المختلفة في كافة الميادين، والمشكلة هنا أن الأسرار الاقتصادية والتجارية والتكنولوجية قد تتسرب إلى المنافسين بسبب الاعتماد على مصادر خارجية في تطوير نظم المعلومات وبخاصة إذا كانت هذه النظم موجهة نحو هدف اكتساب أو امتلاك الميزة التنافسية المستدامة.

فعلى سبيل المثال يمكن إعطاء أوامر للبرنامج بعدم تسجيل قيود معينة في السجلات المالية، وقد يكون ذلك بهدف تحريف البيانات المخزنة في النظام أو تدميرها، أو الاطلاع عليها بدون الحصول على ترخيص مسبق بذلك، أو نسخ واستخدام تلك البيانات بطريقة غير مشروعة.

وعليه يمكن للباحث تعريف مخاطر أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة بأنها تلك المخاطر التي تحدث نتيجة تطوير النظام أو تغيير البرامج وتتمثل في إجراء تغييرات غير مسموح بها، وغير

معتمدة لبرامج النظام المرخصة، من قبل أشخاص غير مخولين بذلك، بإمكان تلك التغييرات إتاحة عمليات تلاعب واحتيال في وقت لاحق، كما تتضمن تمكين المبرمجين في المنشأة من التعامل مع عمليات إدخال البيانات وتشغيلها، وتشمل تلك المخاطر أخطاء في عدم استكمال التعديلات المطلوبة أثناء عمليات التعديل والتطوير، وكذلك فشل المنشأة في تطوير وتحديث النظم والبرامج، وتتمثل أهم تلك المخاطر في حدوث الخطرين التاليين:

1. إجراء تغييرات للنظام وبرامجه بطريقة غير مسموح بها، من قبل أشخاص غير مخولين بذلك، للقيام بعمليات تلاعب واحتيال لاحقة.
2. حدوث أخطاء في عدم استكمال التعديلات المطلوبة أثناء عمليات التعديل والتطوير.

خاتمة المبحث: مما سبق ندرك مدى المخاطر المحدقة بأمن نظم المعلومات المحاسبية، ومدى

الحاجة إلى وجود نظام متكامل للتخفيف من تلك المخاطر وإدارتها لذلك يتعين أن تقوم إدارة المخاطر في أي منشأة بتقييم تلك المخاطر ويكون ذلك من خلال أنظمة داخلية متطورة تعتمد على قاعدة بيانات تتيح إمكانية قياس المخاطر وتحديد لها لكل نوع من أنواع النشاط المختلفة.

وأياً كانت أنواع المخاطر الخاصة بأمن نظم المعلومات المحاسبية المحوسبة، فإنه يتطلب من المنشآت أو الوحدات أو الجهات محل الرقابة تقييم وتحليل تلك المخاطر وما يتعلق بها خصوصاً في مجال: تحديد تلك المخاطر ودرجة أهميتها، وبيان التهديدات الداخلية والخارجية التي تسببت فيها، وبيان حجم تأثير تلك المخاطر على أمن نظم المعلومات المحاسبية، وأخيراً على ضوء ذلك يتم تحديد إجراءات ووسائل الحماية المتبعة للتخفيف أو الحد من تلك المخاطر، وهذا ما سوف نتطرق له في الفصل الثاني من هذه الأطروحة.

3-1: المبحث الثالث: التهديدات الداخلية لأمن نظم المعلومات المحاسبية الموحدة

عرفنا من قبل أن تهديدات أمن نظم المعلومات المحاسبية هي الأحداث والأشخاص والتصرفات المحتملة غير المرغوب فيها والتي يمكن أن تؤدي إلى حدوث مخاطر تحمل تأثيراً سلبياً ومضراً على عناصر ومكونات تلك النظم ومن شأنه أن يسهم في العبث والتدمير أو انقطاع الخدمة، وتؤدي إلى خسارة.

يجب تشخيص المخاطر وتحليلها ومعرفة العوامل الخارجية والداخلية لحدوثها، وجميع ما سبق طرحه في المبحث الثاني من المخاطر التي تهدد أمن نظم المعلومات، ناتجة عن أسباب عديدة، إدارية وإجرائية وفنية (تقنية)، وهذه الأسباب هي المكان الحقيقية والأساسية للمخاطر التي تواجهها نظم المعلومات في المنشآت بصفة عامة وفي القطاع المصرفي بصفة خاصة، وإذا كان ينبغي حماية موارد نظم المعلومات علينا أن نعرف مصادر تلك المخاطر أو التهديدات المسببة لها.⁽¹⁾

وتنشأ تلك المخاطر بسبب التطورات التكنولوجية المتسارعة، والمشكلات الفنية المتزايدة، والأخطاء الكامنة، والأحداث البيئية المتغيرة، والضعف البشري وعدم ملائمة المنشآت للمتغيرات المتلاحقة، وسوء استخدام الأجهزة، وهجمات القرصنة، والفيروسات والبرمجيات الخبيثة، وعدم توافق البرمجيات في بيئة الموردين المتعددة حيث لا توجد للآن مقاييس موحدة ذات طابع دولي.⁽²⁾

وهناك ضرورة كبيرة لدراسة وتحليل القضايا والجوانب غير التكنولوجية التي تتعلق وترتبط بإدارة أمن المعلومات في الدول النامية، وقد أشارت دراسات كثيرة إلى وجود نقص واضح في الاهتمام بالعوامل التي تؤثر في الاتجاهات نحو إدارة أمن المعلومات، ومن هذه العوامل التي ينبغي أن تعطى اهتماماً أكبر في البحث والتحليل: الثقافة التنظيمية والثقافة السائدة على مستوى الدولة (الثقافة الوطنية) والعوامل المختلفة للبيئة الداخلية والخارجية ومستويات فهم وإدراك التأثيرات المختلفة لهذه العناصر.⁽³⁾

إن التهديد (*Threat*) هو مصدر من مصادر الضرر المحتمل الذي قد ينشأ عنه مخاطر أمنية تؤثر تأثيراً سلبياً على أصول نظم المعلومات، وقد اهتمت العديد من الدراسات بتوضيح التهديدات التي يتعرض لها أمن نظم المعلومات المحاسبية في ظل البيئة الالكترونية، ولكنها تباينت في تحديد طبيعة تلك التهديدات وعددها وتصنيفاتها.⁽⁴⁾

والتهديد هو السبب المحتمل لغير المرغوب فيها تأثير على نظام أو منشأة، وهو السبب المباشر الذي أدى إلى وقوع الخطر، وبالتالي فإن التهديدات هي العوامل الداخلية والخارجية (العرضية أو المتعمدة) التي يمكن أن تسبب أنواع

(1) Gerić, Sandro & Hutinski, Željko, (2007), Information System Security Threats Classifications, *Journal of Information and Organizational Sciences*, Vol 31, No 1, University of Zagreb, Croatia, PP: 59-60.

(2) Werlinger, R. & Hawkey, K. & Beznosov, K. (2009), "An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management", *Information Management & Computer Security*, Vol. 17, No.1, PP: 4-19.

(3) أبو فارة، يوسف، (2009)، "دور إدارة أمن المعلومات في فاعلية الحكومة الالكترونية"، *مؤتمر أمن المعلومات والحكومة الإلكترونية*، كوالالمبور، ماليزيا، 12 - 16 ابريل (نيسان) 2009 م، ص14.

(4) Černá, Marie, (2012), "Information Risks and Their Connection With Accounting", *OP. Cit.*, PP: 375-382.

مختلفة من الأضرار التي تلحق بالمعلومات، وتؤثر على سريتها وسلامتها أو على عدم الاتصال من المعلومات و تؤدي في نهاية المطاف إلى خسائر كبيرة.⁽¹⁾

فالتحديات هي الأسباب والمؤشرات الأساسية للمخاطر التي يواجهها أمن نظم المعلومات، ويمكن أن يؤدي إلى احتمالات الكشف أو التعديل أو التدمير، أو الحرمان من استخدام نظم المعلومات، وتحليل التهديد الشامل هو جزء من عملية تقييم المخاطر الشاملة وهو متطلب سابق لأمن المعلومات الشاملة، وبالتالي فإن تقييم التهديد هو مكون رئيسي وخطوة أساسية من تقييم المخاطر الأمنية لنظم المعلومات من أجل وضع برنامج الأمان الذي يحمي بشكل صحيح البيانات الهامة، وموارد النظم، وغيرها من الموارد.⁽²⁾

تقييم التهديدات لأمن المعلومات في المؤسسات المالية هو عنصر أساسي لتقييم المخاطر أمن المعلومات، فمن أجل تحديد أولويات نقاط الضعف لمعالجتها وتقييم الضوابط القائمة، لا بد من فهم دقيق لإمكانات مطلوب مصادر التهديد، ولا سيما بالنسبة للمؤسسات المالية، وهذا النشاط هو متطلب سابق لبرنامج أمن معلومات شاملة والمتطلبات التنظيمية المعلنة، فعندما نعرف التهديدات التي تواجه أصول المعلومات لدينا والخسائر المحتملة، يمكننا أن نبدأ في بناء دفاعات أكثر فعالية باستخدام منهجيات واضحة المعالم لإدارة المخاطر، فمعرفة العدو وفهم الآليات التي يستخدمها هي الخطوة الأولى نحو إيجاد حل لهذه المشكلة.⁽³⁾

والتهديدات الأمنية لنظم المعلومات المحاسبية المحوسبة (CAIS) يمكن تصنيفها وفقاً لمصدرها إلى تهديدات داخلية وتهديدات خارجية⁽⁴⁾، ويمكن تصنيفها إلى أربعة أبعاد هي تهديدات داخلية (سواء البشرية وغير البشرية)، وتلك التهديدات الخارجية (البشرية و غير البشرية).⁽⁵⁾

إن الاعتقاد السائد بأن مخاطر أمن نظم المعلومات تأتي في الأصل من خارج المنشأة ولكن في حقيقة الأمر قد تأتي على العكس من ذلك تماماً إذ تسجل كثير من الحالات في أن السبب يكون من الداخل،⁽⁶⁾ والتهديدات الداخلية هي التهديدات التي يقوم بها منتسبوا المنشأة أو المتعاملين معها والتي تستفيد من نقاط الضعف في النظم والعمليات والتطبيقات، وقد بينت الدراسات بأن أغلب التهديدات مصدرها داخلي.⁽⁷⁾

- (1) Stroe, E. R. & Rusu, A. C., (2011), "Security Risk Management - Approaches and Methodology", *Informatica Economica*, Vol. 15, No.1, Academy of Economic Studies, Bucharest, Romania, PP: 228- 240. & Hayale, Talal H. & Abu-Khadra, Husam A.,(2008),"Investigating Perceived Security Threats of Computerized Accounting Information Systems An Empirical Research applied on Jordanian banking sector ", *Journal of Economic & Administrative Sciences*, Vol. 24, No. 1, UAE, June 2008, PP: 41-67.
- (2) French, Aaron M., (2012), " A Case Study on E-Banking Security – When Security Becomes Too Sophisticated for the User to Access Their Information", *Journal of Internet Banking and Commerce*, Vol. 17, No.2, August 2012, PP: 1-15.
- (3) Whitman, M. E. & Mattord, H. J.,(2010),"The Enemy Is still at the Gates: Threats to Information Security Revisited", *the 2010 Information Security Curriculum Development Conference*, Kennesaw State University, USA, 1-3 October 2010, PP:95-99.
- (4) Gerić, Sandro & Hutinski, Željko,(2007),Information System Security Threats Classifications, *OP. Cit.*, PP: 59-60
- (5) Warkentin, Merrill & Willison, Robert,(2009),"Behavioral and Policy Issues In Information Systems Security: The Insider Threat", *European Journal of Information Systems*, Vol. 18, PP: 101–105, www.palgrave-journals.com/ejis/
- (6) Laudon Kenneth C. & Laudon Jane P.,(2011), "*Management Information Systems- Managing The Digital Firm*" , 12th Ed., Prentice - Hall, Inc, New Jersey, USA, P. 327.
- (7) Mihalache, Arsenie,(2011)," Security of the Accounting Information System Infrastructure", *OP. Cit.*, PP:1339-1345.

التهديدات الداخلية من داخل المنشأة حيث يمكن الوصول منه بسهولة عن طريق موظفيها العاملين في نظم المعلومات نظراً لوجود عدد قليل من العوائق التي يمكن التغلب عليها.⁽¹⁾

وفي رأي الباحث أن التهديدات الداخلية تمثل مؤشرات للمخاطر الناتجة عن مصادر داخلية، أي من داخل بيئة المنشأة، ومن ثم يمكن للمنشأة السيطرة عليها والتحكم فيها بطريقة أسهل من التهديدات الخارجية. والتهديد من الداخل هو الحاضر دائماً ويتجلى في نواح كثيرة وتبين التجربة أن الاعتماد المفرط على التكنولوجيا دون النظر للعوامل الداخلية الأخرى يمكن أن يكون لها نتائج كارثية لإدارة التهديد من الداخل،⁽²⁾ فأكبر الأخطار التي تهدد سلامة وخصوصية أمن النظام يأتي من داخل المنشأة،⁽³⁾ حيث تشكل التهديدات الداخلية الخطر الأكبر على نظام المعلومات المحاسبي إذا ما قورنت مع التهديدات الخارجية التي عادةً ما تحصل على اهتمام الرأي العام،⁽⁴⁾ لأنها تشكل مستوى أكبر بكثير من المخاطر ووفقاً لبعض الإحصائيات في عام 2009م فإن حوالي 80% من المخاطر لنظم المعلومات يأتي من الداخل، وذلك لما يمتلكه الأفراد القائمون عليها من معرفة بطبيعة نظم المعلومات المحاسبية المحوسبة، لذلك فإن كشف التهديدات الداخلية يعتبر من الأمور الصعبة، ولا سيما إذا ما نفذت من قبل جهات عليا في المنشأة.

إن التهديدات من الداخل مثلها مثل وجود ورم في الجسم، إذا تم كشفها ومعالجتها، سيكون لدى المنشأة معاناة على المدى القصير ولكن هناك فرصة جيدة للانتعاش، أما إذا تم تجاهلها فإنه سوف تزداد سوءاً وقد لا تسبب ضرر على المدى القصير، ولكنها من المرجح تؤدي إلى الانهيار على المدى الطويل الأجل.⁽⁵⁾

وفي مختلف الدراسات الاستقصائية التي اتخذت في عام 2011، قدرت المنشآت الأمريكية أن التهديدات الداخلية لديها قد شكلت ما نسبته 50 – 90 % من جميع التهديدات الأمنية المتعلقة بتكنولوجيا المعلومات، ويمكن الوصول إلى استنتاج بأن التهديدات الداخلية تشكل تهديداً حقيقياً وتحتاج إلى معالجة في برنامج أمن نظم المعلومات للمنشأة.⁽⁶⁾ يتناول هذا المبحث طبيعة التهديدات الداخلية على أمن نظم المعلومات المحاسبية المحوسبة والتي تتسبب في حدوث المخاطر الأمنية المختلفة، وبشكل عام فإن التهديدات الداخلية التي تواجه أمن نظم المعلومات المحاسبية المحوسبة يمكن حصرها بالمجموعات التالية :

- (1) Arsenie-Samoil, M. D. (2011). Security of the Accounting Information System Infrastructure. Ovidius University Annals, *Economic Sciences Series*, Vol. 11, No.1, PP: 1339-1345.
- (2) Knapp, Kenneth J. et al., (2009), "Information Security Policy: An Organizational-Level Process Model", *Computers & Security*, No. 28, PP: 493-508, available at www.sciencedirect.com
- (3) Senft, Sandra & Gallegos, Frederick, (2009), *Information Technology Control and Audit*, 3rd Edition, Taylor & Francis Group, LLC, Boca Raton – London – New York, USA, P. 230.
- (4) Shamszadeh, Bagher & Sharif, Abolfazl Azizi, (2012), "Computerized Accounting Information Systems (CAIS) Versus Security Threats", *Journal of Academic Research in Economics*, Vol. 4, No.1, March 2012, Islamic Azad University - Hamadan Branch, Iran, PP: 69-80.
- (5) Colwill, Carl, (2009), "Human Factors in Information Security: The Insider Threat e Who Can You Trust These Days?", *Information Security Technical Report*, Vol. 14, No.4, November 2009, PP: 186-196.
- (6) Miller, David R. et all, (2011), *"Security Information and Event Management (SIEM) Implementation"*, Mc Graw Hill, Network Pro Library, New York, USA, P. 87.

1-3-1: التهديدات الأمنية المتعلقة بفلسفة الإدارة العليا للمنشأة ورويتها نحو المخاطر:

إن فلسفة الإدارة ونمطها التشغيلي لها تأثير كبير على الطريقة التي يتم بموجبها إدارة المنشأة حيث إن الإدارة ومن خلال أنشطتها تزود العاملين بإرشادات واضحة حول أهمية نظام الرقابة الداخلية وهل الإدارة تقبل أنواع معينة من المخاطر؟ وما هي هذه الأنواع؟ حيث أن الإدارة التي تتبنى سياسة قبول مخاطر هامة تختلف نظرتها للرقابة الداخلية عن إدارة تتبنى سياسة متحفظة، ومن المسلم به أنه لا يمكن توفير الحماية الكاملة لأي نظام معلومات، وحتى تكون عملية إدارة المخاطر فعالة وناجحة يجب أن يكون هناك رؤية إستراتيجية فيما يتعلق بمستويات الأمان المطلوبة لنظام المعلومات داخل المنشأة.

إن إستراتيجية - أو سياسة - أمن المعلومات هي مجموعة القواعد التي يطبقها الأشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنشأة وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها وإدارتها.⁽¹⁾ ومجلس الإدارة مسئول عن الإشراف على تصميم وتشغيل الإدارة العليا لإدارة المخاطر، والإدارة العليا المسؤولة تكون في وضع يسمح لها بتخطي نواحي الرقابة المصممة لمنع الغش والاحتيال المرتكب من قبل موظفين آخرين، ومن الأمثلة على ذلك توجيه المرووسين لتسجيل عمليات خاطئة أو إغفال تسجيل بعض العمليات أو إخفاء معلومات تصميم وتشغيل إدارة المخاطر، وكل الأفراد العاملين لديهم بعض المسؤولية عن التنفيذ الناجح لإدارة المخاطر، ولذلك توجد مبادئ لإدارة المخاطر والتي تشمل تقييمها، والرقابة على التعرض لها ومراقبتها. إن توافر الإدارة من الأسباب الرئيسية وراء ضعف نظم الرقابة الداخلية، نتيجة وجود بعض المستويات الإدارية المتعلقة بعمليات معينة.

واحدة من عوامل النجاح الحاسمة لإدارة أمن نظم المعلومات - بما في ذلك تقييم مخاطر أمن المعلومات - هو وجود دعم واضح و التزام من جميع مستويات الإدارة، فمن الصعب تصور كيف يمكن تحقيق أمن نظم المعلومات دون المشاركة النشطة للإدارة،⁽²⁾ وبدون ذلك سوف يكون هناك خلل في تنفيذ وسائل الحماية اللازمة من المخاطر المختلفة وهدر لكثير من الموارد والجهود، وسيؤدي إلى إنتاج تقييمات ضعيفة، والأهم من ذلك سوف يؤدي إلى تجاهل نتائج التقييم،⁽³⁾ ولذلك فإن معتقدات الإدارة تؤثر تأثيراً كبيراً على الالتزام التنظيمي في تنفيذ الضوابط الأمنية.⁽⁴⁾

(1) المري، علي، (2011)، أمن المعلومات ماهيتها وعناصرها وإستراتيجياتها، مرجع سابق، http://www.dralmarri.com/show.asp?field=res_a&id=205

(2) McFadzean, E. & Ezingard, J. N. & Birchall, D., (2007), "Perception of Risk and the Strategic Impact of Existing IT on Information Security Strategy at Board Level", *Online Information Review*, Vol. 31, No.5, PP:622-660.

(3) Al-Ahmad, Walid & Mohammad, Bassil, (2013), "Addressing Information Security Risks by Adopting Standards", *International Journal Of Information Security Science*, Vol. 2, No 2, June 2013, PP: 28-43.

(4) Mohamed, Intan Salwani et. al, (2012), "Assessing Drivers for Organizational Commitment Towards The Security Controls Implementation in The Malaysian Online Service in Computer-Based Accounting System", *Advances in Natural and Applied Sciences*, Vol. 6, No. 8, PP: 1223-1237.

وهناك حقيقة تشير إلى أن العديد من المنشآت لا تأخذ التهديدات على محمل الجد بما يكفي لتنفيذ التدابير المضادة على نحوٍ كافٍ، أو ربما أن إدارات تلك المنشآت ليست على استعداد لاستثمار أموال كافية للحماية من المخاطر المختلفة.⁽¹⁾

وفيما يلي أهم التهديدات الداخلية المتعلقة بفلسفة الإدارة والمسببة لمخاطر أمن نظم المعلومات المحاسبية:

1-1-3-1: عدم إدراك الإدارة العليا لأهمية أمن نظم المعلومات: تنشأ المخاطر نتيجة اللامبالاة وعدم وجود الإشراف المناسب وعدم اتخاذ الإدارات العليا الإجراءات الكفيلة بحماية أمن نظم المعلومات وعدم إدراك واهتمام الإدارة العليا بأهمية أمن نظم المعلومات، وعدم دعم الجهة المعنية بها، وتلك من الأسباب الرئيسة في فشل تطبيق السياسات الأمنية للمنشأة وبالتالي تعريضها للمخاطر.⁽²⁾

فلن تكون أي من مقاييس الحماية والأمن فعّالة بدون توافر عدد من الخصائص ذات التوجه البشري ومنها مساندة الإدارة العليا بصفة خاصة لسياسات ومقاييس وعمليات أمن المعلومات، فجوهر الرقابة الفعّالة في ظل تكنولوجيا المعلومات في المنشأة تكمن في اتجاه إدارتها، فإذا كانت الإدارة العليا تعتقد بأهمية الرقابة الداخلية سوف يشعر بقية أفراد المنشأة بأهميتها، وسوف يتجاوبون بوعي وإدراك مع الضوابط الرقابية الموضوعية، ولكن إذا شعر الأفراد بان الضوابط الرقابية لا تشكل أهمية للإدارة فمن المؤكد جداً ألا تتحقق الأهداف الرقابية بفعالية.⁽³⁾

إن دعم الإدارة العليا أمر ضروري لضمان كفاية الموارد اللازمة في تحسين البنية التحتية لأمن نظم معلومات المنشأة، كما أن دعم الإدارة العليا مهم لضمان أن تؤخذ تقييمات المخاطر على محمل الجد في المستويات التنظيمية الأدنى، فالإدارة يجب أن تكون مطلعة أكثر على مخاطر أمن نظم المعلومات، ويجب أن يزداد وعيها في كل المجالات، وأن مستوى فهمهم العام لأمن نظم المعلومات يتأصل من خلال علاقتها مع البيئة التي تعمل بها.

وعليه يرى الباحث أن إدراك الإدارات العليا لمفهوم وأهمية نظام الرقابة الداخلي ورغبتها ودوافعها تجاه النظام من العوامل المؤثرة في نجاحه وفاعليته في تحقيق أهدافه المرجوة منه، وبالتالي فإن من معوقات تلك النظم، هو عدم إدراك ومعرفة الإدارة العليا بأهمية وحتمية وجوده.

1-1-3-2: عدم وجود سياسات واضحة لإدارة مخاطر أمن نظم المعلومات: ترتبط المخاطر بالأخطاء البشرية، وبفشل الأفراد في الالتزام بسياسات المنشأة وإجراءاتها، وعدم مقدرة الإدارة على دفع الموظفين على الالتزام بسياسات المنشأة والمخاطر الأخرى التي تنشأ بسبب تلاعب بعض الأفراد،⁽⁴⁾ فلا يمكن الحديث عن أمن المعلومات وحمايتها دون إيجاد سياسة واضحة ودقيقة وشاملة تسد جميع الثغرات والتهديدات الأمنية، بمعنى أن أي إخفاق في سن تلك السياسات

(1) Ross, Steven, (2011), "Information Security Matters", *SACA Journal*, Vol.6, PP: 1-2, Available Online: www.isaca.org/journal

(2) Shamszadeh, Bagher & Sharif, Abolfazl Azizi, (2012), "Computerized Accounting Information Systems (CAIS) Versus Security Threats", *Journal of Academic Research in Economics*, Vol. 4, No.1, March 2012, Islamic Azad University - Hamadan Branch, Iran, PP: 69-80.

(3) Arens, Alvin A., Elder, Randal J., & Beasley, Mark S., (2014), *Auditing & Assurance Services: An Integrated Approach*, OP. Cit., P.202.

(4) الذبيبة، زياد & الرمحي، نضال & الجعدي، عمر، (2011)، "نظم المعلومات في الرقابة والتدقيق"، مرجع سابق، ص62.

والإجراءات ينعكس بالسلب على أمن نظم المعلومات في المنشآت،⁽¹⁾ كما أن تطوير المواصفات القياسية والإجراءات هي التي تجعل من تطبيق السياسات الأمنية للمنشأة بصورة آلية سهلة.

وتتمثل سياسة إدارة المنشأة فيما يتعلق بأمن نظم المعلومات، بوجود سياسات جزئية لذلك، مثل تحديد مهام فريق أمن المعلومات وفريق إعداد تغييرات النظام، وفريق تشغيل ومعالجة البيانات والمعلومات، ووجود سياسة لتصنيف المعلومات وفقاً لأهميتها، ووجود سياسة للوصول إلى المعلومات والبرامج من داخل أو من خارج المنشأة، ووجود سياسة للحماية المادية والفنية للأجهزة والبرامج، ووجود سياسة للاستمرارية ومواجهة الكوارث.

إن سياسة نظام الأمن المعلوماتي تعزز وتكمل السياسة الكلية للمنشأة من خلال تحديد المخاطر وتقييمها، وتقليل التهديدات بتقليل احتمالات حدوثها، وتحديد المسؤوليات الأمنية الخاصة وإسنادها إلى أشخاص مختارين، وإعداد خطط الاحتواء للتهديدات وتنفيذها ومراقبة خطط الطوارئ والتدريب على تنفيذها، والرصد والمتابعة لكافة الاختراقات الأمنية.

ومن وجهة نظر الباحث فإن السياسة الأمنية هي مواصفات رفيعة المستوى من الخصائص الأمنية التي ينبغي على نظام معين امتلاكها وهي وسيلة للمصممين، والمقيمين، والمنفذين ومدققي الحسابات للتواصل مع بعضهم البعض، بل هي مخطط لقيادة المشروع من خلال تصميم التحقق من صحة تنفيذ العمليات، وهناك عدة متطلبات لنجاح العملية الرقابية الداخلية على نظم المعلومات المحاسبية المحوسبة منها وجود سياسة أمنية مكتوبة تحدد آلية توزيع الصلاحيات على الموظفين بشكل يتناسب مع الوصف الوظيفي مع ضرورة أن تكون هذه السياسة معتمدة من إدارة التدقيق والإدارة العليا.

وقد يؤدي عدم وجود سياسات واضحة لاستخدام نظام المعلومات إلى مشكلات أمن ضخمة يتعرض لها النظام، كما في حالة أعمال الصيانة عند نقص الأفراد المؤهلين، أو بسبب تغيير ودوران العمالة، أو إدخال تكنولوجيات متقدمة تتطلب مهارات جديدة، أو إبطاء العمل أو توقفه التي يجب مراعاتها من بدء التخطيط لنظم الأمن والشفافية المطلوبة.

1-3-3: عدم قيام إدارة المنشأة بإصدار قرارات وتشريعات خاصة للحد من مخاطر أمن نظم المعلومات: تحدث

المخاطر نتيجة عدم الامتثال للسياسات والمعايير الأمنية والقانونية والالتزامات التنظيمية أو التعاقدية فإذا لم تتعهد الإدارة العليا بالمنشأة بأمن نظم المعلومات بقوة فلن يتوافر الالتزام وكذلك الموارد اللازمة لنجاح إجراءات الأمن، حيث يقع على عاتق الإدارة العليا للمنشأة الالتزام بشكل قوي بتطبيق أمن نظم المعلومات، لأن الإجراءات الأمنية غالباً تكون غير مرغوبة لدى أفراد المنشأة، خاصة وأنه يترتب على عدم الالتزام بها معاقبة الموظفين المخلين بتلك القواعد.

فروح أمن المعلومات يجب أن يأتي من أعلى سلم إداري للمنشأة لتشجيع جميع أفراد المنشأة على الامتثال لقواعد السياسة الأمنية ولوائحها في المنشأة.⁽²⁾

(1) الغثير، خالد & والصبيح، أمل، (2012)، "حال أمن المعلومات في المملكة العربية السعودية"، دراسات المعلومات، العدد (14)، جامعة الإمام محمد بن سعود، الرياض، السعودية، أيار (مايو) 2012، ص: 189 – 205.

(2) Al-Awadi, Maryam, (2009), "A Study of Employees' Attitudes Towards Organizational Information Security Policies in the UK and Oman", OP. Cit., P. 88.

1-3-1-4: شعور إدارة المنشأة بعدم جدوى حماية أمن نظم المعلومات وتقييم مخاطر: تزداد المخاطر عندما يسود

اعتقاد لدى إدارة المنشأة بأن تكلفة تطبيق إجراءات الحماية أكبر من عوائدها المتوقعة، لأن نشاط مواجهة المخاطر كأى نشاط آخر في المنشأة يحتاج إلى نفقات، فأمن نظم المعلومات لا يمكن تنفيذه إذا لم يخصص له ميزانية كافية، ولذلك لا بد من توفير الميزانية اللازمة وتقدير المبالغ المطلوبة سلفاً، ويلاحظ أنه مهما زادت المبالغ المستثمرة لا يمكن أن نصل إلى معالجة كاملة للمخاطر ولكن يمكن جعل المخاطر غير المعالجة أقل ما يمكن، فالإدارة العليا هي التي توفر الدعم المالي لمواجهة المخاطر وذلك يؤدي إلى تشجيع الإدارات الأخرى على الاهتمام بما تكلف به من أنشطة أو ما يطلب منها من بيانات أو مشاركة من جانب أفرادها في اللجان المختلفة،⁽¹⁾ فموافقة الإدارة العليا وضماتها بالموارد الكافية للوضع وتنفيذ خطة التوعية، هي رسالة واضحة إلى المنشأة بأكملها تؤكد على أهمية برنامج أمن المعلومات.⁽²⁾

1-3-1-5: عدم مشاركة إدارة المنشأة للأفراد المختصين لبحث أفضل السبل لمواجهة المخاطر: عدم إشراك

المستخدم في تطوير النظم، يعد السبب الرئيسي لفشل نظم المعلومات، فلكي تكون النظم ناجحة فلا بد من إشراك جميع المجالات الوظيفية للمنشأة في تحديد ثقافة المنشأة وتحديد متطلبات النظام الجديد.⁽³⁾

فلا يمكن استمرار النظام دون تعاون وقبول من قبل الأطراف المستفيدة والمسئولة عن تشغيله وإدارته، وبالتالي لكي تعتبر إستراتيجية أمن نظم المعلومات ناجحة وفعالة وقابلة للتطبيق فلا بد أن يشارك في إعدادها وتنفيذها جميع المستويات الوظيفية التي لها علاقة بتلك الإستراتيجية حيث تسعى تلك المستويات إلى تحقيق أهداف إستراتيجية أمن المعلومات، من خلال بيان الإجراءات المتبعة لتفادي المخاطر وكيفية التعامل معها عند حصولها والجهات المكلفة بالقيام بذلك.

ويرى الباحث بأن مسألة أمن نظم المعلومات قد تكون أحد أهم مبررات مقاومة هذه النظم، حيث أن الهاجس الأمني يلعب دوراً هاماً في تصور قبول هذه النظم لدى الأفراد، وكلما ازداد الأمر تعلقاً بالأسرار والأموال ازداد الرفض والمقاومة، وعلى مطوري النظم وخبراء أمن المعلومات الاستجابة لمثل هذه الهواجس.

1-3-1-6: امتناع الإدارة العليا للبنك عن الإفصاح عن المخاطر: معظم المنشآت تميل إلى وضع غطاء على المخاطر

والجرائم التي ترتكب لديهم لأسباب مختلفة أهمها تجنب الدعاية السلبية،⁽⁴⁾ ويعتقد أن هناك ثلاثة أسباب رئيسية لئتم تجاهل التهديد من الداخل وهي أن هناك منشآت لا تعترف بحدوث تلك التهديدات، وأخرى تخشى الدعاية السيئة ومن السهل أن تكون في حالة إنكار، وهناك سبب كامن ثالث هو أن المنشآت تدرك أن التهديدات الداخلية حقيقية ولكن لا تعرف ماذا تفعل حيالها.⁽⁵⁾

(1) الحميد، محمد دباس & ونيو، ماركو إبراهيم، (2007)، "حماية أنظمة المعلومات"، مرجع سابق، ص ص: 89-91.

(2) Kolb, Nancy & Abdullah, Faisal, (2009), "Developing an Information Security Awareness Program for a Non-Profit Organization", *International Management Review*, Vol. 5, No. 2, PP: 105-110.

(3) Hall, James A., (2013), *Accounting Information Systems*, OP. Cit., P.500.

(4) Olanmi, Omoneye & Olufunke, Lecturer, (2010) "Computer Crimes and Counter Measures in the Nigerian Banking Sector", *Journal of Internet Banking and Commerce*, Vol. 15, No.1, April 2010, PP: 1-10.

(5) Colwill, Carl, (2009), "Human Factors in Information Security: The Insider Threat e Who Can You Trust These Days?", *OP. Cit.*, PP: 186-196.

ويرى أحد الباحثين أن مخاطر أمن نظم المعلومات هي جزء من المخاطر التشغيلية وأن مجلس الإدارة يمكنه حسن إدارة تلك المخاطر من خلال التأكد من وجود الإفصاح والشفافية الكافية بما يختص بالمخاطر الهامة في المنشأة وتوضيح السياسات المتعلقة بإدارة المخاطر، والتأكد من أن منهج الشفافية وإدارة المخاطر يمكن أن يحقق مزايا تنافسية للمنشأة.⁽¹⁾

ويقدر بأن (80-90%) من جرائم التزوير بالحاسوب التي تُكتشف لا يتم التبليغ عنها وسبب ذلك أن المنشأة تعتقد بان نشر ذلك سوف يكون بمثابة دعاية إلى التقليد والغش وفقدان ثقة العملاء الذي يمكن أن يكلف أكثر من التزوير نفسه،⁽²⁾ حيث تتجه كثير من المنشآت إلى التكتم على الأخبار التي تتصل بعمليات الاختراق إما نتيجة الخوف من توجيه النقد لعدم وجود تدابير وقائية مناسبة، أو الخوف من اهتزاز ثقة العملاء بسمعة المنشأة وبمركزها المالي، أو الخوف من تكرار المحاولات من جانب أشخاص قد يسعون إلى استغلال نقطة الضعف التي تم الكشف عنها، لذلك قد يؤدي الكتمان إلى نقصان الوعي وعدم توفر قاعدة كافية من المعلومات يمكن على أساسها وضع سياسة مناسبة للحماية، وتحديد حجم الاستثمارات المطلوبة لمواجهة مثل هذه المخاطر.⁽³⁾

1-3-2: التهديدات الأمنية المتعلقة بالعوامل التنظيمية:

إن الحلقة الأضعف في سلسلة الأمن يبدو أنه غياب أو عدم كفاية الجوانب السلوكية والتنظيمية لأمن نظم المعلومات،⁽⁴⁾ مثل عدم كفاية إجراءات التوظيف وعدم كفاية الموظفين وعدم المرونة التنظيمية عدم وجود الوعي الأمني لدى العاملين وعدم وجود آليات للمتابعة، حيث يتزايد مستوى المخاطر التي تواجه المنشآت مع تزايد حجم المنشأة وانتشارها ودرجة التعقيد والتطور في أنشطتها والخدمات التي تقدمها، ومعظم المخاطر تحدث نتيجة لعدم الضبط الدقيق لأدوات الحماية وفشل الموظفين العاملين في معالجة البرامج من نقاط الضعف الأمنية المعروفة.

كما توجد مشاكل في الاتصالات التنظيمية وهذا ناتج عن أن الأفراد العاملين في الأقسام التي تغذي الحاسوب بالبيانات، ربما لا يعرفون بشكل كامل البيانات المطلوبة منهم، أو توقيتها أو ربما يتقاعسون أو يهملوا في إمداد نظام المعلومات بالبيانات، هذا فضلاً عن تراكم المعاملات لدى المدراء الذين يقومون بالمصادقة عليها، واحتمالات ضياعها في أثناء انتقالها بين المستويات التنظيمية والإدارية المختلفة.⁽⁵⁾

(1) Abu-Musa, Ahmad A., (2009), "Exploring COBIT Processes for ITG in Saudi Organizations: An empirical Study", *The International Journal of Digital Accounting Research*, Vol.9, PP: 99-126.

(2) Romney, Marshall B. & Steinbart, Paul J., (2015), "Accounting Information Systems", OP. Cit., P.155.

(3) الجواد، دلال صادق & الفتال، حميد، ناصر، (2008)، "أمن المعلومات"، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، ص13.

(4) Parakkattu, Sindhuja & Kunnathur, Anand. S., (2010), "A Framework for Research in Information Security Management", *OP. Cit.*, PP: 318-323.

(5) محمد، حيدر صاحب، (2011)، "مسؤولية مراقب الحسابات في تحديد وتقييم مخاطر تكنولوجيا نظم المعلومات المحاسبية لرفع جودة أدائه"، مرجع سابق، ص: 86.

وفيما يلي أهم التهديدات الداخلية المتعلقة بالعوامل التنظيمية المسببة لمخاطر أمن نظم المعلومات المحاسبية:

1-2-3-1: عدم وجود إدارة أو قسم أو لجنة مستقلة، لها صلاحيات كافية لتقييم ومتابعة مخاطر أمن نظم المعلومات

المحاسبية، بهدف حماية تلك النظم: إن أحد أهم أسباب عدم قيام العديد من البنوك بإنشاء دوائر مختصة بإدارة المخاطر بشكل عام وإدارة المخاطر التشغيلية بشكل خاص يعود لعدم فرض ذلك من قبل السلطة الرقابية، مما يتطلب ضرورة إلزام البنوك بذلك انسجاماً مع الممارسات السليمة لإدارة المخاطر حيث يعتبر وجود دائرة المخاطر التشغيلية ووضع إطار وإستراتيجية من أهم شروط الإدارة السليمة للمخاطر، فالاستقلال التنظيمي لنظم المعلومات المحاسبية المحوسبة يعتبر أمراً حتمياً وحيوياً لسلامة وأمن نظم المعلومات، فهناك عدة أنشطة يجب القيام بها بعيداً عن قسم التشغيل الآلي للبيانات، حيث تبدأ كافة العمليات والتغيرات في السجلات الموجودة بالملفات الرئيسية ويتم التفويض بها في الأقسام المستخدمة وليس بواسطة قسم التشغيل الآلي نفسه.

وبالتالي هناك عدة متطلبات لنجاح العملية الرقابية الداخلية على نظم المعلومات المحاسبية المحوسبة منها وجود لجنة عليا تتولى متابعة الأمور المتعلقة بتكنولوجيا المعلومات وأن يكون ضمن أعضائها ممثلون دائمون عن دوائر تكنولوجيا المعلومات والتدقيق الداخلي وعن مجلس الإدارة.

ولذلك يرى الباحث أنه يجب على كل بنك تكليف فريق متخصص للرقابة والتفتيش والتدقيق على مخاطر منظومة العمل المصرفي الإلكتروني ويتبع ذلك الفريق إدارياً جهة مستقلة ويجب أن تتوفر في ذلك الفريق المهارات والخبرات الضرورية مثل الأساليب الإحصائية لدراسة احتمال حدوث تلك المخاطر، وخبرات فنية لمعرفة نقاط الضعف في الشبكات من خلال اختبارات الاختراق، ويقوم بمراجعة التقارير الأمنية اليومية لجميع الحركات التي تمت على جميع الملفات والبرامج في قواعد البيانات، وأن يعمل ذلك الفريق بشكل دائم ومستمر وفق منهاج عمل ومعايير قياسية محددة تتناسب وطبيعة الأنشطة الإلكترونية الممارسة في البنك.

1-2-3-2: غياب التوصيف الدقيق للوظائف: من أهم أسباب مخاطر أمن نظم المعلومات المحاسبية عدم التوصيف

الدقيق للهيكل الوظيفي والإداري الذي يحدد المسؤوليات والصلاحيات لكل شخص داخل الهيكل التنظيمي لدى المنشأة،⁽¹⁾ وبالتالي يتطلب نظام الرقابة الداخلية وجود هيكل تنظيمي يشمل إطار يتم من خلاله تخطيط وتنفيذ ورقابة الأنشطة وصولاً لتحقيق أهداف المنشأة، ويبين المناطق الرئيسية للسلطات والمسؤوليات، وتحديد واضح لخطوط الاتصال والتبعية لمختلف المستويات الإدارية في المنشأة، علماً بأن الهيكل المناسب للمنشأة يعتمد على حجم المنشأة وطبيعة النشاط الذي تقوم به.

1-2-3-3: الفصل غير الواضح بين المهام المتعلقة بنظم المعلومات المحاسبية: هناك أسباب لظهور المخاطر في

المنشآت، منها التساهل مع الأخطاء البشرية، وضعف التوظيف الوظيفي، وعدم وضوح المهمات والواجبات، وعدم وضوح الهيكل التنظيمي، وتشير الإحصاءات إلى أن ما يقرب من نصف عمليات الغش والاحتيال في نظم التشغيل

(1) Werlinger, R. & Hawkey, K. & Beznosov, K. (2009), "An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management", OP. Cit., PP: 4-19.

الإلكتروني للبيانات ترجع إلى عدم الفصل الملائم بين المهام والوظائف المحاسبية،⁽¹⁾ كإشراك بعض العاملين باستخدام نفس كلمات السر أو تبادلها بينهم، مما قد يهدر مبدأ تقسيم العمل،⁽²⁾ والفصل غير الملائم بين المسؤوليات في نظم (البرمجة، التشغيل)، والفصل غير الملائم بين المسؤوليات في نظم (إقرار المعاملات، التسجيل، الحفظ).⁽³⁾

1-3-2-4: النقص الكبير في الموظفين المختصين بأمن نظم المعلومات: إن من أهم معوقات تخفيض مخاطر أمن نظم المعلومات نقص الموارد البشرية المؤهلة في تكنولوجيا المعلومات، والذي تتوفر فيهم الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المتعددة والمطلوبة لذلك، ويتمثل الخطر في ضعف مستوى التأهيل والخبرة للكوادر الإدارية والفنية المرتبطة باستخدام التكنولوجيا، وقد ذكر تقرير لمكتب التحقيقات الفيدرالي (FBI) أن المشكلة الرئيسية لحدوث اختراقات للمؤسسات المالية هو عدم توظيفها للموارد البشرية التكنولوجية الكافية لتأمين الحماية والاكتفاء بطاقم تكنولوجي ضئيل نسبياً كما أن توفر القوى العاملة المدربة تدريباً كاملاً على جوانب أمن المعلومات المختلفة لم يتواءم مع الخطى المتسارعة لصناعة برامج حماية نظم المعلومات.

1-3-2-5: صعوبة وعدم كفاية تدريب وتأهيل وتوعية الموظفين في مجال تقنيات وأساليب أمن نظم المعلومات: من الأسباب التي تؤدي إلى حدوث تلك المخاطر تدريب وإشراف غير مناسب للأفراد، وغياب الإجراءات المكتوبة، وتفويض غير مناسب للصلاحيات،⁽⁴⁾ فالتطور في النظم المحاسبية يرافقه التعرض لعدة مخاطر هامة متعلقة بأمن وسلامة نظم المعلومات المحاسبة المحوسبة لان ذلك التطور لم يكن مصحوباً بتطور مماثل في قدرات الموارد البشرية والكفاءة من قبل المستخدمين لهذه التكنولوجيا وأيضاً لم يترافق مع تطور مماثل في الممارسات والضوابط التي تحكم التوعية والتدريب،⁽⁵⁾ ومرتكبي مخاطر الوصول ناجحين في معظم الوقت ليس فقط بسبب خبراتهم ولكن بعض المنشآت تسهل ذلك عن طريق إهمال تدريب الموظفين وتعريفهم بأمن الحاسوب أو عدم الاستثمار في المعدات التكنولوجية،⁽⁶⁾ فعدم وجود التدريب الأمني يشكل تحدياً لأنه يصعب تنفيذ الضوابط الأمنية عندما لا يكون لدى الأفراد ما يكفي من التوجيه أو التعليم حول أفضل الممارسات لأمن تكنولوجيا المعلومات،⁽⁷⁾ كما أن نقص التدريب والتوعية الملائمة عن أمن المعلومات وأهميته تسهم في الجهل باستخدام نظم المعلومات المناسبة، وبدون تنظيم دورات تدريب ملائمة، قد يجهل كثير من العاملين والمستخدمين بأعراض الأضرار الناجمة من سوء استخدام نظم المعلومات، كما قد لا يستخدمون أي مقاييس أمن حتى البدائية منها، مما قد يؤدي إلى مزاوالات تعود بالإساءة لأمن نظم المعلومات، وقد يؤدي التنوع الكبير لمستخدمي نظام المعلومات والمتعاملين معه (العاملون، المستشارون، العملاء، المنافسون

(1) Malami, Abu Bakar & Zainol, Zaini & Nelson, Sherliza, (2012), "Security Threats of Computerized Banking Systems (CBS): the Managers' Perception in Malaysia", *International Journal of Economics and Finance Studies*, Vol. 4, No. 1, 2012, PP: 21-30, http://www.sobiad.org/eJOURNALS/journal_IJEF/archives/2012_1/abu_bakar.pdf

(2) السانكي، سعد & العواد، حنان، "مخاطر استخدام تكنولوجيا المعلومات وأثرها على أداء نظم المعلومات المحاسبية - دراسة تطبيقية لعينة من الشركات المساهمة المدرجة في بورصة عمان للأوراق المالية"، مرجع سابق، ص: 207-257.

(3) شنيوي، أيمن أحمد، (2006)، "قياس تأثير بعد الصناعة على دور المراجع الداخلي في إدارة المخاطر المرتبطة بنظم المعلومات المحاسبية الآلية"، *مجلة كلية التجارة للبحوث العلمية، كلية التجارة، المجلد 34، العدد 2، الاسكندرية، مصر، سبتمبر 2006*، ص: 1-52.

(4) الذبيبة، زياد & الرمحي، نضال & الجعدي، عمر، (2011)، "نظم المعلومات في الرقابة والتدقيق"، مرجع سابق، ص: 62.

(5) Al Hanini, Eman, (2012), "The Risks of Using Computerized Accounting Information Systems in the Jordanian Banks: Their Reasons and Ways of Prevention", *European Journal of Business and Management*, Vol. 4, No.20, PP: 53-63. www.iiste.org

(6) Olanmi, Omonye & Olufunke, Lecturer, (April 2010), "Computer Crimes and Counter Measures in the Nigerian Banking Sector", *OP. Cit.*, PP: 1-10

(7) Werlinger, R. & Hawkey, K. & Beznosov, K, (2009), "An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management", *OP. Cit.*, PP: 4-19.

والجمهور العام) فيما يتعلق بتوعيتهم وتدريبهم واهتماماتهم المختلفة والمتفرقة في ظهور صعوبات خاصة بأمن المعلومات ونظمها،⁽¹⁾ ووفقاً لديلويت (DELOITTE)، حوالي 45 % من المنشآت العالمية لا تعمل على توعية موظفيها فيما يتعلق بالتهديدات الأمنية، وهذا النقص في الوعي بأمن المعلومات قد يؤدي إلى حدوث مخاطر لأمن نظم المعلومات المحاسبية داخل المنشأة.⁽²⁾

1-3-2-6: الاهتمام غير الكافي بفحص التاريخ الوظيفي والمهني للموظفين الجدد: من أهم التهديدات الداخلية

التنظيمية والتي تسبب المخاطر عدم الاهتمام الكافي بفحص التاريخ الوظيفي المهني للموظفين الجدد مما قد يؤثر على قاعدة وضع الرجل المناسب في المكان المناسب، وعدم إلزام الموظفين بأخذ إجازاتهم الدورية،⁽³⁾ وبالتالي يجب عمل دراسة شاملة للتاريخ الوظيفي السابق لكل الأفراد المتقدمين للوظائف وذلك لتفادي تعيين أفراد سبق لهم ممارسة أي مخالفات، مع ضرورة توافر معايير محددة من القيم الأخلاقية والنزاهة في الموظف الذي يتم اختياره وخاصة الأفراد الذين تتطلب وظائفهم الوصول للمعلومات الحساسة.

ولذلك تعمل السلطات الرقابية على إملاء الشروط الواجب توافرها في الموارد البشرية التي تتولى مسؤوليات الإدارة التنفيذية في البنك، من أهمها الكفاءة والأهلية العلمية، والسمعة الجيدة والخبرة المناسبة، والأمانة، وخلوه من السوابق القضائية... الخ.

1-3-3: التهديدات الأمنية المتعلقة بالتكنولوجيا المستخدمة:

بقدر معرفتنا بما تحمله عملية استخدام تكنولوجيا المعلومات، وأنظمة المعلومات من فوائد جمة لا تحصى، إلا إنها تحمل بين طياتها أيضاً العديد من المخاطر، بحيث أصبح هناك ارتباط وثيق بين استخدام وسائل الاتصالات وتكنولوجيا المعلومات ومخاطر نظم المعلومات المحاسبية، ففي النظام المحوسب يستخدم العقل الإلكتروني الذي صممه الأفراد وفقاً للاعتبارات المصممة والسياسات والإجراءات والخطط المرسومة مسبقاً وبعبارة أخرى لا يمكن تجاوز أي خطأ أعضاها الأفراد،⁽⁴⁾ والتعقيد التكنولوجي هو تحد آخر للأفراد العاملين على حماية أمن نظم المعلومات، ويعد من أهم أسباب عدم التوصل للأمن المطلق، فهذا التعقيد يجعل من الصعب للغاية لصنّاع القرار تصميم السياسات الأمنية التي تغطي جميع التكوينات المحتملة للأنظمة،⁽⁵⁾ وفيما يلي أهم التهديدات التكنولوجية الداخلية المسببة لمخاطر أمن نظم المعلومات المحاسبية:

(1) الشبلي، هيثم حمود، (2009)، "إدارة مخاطر الاحتيال في قطاع الاتصالات"، مرجع سابق، ص 228.
 (2) Kritzing, E & Smith, E.,(2008), "Information Security Management: An Information Security Retrieval and Awareness Model for Industry", *OP. Cit.*, PP: 224 – 231.
 (3) Abu-Musa, Ahmad A.,(2006), "Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations", *OP. Cit.*, PP: 1-26.
 (4) Al-Bashtawi, S. H., & Al-Husban, A. (2013). Determinants of Auditing Electronic Accounting Information Systems, A Case Study in the Jordanian Commercial Banks. *European Scientific Journal*, ESJ, Vol. 9, No. 10.
 (5) Werlinger, R. & Hawkey, K. & Beznosov, K.,(2009), "An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management", *Information Management & Computer Security*, Vol. 17, No.1, PP: 4-19.

1-3-3-1: تقادم الأجهزة والبرامج المستخدمة: بالرغم من المزايا الكبيرة لتكنولوجيا المعلومات فإنه توجد عدة مشاكل عند استخدامها ومنها التقادم التكنولوجي السريع لأجهزة الحاسوب، كما أن تعطل أو تلف الأجهزة يؤدي إلى تلف كبير في المعلومات التي تحتويها، ومدى اهتمام مصممي البرامج بتخطيطها بكفاءة وبطريقة يصعب تعديلها.⁽¹⁾ يمكن تبويب الأخطاء التي تحدث أثناء مرحلة التشغيل تكون ناجمة عن قصور في تصميم برامج التطبيقات، أو قصور في وظائف المعدات الالكترونية، وبالتالي فإن ضعف فاعلية نظم المعلومات المحاسبية في حفظ وتشغيل البيانات وإنتاج المعلومات وتدقيقها وتخزينها واسترجاعها بسهولة ودقة وسرعة، يبرز بشكل واضح وجلي إذا قامت المنشأة بشراء أجهزة برمجيات غير ملائمة أو أنظمة تشغيل غير كفؤة، وعدم إدخال الأجهزة والمعدات التكنولوجية اللازمة لتحديث وتطوير نظم المعلومات المحاسبية، حيث نشهد التصاعد المستمر في السرعة والطاقة التخزينية للأجهزة وتنوعها، وكذلك التطوير لبرامج وتطبيقات عديدة ذات تقنية متقدمة للغاية، خلال فترات زمنية وجيزة، ولا تلبث المنشآت أن تعتاد على تطبيق ما حتى يظهر آخر أحدث.

وفي رأي الباحث يصعب في كثير من الأحيان مواكبة التسارع التكنولوجي مما يجعل التكنولوجيا التي تستخدمها المنشأة قديمة جداً، والمشكلة تكمن بعدم معرفة التقادم في الوقت المناسب.

1-3-3-2: الصعوبة في إيجاد التوليفة المثلى للأجهزة والبرامج: تنشأ مخاطر التشغيل من عدم ملائمة تصميم النظم أو إنجاز العمل أو إهمال الصيانة حيث يؤدي إخفاق النظم وعدم كفاءتها كبطء سرعة أداءها في مواجهة متطلبات المستخدمين على سبيل المثال، وعدم سرعتها في حل المشاكل والصيانة، خاصة إذا زاد الاعتماد على مصادر خارجية في تقديم الدعم الفني بشأن البنية الأساسية اللازمة.

وفي المنشآت المالية مثل البنوك نجد أن درجة الأتمتة عالية، في حين أن التدخل البشري منخفض، حيث تعتمد البنوك على تكنولوجيا معلومات معقدة البنية التحتية والتطبيقات، وكل نظام من أنظمة حماية وأمن المعلومات يُنتج العديد من الإنذارات والسجلات الخاصة به، نظراً لقلة وجود مواصفات قياسية لمنتجات وخدمات أمن المعلومات، مما ينتج عنه صعوبة وتحدي في جعل تلك النظم تعمل مع بعضها البعض بشكل متكامل،⁽²⁾ ويصعب في كثير من الأحيان إيجاد التوليفة المثلى للأجهزة والمعدات والبرامج والنظم الفرعية لتشكيل نظام التشغيل بما يؤمن تحقيق أهداف النظام وتأمين عناصر الرقابة وتقليل الخسارة إلى الحد الأدنى، فمن الناحية الفنية نجد أن نظم المعلومات قد تعمل على أنظمة تشغيل مختلفة، وتعتمد على أنواع كثيرة من بروتوكولات الاتصال، ووضعت من قبل العديد من لغات البرمجة، وتتكون من عدد من التطبيقات غير المتوافقة، وغير المتجانسة.

ومن مقاييس الأمن الشائعة ضرورة توافق البرمجيات في بيئة الموردين المتعددة، وحتى يمكن التوصل لذلك، يصبح من الضروري موافقة منظمات التوحيد القياسي، الموردين، والمنظمات ومستخدمي نظم المعلومات علي المعايير والتوجيهات الحاكمة لقياسات الأمن ذات الطابع الدولي، ومع ذلك نجد كثير من المنشآت القائمة حالياً وخاصة

(1) Laudon Kenneth C. & Laudon Jane P., (2011), "Management Information Systems- Managing The Digital Firm", OP. Cit., P. 7.

(2) NĂSTASE, Pavel & UNCHIAȘU, Simona, (2013), "Implications of the Operational Risk Practices Applied in the Banking Sector on the Information Systems Area", OP. Cit., PP: 101-117.

في المجتمعات النامية لم تجاري حتى الآن التطور والنمو التكنولوجي المرتبط باستخدام نظم المعلومات وتأمينها، فلا يزال هناك قصور واضح ونقص كبير في التقنيين والتوحيد لعدم الأخذ بالمعايير الدولية والتشفير الخاص بالمزاولة الأحسن، إلي جانب قصور الإرشاد والتوعية والحقوق والالتزامات القانونية، مما يزيد في النفقات ويسبب تأخير الأعمال وعدم تكامل البيانات، وإن السماح باستمرار الوضع الراهن يحد من النمو المستقبلي ويؤخر اللحاق بعصر المعلومات والمعرفة.

1-3-3-3: وجود أخطاء في تصميم البرامج والتطبيقات المحاسبية المستخدمة: هناك عوامل فنية تؤدي لفشل نظم المعلومات وهي عديدة ومتنوعة، كما قد تعتبر غير مفهومة في بعض الأحيان، أو تتغير علي الدوام، حيث تعد الأخطاء التصميمية والتقنية من الأسباب الجوهرية لحدوث المخاطر المهددة لنظم المعلومات المحاسبية،⁽¹⁾ ومن أكثر الأخطاء التقنية شيوعاً، حصول أعطال في الأجهزة، أو أخطاء في البرامج، إذ أن هنالك العديد من تلك الأخطاء التي تؤدي إلى مخاطر أمن نظم المعلومات، ومن أبرزها: تسهيل ارتباط نظم المعلومات بالإنترنت قبل تشغيل نظم الحماية، وعدم القيام بتحديث وتطوير النظم عند اكتشاف فجوات ثغرات أمنية فيها، والتصريح بكلمات مرور المستخدمين عبر الهاتف ولأفراد لا يتم التحقق من هويتهم، وعدم الاحتفاظ بنسخ احتياطية واختبارها.

وقد تأتي أخطاء النظام من سوء استخدام الأجهزة والبرمجيات ومنها الأخطاء الكامنة والتحميل الزائد والمشكلات التشغيلية وغير ذلك من العوامل الفنية التي تؤدي لفشل نظم المعلومات وهي عديدة ومتنوعة، كما قد تعتبر غير مفهومة في بعض الأحيان أو تتغير على الدوام وقد تنتج من أعطال كبيرة تؤدي إلى توقف أو إبطاء العمل بصفة دائمة وفي هذه الحالة يجب مراعاة توقيتات الأعطال والتشويش الذي يتعرض له النظام عند التخطيط لأمن المعلومات من البداية.⁽²⁾

ويرى الباحث أن صعوبة التوافق في المعرفة والانسجام بين الأفراد كمحلي النظم والمبرمجين والمشغلين، ينعكس على منطقية كافة مراحل تصميم وتشغيل النظام، وبالتالي يؤدي إلى إنتاج معلومات خاطئة أو غير دقيقة لفترات طويلة.

1-3-3-4: عدم كفاية عمليات الصيانة الدورية: إن نظم المعلومات المحاسبية تواجه بعض الآثار السلبية نتيجة تطبيق نظام الميكنة، ومنها مشكلات تتعلق بتقادم أجهزة الحاسوب، وعدم كفاءة الصيانة لها، ومن أهم المشاكل التي تواجه الحاسبات الالكترونية هو عدم توفر الصيانة الدورية لأجهزة الحاسوب والبرمجيات المستخدمة في تشغيل وحماية نظم المعلومات المحاسبية المحوسبة، وإجراء عمليات الصيانة في حالة توقفها عن العمل وهذه أحد الأخطاء الشائعة في بيئة الحاسبات الالكترونية إضافة إلى ذلك هناك عدد من الأسباب التي تؤثر على عمل النظم المحاسبية منها عدم وضع المعايير لإجراءات التشغيل، إن عدم توفر الفنيين والأخصائيين لأغراض الصيانة يؤدي إلى تعطل أجهزة الحاسوب لفترات طويلة ويصبح عائقاً مهماً أمام استخدامهما، ولذلك ينبغي السعي إلى تكوين شركات متخصصة تقدم خدماتها في

(1) المنصور، كاسر نصر، (2007)، "إدارة المخاطر وإستراتيجية التأمين في ظل تكنولوجيا المعلومات"، المؤتمر العلمي الدولي السنوي السابع، إدارة المخاطر واقتصاد المعرفة، جامعة الزيتونة الأردنية، عمان، الأردن، 16-18 نيسان 2007.

(2) الشبلي، هيثم حمود، (2009)، "إدارة مخاطر الاحتيال في قطاع الاتصالات"، مرجع سابق، ص 226.

هذا المجال،⁽¹⁾ والصعوبة في صيانة وحماية أمن المعلومات والنظم والشبكات قد تنبع من تواجد بيانات متعددة من الأطراف المرتبطة بها كالمتهدين، الموردين، البائعين، الخ.

ولذلك يرى الباحث بأن عدم إجراء اختبارات كافية للبرامج والأجهزة قبل استخدامها للتحقق من عدم وجود ثغرات أو مشاكل فنية فيها قد يؤدي إلى استغلال هذه الثغرات أو الأخطاء في اختراق البرامج أو تدمير الأجهزة وخسارة ما بها من قواعد بيانات أو برامج مخزنة، فهناك ضرورة لعمل صيانة مستمرة للبرامج والأجهزة لتفادي حدوث أخطاء ومشاكل فنية في نظم التشغيل أو التطبيقات بعد الاستخدام.

1-3-3-5: الاعتماد على مزودين قليلي الخبرة: تنشأ المخاطر من إخفاق النظم أو عدم كفاءتها لمواجهة متطلبات المستخدمين وخاصة إذا زاد الاعتماد على مصادر من خارج المنشآت لتقديم الدعم الفني بشأن البنية الأساسية اللازمة، فاعتماد المنشأة في الحصول على الأجهزة والبرامج، والدعم الفني لها على مزودين قليلي الخبرة، ولا يتم التقييم المستمر لوضعهم في السوق قد يعرض المنشأة لمخاطر نظامية، بالإضافة إلى المخاطر الأخرى التي تلحق بسمعتها.⁽²⁾ إن التوجه إلى المصدر الخارجي للحصول على متطلبات العمل الإلكتروني والمتخصص يعتبر بحد ذاته توجهاً إيجابياً حيث يؤدي إلى تقديم الخدمة بفعالية وكفاءة وبالتالي يسمح للبنوك الصغيرة بالمنافسة ولكن من جانب آخر تؤكد تجارب الدول في هذا المجال أن نسبة كبيرة من البنوك متوسطة وصغيرة الحجم تعتمد على المزودين قليلي الخبرة نظراً لانخفاض تكاليفهم، ولكنهم عاجزين عن تقديم الدعم المطلوب في الوقت المناسب، وهذا يؤثر على مقدرة البنك ومزودي الخدمات في مواجهة المشاكل المختلفة عند حدوثها أو القدرة على التعامل مع التطورات التكنولوجية السريعة، ولذلك فإن من أهم متطلبات نجاح العملية الرقابية الداخلية على نظم المعلومات المحاسبية المحوسبة وجود اتفاقيات تعطي الأنظمة المشتراة وأن تكون معتمدة من قبل الإدارة وأنها سارية المفعول، مع ضرورة مراجعة واعتماد جميع الاتفاقيات من قبل المستشار القانوني.

إن على البنوك اختيار المزودين من ذوي السمعة الممتازة، مع التقييم المستمر لوضعهم في السوق ومستوى خدماتهم وتجاوبهم مع المستجدات، مع الاهتمام بموضوع السرية المصرفية، ولا بد من الاعتماد على المصادر الذاتية في تقديم الدعم الفني دون الاعتماد على مصادر خارجية وذلك للعمل على استمرار تقديم خدماتها التجارية إلى عملائها الذين يتوقعون منها السرعة الفائقة في تقديم ما يريدون من خدمات تجارية.

1-3-3-6: عدم التوائم والتوافق ما بين الأنظمة والتطبيقات الموجودة لدى البنك مع الأنظمة والتطبيقات الخاصة بالمنشآت التي قد يتم ربط أنظمة البنك معها: تنشأ مخاطر أمن نظم المعلومات المحاسبية نتيجة أخطاء تكنولوجية من أهمها عدم التوائم والتوافق ما بين النظم والتطبيقات الموجودة لدى البنك مع النظم والتطبيقات الخاصة بالأعمال المصرفية الإلكترونية أو مع نظم المنشآت التي قد يتم ربط أنظمة البنك معها، وقد أثبتت التجارب أن البنوك الصغيرة

(1) الحبيطي، قاسم محسن & والسقا، زياد هاشم، (2011)، نظم المعلومات المحاسبية، وحدة الحدياء للطباعة والنشر، كلية الحدياء الجامعة، الموصل، العراق، 2011.

14/ 10/ 2011 18:38:26 GMT P:28. <http://www.infochacountants.com/resources/articles/20051.pdf>

(2) زيدان، محمد & حمو، محمد، (2010)، "متطلبات أمن المعلومات المصرفية في بيئة الانترنت"، مرجع سابق، ورقة عمل

تواجه صعوبات في مجال موائمة أنظمتها في ظل مواردها المحدودة سواء من حيث، امتلاك البرمجيات والأجهزة الملائمة، وجذب الكوادر المؤهلة.

1-3-4: تهديدات تتعلق بالأفراد العاملين في نظم المعلومات المحاسبية المحوسبة:

هناك اعتقاد سائد بأن الجزء الأعظم من تهديدات نظم المعلومات يأتي غالباً من المصادر الخارجية، ولكن على النقيض من ذلك فإن الأشخاص الذين منحوا حق الوصول المعتمد للنظام قد يكونون أكثر فتكاً بنظم المعلومات أيضاً باعتبارهم قادرين على العبث في نظام الحماية المعد من قبل المنشأة لأنهم أكثر دراية ومعرفة بنظم الرقابة الداخلية للمنشأة⁽¹⁾ ويمكنهم الدخول من خارج المنشأة أو السماح لغيرهم بالقيام بالمهمة من خلال العبث والتلاعب في النظام بطرق متعمدة بغية الاستغلال أو الثراء الذاتي على حسابا للمنشأة التي يعملون بها، وقد يكونوا مؤتمنين أو عاملين من ذوي النوايا الحسنة لكنهم بفعل التعب أو الإرهاق أو التدريب غير الملائم قد يقترفون أفعالا غير متعمدة قد تسهم في حذف كميات كبيرة من البيانات الهامة للمنشأة التي يعملون بها.⁽²⁾

ويتفق الباحث مع الآراء التي تعتبر أن مصادر المخاطر الداخلية الناشئة من أفراد المنشأة أكثر خطورة وتأثيراً من المصادر الخارجية، حيث يعتبر بعض الأفراد العاملين في نظم المعلومات خط الدفاع الأول عن تلك النظم، ولكن من ناحية أخرى قد يكون البعض الآخر هو الحلقة الأضعف حيث يمثل تهديداً أساسياً لها، فقد يكون الشخص المخول بحماية أمن نظم المعلومات هو مصدر الخطر والتهديد إذا أساء استعمال صلاحياته ولم يتقيد بالإجراءات، وتكون بدوافع من عدم الرضا أو الرغبة في الانتقام أو إثبات المهارات الفنية أو تحقيق مكاسب مالية،⁽³⁾ كما أن جهل الموظفين، والفضول والتهور، وإعطاء كلمة المرور إلى الموظفين الآخرين، وتسريب المعلومات عن طريق مستخدمو النظام ومن لهم الحق في الولوج للنظام عن قصد أو غير قصد هي بعض من التهديدات الداخلية.⁽⁴⁾

وعلى الأغلب تتم الأخطاء البشرية الداخلية الحاصلة من قبل الموظفين لأحد سببين، إما لأنهم غير ذي ثقة، فيكون خطأهم هنا مقصوداً ومتعمداً، إذ يقوم الشخص بتسريب معلومات أو إحداث ضرر لكي يستفيد هو مادياً لصالح جهة ما (عميل)، أو انتقاماً منه لأنه متضرر من عمله وغير حاصل على حقوقه، أما السبب الثاني فيكون إهمالاً من الشخص وعدم معرفته بأنه يرتكب خطأ، وهنا يكون خطأ بشري غير مقصود وغير متعمد، وعندما يكون مرتكب الخطر المتعمد ذو خبرة وتخصص كان حجم الضرر أكبر.

وعموماً فإن من أولئك الأفراد الذين قد يمثلون تهديداً لنظم المعلومات هم كل من الكوادر التي تقوم بصيانة الحاسوب، ومنهم ممثلي موردي البرامج حيث تكون لهم حرية كبيرة في الدخول إلى النظام، وقد يقومون بنقل بيانات

(1) الدلاهمة ، سليمان مصطفى، (2013)، "أثر مخاطر استخدام تكنولوجيا المعلومات على أداء نظم المعلومات المحاسبية من وجهة نظر مراجعي الحسابات في المملكة العربية السعودية"، مرجع سابق، ص: 36-11.

(2) Hunker, J. & Probst, C., (2011), "Insiders and Insider Threats – An Overview of Definitions and Mitigation Techniques," *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications*, Vol. 2, No. 1, March 2011, PP: 4-27.

(3) الخضير، سليمان، (2013)، الشامل، مجلة دورية تصدر عن إدارة التسويق في مصرف اليمن البحري الشامل، العدد (8)، صنعاء، اليمن، ص: 18-16.

(4) Shahri, Ahmad & Ismail, Zuraini & Rahim, Nor, (2012), "Security Effectiveness in Health Information System: Through Improving the Human Factors by Education and Training", *Australian Journal of Basic and Applied Sciences*, Vol. 2, No. 12, 2012, PP: 226-233.

أو عمل تعديلات معينة أو غير ذلك من التهديدات، والمبرمجين الذين يقومون بإعداد البرامج أو تعديلها، فهم يمثلون تهديداً من حيث إحداث تعديل غير مرغوب فيه في البرنامج القائم أو كتابة برنامج يقوم بعمل أشياء غير مرغوب فيها، ومشغلي الشبكات: التهديد ينبع من إعطائهم صلاحيات كبيرة خاصة بالحماية وهو ما قد يساء استغلالها، والأشخاص المسؤولين عن نظام المعلومات: مثل المشرفين على النظام، حيث تعطى لهم صلاحيات كبيرة وكلمات مرور متعددة للوصول إلى الملفات السرية والبرامج، كما أنهم قادرون على منح كلمات السر للغير، والمستخدمين للنظام وإن كان هذا محدوداً والتهديد هو من خلال وصولهم إلى الكثير من البيانات التي قد يقومون بالكشف عنها.⁽¹⁾ وبالتالي تتمثل التهديدات الداخلية المتعلقة بالأفراد العاملين بالمنشأة فيما يلي:

1-4-3-1: سوء استخدام الصلاحيات الواسعة المخولة لبعض الأفراد: وفي حقيقة الأمر قد يكون مرتكبي جرائم الحاسبات من العاملين بالمنشأة استخداماً لما لديهم من سلطات وممن لديهم معرفة واسعة بتفاصيل النظام، بهدف تحقيق مصالح خاصة بهم فضلاً عن انعدام الوازع النفسي والأخلاقي.

وأي تلاعب أو احتيال له ثلاثة أركان حافز الإدارة للتلاعب كدافع للأفراد، وإمكانية وقوع التلاعب نتيجة وجود ضعف في نظم الرقابة، واتجاه الأفراد نحو التلاعب كمبرر، ولذلك يرى الباحث أن مثلث التلاعب يمتد إلى أمن نظم المعلومات المحاسبية المحوسبة لأن الأركان الثلاثة المتمثلة في الحافز والإمكانات والاتجاه هي الأركان الهامة المحركة للتلاعب الإلكتروني.

إن سوء الاستخدام المقصود للنظام والوصول غير المتعمد له والنزوع للأذى، وتعتمد التخريب والتدمير والاحتتيال أو السرقة تعتبر مخاطر وتهديدات خطيرة تؤثر سلباً على قابلية نمو حياة النظام والمنشأة المالكة له بل تؤثر على القابلية للبقاء والتواجد،⁽²⁾ نظراً لأن موظفي المنشأة غير الأمناء يكون لديهم صلاحيات الدخول إلى النظام والوصول إلى البيانات، ومن ثم إمكانية تدميرها أو تحريفها أو تعديلها بالإضافة إلى أنهم أكثر دراية ومعرفة من غيرهم بنقاط الضعف ونواحي القصور في الضوابط الرقابية المطبقة في المنشأة،⁽³⁾ وطالما أن الشخص المسموح له بالتعامل مع النظام من الممكن أن يقوم بتغيير أو نسخ أو مسح بعض أو كل البيانات أو المعلومات – سواء عمداً أو بدون عمد – فإن هذا يمثل خطراً كبيراً، ومن أهم الأخطاء الشائعة للمستخدمين إعطاء أمر بالخطأ يؤدي إلى فقد البيانات أو إلغاء ملف أو برنامج أو كل ما هو علي وسائط التخزين.

1-4-3-2: ضعف إدراك بعض العاملين بالنظام لمهامهم الموكولة لهم: إن عدم وعي بعض الأفراد وإدراكهم بمهامهم الموكولة لهم بموجب الصلاحيات المخولة، يترتب عليها أخطاء بشرية فادحة، سواء عند البرمجة والتصميم أو عند التشغيل، حيث تتعرض نظم المعلومات المحاسبية المحوسبة للعديد من المخاطر نتيجة سوء أداء الأفراد العاملين على تلك النظم، وعدم قيامهم بواجباتهم على أكمل وجه، وإهمالهم وعدم كفاءتهم بالقيام بالأعباء في ظل استخدام تكنولوجيا

(1) حجر، عبد الملك إسماعيل، (2009)، "نظم المعلومات المحاسبية"، مرجع سابق، ص 331.

(2) الشبلي، هيثم حمود، (2009)، "إدارة مخاطر الاحتياطي في قطاع الاتصالات"، مرجع سابق، ص 228.

(3) Abu-Musa, Ahmad A., (2006), "Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations", *OP. Cit.*, PP: 1-26.

المعلومات الحديثة⁽¹⁾، ويؤكد ذلك معظم الدراسات السابقة لهذه الدراسة فقد أوضحت إن سوء أداء الموارد البشرية الناتج عن الإهمال أو القصور في الكفاءة سواء كان بحسن نية أو بقصد جعل كثيراً من المنشآت تواجه مخاطر عديدة أثرت في كفاءة المنشأة بسبب سوء أداء العنصر البشري.

وقد يُعزى السبب في أن التطور الهائل في تكنولوجيا المعلومات لم يصاحبه تطور مماثل في القدرات والكفاءات البشرية من مستخدمي هذه التكنولوجيا،⁽²⁾ وكثير من الموظفين يتهاون في تطبيق السياسات الأمنية ويتعاملون بحسن نية - (كنسيان كلمة المرور للدخول للنظام، أو السماح لزملاء باستخدامها) - متجاهلين ما يترتب على هذا التهاون من مخاطر فادحة على المنشأة وعليهم، وعلى الرغم من أن كلمات المرور تطبق عادة على رقابة الوصول إلى معظم نظم المعلومات إلا إنه ما زال هناك عدد قليل من المستخدمين لا يعرف أهمية الحاجة لأمن كلمة المرور والعواقب التي تتمثل في سوء استخدام النظام.

1-3-4-3: إهمال بعض الأفراد العاملين في نظام المعلومات المحاسبية: قد يؤدي إهمال الأفراد العاملين وعدم بذلهم العناية المهنية الكافية لأداء العمل، إلى تسرب معلومات مهمة حيث قد يترك أحدهم جهازه مفتوح ويخرج من مكتبه تاركاً لغيره فرصة التسلل والحصول على ما يريد، أو قد يترك كلمة المرور مكتوبة بجانب الجهاز أو في مكان غير آمن فيستطيع شخص آخر معرفتها، إلى غير ذلك من أنواع الإهمال الذي يحدث نتيجة نقص التأهيل والخبرة والوعي الرقابي، وعدم تدريبهم ومنحهم الوقت اللازم للتدريب على مهامهم.⁽³⁾

فالقصور المعرفي لمستخدمي نظم المعلومات هو مؤشر للأسباب الداخلية الأكثر حدوثاً لمخاطر أمن تلك النظم كنسيان كلمة المرور للدخول للنظام، أو السماح لزملاء العمل باستخدامها، كما أن المستخدم النهائي قد يدخل بيانات خاطئة أو يتبع تعليمات بشكل غير مناسب، وقد يتسبب الخبراء بأخطاء نتيجة تصميمهم أو تطويرهم أو إصلاحهم لبرمجيات نظام معلومات المنشأة.⁽⁴⁾

ومن الأسباب الرئيسية لعملية إهمال الأفراد العاملين هو تهاونهم وضعف إدراكهم لأهمية الاحتفاظ بسرية المعلومات أو عدم معرفتهم بالمعلومات التي تحتاج إلى حماية ومن يمتلك الدافع إلى سرقتها سواء من داخل المنشأة أو من خارجها،⁽⁵⁾ وقد أظهر مسح للتهديدات الأمنية أن ما يقرب من 65 % من جميع التهديدات الأمنية لنظم المعلومات هي أخطاء بشرية سواء عرضية نتيجة السهو أو طبيعة متعمدة.⁽⁶⁾

1-4-4-3: ارتفاع مستوى خبرة بعض العاملين في مجال التشغيل الإلكتروني: إن زيادة خبرة الأفراد في استخدام الحاسبات الآلية في النظم المحاسبية ولكنهم غير مخولين بالوصول للملفات من أهم عوامل ظهور مخاطر نظم المعلومات، حيث يمكن للمبرمج مثلاً الوصول إلى البيانات عمداً لتحقيق مكاسب شخصية خاصة في حالة عدم فعالية

(1) Senft, Sandra & Gallegos, Frederick, (2009), *OP. Cit.*, P.230.

(2) البجيصي، عصام محمد، (2011)، "استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة في الشركات الفلسطينية العامة في قطاع غزة : دراسة تطبيقية"، *مرجع سابق*، ص: 1147-1177.

(3) Humphreys, Edward, (2010), *Information Security Risk Management, Handbook for ISO/IEC 27001*, British Standards Institution (BSI), Available at: <http://shop.bsigroup.com/bip0076> (Accessed May 14, 2012).

(4) Laudon Kenneth C. & Laudon Jane P., (2011), *"Management Information Systems- Managing The Digital Firm"*, *OP. Cit.*, USA, P. 327.

(5) الحميد، محمد دباس & ونيو، ماركو إبراهيم، (2007)، "حماية أنظمة المعلومات"، *مرجع سابق*، ص: 35.

(6) Gerić, Sandro & Hutinski, Željko, (2007), *Information System Security Threats Classifications*, *OP. Cit.*, PP: 59-60.

إجراءات الرقابة الخاصة بالوصول للبيانات والبرامج،⁽¹⁾ فالمهاجم من الداخل إذا كان ماهراً فإنه بمقدوره أن يطمس أي آثار تدل على ارتكابه للهجوم، فالمهاجم من الداخل يتمتع بمزية لا يتمتع بها المهاجمون من الخارج، وهي أنه ليس عرضة لكثير من الإجراءات الاحترازية الأمنية التي يتعرض لها المهاجم من الخارج، ولذلك يمكنه القيام بأعمال يصعب على غيره القيام بها.⁽²⁾

وتشير الدراسات التي أجرتها دائرة المحاسبة العامة في الولايات المتحدة الأمريكية إلى أن الخسائر الناتجة عن جرائم الكمبيوتر تقدر بحدود 1.5 مليون دولار لشركات المصارف المحوسبة في أمريكا، ومن ناحية أخرى يقدر المركز الوطني لبيانات جرائم الحاسوب في لوس أنجلوس بأن 70% من جرائم الحاسوب المسجلة حدثت من الداخل، أي من قبل من يعملون داخل المنشآت، هذا و أن جرائم الحاسوب تزداد بصورة واضحة مما أصبحت تشكل تحدياً خطيراً يواجه الإدارات العليا عموماً وإدارة نظم المعلومات على وجه الخصوص.

وخلصت الدراسات الحديثة في مجال أمن وحماية نظم المعلومات بأن المشاكل التي يسببها موظفو الداخل هي الأكثر والأخطر في مجال السرقات والتخريب والتجسس، وتأتي من قبل المتخصصين في تقنية المعلومات وذلك لزيادة معرفتهم بأسرار النظم ونقاط ضعفها وثغراتها، والضوابط الرقابية المطبقة، مما ينتج عن ذلك مخاطر لنظم المعلومات المحاسبية.⁽³⁾

1-3-4-5: التصرفات الانتقامية للأفراد الغاضبين: تحدث مخاطر أمن نظم المعلومات الناجمة عن الأفراد العاملين في البنوك بشكل اختلاسات وتزوير وسرقات، وذلك لأسباب مالية بهدف اختلاس الأسهم والسندات، أو تغيير البيانات لإيجاد تسويات مالية محظورة إلى جانب سرقة المعلومات وإعادة بيعها لأطراف مناسبة،⁽⁴⁾ أو لأسباب عاطفية للشعور بالظلم نتيجة تخطي الآخرين له في الترقية أو أنه يعامل بصورة لا يراها منطقية وتعرضه للنقد الشديد غير الموضوعي أو عدم وجود نظام حوافز عادل، أو لمجرد إرضاء فضوله الفكري من منطلق التحدي لإثبات خطأ الإدارة عندما أعلنت إن لديها نظاماً آمناً لا يمكن اختراقه.⁽⁵⁾

ويمكن تعريف الغش في مجال الحاسبات الالكترونية بأنه كل تلاعب من قبل الأفراد في البرامج وملفات البيانات، والتشغيل، والمعدات ويؤدي ذلك إلى إلحاق خسائر للمنشأة،⁽⁶⁾ ويجب ملاحظة أن معظم مرتكبي حالات الغش من داخل المنشأة، حيث أجرت لجنة المراجعة البريطانية مسحاً بيّن أن أكثر الناس ارتكاباً لحالات غش الحاسبات هم العاملون في مجال الحاسبات ويرجع ذلك إلى ضعف أساليب الرقابة الداخلية القائمة وعدم الأخذ بالأساليب المتطورة منها، كما أن العاملين بالنظام الذين يتم استبعادهم يعلمون كلمات السر وبالتالي يمكنهم الوصول غير المصرح به للنظام

(1) French, Aaron M., (2012), " A Case Study on E-Banking Security – When Security Becomes Too Sophisticated for the User to Access Their Information", *Journal of Internet Banking and Commerce*, Vol. 17, No.2, August 2012, PP: 1-15.

(2) العثير، خالد سليمان، & القحطاني، محمد عبدالله، (2009)، *أمن المعلومات بلغة ميسرة*، مرجع سابق، ص: 29-30.

(3) Mihalache, Arsenie, (2011), " Security of the Accounting Information System Infrastructure", *Annals of the "Ovidius" University, Economic Sciences Series*, Volume XI, No.1, PP: 1339-1345, <http://ideas.repec.org/a/ovi/oviste/v11y2011i1p1339-1345.html>

(4) الجواد، دلال صادق & القتال، حميد، ناصر، (2008)، " *أمن المعلومات* "، مرجع سابق، ص: 15-16.

(5) Griffin, James S. & Grimaila, Michael, (2008), "Eleventh Annual Conference of the Southern Association for Information Systems (SAIS)", *the Southern Association for Information Systems Conference*, Virginia Commonwealth University, Richmond, Virginia, 13 - 15 March 2008.

(6) محمد، حيدر صاحب، (2011)، "مسؤولية مراقب الحسابات في تحديد و تقييم مخاطر تكنولوجيا نظم المعلومات المحاسبية لرفع جودة أدائه"، *مرجع سابق*، ص: 88.

وارتكاب حالات الغش أو نقل عدوى الفيروسات، ويحدث ذلك أثناء عملهم بسبب معاقبتهم أو بعد إنهاء خدماتهم بسبب فصلهم من العمل، حيث يقوموا بالكشف عن بعض المعلومات السرية.

ويشكل الموظفون الذين فقدوا وظائفهم خطراً كبيراً حيث يقوموا بجمع المعلومات الداخلية سابقاً وأخذ نسخ من البيانات، كما أن الموظفين الحاليين يمكنهم الحصول على دخل إضافي عن طريق بيع بيانات المنشأة إلى المنافسين، والموظفين سواء كانوا سابقين فقدوا وظائفهم أو الحاليين، وبصرف النظر عن دوافعهم فهم يشكلوا مصدر خطر حقيقي لأن لديهم القدرة على الوصول إلى معلومات المنشأة، حيث أوضحت الكثير من الدراسات أن ما نسبته 90 % تقريباً من اختراقات الأمن تأتي من داخل المنشأة.

ومثال ذلك قيام مبرمج كان يعمل في إحدى المنشآت بعد فصله من العمل بإضافة بعض التعليمات على البرامج قبل تركه للعمل، وكان لذلك تأثير على البيانات حيث ألغت قوائم الحسابات المدفوعة للمنشأة، الأمر الذي سبب خسائر مادية ومشكلات كبيرة.⁽¹⁾

1-3-4-6: انخفاض معدل دوران موظفي نظم المعلومات: من الأدوات التي يمكن استخدامها لتحديد وتقييم المخاطر مثل هيكل البنك، وطبيعة أنشطة البنك، والتغيرات التنظيمية ومعدل دوران الموظفين، حيث أن انخفاض معدل دوران موظفي نظم المعلومات لدى المنشأة، واحتفاظهم بأسرار الأنظمة ومفاتيح الحل وعدم تعاونهم مع زملائهم في تبادل المعرفة والخبرة، ووضع العراقيل أمام الموظفين الجدد ذوي الكفاءات العالية من قبل موظفي أنظمة المعلومات القدامى والتأخر في ترقيتهم أو دراسة أوضاعهم، كل ذلك يشكل تهديد على أمن نظم المعلومات المحاسبية، لأن أمن نظم المعلومات تحتاج إلى تعاون كامل من كوادر الموظفين كافة، وذلك لغرض تطبيق سياسات أمن نظم المعلومات التي تضعها الإدارة.⁽²⁾

وتحدثت المخاطر الناجمة عن الأفراد العاملين في المنشآت بسبب حدوث إضراب أو رحيل الأفراد المتخصصين في نظم المعلومات، حيث يؤثر على جاهزية وتوثيق نظم المعلومات ويترتب عليه خسائر ملحوظة.

ومع ازدياد التحديات لأمن نظم المعلومات وزيادة التقنيات المطبقة، زاد العبء على الأشخاص المسؤولين عن أمن نظم المعلومات للتدريب والاستمرار في تعلم الطرق والممارسات الأفضل لحماية المعلومات، وهذا يترجم إلى زيادة الوقت والمبالغ اللازمة للاستمرار في تدريب أفراد أمن المعلومات على المنتجات المتاحة، قد لا يكون المبلغ اللازم لإيجاد أفراد أمن معلومات وتدريبهم هو المشكلة الرئيسة لبعض المنشآت، لكن الوقت اللازم لتدريبهم والاستمرار في تدريبهم هو المشكلة التي تواجه كافة المنشآت، وبخاصة في ظل النقص الحاد في أفراد أمن المعلومات.

(1) الحبيطي، قاسم محسن & السقا، زياد هاشم، (2011)، نظام المعلومات المحاسبية، مرجع سابق، 2

14/ 10/ 2011 18:38:26 GMT P:28, <http://www.infotechaccountants.com/resources/articles/20051.pdf>

(2) Basel Committee on Banking Supervision(BCBS), (2011), "Sound Practices for the Management and Supervision of Operational Risk", Bank for International Settlement(BIS), Basel, Switzerland, February 2011, PP: 6-22, www.bis.org

1-3-5: التهديدات الأمنية المتعلقة بضعف الرقابة الداخلية وإدارة المخاطر في المنشأة:

نظم المعلومات المحاسبية المحوسبة (CAIS) تواجه تهديدات أمنية تنشأ عن ضعف نظم التحكم (CS) الخاصة بها، وفي الوقت نفسه، فإن بقاء المنشأة يعتمد على الإدارة الصحيحة، لأمن وسرية المعلومات الخاصة بها، حيث تشكل أصول المعلومات نسبة كبيرة من القيمة السوقية للمنشأة،⁽¹⁾ فالضعف هو وجود ضعف في نظام الإجراءات لتنفيذ الرقابة الداخلية وغيرها من الأسباب التي يمكن استغلالها لتجاوز أنظمة الأمن والوصول غير المصرح به إلى المعلومات، والضعف في العملية الإدارية، أو قانون يجعل المعلومات قابلة للاستغلال،⁽²⁾ ومن أهم التهديدات الداخلية المسببة لمخاطر أمن نظم المعلومات هو ضعف الضوابط الرقابية الداخلية لتلك النظم، حيث أن التطور في تكنولوجيا المعلومات لم يصاحبه تطوراً مماثلاً في الممارسات والضوابط الرقابية، كما لم يواكب ذلك تطوراً مماثلاً في معرفة وخبرات ووعي العاملين على تلك التقنيات في المنشآت، وهناك أمثلة عديدة من المنشآت التي تم نجاح الخطر فيها بسبب نقص أو قصور في ضوابط الرقابة الداخلية،⁽³⁾ وبالتالي تتمثل التهديدات الداخلية المتعلقة بضعف الرقابة الداخلية في المنشأة بما يلي:

1-3-5-1: عدم كفاية وفعالية الأدوات والضوابط والإجراءات الرقابية المطبقة: لاحظ الباحث أن الكثير من الدراسات في مجال أمن نظم المعلومات لم تميز بشكل واضح بين مخاطر أمن نظم المعلومات وبين عدم كفاية الضوابط الرقابية لأمن تلك النظم، وهذا ما تلافته هذه الدراسة.

إن حدوث أي من مخاطر أمن نظم المعلومات يعد مؤشراً على ضعف في نظام الرقابة الداخلية إما لأن بعض الضوابط مفقودة أو ناقصة، وينشأ ضعف وقصور في أحد أو بعض نظم الرقابة بسبب اختيار نظم رقابة غير ملائمة، أو قد تتبنى المنشأة سياسات إدارية ونظم رقابة ملائمة إلا أنه لا يتم الالتزام بها ويتم مخالفتها عند التنفيذ، فالعديد من أوجه الضعف في الرقابة الداخلية تؤدي إلى الأخطاء المحاسبية والأخطاء المالية ويمكن أن تُعزى إلى عدم كفاية ضوابط تكنولوجيا المعلومات،⁽⁴⁾ كما إن الضوابط التي لم يتم تصميمها بشكل مناسب هي غير فعالة لأنها ببساطة لم تُصمَّم لتحقيق النتيجة المقصودة، أو لم يتم تنفيذها بشكل صحيح، أو قد تكون مفرطة بشكل زائد في وسائل التحكم والسيطرة.⁽⁵⁾

إن عجز التدابير الأمنية لنظم المعلومات وغياب أو ضعف الإجراءات والضوابط الرقابية القادرة على توفير الحماية المناسبة من أهم أسباب المخاطر، لأن ضعف الإجراءات الأمنية، كالضوابط الفنية أو الضوابط المادية أو عناصر التحكم الأخرى قد تشكل تهديداً يتم استغلاله من معظم الحوادث الأمنية، مما يتيح إمكانية اختراق نظم

(1) Hayale, Talal H. & Abu-khadra, Husam A., (2006), "Evaluation of the Effectiveness of Control Systems in Computerized Accounting Information Systems: An Empirical Research Applied on Jordanian Banking Sector", *Journal of Accounting – Business & Management*, No. 13, 2006, PP:39-68.

(2) Stroie, E. R. & Rusu, A. C., (2011), "Security Risk Management - Approaches and Methodology", *OP. Cit.*, PP: 228- 240.

(3) Sani, Alireza & Chaharmahalie, Shahram, (2012), "Internal Accounting Controls", *Engineering and Technology*, World Academy of Science, No. 62, PP: 54-57.

(4) Benaroch, Michel & Chernobai, Anna & Goldstein, James, (2012), "An Internal Control Perspective on the Market Value Consequences of IT Operational Risk Events", *International Journal of Accounting Information Systems*, Vol.13, March 2012, PP:357- 381, Contents lists Elsevier Available at: SciVerse ScienceDirect. <http://dx.doi.org/10.1016/j.accinf.2012.03.001>

(5) Palfi, Cristina & Mureşan, Mariana, (2009), "Survey on Weaknesses of Banks Internal Control Systems", *Journal of International Finance & Economics*, Vol. 9, Issue 1, PP: 106-116.

المعلومات المحاسبية للمنشأة من قبل أشخاص غير مرخص لهم بذلك، سواء أكان ذلك من خارج البنك أو من العاملين فيه،⁽¹⁾ فإجراءات الرقابة غير الكافية تزيد من فرص التلاعب والتزوير، أو تغيير السجلات المحاسبية كالدخول غير المصرح به لنظم المعلومات المحاسبية، وبالتالي من الصعب في هذه الحالة ضمان أن يتم تسجيل المعاملات وتجهيزها، والإبلاغ عنها بشكل صحيح ودقيق.⁽²⁾

ومن أهم أسباب ضعف الإجراءات الرقابية في نظم المعلومات المحاسبية ما يلي:⁽³⁾

1. تصميم تلك الإجراءات دون إعطاء النظام خصوصيته على الرغم من اختلاف النظم المحاسبية في الأهداف والإجراءات والإطار النظري والتطبيقي ولذلك ينبغي دراسة تلك النظم وتحليلها ثم وضع الأسس والأساليب الرقابية الملائمة.
2. عدم استقرار نظم المعلومات المحاسبية، بمعنى أنه كلما وضعت أسس وأساليب أمنية ورقابية لنمط محاسبي فإن تطور هذا النمط يلغي تلك الأسس والأساليب أو يجعلها بحاجة للتحديث من جديد ثم إن التغيير يستوجب دراسة كاملة للنظم المحاسبية، حتى لا تترك ثغرة في النظام سواء أثناء التحول أو بعده يكون من شأنها منع النظام من تحقيق أهدافه.
3. عدم نضوج النظرية المحاسبية واستقرارها للبحث والتطوير ولازال مستمرا في جميع جوانبها ولا زالت تتعرض لتغيرات مستمرة، كما أنها لا زالت تعاني من عدم اتفاق دولي على المبادئ والممارسات المحاسبية المقبولة فتطبيق معايير معينة في دولة ما، لا يعني بالضرورة قبول تطبيقها في دولة أخرى، كما نجد أن المعايير المحاسبية تتغير باستمرار في الدولة الواحدة بسبب عدم ثبات الفكر المحاسبي حتى الآن.
4. عدم وجود قواعد أو ضوابط للسلوك المهني في مهنة المحاسبة يحدد العمل المقبول والعمل غير المقبول، من أهم أسباب الدخول غير المشروع للنظم المحاسبية.

ورغم وجود مشاكل في أساليب الرقابة إلا أن إجراءات الرقابة أكثر أهمية في نظم المعلومات المحاسبية الالكترونية عن تلك المتبعة في النظم اليدوية،⁽⁴⁾ وهناك نوعان من الضعف في نظم الرقابة الداخلية الأول يتعلق بالتصميم والثاني بالتنفيذ، ومن شأن ذلك أن يؤدي إلى عدم منع أو كشف الغش والتلاعب بالقوائم المالية، وإن معالجة هذا الضعف قد لا يميز بين ضعف التصميم عن ضعف التنفيذ، وإن معظم التحسينات تتركز على عيوب تنفيذ نظم الرقابة الداخلية، ويرجع ذلك لزيادة درجة التعقيد في الأنظمة المحوسبة، ومن ثم صعوبة وضع نظم الرقابة الداخلية الكفوءة والفعالة،⁽⁵⁾ وعدم وجود ضوابط فعالة وهيكل سليم للرقابة الداخلية في المنشأة يمكن أن يؤدي إلى مشاكل مختلفة وبالتالي فإن عدم القدرة على تحديد ضوابط فعالة يؤدي إلى خروقات أمنية،⁽⁶⁾ وجميع أنظمة الرقابة الداخلية بغض النظر عن تصميمها تواجه محددات متلازمة معينة بحيث تجعل من الصعب بل من المستحيل الحصول على تأكيد مطلق، وأنه كلما كانت

(1) شاهين، علي عبدالله، (2010)، "نظم الدفع الالكترونية ومخاطرها ووسائل الرقابة عليها دراسة تطبيقية على بنك فلسطين"، مجلة جامعة الأزهر بغزة، مجلد (12)، العدد(1)، ص ص: 511-546.

(2) Beard, Deborah & Wen, H. Joseph, (2007), "Reducing the Threat Levels for Accounting Information System, Challenge for Management, Accountants, Auditors and Academicians", OP. Cit., PP: 34-42.

(3) أحمر، إسماعيل، (2006)، "أسباب ضعف الإجراءات الرقابية في نظم المعلومات المحاسبية - دراسة تحليلية"، مجلة تنمية الرافدين، المجلد (82)، العدد (28)، جامعة الموصل، العراق، ص ص: 42-21.

(4) عمران، جمال، (2008)، "أساليب الرقابة الداخلية في نظم المعلومات المحاسبية الإلكترونية"، مجلة تشرين للدراسات والبحوث العلمية سلسلة العلوم الاقتصادية والقانونية، المجلد 28 العدد 1، ص ص: 12-13.

(5) محمد، حيدر صاحب، (2011)، "مسؤولية مراقب الحسابات في تحديد وتقييم مخاطر تكنولوجيا نظم المعلومات المحاسبية لرفع جودة أدائه"، مرجع سابق، ص: 87.

(6) Mishra, Sushma and Dhillon, Gaurpreet, (2008), "Defining Internal Control Objectives for Information Systems Security: A Value Focused Assessment", ECIS 2008 Proceedings, Paper 210, <http://aisel.aisnet.org/ecis2008/210>

الرقابة الداخلية أكثر تعقيدا كانت الإجراءات أكثر كثافة.⁽¹⁾ ومن المهم افتراض أن التدابير المضادة في نظام المعلومات ليست كافية لمنع التهديدات والمخاطر المحتملة.⁽²⁾

ويرى الباحث أن التحدي الأكبر لإدارة المنشأة هو إيجاد التوازن بين تكلفة تصميم وتنفيذ الرقابة الداخلية وبين المنافع المتوقعة منها لذلك فإن الرقابة المفرطة تكون ذات تكلفة مرتفعة وتعطي نتائج عكسية وبنفس الوقت فإن الرقابة الضعيفة تؤدي إلى مخاطر كثيرة.

1-3-5-2: عدم إصدار تقارير رقابية دورية حول الأنظمة الآلية، ليتم متابعتها وتقييمها: من أسباب ضعف نظم الرقابة

الداخلية الاعتماد المبالغ فيه على مدقق الحسابات من قبل إدارة المنشأة واعتبار أن جميع ما لم يرد في ملاحظات مدقق الحسابات خاطئاً،⁽³⁾ ويعتقد الاتحاد الدولي للمحاسبين (IFAC) أن إدارة المنشآت يجب أن تكون شفافة في الإبلاغ عن هيكل وترتيبات الرقابة الداخلية، والضوابط التي وضعها، وكيف يتم رصدها وتقييمها، وكذلك إدارة المخاطر، في مختلف تقاريرها الداخلية وكذلك الموجهة لأصحاب المصلحة الخارجيين لما من شأنه توفير الثقة والطمأنينة لديهم.⁽⁴⁾ ويجب أن يكون ذلك بشكل متطور ومستمر بما يواكب مستجدات التطور التقني من خلال مراقبة المخاطر المفترضة والمتوقعة وابتكار حلول لها، فلا يوجد نظام معلومات آمن بشكل مطلق إذا لم يكن هناك مواكبة واستمرارية في التطوير لتقليل واحتواء المخاطر المفترضة أو المتوقعة.⁽⁵⁾

المراجعة الداخلية للحسابات ووظائف أمن المعلومات يجب أن تعمل معا بالتآزر: من خلال تصاميم أمن نظم المعلومات، وتنفيذ مختلف الإجراءات والتقنيات لحماية موارد معلومات المنشأة، وتوفير ردود فعل دورية بشأن فعالية تلك الأنشطة جنبا إلى جنب مع اقتراحات للتحسين.⁽⁶⁾

والتنفيذ الناجح لأفضل الممارسات يتطلب الحصول على تقارير ومعلومات ملائمة ومتعلقة بالمخاطر التي تهدد أمن نظم المعلومات، وتأثيراتها، وتكاليف وفعالية أفضل الممارسات حتى تتمكن الإدارة من الاختيار بين حلول بديلة.⁽⁷⁾

1-3-5-3: عدم كفاءة وفعالية إجراءات إدارة المخاطر وعدم القيام بالتقييم الذاتي لمخاطر: من أهم التهديدات الداخلية

المسببة للمخاطر عدم القيام بالتقييم الذاتي بحيث يقوم كل موظف بتحديد المخاطر التي يواجهها لتحديد نقاط القوة والضعف وتقييم إجراءات مواجهتها، وعدم وجود نظام لإدارة المخاطر يتم من خلاله إدارة المخاطر وتقييمها وتقديم التوصيات اللازمة للإدارة العليا للحد منها ومعالجات الاختلالات الموجودة.

إن تقييم وتحليل المخاطر الأمنية هي جزء هام من إدارة المخاطر في المنشأة ويركز أساساً على تحليل نقاط الضعف والتهديدات لموارد نظم المعلومات واتخاذ قرار بشأن الإجراءات الواجب اتخاذها لتقليل المخاطر إلى مستوى

(1) الدوجي، علي حسين، (2008)، " دور مراقب الحسابات في ظل تكنولوجيا المعلومات المعقدة ومخاطر التدقيق"، مرجع سابق، ص ص: 285-304.

(2) Maram, Venkata et al., (2012), "A Study of Risk Management of an Information System by Assessing Threat, Vulnerability and Countermeasure", *OP. Cit.*, PP: 51-53.

(3) أمّرو، إسماعيل، (2006)، "أسباب ضعف الإجراءات الرقابية في نظم المعلومات المحاسبية - دراسة تحليلية"، مرجع سابق، ص ص: 21-42.

(4) International Federation of Accountants (IFAC), (2012), "Effective Governance, Risk Management, and Internal Control", <https://www.ifac.org/publications-resources/effective-governance-risk-management-and-internalcontrol#node-19388> (accessed on 25 December 2012).

(5) Von Solms, Rossouw & Niekerk, Johan van, (2013), "From information security to cyber security", *OP. Cit.*, PP: 97-102.

(6) Steinbart, Paul John et al., (2012), "The Relationship Between Internal Audit and Information Security: An Exploratory Investigation", *International Journal of Accounting Information Systems*, Vol. 13, No. 3, June 2012, PP: 228-243.

(7) Anderson, Evan E. & Choobineh, Joobin, (2008), "Enterprise Information Security Strategies", *Computers & Security*, Vol. (27), No. (1-2), March 2008, PP: 22-29.

مقبول، ومن مبادئ إدارة المخاطر مراقبة المخاطر بإجراء اختبارات دورية للنظم وتتبع الثغرات وحالات عدم الكفاءة وتخفيض حجم المخاطر بهدف التحقق من توافر سياسات وإجراءات مطورة والتزام البنك بها.⁽¹⁾

إن تطبيق نظام التقييم الذاتي للرقابة والمخاطر (CRSA) وهو نظام يعمل على تحديد المخاطر المتعلقة بالأنشطة والوحدات داخل المنشأة والضوابط الواجب وضعها لمواجهتها، وتقييم هذه الضوابط بحيث يتم اختبارها ذاتياً من خلال مسؤولي الأنشطة والوحدات المباشرين، ورفع تقارير دورية لمجلس الإدارة بنتائج الاختبارات.

ويرى الباحث إن ترك الأنشطة والممارسات المصرفية بدون رقابة ومتابعة سيؤدي إلى مشاكل تهدد بخطر فقدان العملاء لودائعهم وفقدان البنوك لرؤوس أموالها وبالتالي إمكانية الإفلاس أو المقاضاة أمام المتعاملين أو وقوع مخالفات على البنك من قبل الجهات المشرفة الحكومية التي تمارس أنواع الرقابة الخارجية على البنوك كالبنك المركزي.

1-3-5-4: غياب المسار المرئي للمراجعة: يعتبر مسار المراجعة (Audit Trail) من أهم وسائل الرقابة الوقائية (السابقة)، ويعني إمكانية التحقق من مسار العمليات المحاسبية في المنشأة وتعقبها وتتبعها بدءاً من المستندات الأصلية، وانتهاءً بالإفصاح عن المعلومات في التقارير المالية،⁽²⁾ أي أن مسار المراجعة يمكن الإدارة من معرفة مصير بيانات العمليات خلال مراحل معالجتها المختلفة سواء في ظل النظام المحاسبي اليدوي، أو الإلكتروني. حيث يكون بالإمكان اكتشاف وتصحيح الأخطاء أثناء القيام بالمعالجات المحاسبية، وفي ظل نظم المعلومات المحاسبية الإلكترونية يصبح مسار المراجعة غير ملموس حيث تتم معالجة البيانات داخلياً في أجهزة الكمبيوتر، ويصعب تتبعه.⁽³⁾

تعد إجراءات الرقابة أكثر أهمية في نظم المعلومات المحاسبية المحوسبة عن تلك المتبعة في نظم المعلومات اليدوية لعدة أسباب أهمها أنه يتم جمع ومعالجة وتخزين بيانات العمليات المحاسبية في صورة غير قابلة للقراءة ولا يمكن للإنسان مراقبة هذه البيانات والتحقق من دقتها وموضوعيتها والتي كان يسهل إجراؤها تحت النظام اليدوي للمعلومات المحاسبية وصعوبة تتبع مسار التدقيق مما قد يترتب عليه احتمال قيام الموظفين غير الأمناء باختلاس مبالغ طائلة من المنشآت التي يعملون بها.⁽⁴⁾

وهناك مجموعة من المشاكل التي يمكن حدوثها في أساليب الرقابة الداخلية ضمن بيئة نظم المعلومات المحوسبة منها إنقاص مسارات التدقيق أو إلغاؤها، فمع ظهور البيئة المستخدمة للحسابات يواجه مراجع الحسابات الداخلي مشاكل عديدة تقتضي منه ضرورة التغلب عليها حتى يستطيع أن ينجز متطلباته المهنية، لأن الرقابة الداخلية في النظم المحوسبة تفقد كثيراً من عناصرها ومساراتها ومن أبرز مظاهر ذلك مسارات العملية المحاسبية المحوسبة غير المنظورة مما يضيع على الرقيب تتبع تلك المسارات كما هو الحال في النظام اليدوي وينعكس ذلك بشكل سلبي على تحقيق أهداف الرقابة الخارجية، فقد يترتب على غياب المسار المرئي للمراجعة وعدم رؤية عمليات إدخال البيانات الإلكترونية وتشغيلها، تخطي الجانب الأمني في حماية البيانات المحاسبية وزيادة المخاطر الأمنية إذ إن سرعة تنفيذ العمليات ووجود معالجة غير مرئية قد يؤدي لحذف أو إضافة أو تعديل غير مرغوب فيه لبيانات محاسبية مهمة، وصعوبة اكتشاف ذلك، حيث يمكن إدخال البيانات مباشرة في الحاسب الآلي دون مستندات تدعم هذه المدخلات، ففي

(1) Feng, Nan & Wang, Harry & Li, Minqiang, (2013), "A Security Risk Analysis Model for Information Systems: Causal Relationships of Risk Factors and Vulnerability Propagation Analysis", *Information Sciences*, Vol. xxx, 2013, PP: 1-17, <http://dx.doi.org/10.1016/j.ins.2013.02.036>

(2) Hall, James A., (2013), *Accounting Information Systems*, OP. Cit., P.40.

(3) الرضا، عقبة كامل، (2008)، "تدقيق الحسابات في ظل نظم المعلومات المحاسبية"، *مراجع سابق*، ص: 1-13.

(4) الذبيبة، زياد & الرمحي، نضال & الجعدي، عمر، (2011)، "نظم المعلومات في الرقابة والتدقيق"، مرجع سابق، ص: 73.

بعض نظم العمليات المباشرة قد يتم إبدال الإثبات الخطى بالإذن بإدخال البيانات بإجراءات أخرى كأساليب رقابة التصريح الموجودة في برامج الحاسب الآلي،⁽¹⁾ وبالتالي يجب الاهتمام بالرقابة الداخلية والتي تؤثر على كفاءة وفعالية نظم المعلومات المحاسبية المحوسبة.

1-3-6: التهديدات الأمنية المتعلقة بحدوث الكوارث غير الطبيعية في المنشأة:

تحدث أحياناً كوارث غير طبيعية ناتجة من البيئة الداخلية للبنك (كالتخريب، والحريق، وتذبذب أو انقطاع التيار الكهربائي أو زيادته بصورة مفاجئة، وتسريب المياه)، تسبب تلك الكوارث تلف جزئي أو تدمير كلي لموارد نظم المعلومات المحاسبية من الأجهزة والبرامج وملفات البيانات المحاسبية المخزنة، ويترتب على ذلك خسائر جسيمة،⁽²⁾ فمثلاً يعد الحريق أياً كان سببه – عمدي أو نتيجة إهمال – من أكبر التهديدات، وعدم الإسراع في السيطرة عليه قد يؤدي إلى تخريب المنشأة كلها، وتظهر تلك التهديدات من خلال اختراق مقاييس الأمن الطبيعية في حالات انقطاع التيار الكهربائي، وسوء استخدام أجهزة التكييف، وتسرب المياه، أو بسبب الغبار والأتربة ... الخ، وقد يتعرض نظام المعلومات المحاسبي للإهمال المباشر في الأماكن المخصصة له، أو غير المباشر في نقاط الربط الجوهرية خارج المنشأة كما في إمداد الكهرباء أو قنوات الاتصال عن بعد.

الخاتمة: يرى الباحث إن تقييم التهديد الشامل هو جزء أساسي من تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة، وتحديد المصادر ذات الصلة بتلك المخاطر، وأن هذه التهديدات الداخلية التي تم استعراضها في هذا المبحث تعتبر شبه ملازمة لنظم المعلومات المحاسبية المحوسبة ومن الضروري أن تتخذ الإدارة العليا سلسلة من الإجراءات التي تحد منها وفي مقدمة هذه الإجراءات رفع كفاءة العاملين وقدراتهم في مراكز الحاسوب، وتهئية الأنظمة الملائمة لطبيعة عمل المنشأة، ووضع الآليات المناسبة للتعامل مع المحيط الداخلي والخارجي للمنشأة بما يؤدي إلى جاهزية واستمرارية أعمالها وفي الوقت عينه ضمان عدم الاستخدام السيئ لمعلوماتها.

وبالتالي يرى الباحث أن تهديدات مخاطر أمن نظم المعلومات المحاسبية المحوسبة كثيرة ومتنوعة، منها داخلية (من داخل المنشأة، يمكن التحكم فيها والسيطرة عليها)، ومنها خارجية (من خارج المنشأة ومن الصعب السيطرة عليها)، والهدف من معرفة وتحديد التهديدات، هو توفير الحماية اللازمة لنظم المعلومات المحاسبية، فمن خلال تحديد مصدر الخطر يتم إيجاد وسائل حماية مناسبة لكل مصدر، فأحياناً تكون الأسباب والعوامل التي أدت إلى حدوث الخطر أكثر تأثيراً من الخطر نفسه، لأنها تعد المسؤول الأول عن حدوث الخطر الحقيقي.

وقد تم مناقشة أهم التهديدات الداخلية في هذا المبحث وسيتم تناول أهم التهديدات الخارجية في المبحث التالي.

(1) Gelinas, Ulric J. & Sutton, Steven G. & Hunton, James E., (2012), *Accounting Information Systems*, 9th Edition, Thomson South-Western, Mason, Ohio, USA., P. 112.

(2) محمد، حيدر صاحب، (2011)، "مسؤولية مراقب الحسابات في تحديد وتقييم مخاطر تكنولوجيا نظم المعلومات المحاسبية لرفع جودة أدائه"، *مرجع سابق*، ص: 84.

1-4: المبحث الرابع: التهديدات الخارجية لأمن نظم المعلومات المحاسبية المحوسبة

تواجه كثير من المنشآت تحديات شاقة في ظل التغيرات التكنولوجية السريعة، وهناك حاجة متنامية وحيوية إلى فهم أفضل للتهديدات الأمنية لنظم المعلومات، للمساعدة على ضمان سلامة المعلومات في التقارير المالية للمنشآت في محاولة لاستعادة ثقة المستثمرين،⁽¹⁾ والتهديدات الخارجية لنظم المعلومات المحاسبية المحوسبة (CAIS) قد تنشأ من مصادر خارجية مثل الكوارث الطبيعية كالأعاصير، والبراكين، والفيضانات، والزلازل، وأعمال المنافسين، وضعف التشريعات والقوانين، بالإضافة إلى التهديدات الجديدة التي برزت مؤخراً مع التقدم التكنولوجي وتتمثل بقرصنة الحاسوب أو البرمجيات الخبيثة، وهذه التهديدات يمكن أن تؤدي إلى تدمير شامل أو جزئي لكافة محتويات النظم المحاسبية كالأجهزة، والبرمجيات، والبيانات، والموظفين والمرافق،⁽²⁾ مما يشكل تهديد حقيقي يترتب عليه خسائر قد تكلف الكثير من الجهد والأموال، وعادة ما تكون هذه الخسائر قاتلة لعدم وجود التخطيط المسبق لمواجهة الطوارئ والتعامل معها.

فالتحديات الخارجية الناجحة ليست شائعة مثل التهديدات الداخلية، إلا أنها تفرض تحدياً مختلفاً إلى حد كبير، وقد أظهرت دراسة أن أكثر من ثلثي الأميركيين ينظرون إلى التهديدات الخارجية، كخطر أعلى للأمن من التهديدات الداخلية، وأن أسباب المخاطر الأمنية تعددت، بحيث أن 30% منها بسبب فيروسات هاجمت الأنظمة، و19% بسبب قرصنة الانترنت ونجاحهم بالحصول على معلومات فائقة السرية واستغلالها بسرقات مالية، و19% بسبب أخطاء بشرية، و7% بسبب حدوث أعطال أو خلل ببرامج الأنظمة، و25% لأسباب أخرى متفرقة،⁽³⁾ وسيتم تناول أهم التهديدات الخارجية على النحو التالي:

1-4-1: التهديدات الأمنية المتعلقة بالتغيير التكنولوجي غير المتوازن:

يعد التطور السريع في تكنولوجيا المعلومات والانتشار الواسع لتلك النظم والبرامج، ورغبة المنشآت في اقتناء وتطبيق أحدث النظم والبرامج الإلكترونية دافع أساسي لاستخدامها في أداء العديد من المهام المحاسبية بصورة أسرع، وقد كانت المحاسبة من أهم المجالات التي تأثرت بهذا التغيير حيث شهد النصف الثاني من القرن الماضي تحولاً سريعاً نحو استخدام نظم المعلومات المحاسبية المحوسبة، ولكن في المقابل فإن هذا التطور التكنولوجي يحمل في طياته العديد من المخاطر الهامة والمتعلقة بالنظم المحاسبية المحوسبة، لأن التطور في الحاسبات وتكنولوجيا المعلومات لم يصاحبه تطور مماثل في الممارسات والضوابط الرقابية، كما لم يواكب ذلك التطور تطور مماثل في خبرات ووعي وكفاءة العاملين لتلك المنشأة من مستخدمي هذه التكنولوجيا.

(1) Tarmidi, M., et al., (2013), "Computerized Accounting Systems Threats in Malaysian Public Services", *OP. Cit.*, PP: 109-113

(2) Mihalache, Arsenie, (2011), "Security of the Accounting Information System Infrastructure", *Annals of the "Ovidius" University, Economic Sciences Series*, Volume XI, No.1, PP:1339-1345, <http://ideas.repec.org/a/ovi/oviste/v11y2011i1p1339-1345.html>

(3) French, Aaron M., (2012), "A Case Study on E-Banking Security – When Security Becomes Too Sophisticated for the User to Access Their Information", *Journal of Internet Banking and Commerce*, Vol. 17, No.2, August 2012, PP: 1-15.

ومع التطور والتقدم الهائل في تكنولوجيا الاتصالات وتبادل المعلومات والانفتاح أصبحنا نواجه كثيراً من المشاكل والصعوبات، وتحيط بنا المخاطر المفاجئة والتهديدات وكلما ازدادنا تقدماً كلما ازدادت تلك المخاطر تعقيداً، وبالتالي تؤثر سلباً على كفاءة أداء نظم المعلومات المحاسبية.⁽¹⁾

وتعمل تكنولوجيا المعلومات سلاحاً ذا حدين، فعندما يتم تسخيرها تسخيراً سليماً، فإنها تؤدي إلى تحسناً هائلاً في الأداء التنظيمي والبشري، وفي نفس الوقت عندما تستغل نظم المعلومات المحاسبية المحوسبة لأغراض خبيثة، من خلال التهديدات التي يملكها الأفراد، يمكن أن يكون لها تأثير سلبي مباشر على تجهيز المعاملات المالية.⁽²⁾

لقد غيرت البيئة التكنولوجية الحديثة التي أفرزتها الثورة التقنية بشكل جوهري كل من حياة الإنسان وعالم الأعمال وحتى شكل ومضمون العملية الإدارية وخلقت أمام الجميع تحديات كبيرة وأسهمت في ظهور مخاطر كثيرة وفرص جديدة،⁽³⁾ وتعتبر مخاطر أمن وسلامة المعلومات من أهم المخاطر التي نتجت عن التطورات المتلاحقة في تكنولوجيا المعلومات وأساليب تداولها، فقد أدى اتساع وتنوع وسائل التكنولوجيا خاصة مع تطور الأنترنت إلى ظهور وتزايد العديد من المخاطر التي تهدد أمن المعلومات المعروضة على مواقع الأنترنت.

1-4-1: التطورات التكنولوجية السريعة والهائلة والمتلاحقة: إن التقدم التقني السريع والطفرة الكبيرة التي حدثت في وسائل الاتصالات وشبكات المعلومات والدخول في عصر العولمة والأنترنت، يجعل الكثير من وسائل الحماية متقدمة بعد مرور فترة من الزمن،⁽⁴⁾ لأن تقدم التقنية خارجياً أسرع من ممارسة الأمن داخل المنشأة، وخاصة عندما تكون تلك التطورات التكنولوجية السريعة والهائلة والمتلاحقة بعد وضع الإجراءات الرقابية، وقد صاحب ذلك ظهور تهديدات ومخاطر جديدة في ساحة الأعمال، تؤثر سلباً على اختصاص وكفاءة وفعالية أمن نظم المعلومات المحاسبية.⁽⁵⁾

إن النمو السريع في تكنولوجيا المعلومات بدرجة مذهلة أصبح عامل مؤثر في تلك المخاطر، فغالباً ما نعتمد على تكنولوجيا حديثة في تطبيقاتنا الحساسة والتي غالباً ما تكون ضعيفة أمام المخاطر المحتملة،⁽⁶⁾ حيث أن كثير من المنشآت التجارية وخاصة في المجتمعات النامية لا تستطيع أن تواكب التطور والنمو التكنولوجي المرتبط باستخدام نظم المعلومات وتأمينها فلا يزال هناك قصور واضح ونقص كبير في التقنيين وعدم الأخذ بالمعايير

(1) Al-Shbiel, Mohanad & Bani Ahmad, Audeh, (2013), "The Risks of Communication Between Department of Internal Control & Computer and Its Impact On the Efficiency of the Accounting Information Systems in the Commercial Banks", *Interdisciplinary Journal of Contemporary Research in Business*, Vol 4, No 11, PP:297-303.

(2) Muhrtala, Tijani & Ogundeji, Mathias, (2013), "Computerized Accounting Information Systems and Perceived Security Threats in Developing Economies: The Nigerian Case", *Universal Journal of Accounting and Finance*, Vol.1, No.1, PP: 9-18.

(3) الجهر، كريمة & العفدة، صالح & أبو سردانة، جمال، (2010)، "أثر مخاطر استخدام التكنولوجيا في جودة عمل المدقق الخارجي دراسة ميدانية في بعض مكاتب التدقيق الأردنية"، *مجلة الزرقاء للبحوث والدراسات الإنسانية*، المجلد (10)، العدد (2)، جامعة الزرقاء، الأردن، ص: 14-32.

(4) الجبوري، ندى، (2011)، "حماية أمن أنظمة المعلومات دراسة حالة في مصرف الرافدين - فرع شارع فلسطين"، *مجلة تكريت للعلوم الإدارية*، العدد (21)، 2011، جامعة تكريت، العراق، ص: 72-94.

(5) Al-Shbiel, Mohanad & Bani Ahmad, Audeh, (2013), "The Risks of Communication Between Department of Internal Control & Computer and Its Impact On the Efficiency of the Accounting Information Systems in the Commercial Banks", *OP. Cit.*, PP:297-303.

(6) الطيطي، خضر مصباح إسماعيل، (2010)، "أساسيات أمن المعلومات والحاسوب"، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، الأردن، ص: 21.

الدولية وعدم تشفير البيانات بنظم المعلومات المحاسبية،⁽¹⁾ وقد أصبح من الحقائق المقبولة أن أي تطور جديد في التكنولوجيا يؤدي إلى زيادة المخاطر الأمنية لنظم المعلومات المحاسبية، حتى مع استخدام جميع التدابير الأمنية، لأن المخاطر مرتبطة بالبشر الذين يستخدمون وينفذون تلك التدابير.⁽²⁾

1-4-1-2: عدم وجود استقرار نسبي لنظام المعلومات: من الأسباب الخارجية للمخاطر التطورات الهائلة في مجال الاتصالات وأجهزة الحاسوب والبرامج وعدم القدرة على مواكبة ومتابعة هذه التطورات، فالحاسب اليوم يعمل في بيئة مثيرة ومعقدة ودائمة التغير، فالبيئة الاقتصادية والقانونية التي يعمل بها المحاسب تتغير بطرق غير متوقعة، ومعدل التطور الحاصل في تكنولوجيا المعلومات اليوم متزايد بشكل سريع لم يسبق له مثيل، كما أن المنشآت التجارية اليوم تقوم بتغيير بنية إدارتها وإدارة أعمالها لكي تستطيع الاستمرار في بيئة يتزايد فيها التنافس.⁽³⁾

إن البقاء في عالم اليوم يتطلب مواكبة متواصلة وناجحة مع متغيرات العصر في سوق الكترونية باتت تضم ملايين المستخدمين ويبلغ حجمها تريليونات الدولارات، ونعتقد أن مستقبل المنشآت التي تفشل في التأقلم مع الفرص والتحديات التي يطرحها هذا الواقع الجديد سيكون محدداً إن لم يكن مستحيلاً، والجميع يخافون التغيير عند استخدام التقنية ويخشون من النتائج التي قد تترتب عليه، وأن كل جديد كما يحمل المزايا فهي ليست مزايا بلا ثمن وإنما هناك ثمن ما يتعين دفعه، ونخشى أن يكون الثمن باهضاً.

ومع كل يوم جديد، ثمة جديد في ميدان التقنيات والبرمجيات والبروتوكولات، وفي كل يوم أمام مبرمج يتفقد ذهنه عن جديد في عالم الكمبيوتر والإنترنت، وهو إما جديد إيجابي يستخدم في رخاء البشرية وضمن الاستخدام الإيجابي للإبداع العقلي، أو جديد سلبي يستثمر لتحقيق أغراض غير مشروعة أو ارتكاب أفعال مجرمة أو أفعال يابأها السلوك الأخلاقي القويم، وبالتالي فإن تحديد المخاطر والثغرات والاعتداءات عملية مستمرة يوماً بعد يوم، وهي هنا ما يميز خطط الأمن بعضها عن بعض.⁽⁴⁾

والواقع أن عجز كثير من المنشآت عن مواكبة التطور السريع في تكنولوجيا المعلومات، بسبب ارتفاع معدلات التغير في تكنولوجيا المعلومات، مقابل ضعف إمكانيات تلك المنشآت سواء المالية أو البشرية لمجاراتها واستيعابها، وذلك يمثل أحد التحديات الرئيسية للمنشآت المصرفية فبالرغم من محافظتها على زيادة الإنفاق على أمن نظم المعلومات لكن يبدو أن ذلك الإنفاق غير كافي للتعامل مع معدل التغيرات في التكنولوجيا،⁽⁵⁾ فمثلاً يحصل أحد البنوك على نظام آلي ومع مرور الزمن يحصل تطور تكنولوجي ويصبح النظام الآلي الموجود غير قادر على مواكبة تلك التطورات، وهنا يستعان بمجموعة من الأفراد لديهم قدر محدود من المعرفة والخبرة

(1) Abu-Musa, Ahmad A.,(2006), "Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations", *OP. Cit.*, PP: 1-26.

(2) Abu-Musa, Ahmad A.,(2010), "Investigating Adequacy of Security Controls in Saudi Banking Sector: An Empirical Study", *Journal of Accounting-Business & Management*, Vol. 17, No.1, PP:1-41.

(3) Romney, Marshal B. & Steinbart, Paul John,(2015), *Accounting Information Systems*, OP. Cit., P.16

(4) المري، عليز، (2011)، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها، *مرجع سابق*، http://www.dralmarri.com/show.asp?field=res_a&id=205

(5) Olanmi, Omoneye & Olufunke, Lecturer, (April 2010), "Computer Crimes and Counter Measures in the Nigerian Banking Sector", *OP. Cit.*, PP: 1-10.

للمحافظة على سرية وأمن المعلومات، الأمر الذي يترتب عليه عدم استطاعة أولئك الأفراد الإلمام باستخدام التكنولوجيا الحديثة.

والتقدم التكنولوجي لن يتوقف، وستظهر تحديات جديدة، وهذه التحديات إذا لم يتم تداركها سريعاً فإنها قد تسبب أضراراً لكثير من مستخدمي نظم المعلومات المحاسبية المحوسبة

ولذلك يرى الباحث أن معدل التطور التكنولوجي في نظم المعلومات المحاسبية يكون أسرع من إجراءات السيطرة والتحكم لضمان أمن نظم المعلومات المحاسبية، وأن استمرار التطور في تكنولوجيا المعلومات يؤدي إلى استمرار الفجوة بين واقع هذه النظم وما قدم من حلول كممارسات وضوابط رقابية، وخاصة تلك النظم التي تعتمد على الدخول والتشغيل المباشر للمعلومات، وذلك يشكل أحد التهديدات الخارجية الهامة المسببة لمخاطر أمن نظم المعلومات المحاسبية.

1-4-3: تصميم أساليب للتلاعب تبني داخل النظام المحاسبي الإلكتروني: أدى التطور السريع في استخدام أساليب تكنولوجيا المعلومات إلى زيادة وسهولة إمكانية التلاعب في المعلومات المحاسبية، علاوة على صعوبة اكتشاف مثل ذلك التلاعب أو حدوث سرقة أو فقدان المعلومات والسجلات دون ترك أثر خاصة في ظل عدم وجود مستندات ورقية،⁽¹⁾ فالتطور التكنولوجي في الاتصال عن بعد قد سهل الوصول إلى نظم المعلومات من أي مكان وبالتالي فهناك احتمال لإمكانية الوصول غير المسموح به وإساءة استخدام نظم المعلومات.

إن التهديدات المتعلقة بتكنولوجيا المعلومات هي تلك التي تنطوي على البرمجيات والأجهزة، البيانات و الشبكة، وتوجد عوامل فنية وأساليب تؤدي لفشل نظم المعلومات المحاسبية المحوسبة وهي عديدة ومتنوعة يصعب اكتشافها، وتعتبر غير مفهومة في بعض الأحيان لغير المتخصصين في مجال النظم والتطبيقات والمواقع فهي تتغير على الدوام وتؤدي إلى إنتاج معلومات محاسبية خاطئة.

1-2-4: عدم توفر بنية تحتية تكنولوجية قوية: لا بد من الإقرار أن هنالك عدم مواكبة للعصر في موضوع التقنيات المعلوماتية بشكل عام في الدول العربية، بل أن هناك ما يشبه الاستسلام في بعض الأحيان أو التسليم في الأحيان الأخرى بالعجز وقصر ذات اليد أمام معضلة تتطلب أكثر ما تتطلب لحلها الإرادة والاستعداد لتحمل تكلفة موازنة العصر الحديث وقد تكون التكلفة مادية وسياسية وإدارية وبالطبع علمية وتشريعية.⁽²⁾

معظم الدول العربية لا تزال تعاني من ضعف الهياكل الأساسية لتكنولوجيا المعلومات والمتمثلة في شبكات الاتصال ونظم المقاييس والمعايير للعمالة المدربة، علاوة على غياب سياسات وطنية للمعلومات متبلورة قومياً وقطرياً، وضعف بنية الاتصالات التقنية، وضعف بنية الكوادر المعلوماتية الوطنية، وضعف الإنفاق على المعلومات ومراكزها، وقد تكون الصعوبة نابعة من مكون النظام الخارجي كما في دوائر الاتصالات عن بعد أو الأقمار الصناعية أو نتيجة لتواصل وترابط مكونات النظام المختلفة معاً.

(1) الطنملي، سهير، (2009)، "دور الرقابة الداخلية في دعم و تفعيل أمن و سلامة المعلومات في البنوك الالكترونية والخلوية: الجزء الأول"، مجلة المال والتجارة، العدد (478)، نادي التجارة بشبين الكوم، المنوفية، مصر، ص ص: 27-48.
(2) الخطيب، محمد، (2012)، أمن المعلومات، مرجع سابق، "ورقة عمل".

وقد أدى التطور التكنولوجي الذي يعيشه عالمنا المعاصر إلى إمكانية تشغيل المواقع البعيدة جغرافياً بمستوى عالٍ من الكفاءة في بيئة عمل أخرى أو في مركز حاسوب آخر بعيد جغرافياً وهذا أوجد مصادر تهديد جديدة لم تكن معروفة من قبل حيث لا يمكن لأحد أن يضمن سلامة البرامج والتأكد من حسن نواياها وخاصة إذا كانت المعلومات المالية والمحاسبية تتمثل عبر شبكات اتصال خارجية.

1-4-2: التهديدات الأمنية المتعلقة بالكوارث الطبيعية والسياسية:

تحدث مخاطر أمن نظم المعلومات المحاسبية بسبب الكوارث الطبيعية والسياسية،⁽¹⁾ مثل الزلازل والعواصف والفيضانات والأعاصير وأعطال التيار الكهربائي والحرائق والحروب وسواء كانت تلك الكوارث طبيعية أو غير طبيعية فإنها قد تؤثر على عمل النظام المحاسبي وقد تؤدي إلى تعطل عمل التجهيزات وتوقفها لفترات طويلة مما يؤثر على أمن وسلامة نظم المعلومات المحاسبية المحوسبة،⁽²⁾ وهذا النوع من الكوارث يصعب التنبؤ به، ويمكن أن يدمر نظام معلومات المنشأة بالكامل وهو ما يعني انهيار المنشأة.⁽³⁾

وتعرف الكارثة بأنها "حادثة كبيرة مفاجئة ينجم عنها خسائر كبيرة في الأرواح والممتلكات، وقد تكون طبيعية مردّها فعل الطبيعة كالأعاصير والفيضانات والسيول، أو قد تكون صناعية أو كارثة فنية مردّها فعل الإنسان سواء كان إرادياً أو لا إرادياً، وتتطلب مواجهتها معونة الحكومة الوطنية، أو على المستوى الدولي إذا كانت قدرة مواجهتها تفوق القدرات الوطنية"، وتعرف الكوارث على أنها ظواهر تحول مفاجئ غير متوقع في نمط الحياة العادية وذات أثر على النشاطات البشرية تتسبب في كثير من الأحيان بأضرار فادحة تتجاوز المنطقة المنكوبة منتجة خسائر في الموارد البشرية والمادية، وتعد العوامل الطبيعية والممارسات الإنسانية من أهم المسببات لمثل هذه الكوارث، ومن أمثلة هذه الكوارث انقطاع التيار الكهربائي لفترات طويلة، أو لأكثر من مرة في الفترات القصيرة، والزلازل القوية، والبراكين، والفيضانات المائية المصحوبة بالشوائب الطينية، والحرائق الناتجة عن الجفاف وارتفاع درجات الحرارة، والأعاصير والعواصف، والتي قد ينتج عنها تأخير أو تدمير أو تعطيل لبعض أو كل من موجودات نظم المعلومات المحاسبية المحوسبة، مما يولد خسائر في المال والوقت والجهد، مع الإشارة إلى أن كافة أشكال الكوارث والأمثلة السابقة منها يمكن أن تحدث بشكل طبيعي نتيجة لتغيرات جيولوجية أو مناخية، أو من الممكن أن تحدث بشكل غير طبيعي ويطلق عليها الكوارث غير الطبيعية، وغالباً ما تكون نتيجة لما يقوم به الإنسان على هذا الكوكب، فالتجارب النووية، ومخلفات التقدم الصناعي والتكنولوجي من أهم أسباب حدوث الزلازل والبراكين وارتفاع درجات الحرارة والحرائق والعواصف.⁽⁴⁾

(1) Shamszadeh, Bagher & Sharif, Abolfazl Azizi, (2012), "Computerized Accounting Information Systems (CAIS) Versus Security Threats", OP. Cit., PP: 69-80.

(2) الذبيبة، زياد & الرمحي، نضال & الجعدي، عمر، (2011)، "نظم المعلومات في الرقابة والتدقيق"، مرجع سابق، ص 66.

(3) عيسى، علا & عاشور، عصاف، (2010)، "مخاطر نظم المعلومات المحاسبية وحوكمة الشركات ومواجهة الأزمة المالية العالمية"، مرجع سابق، ص 408-434.

(4) حريز، سامي & عبودي، زيد، "إدارة الكوارث والمخاطر الأسس النظرية والتطبيقية"، ط1، دار الراية، عمان، الأردن، 2008، ص ص: 15-16.

ويكاد يكون هذا التعريف أكثر تحديداً وشمولاً من غيره؛ فهو يضيف بعداً مهماً للغاية لم يرد في المفاهيم السابقة، وهو توفر فريقٍ لمواجهة الكارثة، ومن هنا يمكن ملاحظة تركيز المفاهيم السابقة على الآثار السلبية للكارثة، وفي المقابل يغفل هذا المفهوم مع ما سبق من مفاهيم جانب الاستعداد المسبق للكارثة.

ويرى الباحث مستنيراً بما سبق، أنه يمكن تعريف الكارثة بأنها فاجعة مفاجئة تحل بمجتمع معين، تؤدي إلى تعطيلٍ جديٍّ لحركة العمل في هذا المجتمع، يتسبب بالخسائر المادية والبشرية والبيئية الكبيرة، مما يتطلب توفر فريق كفاء مدرب مسبقاً للخروج من الكارثة.

وتقع التهديدات الطبيعية والسياسية لنظم المعلومات المحاسبية في مجموعتين أساسيتين هما:

1-2-4-1: حدوث الكوارث الطبيعية: هناك نوع آخر من التهديدات وإن كانت لا تحدث بالمعدل السابق بنفسه إلا إن آثارها مدمرة وخطيرة جداً وهي الكوارث الطبيعية التي يصعب مواجهتها،⁽¹⁾ فمن أهم أسباب المخاطر التي قد تواجه المنشآت ونظمها هي الكوارث الطبيعية والأحداث البيئية الجسيمة مثل البراكين والفيضانات والزلازل، والسيول، والرياح العاتية والأعاصير، وانقطاع التيار الكهربائي لأسباب طبيعية خارجية، والصواعق الكهربائية، والحرائق الطبيعية والموجات الحرارية المرتفعة والرطوبة الزائدة وما شابه ذلك، ويؤدي ذلك إلى حدوث تلف جزئي أو تدمير كلي لموارد نظم المعلومات المحاسبية (أجهزة، وبرامج، وملفات بيانات، وأفراد)، وتؤثر علي الأداء السليم لوظائف نظم المعلومات، وتتسبب بفقدان معلومات هامة أو عدم إتاحتها وتوفرها.⁽²⁾ إن الكوارث الطبيعية والحريق يمثلان تهديداً أمنياً لكل الأنظمة وليس لأنظمة المعلومات وحدها، لكن ذلك التهديد الأمني ربما يكون أقل خطورة وأيسر معالجة في الأنظمة الآلية للمعلومات حيث المرونة في خزن ونقل البيانات، وإمكانية وجود نسخ احتياطية للبرامج والبيانات في أماكن بعيدة ومتعددة.

1-2-4-2: حدوث كوارث غير طبيعية (بشرية): تعبر عن الحوادث غير الطبيعية ذات الصبغة البيئية والتي ينتج عنها تعطيل نظم المعلومات المحاسبية وتوقفها عن العمل لمدة ملموسة كالاضطرابات السياسية والاجتماعية المحلية والإقليمية، والحروب، وأعمال الشغب، والتهديدات الإرهابية، والحرائق وفصل التيار الكهربائي وتعطل أنظمة التكييف والتبريد، وهنا فإن آثار المخاطر الناتجة عن تلك الكوارث لا يقتصر على الآلات والمعدات، بل يتعداها إلى حدوث فقدان في البيانات والمعلومات والبرمجيات، فالنظام بأكمله معرض لخطر الانهيار بسبب تلك الكوارث.⁽³⁾

ومن الصعب جداً منع حدوث جميع الكوارث وذلك يعود للعوامل المسببة لهذه الكوارث ومنها العوامل البشرية والعوامل الطبيعية وقد تكون هذه العوامل مسيطراً عليها أو غير مسيطر عليها، ولذلك سوف يتم التطرق لكيفية مواجهة الكوارث من خلال التركيز على أهمية العمل واستمراريته وعملية التخطيط لمواجهة الكوارث.⁽⁴⁾

(1) محمد، حيدر صاحب، (2011)، "مسؤولية مراقب الحسابات في تحديد وتقييم مخاطر تكنولوجيا نظم المعلومات المحاسبية لرفع جودة أدائه"، مرجع سابق، ص: 84.

(2) Mihalache, Arsenie, (2011), "Security of the Accounting Information System Infrastructure", *OP. Cit.*, PP: 1339-1345.

(3) شتيوي، أيمن أحمد، (2006)، "قياس تأثير بعد الصناعة على دور المراجع الداخلي في إدارة المخاطر المرتبطة بنظم المعلومات المحاسبية الآلية"، مرجع سابق، ص: 52-1.

(4) الحميد، محمد دباس & نينو، ماركو إبراهيم، (2007)، "حماية أنظمة المعلومات"، مرجع سابق، ص: 87.

1-4-3: التهديدات الأمنية المتعلقة بالمخترقون والقرصنة:

من أسباب المخاطر التي يتعرض لها نظام المعلومات المحاسبي المحوسب، جرائم وقرصنة الحاسوب نتيجة تصرفات غير أمينة من قبل أطراف خارجية كالقرصنة والمتطفلين الذين يخترقوا نظم الحماية، رغبة في التحدي، أو لنوايا إجرامية وتجسسية، وقد أشارت العديد من الدراسات بأن (67%) من الشركات الأمريكية قد تم اختراق أمن وسرية نظم معلوماتها،⁽¹⁾ ووفقاً لبرايس ووترهاوس كوبرز (PWC) عدد الخروقات الأمنية للبيانات آخذة في الارتفاع، وفقاً لقاعدة بيانات تحتفظ بها مؤسسة الأمن فإن 879 حادثة اختراق تم الإبلاغ عنها سواء بالضياع أو السرقة، أو التعرض لمعلومات شخصية في عام 2012 بزيادة 30٪ تقريباً عن عام 2011،⁽²⁾ حيث يتم الوصول إلى النظام عن طريق اقتحام الإجراءات الأمنية للنظام أو عن طريق استغلال نقاط الضعف في نظم الرقابة، وقد يهدف القائمون بالاختراق إلى تحقيق ربح من وراء هذا الاختراق أو قد يكون بغرض التسلية، فإذا كان الهدف هو تحقيق ربح فإنه سيهدف إلى اختراق النظم الخاصة بمنظمات محددة ولمعلومات محددة، أما إذا كان الهدف هو مجرد التسلية فإن الاقتحام يتم لنظم وبيانات يسهل الوصول إليها ولا يتوافر لها وسائل الحماية الكافية.⁽³⁾

وأصبح خطر الاختراق أو الاقتحام الإلكتروني لنظم المعلومات المحاسبية والمواقع المعلوماتية خطراً يقلق العديد من المنشآت، فنتيجة المزايا التي وفرتها تكنولوجيا الاتصالات والمعلومات دفع بالعديد من المنشآت إلى إعطاء بعض عملائها وموظفيها صلاحيات الدخول إلى نظم معلوماتها عبر شبكات الاتصالات للحصول على بعض الخدمات التي تقدمها أو القيام بأي عمليات ضرورية، ولكنها بالمقابل واجهت مخاطر عديدة أهمها خطر الاختراق، وعلى الرغم من الموارد الهائلة التي أنفقت من قبل المنشآت لتأمين نظم المعلومات من خلال الضوابط الفنية والإجراءات الرسمية، ظهرت الخروقات الأمنية بشكل متزايد ومستمر،⁽⁴⁾ ويصعب تعقب تلك الاختراقات التي تتم على نظم المعلومات المحاسبية المحوسبة المرتبطة بالشبكات وخاصة الانترنت فهو بيئة مثالية للسرقات والتلاعب وإخفاء آثار الجريمة بشكل متقن ومنقطع النظير وذلك للأسباب والعوامل التالية:⁽⁵⁾

1. إمكانية الدخول من عدة أماكن بسبب الانتشار الواسع لأجهزة الحاسوب والشبكات، فأى شخص يمكنه الدخول إلى الشبكة من أي مكان يتوفر به جهاز حاسوب وخط اتصال.
2. سرعة العملية: قد لا يحتاج المخترق إلى أكثر من بضع دقائق لاختراق موقع معين والتلاعب به ومغادرة الموقع قبل أن يتم تعقبه.

(1) Romney, Marshal, and Steinbart, Paul. (2015). *Accounting Information Systems*, OP. Cit., P. 145.

(2) Drew, Jeef, (Aug. 2012), PwC : Internal audit has to play a more substantial role in information security, *journal of accountancy*, AICPA, USA, <http://www.journalofaccountancy.com/News/20126231> (accessed on 13 September 2013).

(3) عيسى، علاء وعاشور، عصاف، (2010)، "مخاطر نظم المعلومات المحاسبية وحوكمة المنشآت ومواجهة الأزمة المالية العالمية"، *مجلة الفكر المحاسبي*، المجلد (14)، العدد (2)، كلية التجارة، جامعة عين شمس، القاهرة، مصر، ص: 408-434.

(4) Parakkattu, Sindhuja & Kunnathur, Anand. S., (2010), "A Framework for Research in Information Security Management", *Northeast Decision Sciences Institute Proceedings (NEDSI)*, March 2010, PP: 318-323.

(5) زبار، سلمان عبود، (2010)، "معايير تطوير نظم المعلومات الإدارية عبر شبكة المعلومات الدولية دراسة تطبيقية في شركة الفرات العامة للصناعات الكيماوية"، *مجلة جامعة بابل للعلوم الإنسانية*، المجلد 18، العدد (2)، 2010، ص: 343-367.

3. تباعد المسافات: حيث تغطي تلك الشبكات مساحات جغرافية كبيرة وقد يكون المخترق لموقع ما يبعد آلاف الكيلومترات وفي بلد آخر ، فالإنترنت هي شبكة صممت بشكل عالمي.
 4. عدم وجود هوية محددة ، لا يمكن معرفة ماهية المخترق ولا بأي شكل من الأشكال.
 5. عدم وجود قوانين دولية : فشبكة الانترنت شبكة عالمية ذات معايير موحدة بالاستخدام فقط.
 6. إمكانية إتلاف بيانات جهاز الحاسوب: في حالة شعور أي مخترق بإمكانية تعقبه يستطيع إتلاف بيانات جهازه بضغطة زر بسيطة، مما يجعل عملية تعقبه عديمة الجدوى.
 7. حماية الحسابات المصرفية: هناك الكثير من الحسابات المصرفية محمية من اطلاع الغير عليها، وبالتالي يستطيع المخترق استخدام هذا النوع من الحسابات دون القلق من آلية تعقبه.
- ويوماً بعد يوم يتم ابتكار المزيد من التقنيات والبرمجيات الأكثر تعقيداً والأكثر حنكة وذكاء وفي المقابل فإن فهم عمل الأنظمة من قبل المتطفلون أصبحت عملية غير صعبة وممكنة حيث أصبح هؤلاء القراصنة والمتطفلين ماهرين في تحديد نقاط الضعف في الأنظمة والكشف عنها للحصول على امتيازات إضافية والتي تسمح لهم بالقيام بالعمليات التخريبية والسرقات والتطفل على النظام.⁽¹⁾
- والمخترقون هم جماعة يمتلكون خبرة واسعة في البرمجة، وشبكات الاتصال، ولهم القدرة على تخطي الحواجز التقنية لحماية الشبكات، وذلك بسبب ممارساتهم الطويلة وخبراتهم الواسعة في استيعاب لغات البرمجة ونظم التشغيل، والمخترقون إما هاكرز (*Hackers*) أو كراكرز (*Crackers*)، ويلاحظ بأن بعض الذين يقومون بالهجوم على نظام المعلومات من أجل المتعة والتحدي والذين يسمون بالقراصنة (*Hackers*) وهو مشتق من مصطلح القرصنة (*Hacking*) وعادة لا تكون لهم النية للتدمير أو السرقة وإنما تكون لديهم الرغبة في الشعور بالذكاء والقوة ويتفاخرون بمقدرتهم على الاختراق (الوصول غير المخول)، ومع هذا يترتب على ذلك تدمير خطير⁽²⁾، فهم مجرد متطفلون دافعهم إثبات الذات، وتتألف هذه الفئة أساساً من مراهقين وشباب عاطل عن العمل تتراوح أعمارهم بين 18-35 سنة،⁽³⁾ أما الفئة الأخرى فتسمى الكراكرز (*Crackers*) وهي كلمة مأخوذة من الفعل (*Crack*) بالإنجليزية وتعني الكسر أو التحطيم وهي الصفة التي يتميزون بها،⁽⁴⁾ ويتشابهون مع الهاكرز في قدرتهم الفائقة على الاختراق وتخطي إجراءات وبرامج الحماية للمواقع ونظم المعلومات، والاستفادة من نظام الانترنت المفتوح، إلا أن دوافعهم حاقدة وتخريبية، حيث يقومون بالعبث بالبيانات والمعلومات المخزنة على الحواسيب والشبكات وتكون لديهم نية إجرامية لسرقة البيانات وتدمير النظام، ويمكنهم القيام بالعديد من الأفعال التي تضر بأصول نظم المعلومات، ومنها الوصول غير المصرح به إلى النظام، وسرقة المعلومات السرية للمنشأة وعملائها، والتجسس الصناعي، وتدمير المعلومات والبيانات أو تحريفها، وإدخال بعض فيروسات الحاسوب إلى النظام وشل حركة النظام.⁽⁵⁾

(1) الطيطي، خضير مصباح إسماعيل، (2010)، "أساسيات أمن المعلومات والحاسوب"، مرجع سابق، ص20.

(2) حجر، عيد الملك إسماعيل، (2009)، "نظم المعلومات المحاسبية"، مرجع سابق، ص 332.

(3) الشبلي، هيثم حمود، (2009)، "إدارة مخاطر الاحتيال في قطاع الاتصالات"، مرجع سابق، ص44.

(4) صقر، ممدوح الشحات، (2007)، "أمن المعلومات"، تدوة أمن وحماية نظم المعلومات في المؤسسات العربية، القاهرة، مصر، 3-7 يونيو 2007، ص30.

(5) Da Veiga, A & Eloff, J.H.P., (2010), "A framework and Assessment Instrument for Information Security Culture", *Computer & Security*, Vol.29, No.4 PP.:196-207.

- ويرى الباحث أن مخاطر اختراق نظم المعلومات المحاسبية ليست بالجديدة في عالم الأعمال، إلا أن الجديد فيها يكمن في توسعها وزيادتها إذ أصبحت شبه ظاهرة ترافق النشاط الاقتصادي لمختلف المنشآت وتكلفتها مبالغ كبيرة، وقد لا تترك هذه المخاطر أثراً ملموساً مما يصعب من عملية مقاضاة الفاعلين وتتبع أثرهم، والأكثر من ذلك فإن هناك قناعة لدى كثير من المنشآت بأنها لا تكشف تلك المخاطر التي تتعرض لها لسببين رئيسيين هما:
1. اعتقادها بعدم جدوى القضية بالوصول إلى المجرمين لغياب الأثر المادي فضلاً عن تكبدتها مصاريف إضافية تضاف إلى خسائر تلك المخاطر.
 2. أن الكشف عن مخاطر الاختراق قد يفقد المنشأة الكثير من عملائها ويؤثر على سمعتها في السوق مما قد يسبب لها ضرر معنوي تفوق قيمته الضرر الذي سببه خطر الاختراق.

1-4-4: التهديدات الأمنية المتعلقة بدخول فيروسات وبرمجيات الحاسوب الخبيثة للنظام:

برامج الحاسوب تمثل عنصراً مهماً من عناصر نظم المعلومات المحاسبية، ومن المحتمل أن تكون مجالاً خصباً للتهديدات التي تتعرض لها تلك النظم، حيث قد تشمل هذه البرامج على فيروسات وبرمجيات خبيثة وضارة مما قد يعرض سلامة وتكامل وسرية بياناته وخصوصيتها للخطر المتزايد، فقد أدى الانتشار الواسع في استخدام الشبكات الداخلية والخارجية مجموعة كبيرة من التهديدات المسببة للمخاطر التي تتعرض لها نظم المعلومات المحاسبية المحوسبة، والتي من أهمها الإصابة بالبرامج الخبيثة، والتي تمثل مجموعة من الكائنات البرمجية القادرة على الاستنساخ بشكل ذاتي إلى مجموعة من التطبيقات والبرامج التنفيذية لنظم المعلومات، وتنتشر على نطاق واسع داخل ذاكرة الحاسوب، مسببة مخاطر على أمن نظم المعلومات المخزنة على ذاكرة الحاسوب، وجميع الحاسبات المتصلة به عبر الشبكات، ومن تلك المخاطر منع مستخدمي نظم المعلومات من الوصول للبيانات والمعلومات، وإخفاء نظم التشغيل الرئيسية، وأخطاء وتشويش في استرجاع البيانات والمعلومات المخزنة، وخط أو دمج البيانات والمعلومات المخزنة بعضها مع بعض، والتعديل والحذف التلقائي لبيانات ومعلومات قواعد البيانات بطريقة خارجة عن سيطرة القائمين عليها، وإتلاف وتدمير نظم وبرامج الحماية المستخدمة في المنشأة، فهي وسائل فنية تستخدم لتعطيل النظام وتشويه وإتلاف أو تحريف بياناته المختلفة والتي قد تتلف البيانات أو تعطل النظام وتؤثر على عملية تشغيل البيانات، وتشير الدراسات الأمريكية بأن حجم الخسائر الاقتصادية بسبب هجمات الفيروسات لعام 2010 م بلغت (60) بليون دولار.⁽¹⁾

والبرمجيات الخبيثة (Mal-ware): هي نوع من التهديدات الأمنية والتي تشمل مجموعة متنوعة ومختلفة من البرمجيات التي تستغل للتدمير سواء تدمير النظام أو البرمجيات أو المعطيات أو الملفات أو الوظائف أو تستثمر للقيام بمهام غير مشروعة مثل الاحتيال أو التجسس أو التخريب أو استنزاف الموارد (الوقت، المعالج، الذاكرة، وحدة التخزين، سعة النقل الشبكي)،⁽²⁾ وتشير للبرامج الضارة أو العدائية أو المتطفلة أو المزعجة التي تتسلل مستترة إلى نظم المعلومات المحوسبة وشبكتها، وهي تهديدات مزروعة في النظم وتستغل لتدمير أو سرقة

(1) Romney, Marshal, and Steinbart, Paul. (2015). *Accounting Information Systems*. OP. Cit., P. 145.

(2) Madani, Haider H., (2009), "The Role of Internal Auditors in ERP-Based Organizations", *Journal of Accounting & Organizational Change*, Vol. 5 No. 4, PP: 514-526, available at: www.emeraldinsight.com/1832-5912.htm

البيانات والمعلومات الهامة وكذلك برامج النظام، ومن الصعب إزالتها، وأسمها مشتق من كلمتين هما خبيثة (Malicious) و برامج (Software)، وهي قادرة على اختراق دفاعات نظم المعلومات وبشكل متزايد، وتشمل هذه الفيروسات (Viruses)، والديدان الالكترونية (Worms) أو القنابل الموقوتة والمنطقية (Logical Bombs)، وبرامج التجسس (Spy-Ware)، وأحصنة طروادة (Trojan Horses)، وبرامج الهجوم (Attack Scripts)،⁽¹⁾ وغيرها من البرمجيات غير المرغوب فيها، والجامع المشترك بين هذه البرمجيات أنها برمجيات ضارة تستغل للتدمير أو الاحتيال، وفيما يلي الأنواع المختلفة من تلك البرمجيات:

1-4-4-1: الفيروسات (Viruses): وهي عبارة عن برامج مستقلة عن النظام تقوم بتحميل نفسها ضمن برمجيات الحاسوب ونسخ نفسها بشكل متكرر وبدون معرفة المستخدم الفعلي للنظام.⁽²⁾

وهي أحد البرامج الخبيثة والتي تم تصميمها وكتابتها من قبل مبرمجين محترفين بهدف إحداث أكبر ضرر ممكن بنظام المعلومات (أجهزة وبرامج ومعلومات مخزنة)، وتتفاوت المخاطر التي تحدثها الفيروسات فقد تقتصر على التحكم في بعض عمليات النظام وقد تمتد إلى البرامج المهمة والملفات الضرورية للنظام وتدمرها أما أشدها ضرراً هي تلك الفيروسات التي تتمكن من التأثير على الجهاز نفسه بحيث تتلف وسائط تخزينه ودوائره الالكترونية، وقد يصل الأمر إلى توقف تلك النظم عن العمل وبالتالي توقف الخدمات المقدمة للمستخدمين.

وتعد الفيروسات من أخطر التهديدات التي تواجه أمن وسلامة نظم المعلومات بسبب تعدد أنواعها وظهور أنواع جديدة كل يوم مع سرعة انتشارها عبر شبكة الانترنت، وتختلف الفيروسات في طرق عملها فمنها ما يعمل بمجرد الدخول إلى النظام ومنها ما ينتظر أمر تشغيل معين من المستخدم حتى تبدأ نشاطها ومنها ما يتم توقيته بتاريخ أو ساعة معينة حتى تبدأ بمهامها التخريبية،⁽³⁾ وللفيروسات القدرة على ربط نفسها بالبرامج الأخرى وإعادة إنشاء نفسها حتى تبدو كأنها تتكاثر وتتوالد ذاتياً، ولها القدرة على الانتشار بين البرامج المختلفة وبين المواقع المختلفة في الذاكرة حتى تحقق أهدافها التدميرية.⁽⁴⁾

ومن خصائص الفيروسات القدرة على الاختراق والانتشار والتخفي والتدمير، فيروس الحاسوب هو عبارة عن برنامج يستطيع أن يلحق أو يرفق نفسه ببرنامج آخر (برنامج مضيف) وبالتالي يلوث أو يعدي البرنامج الذي يرتبط به ويضاعف نفسه وينتشر بسرعة إلى البرامج والملفات الأخرى،⁽⁵⁾ وقد سمي الفيروس بهذا الاسم لتشابه آلية عمله مع تلك التي تصيب الكائنات الحية، بعدد من الخصائص، كخاصية الانتقال بالعدوى، أو كونه كائناً غريباً يقوم بتغيير حالة الكائن المصاب، إضافة إلى الضرر الذي يعقبه إن لم يتم العلاج.

وتتعدد الآثار الناتجة عن الفيروسات فقد يقوم الفيروس بتدمير أو تشويه بعض أو كل الملفات والبيانات المخزنة في نظام المعلومات، كما قد يقوم بنسخ نفسه آلاف المرات وبسرعة فائقة مما يعوق عمل النظام

(1) Warkentin, Merrill & Willison, Robert, (2009), "Behavioral and Policy Issues In Information Systems Security: The Insider Threat", *OP. Cit.*, PP: 101-105.

(2) Laudon Kenneth C. & Laudon Jane P., (2011), "*Management Information Systems- Managing The Digital Firm*", *OP. Cit.*, P. 525.

(3) القرى، ميسون محمد، (2007)، "أمن المعلومات المحاسبية"، مرجع سابق، من الموقع: www.maysoon.ws/archives/420، بتاريخ 1-2-2014، س: 6:06 صباحاً.

(4) الشبلي، هيثم حمود، (2009)، "إدارة مخاطر الاحتيال في قطاع الاتصالات"، مرجع سابق، ص 92.

(5) حجر، عبد الملك إسماعيل، (2009)، "نظم المعلومات المحاسبية"، مرجع سابق، ص 334.

والاتصالات في الشبكة،⁽¹⁾ والأفعال التي يقوم بها الفيروس واسعة النطاق حيث يقوم بتدمير البيانات وسرقة المعلومات واعتراض أو منع تشغيل الحاسوب أو القيام بأشياء غريبة مثل إعادة إقلاع الحاسوب أو اضطراب الشاشة، بل إن أثر الفيروسات يتعدى الحاسوب إلى التأثير على العملاء وسمعة المنشأة.⁽²⁾

إن الفيروسات تسبب مخاطر شديدة سواء على البرامج أو المعدات، حيث تستطيع الفيروسات توقيف البرامج أو تعديل وظائفها نتيجة نسخ أوامر الفيروس مكان جزء من أوامر البرامج، ويعمل الفيروس على إبطاء تشغيل الحاسوب، وتدمير قطاع التحميل وهو ذلك الجزء من القرص الصلب الذي يحتوي على الأوامر والإرشادات لتشغيل الحاسوب، وفي هذه الحالة يتطلب إعادة تهيئة القرص مما يؤدي إلى فقدان جميع البيانات والبرامج المخزنة ولذلك يفضل الاحتفاظ بنسخ احتياطية من البيانات والبرامج، كما تتسبب الفيروسات تدمير جدول توزيع الملفات مما يصعب الوصول إلى أي ملف على القرص، كما يصيب جدول مواقع الملفات أثناء تكرار نفسه مما يجعل القرص الصلب غير قابل للقراءة وبالتالي تفقد كافة المعلومات الموجودة على القرص الصلب، كما أن الفيروسات تسمح بالتجسس على نظم المعلومات التي تستخدم تكنولوجيا الشبكات والاتصالات حيث تسمح بالدخول للنظام والحصول على بيانات سرية، بهدف تحقيق مكاسب شخصية، ومثلما للفيروسات مخاطر على برامج النظام، فإن لها مخاطر على المكونات المادية للنظام حيث تعمل على إجهاد الأجزاء الميكانيكية للحاسوب بما قد يسبب تدميرها.⁽³⁾

ويمكن الإحساس بوجود الفيروسات في النظام من خلال سلسلة من الأعراض التي تظهر عند الاستخدام ومنها على سبيل المثال تكرار رسائل الخطأ في أكثر من برنامج، وظهور رسالة تعذر الحفظ لعدم كفاية مساحة الذاكرة، وتكرار اختفاء بعض الملفات التنفيذية، وحدوث بطء شديد في إقلاع نظام التشغيل أو تنفيذ بعض التطبيقات، ورفض بعض التطبيقات للتنفيذ، وتوقف النظام عن العمل لأسباب غريبة، وحصول أخطاء غريبة ومبهمة، وزيادة حجم بعض الملفات، وإعطاء رسائل أو رموز غريبة على الشاشة، وفقدان تعليمات برنامج معين أو حصول تشويه في تعليماته، وعدم القدرة على التحكم في دليل ملفات المستخدم أو حذفها وكذلك ملفات نظم التشغيل،⁽⁴⁾ فعندما ينتشر الفيروس يأخذ مساحة ويجعل أداء الحاسوب بطيئاً جداً، ويحتاج إلى وقت طويل لتحميل البرامج، ويجعله غير قادر على حفظ البيانات، فمثلاً أحد الفيروسات أغلق بنكاً يحتوي على 200 سيرفر وألف جهاز حاسوب لمدة 4 أيام،⁽⁵⁾ وكما أشارت الدراسات الأمريكية فإن حجم الخسائر الاقتصادية بسبب هجمات الفيروسات لعام 2010م وحده بلغت (60) مليار دولار.⁽⁶⁾

1-4-4-2: ديدان الحاسوب (Worms): وهو نوع خاص من البرامج الخبيثة يصيب نظام المعلومات المرتبط بالشبكات بالخلل، وذلك بتكرار نفسها بسرعة حتى لا تترك للبرامج التشغيلية متسعاً للعمل وبالتالي تعطيل العمل،

(1) Arens, Alvin A., Elder, Randal J., & Beasley, Mark S., (2014), *Auditing & Assurance Services: An Integrated Approach*, OP. Cit., PP: 740-742.

(2) الخضير، سليمان، (2013)، *الشامل*، مرجع سابق، ص: 16-18.

(3) الجواد، دلال صادق & الفتال، حميد ناصر، (2008)، "أمن المعلومات"، مرجع سابق، ص: 77-81.

(4) الذبيبة، زياد & الرميحي، نضال & الجعدي، عمر، (2011)، "نظم المعلومات في الرقابة والتدقيق"، مرجع سابق، ص: 68.

(5) حجر، عبد الملك إسماعيل، (2009)، "نظم المعلومات المحاسبية"، ص: 335.

(6) Romney, Marshall B. & Steinbart, Paul J., (2015), *Accounting Information Systems*, OP. Cit., P. 145.

فدودة الحاسوب هي برنامج يهدف إلى نشر نفسه من نظام إلى نظام، حيث تشن هجوماً مديراً للانتقال من حاسوب إلى آخر عبر الشبكة، وهي عبارة عن كود يسبب أذى للنظام وتتميز بقدرتها على إعادة توليد نفسها بمعنى أن أي ملف أو جهاز متصل بالشبكة تصل إليه الدودة يتلوث وتنتقل هذه الدودة إلى ملف آخر أو جهاز آخر في الشبكة وهكذا تنتشر الدودة وتتوالد إلى حد استنفاد موارد النظام، مما يؤدي إلى بطء ملحوظ في أدائه، فهي لا تنفذ أي عمل تخريبي كحذف أو تغيير الملفات إنما تنتشر فقط عن طريق نسخ نفسها من خلال أجهزة الحاسوب والشبكات مما يؤدي إلى إشغال موارد النظام والشبكة بشكل كبير، وهناك من يرى أنها برامج هجومية (*Attack Scripts*) تستفيد من الثغرات الأمنية ونقاط الضعف الموجودة في شبكات المعلومات من أجل شن هجوم على أجهزة الحاسب في الشبكة، وتقوم معظم هذه البرامج بتدمير قوائم الانتظار للخدمات المختلفة عن طريق إغراق المساحات الوسيطة بالبيانات.⁽¹⁾

ولا يوجد فرق بين الفيروسات وديدان الحاسوب من حيث الوظيفة والتكوين، ولكن هناك اختلاف بسيط بينهما إذ يتطلب عمل الفيروسات توفر بيئة مناسبة تساعد على انتشارها وتكاثرها، عكس الديدان التي لا تحتاج إلى مستلزمات للقيام بعملها بنجاح، كما أن فيروسات الحاسوب تتطلب من المستخدم تنشيط الفيروس وذلك من خلال فتح أو الضغط على الملف المنفذ لعمل الفيروس، بينما ديدان الحاسوب لا تتطلب قيام المستخدم بتنشيطها من أجل إصابة مواقع أخرى ويمكن أن تكرر نفسها بشكل أسرع من الفيروس عن طريق استكشاف نقاط الضعف في نظم التشغيل، لذلك فدودة الحاسوب مشابهة للفيروس فيما عدا أن الدودة لا تحتاج أن ترفق ببرنامج آخر لتنتشر وإنما يمكن أن تعمل مستقلة.

ومن أشهر مخاطر ديدان الحاسوب التخريبية وأشدّها تأثيراً تلك الهجمات التي يكون هدفها حجب الخدمة حيث تنتشر الدودة على عدد كبير من الأجهزة ثم توجه طلبات وهمية لجهاز خادم معين (يكون المبرمج قد حدد الخادم المستهدف من خلال برمجته للدودة) فيغرق الخادم بكثرة الطلبات الوهمية ولا يستطيع معالجتها جميعاً مما يسبب توقفه عن العمل، وهذه الديدان استهدفت مواقع كثير من الشركات العالمية أشهرها مايكروسوفت.

1-4-4-3: برامج التجسس (*Spy-Ware*): هي مجموعة من البرامج يتم تحميلها أو تركيبها بشكل سري (مخفي) داخل مجموعة من البرمجيات الحرة الخاصة بالنظام لتؤدي وظيفة تجسسية مقنعة دون موافقة وعلم مستخدم النظام،⁽²⁾ ومن الآثار السلبية لهذا النوع من البرامج قدرتها على السيطرة على النظام المستهدف بشكل جزئي، حيث تقوم بتسجيل ونسخ البيانات والمعلومات المخزنة على ذاكرة الحاسوب المصاب، وإرسالها عن طريق الانترنت إلى مصمم هذا البرنامج، حيث تقوم بفتح الثغرات الأمنية (نقاط الضعف) في النظام للقراصنة للقيام ببعض الإجراءات في النظام دون علم المستخدم، وهي تراقب سلوك المستخدم من خلال مراقبة كتابته

(1) داود، حسن طاهر، (2004)، "أمن شبكات المعلومات"، مركز البحوث، معهد الإدارة العامة، الرياض، السعودية، ص: 168-169.

(2) Calder, Alan & Watkins, Steve, (2008), *IT Governance : A Manager's Guide to Data Security and ISO27001/ISO 27002*, 4th Edition, KOGANPAGE, London, United Kingdom and Philadelphia, USA, P.182.

والمواقع التي يزورها وهدف تلك البرامج ينحصر في استسقاء معلومات سرية مثل كلمات المرور وأرقام حسابات مصرفية ولأغراض تجارية مثل محركات البحث أو معرفة أنماط المستخدم الاستهلاكية.⁽¹⁾

ومن أشهر برامج التجسس برنامج الباب الخلفي (*Backdoor*) وهو عبارة برنامج في ظاهره مفيد ومغري للمستخدم ولكنه في الواقع عبارة عن ثغرة تترك عمداً في النظام لكي يتمكن المخترق من خلالها الوصول للنظام، وبرنامج حصان طروادة (*Trojan Horse*) وهو عبارة عن برنامج صحيح وقانوني يُزرع تلقائياً في النظام لإجراء عمل مفيد ولكن ضمنه تنفذ شفرات مخفية (غير مرئية) تسمح بوصول غير مخول للحاسوب بهدف تدمير البيانات والملفات،⁽²⁾ وهو برنامج يسمح للقرصنة بالتحكم عن بعد في نظام الضحية في أي وقت في المستقبل، وقد سمي هذا البرنامج بحصان طروادة لأنه يذكر بالقصة الشهيرة لحصان طروادة، فقد اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها، حيث يقوم البرنامج بإرسال المعلومات المطلوبة للشخص زارع البرنامج مثل كشف كلمات السر أو نقل بيانات، وأرقام بطاقات الائتمان المصرفية وغيرها، كأن يستخدم برنامج معالجة كلمات ظاهرياً لتحرير وتنسيق النصوص في حين يكون غرضه الحقيقي طباعة كافة ملفات النظام ونقلها إلى ملف مخفي بحيث يمكن للمخترق أن يقوم بطباعة هذا الملف والحصول على محتويات النظام.⁽³⁾

ويعتد ذلك البرنامج من أكبر مهددات أمن قاعدة بيانات نظم المعلومات المحاسبية المحوسبة، حيث لا يتمكن النظام من معرفة هل الأمر حقيقي أم وهمي وكل محاولات الحماية من كلمات مرور وتشفير لا تجدي بسبب وجود ذلك البرنامج الذي يسمح للمخترق برؤية النص واضح قبل تشفيره.

وتأخذ برامج التجسس أشكال مختلفة، فمن الممكن أن يكون هذا البرنامج على شكل مشغل موسيقى عالي الجودة، أو على شكل لعبة ممتعة، أو على شكل باحث انترنت وذلك لتشجيع مستخدم الحاسوب على تفعيل البرنامج أطول مدة ممكنة مع قدرة هذه البرامج على التشغيل التلقائي، وقد قامت شركة ميكروسوفت بحماية زبائنها من تلك المخاطر من خلال برنامج اكتشاف برامج التجسس، وبعد 15 شهراً تمكن البرنامج من اكتشاف (16) مليون شكل من أشكال برامج التجسس الخبيثة العاملة على ما يقارب (6) مليون حاسب آلي في الولايات المتحدة الأمريكية، وكان من أهمها برنامج تجسس على مراكز معلومات الجيش الأمريكي من قبل مجموعات موجودة في الصين، وبرامج تجسس تعرضت لها الشركة نفسها.

وعلى الرغم من أن العقد الماضي كان الأفضل بخصوص دفاعات الإنترنت، إلا أن أمن الإنترنت سيبقى الهم الرئيسي لعشر سنوات مقبلة، والسبب الرئيسي في ذلك هو ظهور عصابات الجريمة المنظمة عبر الإنترنت، ودخول الحكومات في أعمال هندسة البرمجيات الخبيثة بغرض التجسس والهجوم على الدول الأخرى، وما دامت المجموعتان المنتجتان للبرمجيات الخبيثة، (المجموعة المدعومة من قبل الدول، والمجموعة التي تحركها الدوافع المالية)، فاعلّتين فإنه من غير المحتمل أن يكون هناك نظام حاسوب آمن بنسبة 100%.⁽⁴⁾

(1) الغثير، خالد سليمان، & القحطاني، محمد عبدالله، (2009)، *أمن المعلومات بلغة ميسرة*، مرجع سابق، ص85.

(2) الحمامي، علاء والعاني، سعد، *تكنولوجيا أمنية المعلومات وأنظمة الحماية*، الطبعة الأولى، دار وائل للنشر والتوزيع، عمان، الأردن، 2007، ص22.

(3) Gerić, Sandro & Hutinski, Željko, (2007), *Information System Security Threats Classifications*, *OP. Cit.*, PP: 59-60.

(4) Hypponen, Mikko, (2013), "Cyber Threats Unlikely to Disappear, Says Security Researcher", *INFOSEC 2013*, 23-25 April 2013, London, UK..

4-4-4-1: القنبلة الموقوتة والمنطقية (Time & Logical Bomb): القنبلة الموقوتة هي عبارة عن برامج

تزرع لتدمير نظام ما في وقت أو تاريخ محدد بينما القنبلة المنطقية عبارة عن برامج تزرع لتدمير النظام ويتم تشغيلها عند حدوث ظروف معينة أو عند تنفيذ أوامر محددة لتجاوز نظم الحماية والأمن في النظام، وغالباً ما تزرع مثل هذه البرامج من قبل الموظفين الذين يشعرون بالتهديد في وظائفهم.

وتقوم تلك البرمجيات بمجموعة من الأوامر التي من شأنها أن تجعل برامج النظام تقوم بأداء وظيفة أخرى غير تلك التي صممت من أجلها، وتتميز بأنها تظل كامنة وخاملة غير مؤذية حتى يقرر المخرب تشغيلها لتنفجر في وقت وتاريخ محدد أو بعد استخدام البرنامج لعدد محدد من المرات، وقد تؤدي إلى الشلل التام للأجهزة، وقد تؤدي القنبلة إلى تخريب بعض البرامج أو مسح بعض البيانات أو كليهما وبالتالي تعطيل النظام عن العمل.

ويرى الباحث بأن خطورة الفيروسات والبرمجيات الخبيثة بأنواعها المختلفة لا تقتصر على أمن قاعدة بيانات النظام فحسب ولكن اتصال نظم المعلومات المحاسبية المحوسبة بشبكة الانترنت قد ساعد على زيادة حدة خطورتها التي قد تصل إلى حد انهيار النظام وفقدان المعلومات الهامة مما يتطلب إجراءات رقابية قوية لحماية كل المنافذ والفرص التي يمكن أن تُستغل في حدوث هجوم الفيروسات لنظم معلومات المنشأة، كما أن إجراء تحليل مباشر لحركة المرور والسلوك في معدات تكنولوجيا المعلومات قد يعطي لمحة عن أي تحرك مريب يمكن أن يبدأ عن طريق برمجيات التجسس ويؤكد وجود هذه التهديدات مدى أهمية بدء إجراءات أمن أنظمة المعلومات انطلاقاً من تقييم مكامن الضعف، والحوكمة، وسياسة الأمن.

5-4-1: التهديدات الأمنية المتعلقة بالمنافسة الاقتصادية بين المنشآت:

إن الاعتماد على التبادل الإلكتروني للبيانات، وممارسة التجارة الإلكترونية، يعتبر بمثابة بيئة خصبة لاختراق نظم المعلومات المحاسبية للمنشآت، من قبل المنافسين للمنشأة، ومن المعروف أن المنشآت التجارية الكبرى تعيش فيما بينها منافسة مستمرة وقد بينت الدراسات الحديثة أن عدداً من كبريات المنشآت التجارية يجرى عليها أكثر من خمسين محاولة اختراق لشبكاتها كل يوم.⁽¹⁾

وقد عرفنا - في المبحث الأول من هذا الفصل - أن المنشآت أصبحت تعتمد بشكل متزايد على نظم المعلومات المحاسبية والبيانات المخزنة على تلك النظم، وذلك لتحقيق أهدافها بكفاءة وفعالية، وأن زيادة الاعتماد على التكنولوجيا، وتوسع أنشطة البنوك في ممارسة أنشطتها على المستوى العالمي، والظروف العالمية الاقتصادية والسياسية الحديثة، والتطورات الاجتماعية والثقافية أسهمت وتسهم جميعها بشكل متزايد في إيجاد بيئة مضطربة للمنظمات، وصعوبة الحفاظ على نظم المعلومات (IS) المرتبطة بعضها عبر شبكات الاتصال، واستخدامها في مجال الأعمال التجارية.⁽²⁾

(1) صقر، ممدوح الشحات، (2007)، "أمن المعلومات، مرجع سابق، ص 28.

(2) Warkentin, Merrill & Willison, Robert, (2009), "Behavioral and Policy Issues In Information Systems Security: The Insider Threat", OP. Cit., PP: 101-105.

وقد يتمكن المنافسون من اقتحام نظم معلومات المنشأة رغبة منها في الوصول والاطلاع على البيانات والمعلومات السرية كأسعار السلع والخدمات وعروض المناقصات وحسابات العملاء، وحجم النشاط وغيرها من المعلومات الهامة والتي يصعب حصرها، وقد تتعرض المنشأة لنفس التهديدات من العملاء والموردين، وبالتالي إمكانية سرقة معلومات هامة قد تكون على درجة من السرية ويمكن الاستفادة منها مالياً.

ومن الأسباب الخارجية لحدوث المخاطر زيادة حدة المنافسة بين البنوك والذي جعلتها تقوم بتقديم الخدمات المصرفية الإلكترونية لإشباع رغبات عملائها دون مراعاة الآثار التي يمكن أن تحدث عند الاستخدام الفعلي.

1-4-6: التهديدات الأمنية المتعلقة بضعف الرقابة الخارجية على نظم المعلومات المحوسبة:

نجد أن بعض البنوك التجارية قد عانت خلال الفترات الماضية من انتكاسات والتي أدى البعض منها إلى انهيارات لبعض البنوك، حيث كان من مسببات ذلك الانهيار فشل التدقيق الخارجي أو الداخلي في تحديد نقاط الغش والاحتيال، فإلى وقت قريب لوحظ أن الفعاليات الإلكترونية في معظم المؤسسات المصرفية العربية مغلقة أمام الرقابة والتفتيش الخارجي ويعود ذلك لعدة أسباب، من أهمها عدم وجود الكفاءات المناسبة لهذا النشاط وكذلك معارضة دوائر تكنولوجيا المعلومات لذلك، وفي الواقع إن من واجب مجلس الإدارة والإدارة العليا في أي منشأة مصرفية أن تخضع العمليات والأنشطة والخدمات الممارسة بوسائل أو أدوات إلكترونية ودوائر تكنولوجيا المعلومات إلى الرقابة والتفتيش ومتابعة التنفيذ لاكتشاف وتصحيح الأخطاء ومنع الاختراقات الداخلية والخارجية وحماية موجودات ومعلومات المنشأة.

إن عدم وجود آلية رقابية متمثلة في عملية التفتيش والمراجعة والتدقيق وفق السياسة الأمنية للمنشأة وتطبيقها بشكل كلي، يؤدي إلى عدم تقيد الموظفين بالسياسات والتراخي في تطبيقها مما يشكل تهديداً للمنشأة، كما وأن عدم وجود كوادرمؤهلة للقيام بمهام المراجعة والتدقيق يساهم بشكل مباشر في هذه المشكلة.

إن تأثير تكنولوجيا المعلومات والاتصالات من القضايا المعاصرة على مراجعة البيانات المالية للعميل، حيث أصبحت مستوى المهارات في مجال تكنولوجيا المعلومات مصدر قلق كبير لمقدمي خدمات التدقيق، ويجب ردم الفجوة بين مهارات مدققي تكنولوجيا المعلومات والاتصالات، ومهاراتهم في الوضع الراهن،⁽¹⁾ ويواجه المدقق الخارجي للحسابات تحدياً صعباً يتمثل بصعوبة تحديد مخاطر تكنولوجيا المعلومات وتقييمها عند تكلفه بتدقيق المنشآت التي تعمل في ظل بيئة تكنولوجيا نظم المعلومات المحاسبية المحوسبة وخاصة تلك المرتبطة بالإنترنت، وترجع أسباب ذلك إلى عدم توفر الخبرة والمهارة الفنية الكافية والمعرفة الأساس بنظم المعلومات المحوسبة ومكوناتها ووظائفها وإمكانياتها التشغيلية والبرمجية والتدقيقية لدى بعض مراقبي الحسابات نتيجة وقوفهم موقف

(1) Anomah, Sampson & Agyabeng, Owusu, (2013), "Evaluating Internal Controls in A Computerized Works Environment – A Risk to Audit Professionals and A Challenge to Accountancy Training Providers", Research Journal of Finance and Accounting, Vol.4, No.1, PP: 132- 143, www.iiste.org

المتفجر بإزاء التقدم التكنولوجي لنظم المعلومات المحاسبية المحوسبة، وعدم وجود نية حقيقية وجادة لتعلم هذه التكنولوجيا وملاحقتها مما ينذر بتأخر مهنة المحاسبة والتدقيق محليا وعربيا في هذا المجال.⁽¹⁾ وتُعد المهارات والتخصص وإستراتيجية الاتصال الفاعلة بين الإدارة والمحاسبين والمدققين من الأمور المهمة في تخفيض المخاطر الناشئة عن نظم المعلومات المحاسبية المحوسبة واعتماد إستراتيجيات وسياسات فاعلة،⁽²⁾ فحدوث تلك التطورات التكنولوجية أدت إلى إضفاء أعباء جديدة مرتبطة بالمخاطر الناجمة عن تكنولوجيا المعلومات إلى كثير من المهن وأهمها مهنة التدقيق،⁽³⁾ حيث أدى استخدام التكنولوجيا إلى تغيير في تقنية جميع ومعالجة المعلومات المحاسبية الأمر الذي انعكس بدوره على مهنة التدقيق في صورة تغييرات جوهرية للأساليب التقليدية في التعامل مع تلك المعلومات وتعدد في الخدمات التي يمكن تقديمها وذلك للتقليل من المخاطر التي تصاحب استخدام التكنولوجيا،⁽⁴⁾ وبالتالي نتيجة للمخاطر الأمنية التي تتعرض لها النظم المحوسبة في بيئة الأعمال المعاصرة فإن ذلك وضع تحديات أمام مهنة المحاسبة والمراجعة مما أدى إلى ضرورة تطوير مداخل ممارسة مهنة التدقيق ووجود نظم للفحص والرقابة الالكترونية المستمرة.

ولذلك يجب على المدقق أخذ المخاطر الأمنية في الاعتبار عند اختيار وتطبيق إجراءات الرقابة الداخلية على تنفيذ العمليات الإلكترونية،⁽⁵⁾ وتعتبر تلك المخاطر تحديا أمام مدققي الحسابات، للتحقق من مدى فاعلية وكفاءة النظم المحوسبة والبرامج المستخدمة، ومن ثم التحقق من وجود نظم رقابية وضوابط تشغيلية، إضافة للوقوف على مدى التزام المنشأة بالضوابط الرقابية الموضوعة وعلى مدى سلامة النظام المحاسبي ونظام الرقابة الداخلية، ومدى التزام العاملين بها، علاوة على تقييم المدقق لمدى إلمام الإدارة بالمخاطر التي يمكن أن تتعرض لها المنشأة، وبالتالي توجيه إدارة المنشأة بضرورة مراجعة خططها بشأن التغلب على أية نقاط ضعف يتم اكتشافها، ومتابعة مدى التزام البنك بتنفيذها.

ويجب على المراجعين الداخليين في هذا الشأن أن يبذلوا أقصى جهودهم لبيان تصوراتهم من خلال تقييم دوري ومستقل وموضوعي بخصوص مخاطر تكنولوجيا المعلومات وكذلك اقتراح الخطط والاستراتيجيات والإجراءات المتعلقة، وتطبيق الآلية المناسبة بشكل ثابت ومتناسق ومتكامل، ويمكن لهذه التقييمات أن تساعد في الحفاظ على أو تحسين كفاءة وفعالية إدارة المنشأة لتلك المخاطر.⁽⁶⁾

إن عدم وجود آلية رقابية متمثلة في عملية التفتيش والمراجعة والتدقيق وفق السياسة الأمنية للمنشأة وتطبيقها بشكل كلي، يؤدي إلى عدم تقيد الموظفين بالسياسات والتراخي في تطبيقها مما يشكل تهديداً للمنشأة، كما وأن عدم وجود كوادر مؤهلة للقيام بمهام المراجعة والتدقيق يساهم بشكل مباشر في هذه المشكلة، ولذلك يجب على مدققي

(1) محمد، حيدر صاحب، "مسؤولية مراقب الحسابات في تحديد و تقييم مخاطر تكنولوجيا نظم المعلومات المحاسبية لرفع جودة أدائه"، **مرجع سابق**، ص 4.
(2) Beard, Deborah & Wen, H. Joseph, (2007), "Reducing the Threat Levels for Accounting Information System, Challenge for Management, Accountants, Auditors and Academicians", **OP. Cit.**, PP: 34-42.
(3) الشرايري، عادل، (2009)، "سياسات وإجراءات التدقيق الداخلي في ظل بيئة تكنولوجيا المعلومات في البنوك الأردنية"، **مجلة جامعة تشرين للبحوث والدراسات العلمية - سلسلة العلوم الاقتصادية والقانونية**، المجلد (31)، العدد (1)، جامعة تشرين، اللاذقية، سوريا، ص ص: 47-72.
(4) الجور، كريمة & البلداوي، شاكر & والبياتي، محمود جلال، (2011)، "دور المدقق الداخلي والخارجي في إدارة مخاطر التكنولوجيا - دراسة تحليلية مقارنة"، **مرجع سابق**، ص ص: 22-35.
(5) ديبان، السيد عبد المقصود، كشك، وليد السيد، (2002)، "الاتجاهات الحديثة في الرقابة الداخلية على أمن نظم المعلومات في ظل التجارة الإلكترونية ودور المعايير الدولية"، **مؤتمر التجارة الإلكترونية - الأفق والتحديات**، كلية التجارة - جامعة الإسكندرية، مصر، 25-27 يوليو، ص ص: 513-524.
(6) Federal Financial Institutions Examination Council (FFIEC), (2012), **"Audit"**, HANDBOOK, April 2012, P. 49.

الحسابات الخارجيين أن يكونوا على دراية بالتهديدات الأمنية والتأكد من تطبيق الضوابط الرقابية والتقنيات المناسبة المتوفرة لدى المنشأة للمحافظة على أمن وسلامة جمع ومعالجة البيانات، وتوليد المعلومات، وإدارة قواعد البيانات في نظم المعلومات المحاسبية وتقديم المشورة حول المخاطر الأمنية،⁽¹⁾ وعدم التأهيل العلمي والعملية للمراجع يزيد من حدة هذه المخاطر، ويوجد مخاطر أخرى لم تكن موجودة، مما يستلزم ضرورة توافر التأهيل العلمي والعملية الملائم في المراجع والفريق الذي يعمل معه، بما يمكنه من اكتشاف هذه الأخطاء وحالات الغش أثناء تنفيذ عملية المراجعة، ولذلك ينبغي على مدققي الحسابات، القيام بتطوير أنفسهم، وأساليبهم الفنية المستخدمة في تدقيق الحسابات، بما يتفق مع التطورات التكنولوجية، ولاسيما أن التطور التكنولوجي يفرض عليهم أن يقوموا بتدقيق منشآت ومؤسسات تستخدم نظاماً محاسبية محوسبة، وأن الأعمال المحاسبية تعتبر من أكثر الأعمال اعتماداً على تكنولوجيا المعلومات في الوقت الراهن.

ويتوقف دور المراجع الخارجي في تقييم نظام الرقابة الداخلية على بذله العناية المهنية المناسبة، عن طريق التأكد من وجود ضوابط الرقابة الداخلية المناسبة للنظم المحوسبة،⁽²⁾ حيث يعد مسؤولاً عن اكتشاف حالات الغش إذا لم يتم ببذل العناية المهنية اللازمة، وإذا قام باستخدام طرق وأساليب المراجعة أقل من المستوى المطلوب لتبديد الشك والريبة،⁽³⁾ وهناك حاجة للمدققين الخارجيين للحصول على فهم أفضل لكيان المنشأة وبيئتها، بما في ذلك الضوابط الداخلية، من أجل التعرف على مخاطر الأخطاء الجوهرية في البيانات المالية وما يقوم به الكيان للحد من المخاطر؛ إجراء تقييم أكثر دقة للمخاطر الأخطاء من البيانات المالية بناء على هذا الفهم، وتحسين الربط بين المخاطر وتقييم طبيعته وتوقيت، وإجراءات التدقيق التي أجريت استجابة لتلك المخاطر.⁽⁴⁾

وينبغي على مديري ومدققي الحسابات العمل معاً عند تقييم المخاطر في جميع الإدارات والوظائف لتحديد معقولة تلك المخاطر، وتحديد ما إذا كانت إجراءات التدقيق لأمن المعلومات وافية وكافية لمواجهة المخاطر في مجال أمن نظم المعلومات والأعمال المصرفية الإلكترونية.⁽⁵⁾

ومن وسائل ضبط مخاطر تكنولوجيا المعلومات التدقيق المستمر المعتمد على تكنولوجيا المعلومات أحد الأساليب التي تمكن من كسب فهم معقول لنظم معلومات العميل على مدار فترة زمنية طويلة،⁽⁶⁾ فالتحول من نظام نظام التدقيق اليدوي إلى نظام التدقيق الإلكتروني أصبح ضرورة ملحة للنهوض بمهنة التدقيق ودخوله عصر تكنولوجيا المعلومات، وهذا التغير في الأسلوب أدى إلى اختلاف أساليب المراجعة والتدقيق، في تقييم المخاطر واستخدام أدوات وإجراءات وبرامج متخصصة في تكنولوجيا المعلومات في استكمال عملية التدقيق

(1) Beard, Deborah & Wen, H. Joseph, (2007), "Reducing the Threat Levels for Accounting Information System, Challenge for Management, Accountants, Auditors and Academicians", OP. Cit., PP: 34-42.

(2) Anomah, S., & Agyabeng, O. (2013). Evaluating internal controls in a computerised works environment—a risk to audit professionals and a challenge to accountancy training providers. OP. Cit., PP:132-143.

(3) (الريبيدي، محمد علي، (2012)، "تقييم نظام الرقابة الداخلية في المنشآت المستخدمة لتكنولوجيا المعلومات - دراسة ميدانية في مكاتب المراجعة اليمنية"، المجلة العربية للمحاسبة، العدد (15)، جامعة البحرين، تشرين أول (أكتوبر) 2012، ص ص: 89-122.

(4) Beard, Deborah & Wen, H. Joseph, (2007), "Reducing the Threat Levels for Accounting Information System, Challenge for Management, Accountants, Auditors and Academicians", OP. Cit., PP: 34-42.

(5) Federal Financial Institutions Examination Council (FFIEC), "Audit", HANDBOOK, April 2012, P.36.

(6) (الشرابي، عادل، (2009)، "سياسات وإجراءات التدقيق الداخلي في ظل بيئة تكنولوجيا المعلومات في البنوك الأردنية"، مرجع سابق، ص ص: 47-72.

الإلكتروني،⁽¹⁾ فأداء خدمات التدقيق بشكل سنوي لم يعد كافياً حيث ساعدت تقنية المعلومات على أن تصبح المعلومات الإلكترونية والرقمية أكثر مرونة وأسهل استحواداً وأيسر في نقلها من طرف لآخر وأسهل في تخزينها وتلخيصها وتنظيمها مقارنة بالمعلومات الورقية ومن ثم يجب تدقيقها من خلال تدقيق الكتروني مستمر،⁽²⁾ ولذلك توسعت الخدمات التي تقدمها مكاتب التدقيق في ظل عصر تكنولوجيا المعلومات إلى تطور التدقيق من التدقيق التقليدي اليدوي إلى خدمات التصديق (*Attestation*) وإلى خدمات التأكيد (*Assurance*)، بتقديم خدمات تأكيد الثقة للنظم والمواقع (*Sys & Web -Trust*)، من خلال إضفاء التأكيد أو التوكيد لكل من الإدارة، والمعملاء، والموردين، والملوك، والهيئات الحكومية، والجهات الأخرى المعنية على أن إضفاء بأن نظام المعلومات ومواقعها الإلكترونية آمنة وموثوق بها، والتأكيد على أن نظم معلومات المنشأة تم تصميمها، ويتم تشغيلها بطريقة ملائمة، وأن الأدوات المستخدمة توفر السلامة والأمن والخصوصية وإمكانية الاعتماد على البيانات المناسبة.⁽³⁾

وتقوم سلطات الرقابة بتقييم أنظمة المعلومات و أنظمة التقارير أو التوثيق لدى المنشأة المصرفية، بغرض تحديد مواطن الضعف التي تؤدي إلى تشويه أداء المهام الملقاة على عاتق الإدارات العليا والتنفيذية و انحراف القرارات، وبالرغم من الجهود المعتبرة والتي بذلت في كثير من الدول من أجل تكييف النظم الرقابية والقوانين المصرفية، ولكن يجب على الهيئات التنظيمية الإشرافية البقاء متيقظة، ويجب التنسيق والتوافق بين القوانين وكذلك تعزيز التعاون الدولي في هذا المجال،⁽⁴⁾ وفي بعض دول العالم لا يشترط إشراف البنك المركزي على البنوك العاملة سواء كانت بنوك تقليدية أو بنوك إلكترونية بينما في اليمن فإن البنوك تخضع لإشراف البنك المركزي سواء أثناء قيامها بعملها التقليدي أو أثناء قيامها بعمليات مصرفية إلكترونية و إصدار وسائل دفع إلكترونية لنقود إلكترونية، ولكن في الواقع لا يقوم البنك المركزي والسلطات الرقابية الرسمية بتكثيف حملات تفتيشية مفاجئة لتقييم مخاطر أمن نظم المعلومات المحاسبية لدى البنوك، وإلزامها برفع تقارير بهذا الشأن.

ويجب على السلطة الرقابية القيام بإجراء تقييمات مستقلة وبصفة دورية للإستراتيجيات والسياسات والخطوات والممارسات المطبقة المتعلقة بالمخاطر الأمنية لنظم المعلومات المحاسبية، وإلزام البنوك برفع تقارير دورية حول تلك المخاطر، وأن تكون هذه التقارير ذات كفاءة عالية بشكل يضمن إطلاع وإعلام السلطة الرقابية بالتطورات التي تحدث في البنوك في الوقت الملائم.

ويرى الباحث من منطلق وظيفة البنك المركزي اليمني في الرقابة على الجهاز المصرفي وتمشياً مع الاستخدام الكبير لنظم المعلومات - وبشكل خاص نظم المعلومات المحاسبية - من قبل البنوك التجارية في اليمن فلا بد للبنك المركزي من تطوير أدواته الرقابية على هذه النظم من أجل التأكد من سلامتها وتوافقها مع مبادئ إدارة مخاطر العمل المصرفي الإلكتروني، وذلك من خلال إعداد برنامج للرقابة على تلك النظم.

(1) العرود، شاهر & الختاتنة، وحيد & الشرفاء، أمجد، (2011)، " تأثير تطبيق مدققي الحسابات لأساليب تكنولوجيا المعلومات على إتمام عملية التدقيق الإلكتروني في الأردن"، *مجلة المحاسبة والإدارة والتأمين*، العدد رقم (78)، كلية التجارة، جامعة القاهرة، مصر، ص: 1-28.

(2) الجهر، كريمة & البلداوي، شاكر & البياتي، محمود جلال، (2011)، " دور المدقق الداخلي والخارجي في إدارة مخاطر التكنولوجيا - دراسة تحليلية مقارنة"، *مراجع سابق*، ص: 22-35.

(3) الدوغجي، علي حسين، (2008)، " دور مراقب الحسابات في ظل تكنولوجيا المعلومات المعقدة ومخاطر التدقيق"، *مراجع سابق*، ص: 285-304.

(4) مريم، بن الشريف، (2011)، "الأعمال المصرفية الإلكترونية: الرهانات والتحديات وإشكالية الإشراف والرقابة المصرفية"، *الملحق العلمي الدولي الرابع "عصرنة نظام الدفع في البنوك الجزائرية وإشكالية اعتماد التجارة الإلكترونية في الجزائر - عرض تجارب دولية"*، معهد العلوم الاقتصادية، المركز الجامعي خميس مليانة، الجزائر، 27-26 نيسان (أبريل) 2011.

1-4-7: التهديدات الأمنية المتعلقة بضعف التشريعات والقوانين المحلية في مجال تكنولوجيا

المعلومات:

من العوامل التي يجب النظر فيها عند تقييم مخاطر أمن نظم المعلومات المحاسبية المتطلبات القانونية والتعاقدية ذات الصلة،⁽¹⁾ حيث تنطوي نظم المعلومات المحاسبية على علاقة وثيقة بالتشريعات القانونية والمهنية، فالقوانين والتشريعات تحدد شكل ومضمون البيانات والمعلومات المالية للمنشأة ومتطلبات الإفصاح عن البيانات المالية التي يجب على إدارة المنشأة الالتزام بها واتخاذ كافة الإجراءات التي تساعد على الإيفاء بمسؤولياتها واكتشاف حالات عدم الالتزام ويستلزم ذلك تصميم نظم المعلومات للمنشأة بما يحقق تلك المتطلبات ويلبي الاحتياجات المختلفة من البيانات المالية،⁽²⁾ حيث يخضع تصميم نظم المعلومات المحاسبية وتشغيلها للعديد من القيود والمتطلبات القانونية والتشريعية والتعاقدية مثل حقوق الملكية الفكرية وحماية خصوصية البيانات الشخصية الخاصة بالعملاء، ومتطلبات ضوابط التشفير، والمتطلبات القانونية المرتبطة بإمساك الدفاتر، ويؤدي عدم التزام المنشأة بتلك المتطلبات إلى تعريضها للعديد من أشكال الخسائر، مثل الغرامات والجزاءات والتعويضات والأحكام القضائية والتأثير السلبي على سمعتها.

إن الهدف من الأمن القانوني تحقيق عدة غايات: غايات وقائية وغايات علاجية، و"درهم وقاية خير من قنطار علاج"، ولذلك لا بد من وجود الأسس والمستلزمات والأركان الضرورية لقيام التعامل الإلكتروني بشكل قانوني سليم، فالحماية التقنية وسيلة وقاية ودفاع وفي حالات معينة وسيلة هجوم ولا تتكامل حلقات الحماية دون الحماية القانونية عبر النصوص القانونية التي تحمي من إساءة استخدام الحواسيب والشبكات فيما يعرف بجرائم الحاسوب والانترنت والاتصالات والجرائم المالية الإلكترونية التي تناولناها فيما تقدم وبالتالي تتكامل تشريعات البنوك والتجارة الإلكترونية مع النصوص القانونية لحماية المعلومات، وفي هذا الصدد لا بد من التطرق للنقاط التالية:

1-4-7-1: عدم تحديث القوانين المحلية: نظراً لحدوث مخاطر الحاسوب والإنترنت، والتطور السريع لتقنية الحاسوب والإنترنت، فإن التشريعات والقوانين للدول المختلفة قد عجزت عن مواكبة هذا التطور السريع لجرائم الحاسوب، وبالتالي فإن القوانين جنائية كانت أو مدنية أو تجارية، تفتقد إلى كثير من النصوص القانونية اللازمة لمواجهة تلك الجرائم،⁽³⁾ فمثلاً تفتقد كثير من القوانين إلى وجود قواعد تنظم تفتيش الحاسوب عند اتصاله بحاسوب آخر خارج إقليم الدولة ويترتب على ذلك الكشف على بيانات ومعلومات الحاسوب الآخر، وهي ذات طبيعة معنوية لا مادية، كما أن التشريعات والقوانين في العديد من دول العالم لا تحدد الأفعال المجرمة.⁽⁴⁾

(1) The Office of the Government Chief Information Officer, (2012), "Security Risk Assessment & Audit Guidelines", Version:5.0, The Government of the Hong Kong Special Administrative Region, September 2012, P.32.

(2) DELOITTE, (2009), International Financial Reporting Standards, Electronic Version. Available at : <http://www.lasplus.com/fs/29modelsfs.pdf>, P. 19.

(3) Yang, L.H., (2011), "Information Security in Network Finance and Its Countermeasures", Engineering Education and Management, LNEE, Springer-Verlag Berlin Heidelberg, PP: 651-656. . <http://aisel.aisnet.org/pacis2007/74> ACCESSED ON 8/2012

(4) العبيدي، أسامة، (2012)، "جريمة الدخول غير المشروع إلى النظام المعلوماتي - دراسة قانونية في ضوء القوانين المقارنة"، دراسات المعلومات، العدد (14)، جامعة الإمام

محمد بن سعود، الرياض، السعودية، أيار (مايو) 2012 صص: 9- 68.

من أهم التهديدات المسببة لمخاطر أمن نظم المعلومات المحاسبية عدم تحديث القوانين المحلية النافذة التي تهدف إلى حماية أمن نظم المعلومات، سواء كانت قوانين جنائية أو مدنية أو تجارية، فهي تفتقد إلى كثير من النصوص اللازمة، ولا تزال الكثير من القوانين والأنظمة والتشريعات غير منسجمة مع متطلبات الأعمال الإلكترونية.

إن نظم المعلومات المحوسبة ليست محصنة فهي اليوم عرضة لمخاطر جديدة تهدد استمرارها في المستقبل وقد برزت هذه المخاطر بعد أن استغل القراصنة الثغرات الفنية في تلك النظم، واستفادوا من الثغرات القانونية في النظم التشريعية التي لم تعد ملائمة لرعاية العمل الرقمي، فإذا ما تأخرت القوانين والتشريعات اللازمة لمواجهة هذه الظاهرة الإجرامية، الجديدة فسوف نواجه عشوائية سيبرية كذلك العشوائية العمرانية التي نتجت عن تأخر قوانين التطوير العمراني،⁽¹⁾ فالتحديث والتطوير في الأنظمة الرقابية للعمليات المصرفية الإلكترونية يجب أن يواكبه تحديثاً مماثلاً في القوانين المصرفية.

1-4-7-2: الغموض التشريعي بشأن العمليات المصرفية الإلكترونية: تنشأ بعض المخاطر بسبب الغموض التشريعي والتنظيمي بشأن اختصاص وانطباق القوانين واللوائح والضوابط المعمول بها لتحديد الحقوق والالتزامات القانونية خاصة المتعلقة بالعمليات المصرفية الإلكترونية، ومن ذلك عدم المعرفة القانونية لبعض الاتفاقيات المبرمة باستخدام وسائل الوساطة الإلكترونية،⁽²⁾ وندرة ظاهرة الخبراء العاملين في مجالات قوانين المعلومات والاتصالات سواء في مجال وضع التشريعات واللوائح الخاصة بتلك الأنشطة، والعمل على تطبيقها وسلامة تنفيذها من الوجهة الواقعية، الفنية والقانونية، حيث تنشأ المخاطر القانونية (Legal Risks) نتيجة الغموض أو الصعوبة في إمكانية تطبيق القوانين الخاصة بتحديد الحقوق والالتزامات القانونية الناتجة عن التعاملات المصرفية الإلكترونية، أو عدم وجود قوانين وقواعد لتنظيم الأعمال المصرفية الإلكترونية في بعض الدول، أو عدم توضيح الجوانب القانونية والقواعد المتصلة بالأعمال المصرفية وحماية حقوق العملاء من خلال مواقع البنوك على شبكة الانترنت.

ولذلك ينبغي بذل مزيد من الجهود على المستويين القطري والإقليمي من أجل معالجة النقص في الأطر القانونية الخاصة بالجرائم المعلوماتية، فالغاية من التشريعات على صعيد البنوك الإلكترونية هي الاعتراف بمختلف وسائل العمل المصرفي الإلكتروني وتطبيقاته وحلوله، وتيسير سائر الخدمات المصرفية الإلكترونية، لضمان الامتثال واستيفاء جميع المتطلبات القانونية اللازمة لأمن محتوى البيانات المتبادلة ذات الطبيعة المالية وسلامته، وتعزيز الثقة بالبيئة وخدماتها وتطبيقاتها، وكذلك تعزيز التعامل التفاعلي بين العميل ومواقع البنوك والخدمات المالية الإلكترونية.⁽³⁾

(1) عميش، رحاب، (2009)، "الجريمة المعلوماتية"، المؤتمر العلمي المغربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ليبيا، 28 - 29 تشرين أول (أكتوبر).

(2) قديمي، ثائر عدنان، (2010)، "الصيرفة الإلكترونية في المصارف التجارية الأردنية - دراسة تطبيقية لدور الخصائص الشخصية: المعوقات ومقومات النجاح"، المجلة العربية للإدارة، المجلد (30)، العدد (1)، يونيو 2010، عمان، الأردن، ص: 113-142.

(3) اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، (2009)، "بناء الثقة بالخدمات الإلكترونية في منطقة الإسكوا"، 10 مارس 2009، ص: 46.

1-4-7-3: اختلاف التشريعات القانونية بين الدول: توجد قيود قانونية متمثلة في اختلاف التشريعات القانونية التي تنظم التعاملات المصرفية الالكترونية والتجارة الالكترونية بين الدول وذلك يؤدي إلى تنازع القوانين واختصاصات المحاكم في فض النزاعات التي تنشأ عنها وأي من القوانين يجب تطبيقها، ومن أهم تلك التشريعات، التشريعات الخاصة بحماية برامج الحاسوب، تشريعات التجارة الالكترونية ومن ضمنها تشريعات معايير الأمن المعلوماتي، والتشريعات المالية والمصرفية فيما يتصل بالمال الإلكتروني وتقنيات الخدمات المصرفية، وتشريعات حماية الخصوصية، فبالرغم من أن عدد كبير من دول العالم خاصة الدول المتقدمة قد قامت بوضع تشريعات تقن العمل المصرفي الإلكتروني وتحمي حقوق المتعاملين بها إلا أن معظم الدول النامية لم تقم بهذه الخطوة بعد، وبالتالي تشكل عائق أمام النشاط المصرفي الإلكتروني.

وبالتالي يرى الباحث أن وجود القوانين والتشريعات الموحدة والتي تحدد معايير وشروط المعالجة الآلية للبيانات له دور كبير في مواجهة التأثيرات السلبية.

1-4-7-4: عدم وجود أطر تشريعية وقانونية متناسقة ومتجانسة لمعاقبة مرتكبي جرائم الحاسوب: يمكن الدخول إلى الإنترنت والتعامل عن طريقها في كافة أنحاء الكرة الأرضية، وأصبحت الإنترنت اليوم تشهد تعايشاً مستمرا في جميع المجالات العلمية والبحثية والاقتصادية، بل والسياسية والاجتماعية على السواء وعليه فليس من المهم تطبيق القوانين والتشريعات ذات العلاقة بأمن المعلومات في البلد الموجودة به المنشأة، بل يجب أن تطبق كافة التشريعات والقوانين الملزمة في البلدان التي يوجد بها عملاء لتلك المنشأة،⁽¹⁾ لأن نظم المعلومات غالبا ما تتعدى الحدود القومية أو الوطنية المحدودة، فهي مشكلة تتطلب تعاوناً دولياً مكثفاً للتغلب عليها،⁽²⁾ وهو ما يقودنا إلى ضرورة التعرض إلى تحديات الجريمة المعلوماتية في ظل الفراغ التشريعي اليمني في مواجهة هذه الجرائم من جهة، وتحديات الجريمة المعلوماتية العابرة للحدود الإقليمية من جهة أخرى.

وتنتج المخاطر لعدم التوافق ما بين النشاطات المصرفية الإلكترونية وبين التشريعات التي تعالج الأنشطة المصرفية التقليدية وتشريعات المعاملات الإلكترونية والتصديق الإلكتروني والتشغيل وأنظمة التخويل، والتشريعات المتعلقة بالمحافظة على سرية بيانات العملاء، كما أن تعامل البنك مع عملاء من دول أخرى قد يعرضه لمخاطر قانونية تتمثل بعدم تفهم تشريعات الدول الأخرى مثل تشريعات حماية المستهلك، وغسيل الأموال، والتحويل الإلكتروني للنقود وغيرها من التشريعات وحماية متطلبات و قوانين الخصوصية.⁽³⁾

إن عدم وجود العقوبة القانونية الشديدة التي تجعل من يريد القيام بعملية اختراق يفكر ألف مرة ومرة قبل القيام بتلك المحاولة، هو العامل الأهم في زيادة عمليات الاختراق، فقد ارتفع عدد الجرائم الالكترونية المنظمة نظراً لوجود ثغرات في التشريعات الوطنية والإقليمية مما يجعل من الصعوبة ملاحقة المجرمين،⁽⁴⁾ ولذلك لا يمكن أن يتم حماية المعلومات على الصعيد الوطني إلا إذا تم التنسيق والتعاون بين القطاع العام والقطاع الخاص والهيئات

(1) عميش، رحاب، (2009)، "الجريمة المعلوماتية"، مرجع سابق، ورقة عمل.

(2) Zafar, Humayun, (2013), "Human resource information systems: Information security concerns for organizations", *Human Resource Management Review*, No. 23, 2013, PP: 105-113, <http://dx.doi.org/10.1016/j.hrmr.2012.06.010>

(3) Dahbur, Kamal & Mohammad, Bassil & Tarakji, Ahmad, (2011), "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing", *OP.Cit.*

(4) توريه، حمدون، "البث عن السلام السيبراني"، الاتحاد الدولي للاتصالات، يناير 2011، ص97.

الوطنية واستعداد الدول للتعاون فيما بينها على المستوى المحلي والإقليمي والدولي لحماية المعلومات والتصدي للمخاطر التي تهدد إتاحتها وسريتها ودقتها، بشرط أن تقوم كل دولة بوضع إستراتيجية وطنية ووضع سياسات مرنة وسن قوانين خاصة للحد من إساءة استخدام المعلومات ووسائل الاتصال.⁽¹⁾

ولذلك يرى الباحث أنه من الضروري أن تعمل الدول على تنسيق أطرها القانونية لمكافحة الجرائم المعلوماتية وتيسير التعاون الدولي الديناميكي متعدد الجوانب، لوضع إطار قانوني وتنظيمي مشترك، وإقامة نظام لتحديث هذه القوانين على أساس منتظم لمعالجة الطبيعة المتغيرة للتهديدات والمخاطر التي يتعرض لها أمن نظم المعلومات المحاسبية، مع الأخذ في الاعتبار المعايير الخاصة بكل دولة.

1-4-8: التهديدات الأمنية المتعلقة بنقص الوعي الإلكتروني لدى عملاء البنك:

من الأسباب الخارجية للمخاطر نقص الوعي الإلكتروني لدى العملاء حيث أن جزء لا يستهان به ليسوا على دراية كافية بهذا المجال، فالتكنولوجيا قد تكون بلا فائدة لمن لا يملك القدرة والمعرفة على التعامل معها، وترجع المخاطر المتصلة بهذا الجانب إلى انخفاض وعي العملاء وعدم إلمامهم الكافي بكيفية استخدام نظام الانترنت المصرفي وعدم إحاطتهم بإجراءات التأمين والوقاية، أو سماحهم لعناصر أخرى بالدخول إلى حساباتهم من خلال إفشاء المعلومات الشخصية والخاصة بإجراءات الدخول وكلمة المرور (Password)، واسم المستخدم User Name، أو رقم الحساب وغيرها من بيانات بطاقات الائتمان.⁽²⁾

وقد يؤدي التنوع الكبير لمستخدمي نظم المعلومات المحاسبية المحوسبة والمتعاملين معها (العاملين، المستشارين، العملاء، المنافسين والمساهمين) فيما يتعلق بعدم توعيتهم وتدريبهم واهتماماتهم المختلفة والمتفرقة إلى ظهور صعوبات خاصة بأمن المعلومات ونظمها، وبالتالي فإن ضعف الوعي بأمن المعلومات وأمن الاتصالات في المنشأة من أكبر مصادر الخطر وتقيد التقارير العالمية التي تخص أمن وحماية المعلومات في العالم بأن نسبة اختراق أجهزة وشبكات الحاسوب ترجع إلى عدم وعي المستخدم بضرورة أمن وحماية المعلومات، بسبب عدم إحاطة العملاء بإجراءات التأمين الوقائية الواجب القيام بها أو السماح لعناصر غير مرخصة بالدخول على الشبكة أو القيام بعمليات غسيل أموال باستخدام معلومات العملاء الشخصية.⁽³⁾

إن نقص الوعي الإلكتروني لدى عملاء البنك وعدم إتباعهم إجراءات التأمين الوقائية الواجبة لبياناتهم الشخصية، وضعف دور البنك في القيام بتوعيتهم تعد مهدد خارجي ومصدر لنشوء المخاطر، وللأسف تعليمات الأمن على شبكة الإنترنت تفشل لعدم فهم المستخدمين لتلك التعليمات،⁽⁴⁾ وبالتالي فإن استخدام العملاء لخدمات البنك بشكل خاطئ مقصود أو غير مقصود، لعدم توافق النظم المحوسبة مع عادات وثقافة العملاء، قد يؤدي إلى نتائج عكسية تؤدي إلى ابتعاد العملاء عن هذا البنك أو تحميل البنك خسائر مادية مباشرة، من هنا نرى أنه من

(1) غنوم، أيمن، "أمن المعلومات"، (2009)، مجلة البنوك، جمعية البنوك في الأردن، عمان، الأردن، نسخة إلكترونية.

(2) Olasanmi, Omonye & Olufunke, Lecturer, (April 2010), "Computer Crimes and Counter Measures in the Nigerian Banking Sector", Journal of Internet Banking and Commerce, Vol. 15, No.1, PP: 1-10.

(3) شاهين، علي عبدالله، "نظم الدفع الإلكترونية ومخاطرها ووسائل الرقابة عليها دراسة تطبيقية على بنك فلسطين"، مراجع سابق، ص: 511-546.

(4) Oghenerukeybe, Egwali Annie, (April 2009), "Customers Perception of Security Indicators in Online Banking Sites in Nigeria", OP. Cit., PP: 1-10.

واجب البنك أن يقوم بتوعية العملاء وتعريفهم بالاحتياطات الأمنية الواجب اتخاذها وحدود مسؤوليتهم، ومسؤولية البنك، فتغيير سلوك الموظفين موقف إيجابي لأمن المعلومات من خلال تعزيز وتوعية المستخدمين زيادة الثقافة الأمنية للمنشأة وبالتالي تحسين فعالية الأمن وهذا يتطلب زيادة التركيز على تعليم الموظفين لضمان ثقافة الأمن للمستخدمين النهائيين⁽¹⁾

ومن خلال ما سبق يرى الباحث أنه ينبغي على إدارة المنشأة العمل على حماية بياناتها بكافة أشكالها، فنظم المعلومات المحاسبية المحوسبة تكون عرضة للمخاطر أكثر من غيرها من النظم ولذلك لا بد للإدارة من وضع قيود على المستخدمين تحد من إمكانية التلاعب بالبيانات أو العبث بها سواء من أطراف داخل المنشأة أو خارجها. **الخاتمة:** في هذا البحث تم تسليط الضوء على التهديدات الخارجية المسببة لأمن نظم المعلومات المحاسبية المحوسبة، وهي تهديدات أمنية كبيرة كالحوادث الطبيعية (الفيضانات والحرائق والزلازل)، أو القرصنة والمخترقين.

تواجه نظم المعلومات والاتصالات من قبل مجموعة كبيرة ومتنوعة من التهديدات ولا يوجد باحث أو مؤلف أو مرجع يقدم قائمة شاملة للمخاطر والتهديدات وثغرات الحماية، لأن ذلك يعني الوقوف على كل الوسائل التقنية والوقوف على كل الاستخدامات إضافة إلى تصور ما لا يمكن للعقل تصوره من أغراض وبواعث محركة للهجوم تمتد عبر طريق يضم أكثر الأشخاص احترافاً للجريمة مع أكثرهم بساطة، ويضم هواة وخبراء، ويضم حاقدين وحسني النية، ويضم جواسيس يلفظهم المجتمع وآخرين يتظاهر من اجلهم بوصفهم أبطالاً شعبيين الخ.⁽²⁾ وبمجرد أن يتم تحديد الأسباب التي تولد مثل هذا الخطر، يجب إشعار إدارة المنشأة في طلب لاتخاذ الإجراءات التصحيحية المناسبة لتقليل تلك المخاطر.⁽³⁾

إن مجرد رد الفعل تجاه المخاطر لا يكفي خاصة في ظل الظروف والمتغيرات المعاصرة، فالمطلوب هو أخذ زمام المبادرة ومحاولة التوصل مسبقاً إلى معرفة المخاطر التي يمكن الحيلولة دونها، وما هي الإجراءات اللازمة لمواجهة هذه المخاطر، وذلك لن يتأتى إلا من خلال مجموعة من المؤشرات التي تساعد المنشأة على معرفة وإدراك المخاطر قبل حدوثها، والجدير بالذكر أن ذلك مفيد للمخاطر المتكررة، أما المخاطر المفاجئة والتي تحدث دون سابق إنذار، فيصعب توقع حدوثها من خلال تلك المؤشرات.

إن أنواع التهديدات الداخلية والخارجية التي تتعرض لها نظم المعلومات المحاسبية المحوسبة، تتطلب تضافر الجهود الفنية المتمثلة بالتكنولوجيا الحديثة للحاسبات بشقيها البرمجيات (Software) والمعدات (Hardware) فضلاً عن إجراءات الرقابة المتعلقة بأمن المعلومات والمعدات لتشكل عناصر مهمة للحد من التهديدات المحتملة لنظم المعلومات المحاسبية.

(1) Shahri, Ahmad & Ismail, Zuraini & Rahim, Nor, (2012), "Security Effectiveness in Health Information System: Through Improving the Human Factors by Education and Training", *OP. Cit.*, PP: 226-233.

(2) Al-Awadi, Maryam, (2009), "A Study of Employees' Attitudes Towards Organizational Information Security Policies in the UK and Oman", *OP. Cit.*, P.13.

(3) Brandas, C. & Stirbu, D. & Didraga, O., (2013), "Integrated Approach Model of Risk, Control and Auditing of Accounting Information Systems", *Informatica Economică*, Vol. 17, No. 4, West University of Timisoara, Romania, PP: 87-95.

خلاصة الفصل الأول:

تناول الباحث في هذا الفصل وصفاً نظرياً لطبيعة أنواع المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة، حيث تناول المبحث الأول: طبيعة أمن نظم المعلومات المحاسبية المحوسبة من خلال التعرف على ماهية نظم المعلومات المحاسبية المحوسبة، وأنواع نظم المعلومات المحاسبية المحوسبة على أساس بيئة التشغيل البيانات، ودورة تجهيز البيانات في تلك النظم ووظائفها المختلفة، وتعريف مفهوم أمن نظم المعلومات المحاسبية المحوسبة، وتوضيح المبادئ والأهداف الأساسية لأمن تلك النظم، وإبراز مدى أهمية أمن نظم المعلومات المحاسبية المحوسبة، وبيان مكونات أمن تلك النظم، ومعرفة المحاور والأنماط الأساسية لأمن تلك النظم وفقاً لمستويات الحماية، وكذلك بيان الاعتبارات التي يجب مراعاتها لضمان فعالية وكفاءة أمن تلك النظم.

وتناول المبحث الثاني: طبيعة مخاطر أمن نظم المعلومات المحاسبية المحوسبة، ومفهوم مخاطر أمن نظم المعلومات المحاسبية المحوسبة، مع عرض وجهات النظر المختلفة لتصنيف وتبويب مخاطر أمن نظم المعلومات المحاسبية المحوسبة من حيث مصدرها، أو من حيث النية من وراء إحداثها، أو من حيث المتسبب بها أو تصنيفها على أساس الأصول (المادية أو الفنية) المستخدمة في النظام أو على أساس تأثيرها المباشر وغير المباشر على أمن نظم المعلومات، أو طبقاً لقابلية المخاطر للاكتشاف، أو على أساس علاقتها بمراحل النظام المحاسبي، أو طبقاً لتكنولوجيا المعلومات المستخدمة في النظام، أو طبقاً لمواضع المعلومات أو عناصر النظام محل الحماية.

وتم في هذا المبحث وضع تصور شامل لأنواع مخاطر أمن نظم المعلومات المحاسبية المحوسبة من حيث يتناول المخاطر التي تهدد أمن الأفراد العاملين في نظم المعلومات المحاسبية المحوسبة، والمخاطر التي تهدد الأمن المادي لتلك النظم، والمخاطر التي تهدد أمن الوصول البرمجي لنظم المعلومات المحاسبية المحوسبة، المخاطر التي تهدد أمن التخزين غير المتصل بقاعدة بيانات تلك النظم، والمخاطر التي تهدد أمن مدخلات تلك النظم، والمخاطر التي تهدد أمن عمليات تشغيل تلك النظم، والمخاطر التي تهدد أمن مخرجات تلك النظم، وكذلك المخاطر التي تهدد أمن تبادل البيانات عبر شبكات نظم المعلومات المحاسبية المحوسبة، وأخيراً المخاطر التي تهدد أمن تعديل وتطوير تلك النظم.

وتناول المبحثين الثالث والرابع التهديدات المختلفة التي تسبب مخاطر أمن نظم المعلومات المحاسبية المحوسبة سواء كانت تهديدات داخلية من داخل المنشأة أو تهديدات خارجية من خارج المنشأة المستخدمة لنظم المعلومات المحاسبية المحوسبة.

وبعد أن تناول الباحث دراسة الجوانب المتعلقة بالمخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة وفي ضوء ذلك يقوم الباحث في الفصل التالي بدراسة تقييم تلك المخاطر وما يتعلق بها خصوصاً في مجال: تحديد معايير وأسس تقييم المخاطر الصادرة من الهيئات المختصة المحلية والدولية، وبيات طبيعة ومراحل وأدوات تقييم مخاطر أمن نظم المعلومات المحاسبية، وبيان حجم تأثير تلك المخاطر على عناصر أمن نظم المعلومات المحاسبية، وأخيراً على ضوء ذلك يتم تحديد إجراءات ووسائل الحماية المتبعة للتخفيف أو الحد من تلك المخاطر.

الفصل الثاني

تقييم مخاطر أمن نظم المعلومات المحاسبية

الفصل الثاني: تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة

مقدمة:

تطرقنا في الفصل الأول إلى المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة، مما يتطلب من الإدارة الناجحة تحديد وتحليل هذه المخاطر من منظور متكامل لمحاولة إدارتها والتقليل من آثارها السلبية. إن اعتماد المنشآت كلياً على آلية الرقابة الداخلية التقليدية أصبح غير كافٍ حالياً، فقد ظهرت الحاجة إلى بناء أدوات وعمليات خاصة لمواجهة مخاطر العمليات المصرفية يمكنها تقديم الأمن والسلامة للمنشأة، وفي أغلب الأحيان قد لا تجاري نظم الرقابة المصممة في نظم المعلومات المحاسبية المحوسبة التغيرات والتطورات في مجال الصيرفة الالكترونية، ولذلك أصبح من الضروري إعادة تصميم الإجراءات الرقابية اللازمة للسيطرة على المخاطر في ظل الأزمات الاقتصادية العالمية المتعاقبة.

والجدير بالذكر أن نظم المعلومات المحاسبية الذي يمكن الوثوق فيها هي تلك النظم التي تكون قادرة على العمل بدون أخطاء جوهرية أو فشل خلال فترة محددة في بيئة معينة وبالتالي فإن تحقيق الثقة في نظم المعلومات المحاسبية لن يتحقق إلا من خلال وجود إطار لتقييم وإدارة مخاطر نظم المعلومات المحاسبية والتي تعد أحد دعائم آلية حوكمة تكنولوجيا المعلومات الذي يرتبط بالتوجه العام نحو حوكمة المنشآت.⁽¹⁾

إن تقييم المخاطر الأمنية لنظم المعلومات المحاسبية هو أمر حيوي لمعظم المنشآت، ليس فقط لتحديد و ترتيب أولويات أصول المعلومات ولكن أيضاً لتحديد ورصد المخاطر والتهديدات المختلفة وفرص حدوثها، وتأثيرها على المنشآت المعنية، وتلك المخاطر تعد جزءاً جوهرياً في انشغالات أي منشأة، كيف لا !! وهي أحداث قد تؤدي إلى منع المنشأة جزئياً أو كلياً من تحقيق أهدافها،⁽²⁾ ولذلك فإن المخاطر التي تواجه أمن نظم المعلومات المحاسبية المحوسبة بحاجة ماسة إلى إدارة واعية قادرة على مواجهتها حتى لا تؤثر تأثيراً سلبياً على قدرة نظم المعلومات المحاسبية في المنشأة على تحقيق أهدافها، وعلى بقاء المنشأة واستمرارها في مزاولة النشاط، وذلك يتطلب إجراء تقييم لتلك المخاطر لمعرفة حجمها وأسبابها وقدرة نظم الرقابة الداخلية في المنشأة بالتصدي لتلك المخاطر ومواجهتها.

وعليه يرى الباحث أن فهم تلك المخاطر وتطبيق منهجية علمية لتقييمها، ومعدلات تكرارها، ومعرفة العوامل المسببة لها، والآثار السلبية الناتجة عنها، وذلك تمهيداً لاختيار أنسب أسلوب لمواجهة المخاطر، وهو أمر ضروري لتكون المنشآت المختلفة قادرة على خلق بيئة آمنة لنظم المعلومات المحاسبية المحوسبة بكفاءة وفعالية.

وفي هذا الفصل يتم تسليط الضوء على بعض المعايير والإرشادات لتقييم المخاطر التي تواجه أمن نظم المعلومات المحاسبية، ومنهجيات التقييم، ثم تقييم آثار تلك المخاطر على أمن نظم المعلومات المحاسبية، ملقياً بذلك الضوء على أهمية الضوابط الرقابية ووسائل وإجراءات الحماية الداخلية عند اتخاذ الوسائل الوقائية والدفاعية لتجنب تلك المخاطر وتقليل آثارها وانعكاساتها السلبية، وكيفية تفادي تلك المخاطر والتهديدات من خلال محاولة إيجاد حلول مناسبة تساعد باستغلال تلك النظم بشكل آمن والاستفادة منها بشكل يخدم المتعاملين بها.

(1) عيسى، علا & وعاشور، عصافيت، (2010)، "مخاطر نظم المعلومات المحاسبية وحوكمة المنشآت ومواجهة الأزمة المالية العالمية"، مجلة الفكر المحاسبي، المجلد (14)، العدد (2)، كلية التجارة، جامعة عين شمس، القاهرة، مصر، ص: 408-434.

(2) Shamala, Palaniappan & Ahmad, Rabiah & Yusoff, Mariana, (2013), "A conceptual Framework of Info Structure for Information Security Risk Assessment (ISRA)", OP. Cit., PP: 45-52.

2-1: المبحث الأول: أهم المعايير والأطر الدولية لتقييم مخاطر أمن نظم المعلومات المحاسبية

لتبسيط الضوء على أهمية تقييم وإدارة مخاطر أمن تكنولوجيا المعلومات، هناك العديد من المبادئ والمعايير التوجيهية لتوجيه مثل هذه الممارسات، فقد ظهرت العديد من معايير أمن المعلومات على المستوى الدولي التي تشكل الأساس الذي تعتمد عليه إدارة مخاطر أمن نظم المعلومات فضلاً عن أنها الأساس الذي يمكن الاعتماد عليه عند تصميم أنظمة الرقابة الداخلية على أمن نظم المعلومات.⁽¹⁾

معظم المعايير هي أدوات تصف بشكل عام إطار إدارة المخاطر وبشكل ملموس لا يتم عرض مقاييس الأمن كاملة وتطبيقها بوصفها سحرية، وينشأ هذا الوضع من حقيقة أن كافة المنشآت لا تعترف بكافة المخاطر الأمنية.⁽²⁾

ومما لا شك فيه أن أمن نظم المعلومات تلعب دوراً مهماً في حماية أصول المنشأة وكثيراً ما نسمع في الأخبار عن الحوادث الأمنية لأمن نظم المعلومات مثل تشويه المواقع، وقرصنة الخوادم، وتسرب البيانات والمعلومات و لذلك فإن المنشآت بحاجة ماسة إلى أن تدرك الحاجة إلى تكريس المزيد من الموارد لحماية أصول نظم المعلومات، ويجب التنبيه لمخاطر أمن نظم المعلومات المحاسبية في كل من القطاع الحكومي وقطاع الأعمال.⁽³⁾

وعلى المنشآت عموماً والبنوك خصوصاً تطوير نظم حماية ملائمة وبما يتناسب والمعايير والقواعد المعمول بها دولياً على أصعدة التأكد من هوية العملاء وشرعية التوقيع الإلكتروني والتشفير وخلافه، وعلى المستوى الدولي يتعين على السلطات الدولية تشجيع عملية تطوير منهج شامل لإدارة مخاطر أمن نظم المعلومات المحاسبية.

إن وجود مجموعة من الضوابط والإجراءات التي توفر الثقة في المعلومات الإلكترونية المنشورة على مواقع المنشآت الاقتصادية المختلفة يسهل للعديد من الهيئات الدولية تقييم مدى التزام المنشآت بتلك الضوابط والإجراءات قبل منحها ترخيص مزاولة نشاطها التجاري، وقد أصدرت تلك الهيئات مجموعة من المعايير والشهادات الخاصة بأمن وسلامة نظم المعلومات المحاسبية المحوسبة.

وتختلف محاور هذه المعايير بحسب الجهة التي يصدر عنها المعيار كالبنوك واتحادات المستهلكين وهيئات تكنولوجيا المعلومات وغيرها ومنها ما يتعلق بالمعاملات التجارية وكيفية إتمامها وفرض استخدام برامج حماية معينة ونظم أمان وشفرات الكترونية وغيرها من التقنيات المتعلقة بالحفاظ على السرية، أما المعايير الصادرة عن الجهات المحاسبية فإنها تركز على مصداقية الأعمال التجارية ونزاهتها وأمن المعلومات والبيانات وحمايتها والاهتمام بخصوصيتها.

إن حماية المنشأة وأصولها وإدارة المخاطر عن طريق تحديد الأصول، واكتشاف التهديدات وتقييم المخاطر وتوفير التوجيه لأنشطة الأمن عن طريق صياغة سياسات أمن المعلومات والإجراءات والمعايير والمبادئ التوجيهية.⁽⁴⁾

(1) الدوغجي، علي حسين، (2008)، " دور مراقب الحسابات في ظل تكنولوجيا المعلومات المعقدة ومخاطر التدقيق"، مرجع سابق، ص 285-304.

(2) Munteanu, Adrian, (2006), "Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma", Managing Information in Digital Economy: Issues & Solutions, Proceedings of the 6th International Business Information Management Association (IBIMA) Conference, Faculty of Economics and Business Administration, Alexandru Ioan Cuza University, Romanian, 19-21 June, PP: 227-232.

(3) المدرع، فهد فايز، (2012)، "المعايير العالمية لأمن المعلومات"، مركز التميز لأمن المعلومات، الرياض، السعودية، نسخة الكترونية، مستخرجة بتاريخ 25-9-2012، 8:36 مساءً.

(4) Wikipedia, (2014), .(OP. Cit),

http://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Information_Security_and_Risk_Management , Accessed 26/02/2014, in 08:33 GMT

إن المنشآت بحاجة ماسة إلى أن تدرك الحاجة الماسة إلى تكريس المزيد من الموارد لحماية أصول المعلومات وبما أنه لا يمكن أن نضمن حماية للمنشأة بنسبة 100 %، لذلك نحن بحاجة لوضع مجموعة من المقاييس أو المعايير التي يمكن من خلالها تحقيق مستوى ملائم من الأمن.

في هذا الإطار من المفيد الإطالة المختصرة على ما أنتجت الجهود الدولية في هذا المجال والاستفادة من الخبرات المتراكمة في هذا الصدد مع الإشارة إلى أن هذه الجهود في معظمها لم تراعي مبدأ التطور واقتصرت على الفترة الزمنية التي صدرت بها دون تحديثها أو تطويرها.

ومن خلال هذه المقدمة فإننا سنذكر أهم المعايير العالمية التي تساعد على تحقيق الحد الأدنى لأمن المعلومات مثل الأيزو (ISO) وكوبيت (COBIT) ونيس (NIST) وكذلك بعض القوانين المرتبطة بأمن المعلومات مثل سوكس (SOX)، وكوسو (COSO)⁽¹⁾، وهذه المرجعيات هي مجرد واحدة من العديد من الأدوات المتاحة لإجراء تقييمات مخاطر أمن نظم المعلومات وأدوات تقييم لتلك المخاطر أكثر تقدماً.

إن تنفيذ أفضل الممارسات ينبغي أن تكون متسقة مع إدارة المخاطر في المنشأة وأطر الرقابة المناسبة، وتتكامل مع الأساليب والممارسات الأخرى التي يتم استخدامها، ويجب أن يتم تحديد معايير تقييم المخاطر للمؤسسة بهدف تحديد الأصول الهامة ومن ثم تحليل نقاط الضعف والتهديدات المحتملة لتلك الأصول من خلال تقييم معايير الصناعة المحدد أو المبادئ التوجيهية أيزو (ISO 2700)، وكوبيت (COBIT)، نيس (NIST 53-800)، كمبادئ توجيهية - التي تنطبق على حالات التعرض ضمن بيئة العمل السحابية، وبالنسبة للمنشآت التي هي عرضة للتهديدات والمخاطر أكثر من غيرها، فمن المنطقي أن تكيف تلك المبادئ التوجيهية لكل معيار تنظيمي أو توجيهي حسب مقتضى الحال.

2-1-1: مفهوم معايير أمن نظم المعلومات:

من المهم أن نفهم العلاقة بين السياسات والمبادئ والمعايير والممارسات والتي تتسجم وفق تسلسل هرمي، فالسياسة تنص على الهدف بشكل عام، أما المبدأ التوجيهي فهو خطوط إرشادية ونصائح عملية حول آلية تحقيق أهداف السياسة، وهو وثيقة تصف أفضل الممارسات، وتوصيات توضح ما ينبغي القيام به لتحقيق هدف ما،⁽²⁾ بينما المعايير تهتم بتحديد المطلوب إنجازه في شروط محددة، أما الإجراءات تركز على آلية وكيفية تلبية وتنفيذ المعايير.⁽³⁾

ومنظمة المعايير هي أي كيان يملك نشاط أولي أو متطور في إصدار ومراجعة وتعديل، وتفسير، المعايير التي تلبى مصالح قاعدة عريضة من المستخدمين، والضوابط المعيارية هي نتيجة ثانوية للثقافة الأمنية السائدة، التي هي مجمل أنماط من السلوك في المنشأة التي تساهم في حماية المعلومات من جميع أنواع المخاطر.

وفي هذا الصدد يجب أن نميز بين الإطار والمعيار، فالمعيار هو شيء ثابت ومحدد وينبغي إتباعه لتحديد الأسلوب المناسب للقيام بعملية معينة، أما الإطار فهو شيء واسع ومرن وغير محدد دائماً للقيام بعمل ما خطوة خطوة،⁽⁴⁾ كإطار (COSO) و (COBIT) لمعالجة القضايا المتعلقة بتحديد الضوابط الداخلية للأمن.

(1) المدرع، فهد فايز، (2012)، "المعايير العالمية لأمن المعلومات"، مرجع سابق.

(2) ISO/IEC 27000, (2012), "Information technology - Security techniques - Information security management systems - Overview and vocabulary", OP. Cit., Available at: <http://www.27000.org> (Accessed July 14, 2013). & Alramahi, N. M., Barakat, A. I., & Haddad, H. (2014). Information Technology Governance Control Level in Jordanian Banks Using: Control Objectives for Information and Related Technology (COBIT 5). *Information Technology*, Vol.6, No.5.

(3) Tofan, Dan, (2011), "Information Security Standards", *Journal of Mobile, Embedded and Distributed Systems*, Vol. III, No.3, Academy of Economic Studies Bucharest, Romania, PP: 128-135.

(4) Olivia, (2011), *Difference Between Standard and Framework*. Available to: <http://www.differencebetween.com/difference-between-standard-and-vs-framework/> (3-5-2011).

ويعرف المعيار بأنه مجموعة محددة مسبقاً من القواعد و الشروط أو المتطلبات المتعلقة بتعريف المصطلحات، وتصنيف المكونات، وتحديد المواد، أو إجراءات الأداء، وتخطيط العمليات، والقياسات الكمية أو الجودة لتوصيف المواد، المنتجات، الأنظمة، الخدمات أو الممارسة، حيث يعرف معيار أمن نظم المعلومات: بأنه هو المعيار التقني للمساءلة لأنه يمثل مجموعة من المتطلبات التي يجب على منتج أو نظام ما تحقيقه، على افتراض مطابقة المنتج أو النظام مع مستوى معين يوضح أنه يستوفي جميع المواصفات القياسية.⁽¹⁾

2-1-2: أهمية استخدام المعايير لتقييم وإدارة مخاطر أمن نظم المعلومات:

تم اقتراح مبادئ توجيهية لإدارة أمن نظم المعلومات ممثلاً بالأطر والمعايير الدولية المختلفة، *COSO*، *COBIT*، *BS7799* ومشتقاته (*BS ISO / 2000 : IEC17799*)، للحصول على شهادات من لجان خارجية محايدة وموثوقة تثبت أن المنشأة امتثلت للمبدأ التوجيهي.⁽²⁾

هذه المعايير والإرشادات منحت المنشآت الخطوط العريضة لاعتماد وتحسين الضوابط ذات الصلة التي تناسب ظروفها الخاصة والحفاظ عليها في مواجهة التغيرات الداخلية والخارجية، كما ألزمت المنشآت امتلاك تعريفات واضحة على تدابير الرقابة، وتقديم ضمانات لحماية أمن نظم المعلومات، وجعلت متطلبات زيادة الامتثال لأمن تكنولوجيا المعلومات وإدارة مخاطرها مسؤولية لا غنى عنها لمديري تكنولوجيا المعلومات وعلى نحو متزايد.⁽³⁾ وتعمل تلك المعايير على الترويج للممارسات السليمة وبطريقة غير إلزامية، ونحن بحاجة إلى معايير لأمن نظم المعلومات يتم قبولها واستخدامها بالإجماع و يعطي إمكانية المقارنة بين نظام الأمن لأي منشأة مع إطار محدد من المرجعية المعتمدة على مستوى دولي، فمثلاً مجموعة معايير *ISO 9000* بشأن نظام إدارة الجودة، تُعد مرجعية مشتركة للعديد من المنشآت بغض النظر عن نوعية نشاطها فهي معايير ضمان للخصائص المرغوبة من المنتجات والخدمات مثل الجودة والسلامة، والموثوقية، والكفاءة والتبادلية، و بتكلفة اقتصادية، وعلى غرار معايير مراقبة الجودة، يأتي دور معايير أمن نظم المعلومات الأساسية لبيان أن ممارسات المنشآت فيما يخص أمن نظم المعلومات يتوافق مع أفضل الممارسات والإجراءات العالمية،⁽⁴⁾ حيث يمكن للمعايير تحليل المخاطر، والضوابط الأمنية وتخفيض مخاطر أمن المعلومات (أي الحد من احتمال حدوثها، و/ أو الأثر الناجم عن حدوثها على أمن نظم المعلومات)، حيث تقوم تلك المعايير بدعم عملية تحديد وتنفيذ وتشغيل وصيانة شاملة لإدارة مخاطر أمن نظم المعلومات والضوابط الأمنية، بطريقة منظمة وفعالة ومتسقة ومتكاملة وكفوءة من حيث التكلفة، تلبي احتياجات المنشأة عبر عمليات ومواقع مختلفة،⁽⁵⁾ وبشكل عام أصبح استخدام معايير أمن نظم المعلومات ضرورة ملحة لأي منشأة للأسباب التالية:

1. **تشارك المعرفة:** لأن معايير امن نظم المعلومات تتبع قطاعاً متغيراً بشكل متسارع، فإن وجود مجموعة كبيرة من الأشخاص مهتمين في معيار معين يوفر تشاركية أكبر في المعلومات ويمنح سرعة في الحصول على المعلومة المطلوبة ويوفر أيضاً معرفة بالاتجاهات المستقبلية والتقنيات الجديدة المستخدمة في مجال أمن المعلومات، وبالتالي

(1) Tofan, Dan, (2011), "Information Security Standards", *OP. Cit.*, PP: 128-135.

(2) Siponen, Mikko & Willison, Robert, (2009), "Information Security Management Standards: Problems and Solutions", *Information & Management*, Vol.46, No.5, PP: 267-270.

(3) خليل، عطا الله ورّاد، (2011)، " آليات أمن المعلومات في ظل الانفتاح المعلوماتي "، *مجلة الفكر القانوني والاقتصادي*، العدد 4، يوليو 2011، كلية الحقوق، جامعة بنها، مصر، ص ص: 589 – 641.

(4) Tofan, Dan, (2011), "Information Security Standards", *OP. Cit.*, PP: 128-135.

(5) ISO/IEC 27000, (2012), "Information technology - Security techniques - Information security management systems - Overview and vocabulary", *OP. Cit.*, Available at: <http://www.27000.org> (Accessed July 14, 2013).

- تثقيف وتدريب المسؤولين عن النظم على إدارة شاملة لمخاطر أمن نظم المعلومات، وتوفير المبادئ والمفاهيم الرئيسية، كعلة مشتركة، واضحة التوجيه والإرشاد، أصبح أكثر إلحاحاً.⁽¹⁾
2. **وسيلة مثلى لمتابعة تنفيذ الضوابط الرقابية:** تساعد المعايير أي منشأة في التحكم ومراقبة الأنشطة والمهام الخاصة بأمن المعلومات فيها والتأكد من أنها في مستوى متميز مقارنة بمثيلاتها من المنشآت، خاصة إذا جاء الحكم عن طريق طرف ثالث وهو المنظمة المسؤولة عن المعيار مما يعطي رأياً محايداً للمنشأة ومقبولاً من جميع الأطراف، فمن أجل تنفيذ الضوابط الأمنية المعلومات لتلبية متطلبات المنشآت فضلاً عن مجموعة من الضوابط للعلاقات التجارية مع المنظمات الأخرى فالطريقة الأكثر فعالية للقيام بذلك هو أن يكون هناك معيار مشترك بشأن أفضل الممارسات لأمن وإدارة نظم المعلومات (مثل *ISO / IEC 17799:2005*) وبالتالي يمكن للمنشآت الاستفادة من أفضل الممارسات الشائعة على مستوى دولي، لحماية عملياتها وأنشطتها الخاصة باحتياجات العمل.⁽²⁾
3. **أفضل الممارسات:** تم تطوير هذه المعايير بناء على تجارب وخبرات المئات من الأفراد والمنظمات وبالتالي فإن هذه المعايير تحتوي على مجموعة كبيرة جداً من أفضل الممارسات الموجودة في مجال أمن نظم المعلومات، ولا يمكن مقارنتها بجهود وخبرات منشأة واحدة بل إن دمجها مع ممارسات هذه المنشأة سيؤدي حتماً إلى مستوى أفضل في هذا المجال، وكذلك استكشاف الأطر القائمة المستخدمة في إدارة المخاطر، والهدف من ذلك يتمثل في توفير معايير الاختيار للحصول على أفضل معيار أو اقتراح إجراء أفضل نهج للتقييم.⁽³⁾
4. **وضوح الهيكلية:** وفرت المعايير عادةً نموذجاً واضحاً يجعل تبنيه يعطينا صورة واضحة عن الهيكلية الإدارية والتنظيمية التي يمكن للمنشأة إتباعها، وهذا يجعل المنشأة تعرف المسئول عن كل مهمة من مهام أمن نظم المعلومات.
5. **توفير الوقت:** نظراً للأهمية الكبرى لعامل الزمن في هذا العصر التنافسي لم تعد المنشآت بحاجة إلى إنشاء وتطوير خطة أو نموذج خاص بالمنشأة تستغرق وقتاً طويلاً وبناء على خبرات محدودة فقط في حين أن هناك معيار موجود ومعترف به دولياً وتم تطويره عن طريق خبرات مشتركة.
6. **تعزيز الثقة لدى الأطراف ذات العلاقة بالمنشأة:** توفير لغة مشتركة وأساس مفاهيمي متوافق ومتكامل لأمن نظم المعلومات المحاسبية على نطاق واسع، يسهل ويعزز الثقة في المنشأة ونظمها لدى الشركاء التجاريين، لا سيما إذا تطلب الأمر شهادات معتمدة من قبل هيئة دولية معينة كالمنظمة الدولية للمعايير مثلاً، كما أن ذلك يؤدي إلى زيادة في ثقة أصحاب المصلحة في المنشأة؛ وتلبية احتياجاتهم وتوقعاتهم.
7. **تصميم وتنفيذ الأنظمة والحلول التي تتلاءم مع التخفيف المطلوب من آثار المخاطر.**
8. **مراجعة المخاطر والأنظمة والحلول والسياسات والإجراءات والعمليات** في ظل المخاطر الجديدة والتقنيات الحديثة والأحداث ومراحل تطوير الأنظمة المعتادة.

ومن منظور المنشآت التجارية، فإن أهم دور للأسس هو أنها تكمل وتتكامل مع السلسلة الحالية للأعمال والأساليب والسياسات التجارية في مجال أمن تكنولوجيا الاتصالات والمعلومات، وتستطيع الأسس عن طريق توفير مجموعة رئيسية من المبادئ العامة أن تربط إطار عمل المنشآت التجارية الحالي بإطار اجتماعي أكبر، كما أنها ترتبط بالأطر

(1) The Committee of Sponsoring Organizations Tread-way Commission (COSO), (2004), *Enterprise Risk Management-Integrated Framework: Executive Summary*, AICPA, New York, USA, September 2004, PP: 1-7, <http://www.coso.org/IC-Integrated-Framework-summary.htm>

(2) Tofan, Dan, (2011), "Information Security Standards", *OP. Cit.*, PP: 128-135.

(3) Al-Ahmad, Walid & Mohammad, Bassil, (2013), "Addressing Information Security Risks by Adopting Standards", *OP. Cit.*, PP: 28-43.

القانونية والتنظيمية الصارمة بشكل متزايد والتي تدار وفقاً لها المنشآت التجارية عالمياً، وتتطلب تلك الأطر ومنها إطار العمل على مراقبة مخاطر العمليات في القطاع المالي الصادرة عن بنك التسويات العالمية (بازل2) بصورة متزايدة أن تضطلع المؤسسات التجارية بعملياتها بأسلوب إدارة أمن.⁽¹⁾

من هنا يرى الباحث بأن الأغراض العامة لتوجيهات ومعايير أمن المعلومات التي تشكل وتطبق من قبل الأجهزة والمنظمات المعنية بالتوحيد القياسي والمعايرة هو مساعدة عمليات التطوير اللاحقة لنظم المعلومات واستخدامها. وبذلك ينظر إلى هذه الأطر المنظمة والحاكمة كضرورة لا بد منها لزيادة الوعي بالمخاطر التي تواجه نظم المعلومات وإعادة تأكيد مدى مصداقيتها وجودتها، كما تتطلب من المنشآت والمصالح المختلفة التنسيق فيما بينها لخلق إطار شامل لأمن نظم المعلومات. كما تهدف التوجيهات والمعايير إلى زيادة الوعي بأهمية أمن نظم المعلومات، ومقاومة الاختراقات التي تواجهها من الداخل والخارج، وتجميع إحصائيات تخص أمن المعلومات بالمنشأة المعنية، وعلى هذا الأساس، ينظر إلى أغراض توجيهات ومعايير أمن المعلومات، على أنها تحقق التالي:⁽²⁾

1. زيادة الوعي بالمخاطر التي تواجه نظم المعلومات وبطرق التأمين المتوفرة للتغلب على هذه المخاطر.
2. إنشاء إطار عام لمساعدة أولئك المسؤولين في المنظمات والهيئات العامة والخاصة لتطوير وتنفيذ مقاييس وإجراءات ومزاوالت متناسقة مع أمن المعلومات ونظمها.
3. دعم التعاون بين القطاعات والمنشآت المختلفة في تطوير وتنفيذ هذه المقاييس والإجراءات والمزاوالت.
4. رعاية الثقة فيما يتصل بنظم المعلومات وبالطريقة التي تقدم بها للمستخدمين.
5. تسهيل تطوير واستخدام نظم المعلومات على كافة المستويات القطاعية، الوطنية والدولية.
6. دعم التعاون الدولي في تحقيق أمن نظم المعلومات.

3-1-2: الإطار المستند إلى أهداف الرقابة على المعلومات والتكنولوجيا ذات الصلة (COBIT):

وهو يقابل سلسلة من المبادئ التوجيهية والمبادئ التي تعمل على بدء وتنفيذ وصيانة وتحسين إدارة تكنولوجيا المعلومات في المنشآت،⁽³⁾ تم تأسيس وبناء وتطوير أهداف الرقابة على المعلومات والتكنولوجيا ذات الصلة (COBIT) عام 1992م من قبل معهد حوكمة تكنولوجيا المعلومات (ITGI) والذي يعمل على النهوض والتفكير بالمعايير الدولية في توجيه ومراقبة تكنولوجيا المعلومات للمنشآت، وهو معهد تابع لجمعية التدقيق والرقابة على نظم المعلومات (ISACA)، وهي جمعية رائدة عالمياً في مجال تكنولوجيا المعلومات تأسست عام 1969م وتضم حتى عام 2011م أكثر من (86000) عضو في أكثر من 160 دولة، معظمهم من الخبراء من الصناعة، والأوساط الأكاديمية والحكومية، وأمن وحوكمة تكنولوجيا المعلومات، ضمن 200 جمعية تابعة للجمعية الأم، وتقوم برعاية

(1) Organization For Economic Co-Operation And Development (OECD), (2002), "OECD Guidelines for the Security of Information Systems and Network: Towards a Culture of Security". The Council of the OECD, Paris, France, 25 July 2002, PP:1-30, Retrieved 22 April 2013, at <http://www.oecd.org/dataoecd/16/22/15582260.pdf>

(2) هوارى، معراج & عبيرات، مقدم "إدارة مخاطر الأمن وشفافية المعلومات لنظم المعلومات في ظل البيئة الرقمية"، كلية الاقتصاد وعلوم التسيير، جامعة الأغواط، من الموقع: <http://www.docstoc.com/docs/145138300>

(3) Gehrman, Maico, (2012), "Combining ITIL, COBIT and ISO/IEC 27002 for Structuring Comprehensive Information Technology for Management in Organizations", *Navus - Revista de Gestão e Tecnologia, Florianópolis, SC, Vol. 2, No. 2, Jul. 2012, PP: 66 – 77.*
& Information Systems Audit and Control Association (ISACA), (2012), *COBIT 5 for Information Security - Preview Version*, , Printed in the United States of America, USA, <http://www.isaca.org/cobit5info-sec>

النشاطات البحثية في أمن المعلومات وحوكمة النظم وتدقيقها، والسيطرة على مخاطرها، وتمنح شهادة مدير أمن معلومات معتمد (CISM) وشهادة مدقق نظم معلومات معتمد (CISA).⁽¹⁾

أهداف رقابة تكنولوجيا المعلومات ذات الصلة (COBIT) هو إطار عمل مفتوح يطبق بشكل عام للسيطرة على أمن ورقابة نظم التحكم في تكنولوجيا المعلومات، وهو مقبول عموماً من قبل مهنة المحاسبة، و يسمح بإدارة وقياس ممارسات الأمن و السيطرة على بيئة تكنولوجيا المعلومات،⁽²⁾ حيث يتمثل الهدف الأساسي من هذا الإطار في وضع معايير دولية للأساليب والوسائل الجيدة لحماية أمن العمليات المتعلقة بتكنولوجيا المعلومات وتكون قابلة للتطبيق ومقبولة قبولاً عاماً،⁽³⁾ فهو يبحث في تطوير ونشر وتعزيز موثوقة ما يصل للوقت الحاضر من مجموعة دولية من أهداف الرقابة لتكنولوجيا المعلومات المقبولة عموماً لاستخدامها يوماً بعد يوم.⁽⁴⁾

وهو تطور استراتيجي كبير كإطار عمل من أجل حوكمة وإدارة تكنولوجيا المعلومات للمنشأة، ويأتي كاستجابة للحاجة لوضع إطار مرجعي للسيطرة الأمنية في مجال تكنولوجيا المعلومات، من خلال مجموعة إرشادات لمساعدة محترفي أمن تكنولوجيا المعلومات في فهم واستخدام وتنفيذ وتوجيه المعلومات الهامة والأنشطة المتصلة بالأمن واتخاذ قرارات أكثر استنارة حيث يشتمل على أحدث الأفكار في مجال حوكمة المنشآت وإدارة التقنيات ويوفر المبادئ والممارسات المقبولة عالمياً والأدوات والنماذج التحليلية للمساعدة في زيادة الثقة في نظم المعلومات.⁽⁵⁾

وهذا الإطار يوائم بين الموارد وعمليات تكنولوجيا المعلومات مع أهداف الأعمال، وفق متطلبات الجودة والأمن والائتمان، حيث يركز على ثلاثة أبعاد هي الأهداف والموارد والعمليات (أهداف المنشأة، وموارد تكنولوجيا المعلومات، وعمليات تكنولوجيا المعلومات)، فهو إطار نظري معياري للسيطرة على موارد تكنولوجيا المعلومات تم تصميمه كإطار وفق سلسلة من الضوابط اللازمة التي تساعد على تلبية متطلبات فعالية وكفاءة، وسرية ونزاهة وتوافر، وامتثال وموثوقية المعلومات، من خلال مجموعة من الأهداف والمبادئ التوجيهية الدولية تستخدم لحوكمة تكنولوجيا المعلومات، وكذلك تتيح للمدراء سد الفجوة بين متطلبات الرقابة والقضايا التقنية والمخاطر التجارية، فهو يركز على مخاطر محددة حول أمن تكنولوجيا المعلومات بطريقة بسيطة.⁽⁶⁾

وقد نشرت الطبعة الأولى من إطار COBIT في عام 1996، والطبعة الثانية في عام 1998، والثالثة طبعة عام 2000، والطبعة الرابعة عام 2005،⁽⁷⁾ وآخر تحديث لذلك الإطار حتى الآن يتمثل في الطبعة الخامسة والتي صدرت صدرت في 21 نوفمبر 2013م.

وهي الخطوط العريضة لمنهجية وظيفة أمن المعلومات ويعتمد على كل من البحث وتجربة العالم الحقيقي، ويتكون من بيان المبادئ والأهداف واسعة النطاق كما تشمل على المعايير وهي توصيات للتنفيذ، من أجل الحفاظ على أمن المعلومات ويتم مراجعة المعيار وتحديثه كل سنتين، بالإضافة إلى مستوى الممارسة الجيدة، وقوى الأمن

(1) Tofan, Dan, (2011), "Information Security Standards", *OP. Cit.*, PP: 128-135.

(2) Abu-Khadra, Husam & Chan, Joseph & Pavelka, Deborah, (2012), "Incorporating the COBIT Framework for IT Governance in Accounting Education", *Communications of the IIMA*, Vol.12, No. 2, 2012, PP: 81-92.

(3) الطنملي، سهير، (2009)، "دور الرقابة الداخلية في دعم و تفعيل أمن و سلامة المعلومات في البنوك الالكترونية والخلوية: الجزء الأول"، *مرجع سابق*، ص ص: 27-48.

(4) Bagranof, Nancy A. & Simkin, Mark G. & Norman, Carolyn S. (2010), *Accounting Information System*, *OP. Cit.*, P. 356.

(5) American Institute of Certified Public Accountants & Canadian Institute of Chartered Accountants, (AICPA), (2012), *COBIT 5 for Information Security - Preview Version*, . Printed in the United States of America, USA, <http://www.isaca.org/cobit5info-sec>

(6) Al-Zwyalif, Inaam M., "IT Governance and its Impact on the Usefulness of Accounting Information Reported in Financial Statements", *International Journal of Business and Social Science*, Vol. 4, No. 2, February 2013, PP: 83-94.

(7) Abu-Musa, Ahmad A., (2009), "Exploring COBIT Processes for ITG in Saudi Organizations: An empirical Study", *OP. Cit.*, PP: 99-126.

الداخلي أيضا تشرف على برنامج القياس نصف سنوية والتي تعرف باسم مسح حالة أمن المعلومات، ويتم فحص المنشآت المشاركة على فعالية نظم الأمن و يتم قياس النتائج مع بعضها البعض،⁽¹⁾ وكل هذا من العوامل الأساسية التي تعمل على تحسين عمليات المنشآت وإدارة الموارد وتحسين عائد الاستثمار وكفاءة إدارة المخاطر والحد من المخاطر الكبيرة.⁽²⁾

■ **مكونات إطار (COBIT):** يشتمل هذا الإطار عموماً على المعايير الدولية المعمول بها و المقبولة للممارسة الجيدة في إدارة تكنولوجيا المعلومات والسيطرة عليها،⁽³⁾ وقد تألفت كوبيت (COBIT) من ثلاث مجموعات رئيسية هي: أهداف العمل، وموارد تكنولوجيا المعلومات، و العمليات القائمة على تكنولوجيا المعلومات،⁽⁴⁾ وفيما يأتي أبرز مكونات هذا الإطار المختص بأمن المعلومات في بيئة تستخدم تكنولوجيا المعلومات وهي:

أولاً: المتطلبات الأساسية ومعايير المعلومات: لتنفيذ أهداف المنشأة، يجب أن تتوفر بالمعلومات المتطلبات الأساسية وهي الجودة ومسؤولية الأمن والموثوقية، وأن تتوافق خصائصها مع معايير رقابية معينة وهي معايير دولية تتعلق بخصائص المعلومات، وتتمثل فيما يلي:⁽⁵⁾

- **متطلبات الجودة:**

1. **الفعالية (Effectiveness):** تتعلق بكونها وثيقة الصلة بأهداف العملية التجارية وذلك بأن تكون المعلومات ملائمة وموثوقة ومرتبطة بتحقيق أهداف المنشأة، بتلبيتها للتوقعات.

2. **الكفاءة (Efficiency):** أن يتم تجهيز المعلومات وتقديمها في ضوء أفضل استخدام ممكن للموارد.

- **متطلبات الأمن:**

3. **السرية (Confidentiality):** بواعث قلق تتعلق بحماية المعلومات الحساسة من الكشف غير المصرح به لغير المخولين بذلك.

4. **السلامة والكمال (Integrity):** أن تكون المعلومات صحيحة ودقيقة وشاملة، وفقاً لقيمة الأعمال والتوقعات.

5. **التوافر أو الإتاحة (Availability):** أن تكون المعلومات متاحة عند الحاجة إليها من الأطراف المختلفة حاضراً ومستقبلاً، ويتعلق الأمر أيضاً بالحفاظ على الموارد اللازمة والقدرات المرتبطة بها.

- **متطلبات الثقة:**

6. **الامتثال (Compliance):** الالتزام بالسياسات الداخلية والقوانين واللوائح والتعليمات، وكذلك الالتزام بالترتيبات التعاقدية المرتبطة بالنشاط، وأي معايير عمل مفروضة من الخارج.

7. **الموثوقية (Reliability):** تتصل بتزويد الإدارة بالمعلومات الموثوق بها، واللازمة لممارستها لمسؤولياتها.

(1) Tofan, Dan, (2011), "Information Security Standards", **OP. Cit**, PP: 128-135.

(2) Orakzai, T. (2014). **COBIT, ITIL and ISO 27002 Alignment for Information Security Governance in Modern Organisations**. Electronic copy available at: <http://ssrn.com/abstract=2385845>

(3) Abu-Musa, Ahmad A., (2010), "Investigating Adequacy of Security Controls in Saudi Banking Sector: An Empirical Study", **OP. Cit**, PP: 1-41.

(4) Mansour, Ebrahim et. al., (2009), "Examine the Existence of (Sys Trust) Model and its Impact on Jordanian Commercial Banks Performance", **European And Mediterranean Conference On Information Systems**, 13~14 July 2009, Crown Plaza Hotel, Izmir, Turkey.

(5) Tuttle, Brad & Vandervelde, Scott D., (2007), "An Empirical Examination of Cobit As An Internal Control Framework for Information Technology", **International Journal of Accounting Information Systems**, Vol.8, PP: 240-263.

ثانياً: موارد تكنولوجيا المعلومات: أشار الإطار العام لكوبت إلى موارد تكنولوجيا المعلومات المتمثلة في: النظم المحوسبة اللازمة لتجهيز البيانات والمعلومات من خلال نظم التشغيل وإدارة قاعدة البيانات والشبكات والبيئة التي تساعد على تشغيل التطبيقات، والكوادر البشرية اللازمة لعمليات التخطيط والتنفيذ وتقديم الخدمات والدعم والمتابعة والتقييم.⁽¹⁾

ثالثاً: عمليات تكنولوجيا المعلومات (Information Technology Process): من أجل السيطرة على تكنولوجيا المعلومات وفقاً لإطار COBIT تم تحديد مجموعة مكونة من 34 هدف رقابي، حيث يختص كل هدف منها بعملية من العمليات رفيعة المستوى والتي تم تصنيفها ضمن أربعة مجالات وهي التخطيط والتنظيم، الحيازة والتنفيذ، التسليم والدعم، والرصد، كما يلي:

1. **التخطيط والتنظيم (Planning & Organization):** ويتكون هذا المستوى من أحد عشر هدفاً فرعياً للرقابة بحيث يشمل مجاًلاً واسعاً من التخطيط الاستراتيجي لتكنولوجيا المعلومات وتكوين هندسة ومعمارية المعلومات المتعلقة بالمنشأة، إلى إدارة مشاريع معينه مثل إدارة استثمارات تكنولوجيا المعلومات، وإدارة الموارد البشرية وتقدير المخاطر وإدارة الجودة، كما يسلط الضوء على الشكل التنظيمي والبنية التحتية لتكنولوجيا المعلومات هو أن تأخذ من أجل تحقيق أفضل النتائج وتوليد أكبر قدر من الفائدة من استخدام تكنولوجيا المعلومات.⁽²⁾
2. **الحيازة والتنفيذ (Acquisition and implementation):** بعد التخطيط فإن المنشأة تحتاج للحصول على نظم المعلومات وتنفيذها، وهذا المستوى يتكون من ستة أهداف للرقابة مثل إدارة التغيير، وتصميم واختيار النظم وتطوير ومراقبة الإجراءات والحصول على تكنولوجيا البنية التحتية للمنشأة، كما يتناول هذا المجال أيضاً وضع خطة الصيانة التي ينبغي أن تعتمد عليها المنشأة من أجل إطالة عمر نظام تكنولوجيا المعلومات ومكوناته، واستمرارية العمل.⁽³⁾
3. **الاستلام والدعم (Delivery and Support):** تمتاز مشاريع تكنولوجيا المعلومات بأنها تظهر للعيان بعد تنفيذها وهذا المستوى له ثلاثة عشر هدفاً للرقابة ومنها إدارة العمليات، إدارة التسهيلات المقدمة للعمليات، إدارة البيانات، إدارة المشاكل والحوادث، خدمات الدعم للمستخدمين، وإدارة الأمن والاستمرارية وإدارة البيانات والمرافق التشغيلية، وتشمل هذه العمليات دعم القضايا الأمنية والتدريب، وغيرها.⁽⁴⁾
4. **الرصد والتقييم (Monitoring & Evaluation):** وهذا يعني أنه يجب على المنشآت أن تراقب عملياتها وتضمن مستوى معقول من الرقابة الداخلية وتحصل على ضمانات مناسبة بأداء مهامها، كما أنه يجب إجراء تقييم مستقل لمدى فعالية نظام تكنولوجيا المعلومات في قدرتها على تلبية الأهداف التي صممت من أجلها.⁽⁵⁾

وفي كل مجال من المجالات الأربعة هناك عمليات محددة ينبغي أن تتصدى لها المنشأة لتحقيق أهداف الرقابة ذات الصلة مفصلة ومحددة، من خلال تنفيذ أفضل الممارسات التي يجب الوفاء بها من أجل تحقيق مستوى عال من السيطرة، حيث يوفر COBIT المبادئ التوجيهية لرقابة واسعة رفيعة المستوى لكل عملية من عمليات تكنولوجيا

(1) حجر، عبد الملك إسماعيل، (2009)، نظم المعلومات المحاسبية، مرجع سابق، ص 391.

(2) Tofan, Dan, (2011), "Information Security Standards", OP. Cit., PP: 128-135.

(3) Abu-Musa, Ahmad A., (2009), " Exploring COBIT Processes for ITG in Saudi Organizations: An empirical Study", OP. Cit., PP: 99-126.

(4) Information Systems Audit and Control Association (ISACA), (2012), COBIT 5 for Information Security - Preview Version, , Printed in the United States of America, USA, <http://www.isaca.org/cobit5info-sec>

(5) *Ibid.*, <http://www.isaca.org/cobit5info-sec>

المعلومات. (34 هدف رقابي، و318 مبدأ توجيهي)، والتي تحتوي على السياسات، والإجراءات والممارسات والمسؤوليات التنظيمية والمبادئ التوجيهية لتدقيق الحسابات ربطت مع الأهداف الرقابية، ومنها كشف الانتهاكات الأمنية الهامة وتسجيلها، وضمان أن يتم الإبلاغ عنها فوراً والتصرف حيالها في الوقت المناسب، على سبيل المثال لضمان أمن نظم المعلومات يحدد متطلبات العمل التي يمكنها من الوصول إلى نظم المعلومات والبرامج والبيانات وإمكانية السيطرة عليها مع أنشطة تكنولوجيا المعلومات محددة مثل استخدام الجدران النارية، والتشفير، و أدوات المصادقة.

وكل عملية من عمليات المنشأة وتقنية المعلومات الخاصة بها يجب أن تركز على واحدة أو أكثر من الصفات السبع للمعلومات والتي تستخدم هنا كمعايير، وترتبط كل عملية مع واحد أو أكثر من خمسة موارد تكنولوجيا المعلومات التالية وهي: الأفراد، والمعطيات، والنظم التطبيقية، والتكنولوجيا، والمرافق.

2-1-4: المبادئ العامة لأمن المعلومات الصادرة عن منظمة التعاون الاقتصادي والتنمية (OECD):

في 25 من تموز (يوليو) 2002م⁽¹⁾ اعتمدت لجنة تكنولوجيا المعلومات والاتصالات التابعة لمنظمة التعاون الاقتصادي والتنمية (OECD) التي يقع مقرها في باريس بفرنسا، أسس ومبادئ لأمن الشبكات ونظم المعلومات - نحو ثقافة أمنية، وتلك الأسس والمبادئ هي توجيهات إرشادية غير إلزامية، ولكن يجب أن يتم مراعاتها عند تصميم وإعداد توجيهات ومعايير أمن المعلومات، وتتكون من تسعة مبادئ تضم إطار عمل يتعلق بمسائل الأمن، وكان أسلوب التعبير عن المبادئ موجزاً لتيسير فهمها لكل المشاركين، وتوضيح أهميتها ولتكيف قابليتها للتطبيق في مجتمع الأعمال.⁽²⁾

أهداف هذه المبادئ التوجيهية: تلقى المبادئ الأساسية الضوء على ضرورة الوعي بالمخاطر، والحاجة لاتخاذ إجراءات إيجابية فيما يتصل بتلك المخاطر، والحاجة لتنفيذ تلك الإجراءات في الوقت المناسب، وتتناول المبادئ الاجتماعية مسائل ذات صلة بالسلوك والعدل والانفتاح والشفافية والقيم، والأربعة مبادئ الأخيرة قابلة للتنفيذ بطبيعتها بشكل أكبر، وتتناول مراحل الأمن، وتهدف هذه المبادئ إلى تحقيق ما يلي:⁽³⁾

1. رفع الوعي حول المخاطر التي تتعرض لها نظم المعلومات، بتحديد وتقييم تلك المخاطر، وتشجيع ثقافة الأمن كوسيلة لحماية أمن نظم المعلومات للتغلب على تلك المخاطر.
2. إنشاء إطار عام يساعد على فهم طبيعة المخاطر المتعلقة بالأمن واحترام القيم الأخلاقية في تطوير وتنفيذ السياسات المتناسقة والممارسات والتدابير والإجراءات المتناسقة لمعالجة مخاطر أمن نظم المعلومات.
3. تشجيع وتعزيز التعاون الدولي بين القطاعات والمنشآت المختلفة على المشاركة في تبادل المعلومات ذات الصلة بوضع وتنفيذ ذلك الإطار (تطوير وتنفيذ الضوابط والإجراءات)، باعتبار الأمن هدف للجميع.
4. تعزيز الثقة في نظم المعلومات لدى مستخدميها على كافة المستويات القطاعية، القومية والدولية.

(1) * تم إعداد هذه المبادئ لأول مرة عام 1992م، وتم تنقيحها في عام 1997م، وتسارعت الجهود عقب 11 أيلول (سبتمبر) 2001 م، لتصدر بشكلها النهائي في تموز (يوليو) 2002م.

(2) Organization For Economic Co-Operation And Development (OECD), (2002), "OECD Guidelines for the Security of Information Systems and Network: Towards a Culture of Security", OP.Cit., PP:1-30, Retrieved 22 April 2013, at <http://www.oecd.org/dataoecd/16/22/15582260.pdf>

(3) Ibid, PP:1-30, Retrieved 22 April 2013, at <http://www.oecd.org/dataoecd/16/22/15582260.pdf>

مكونات أطار المبادئ العامة التوجيهية لأمن المعلومات الصادرة عن منظمة التعاون الاقتصادي والتنمية:

تنقسم الأسس والمبادئ التسعة إلى ثلاث فئات رئيسية هي الأولى المبادئ الأساسية (1-3) وتتمثل في الوعي والمسؤولية والاستجابة، والثانية المبادئ الاجتماعية (4-5) وتتمثل في الأخلاق والديمقراطية، والثالثة مبادئ مراحل الأمن (6-9) وتعلق بتقييم المخاطر، وتنفيذ وتصميم الأمن، وإدارة الأمن، وإعادة التقييم، يتم مناقشتها بإيجاز كما يلي: (1)

المبدأ (1) الوعي (Awareness): "يجب أن يكون أصحاب المصلحة على بينة من الحاجة لضمان سلامة الأنظمة والشبكات واتخاذ ما بوسعهم المتخذة لتعزيز الأمن".

فالوعي بالمخاطر والضمانات المتاحة هو خط الدفاع الأول لأمن نظم وشبكات المعلومات. ويقصد بهذا المبدأ مساعدة الأفراد المهتمين قانونياً بنظم الأمن على التعلم والتعرف عن أمن نظام المعلومات، بسبب الترابط والاعتماد المتبادل لأصحاب المصلحة، فالمستخدم النهائي أو العميل الذي يختار بنك معين، قد يكون له اهتمام شرعي في معرفة سياسات الأمن لهذا البنك والبنوك الأخرى، واعتماداً على سياسات الأمن المستخدمة تسوق وتروج الخدمات المصرفية كأداة لجذب العملاء، وحتى يمكن اكتساب الثقة في نظام المعلومات، يجب أن يكون الملاك ومقدمو ومستخدمو النظام قادرين وجاهزين في التوعية عن أمن المعلومات، كما يجب عليهم أيضاً أن يكونوا متضمنين في حفظ وصيانة الأمن. وبذلك يصبح مبدأ التوعية هاماً في اكتساب المعرفة الملائمة والتعرف على تواجد مزاوالات وإجراءات لأمن النظام.

المبدأ (2) المسؤولية (Responsibility): "جميع أصحاب المصلحة هم مسؤولين عن أمن نظم وشبكات المعلومات"، فأصحاب المصلحة التي تعتمد على نظم المعلومات المرتبطة بها محلياً وعالمياً (من يمتلكها ومن يقدموها ومن يستخدمها وكل الأطراف الأخرى المرتبطة والمهتمة بها) هم مسؤولين عن أمن نظم المعلومات وبشكل فردي كلاً فيما يخصه، ويجب عليهم بانتظام تقييم السياسات والممارسات والتدابير والإجراءات للتأكد من أنها صالحة للبيئة.

وهذا المبدأ يتفق مع ما دعت إليه لجنة بازل للرقابة المصرفية بضرورة تحديد الإدارة العليا إطاراً لإدارة مخاطر العمليات وأن تتحمل الإدارة العليا المسؤولية عن ذلك إطار.

المبدأ (3) الاستجابة (Response): ينبغي لأصحاب المصلحة التصرف على وجه السرعة وفي الوقت المناسب وبروح من التعاون لمنع وكشف والرد على حدوث المخاطر الأمنية.

إدراكاً لترابط نظم المعلومات والشبكات واحتمال حدوث ضرر سريع وعلى نطاق واسع، فينبغي لأصحاب المصلحة التصرف على وجه السرعة وبروح من التعاون لمعالجة المخاطر الأمنية، ينبغي التعاون والمشاركة في المعلومات حول التهديدات ونقاط الضعف ووضع إجراءات للتعاون السريع والفعال لمنع وكشف الحوادث الأمنية والاستجابة، كلما كان ذلك ممكناً وهذا قد ينطوي على تبادل المعلومات والتعاون عبر الحدود.

وهذا المبدأ يتفق مع ما دعت إليه لجنة بازل للرقابة المصرفية بضرورة وجود خطط استمرارية المنشآت التجارية وخطط جاهزة للطوارئ.

(1) Ibid, PP:1-30, Retrieved 22 April 2013, at <http://www.oecd.org/dataoecd/16/22/15582260.pdf>

المبدأ (4) الأخلاق (Ethics): وينص على أنه "ينبغي لأصحاب المصلحة احترام المصالح المشروعة للأطراف الأخرى"، فنظم المعلومات منتشرة في مجتمعاتنا وأصحاب المصلحة يجب أن يكونوا على بينة من الضرر الذي يمكن أن يتسبب للآخرين من خلال تراخي السلوك الأخلاقي لذلك ينبغي لأصحاب المصلحة تطوير وتبني أفضل الممارسات الأمنية التي تعزز السلوك الذي يحترم المصالح والحقوق الشرعية للآخرين مع مراعاة المتطلبات الأمنية. وهذا المبدأ يتفق مع ما دعت إليه لجنة بازل للرقابة المصرفية بضرورة الإفصاح العلني بشكل كاف للسماح بتقييم آليات مراقبة مخاطر العمليات.

المبدأ (5) الديمقراطية (Democracy): "يجب أن يكون أمن النظم متوافق مع القيم الأساسية للمجتمع الديمقراطي"، يجب ضمان السلامة وفقاً لقيم معترف بها من قبل المجتمعات الديمقراطية، بما في ذلك حرية تبادل الأفكار والتدفق الحر للمعلومات، وسرية المعلومات والاتصالات، وتوفير الحماية الكافية للمعلومات ذات الطابع الشخصي، والانفتاح والشفافية.

حيث تقاس متطلبات أمن نظم المعلومات في مواجهة الاهتمامات الشرعية لكل الأطراف المعنية من مطورين ومشغلين ومستخدمين يرتبطون باستخدام المعلومات وتدفعها بهدف الوصول للتوازن طبقاً للمجتمع الديمقراطي، وقد يفترض البعض بأن ذلك قد يؤدي إلى قيود في الوصول للبيانات والمعلومات وفي تدفقها وحركتها علماً أنه علي العكس، فالأمن يعزز الوصول للمعلومات وتدفعها من خلال توفير نظاماً أكثر دقة وموثوقية وتوافراً، علي سبيل المثال، يساعد انسجام وتوافق توجيهات ومعايير الأمن الفنية في منع تكاثر النظم المتفرقة غير المترابطة معاً، وبذلك توجد ضرورة في توافق أمن نظم المعلومات من حيث استخدامها وتدفعه بعدالة وتوازن في المجتمع الديمقراطي.

وهذا المبدأ يتفق مع ما دعت إليه لجنة بازل للرقابة المصرفية بضرورة تقييم الأساليب والإجراءات والسياسات التي تتصل بمخاطر العمليات من طرف خارجي مستقل، والإفصاح العلني بشكل كاف للسماح بتقييم آليات مراقبة مخاطر العمليات.

المبدأ (6) تقييم المخاطر (Risk Assessment): "يجب على أصحاب المصلحة إجراء تقييمات للمخاطر"، حيث يساعد تقييم المخاطر تحديد التهديدات ونقاط الضعف، ويجب تغطية واسعة وكافية لكل من العوامل الرئيسية الداخلية والخارجية، مثل التكنولوجيا والمكونات المادية والعوامل البشرية، والسياسات، ويعمل ذلك التقييم على تحديد مستوى المخاطر المقبولة ويسهل اختيار الإجراءات الرقابية المناسبة لإدارة المخاطر من الأضرار المحتملة لنظم المعلومات، ويجب أن يأخذ تقييم المخاطر في الاعتبار الضرر على الآخرين أو الناجم من الآخرين بفضل الترابط المتزايد في نظم المعلومات.

وهذا المبدأ يتفق مع ما دعت إليه لجنة بازل للرقابة المصرفية بضرورة تقييم مخاطر العمليات لكل الأنظمة الجديدة.

المبدأ (7) تنفيذ وتصميم الأمن (Security Design and Implementation): ينبغي دمج الأمن باعتباره عنصراً أساسياً من نظم المعلومات، فالأمن عنصراً أساسياً وجزءاً لا يتجزأ من تصميم النظام، وتحتاج الأنظمة والسياسات أن تصمم بشكل صحيح، وتنفذ بشكل متناسق لتحسين الأمن، من خلال تصميم واعتماد الضمانات المناسبة والحلول المناسبة لتجنب أو الحد من الأضرار المحتملة من التهديدات ونقاط الضعف.

وكلا الضوابط التقنية وغير التقنية مطلوبة ويجب أن تكون متناسبة مع قيمة موارد النظم المحمية، حيث تختلف هرمية نظم المعلومات وحاجاتها الأمنية من قطاع لآخر ومن منشأة لأخرى، أي لا يوجد حل واحد لمشكلات وقضايا

الأمن المختلفة والمتعددة، وبالتالي يجب مراعاة التصميم المناسب حيث لا يتطلب كل نظام معلومات أقصى درجة من الأمن، كما أنه من المهم ألا تكون النظم آمنة بدرجة غير كافية، أي أنه من غير الجدوى أن تتعدى إجراءات الأمن المتطلبات المعقولة للنظام.⁽¹⁾

وهذا المبدأ يتفق مع ما دعت إليه لجنة بازل للرقابة المصرفية بضرورة أن تتحمل الإدارة العليا المسؤولية عن إطار مخاطر العمليات.

المبدأ (8) إدارة الأمن (Security Management): ينبغي أن تقوم إدارة الأمن على تقييم المخاطر بشكل ديناميكي وشامل لتغطية جميع مستويات أنشطة المنشأة وجميع جوانب عملياتها، وينبغي أن تشمل، مسبقاً استراتيجيات لمنع المخاطر الناشئة والكشف أو التخفيف منها، والصيانة المستمرة، والمتابعة والتدقيق.

أمن نظم المعلومات يكون ذا فاعلية وكفاءة عند تصميم النظام ذاته، ويختص مبدأ التكامل (Integration) بالضوابط والإجراءات الخاصة بأمن المعلومات التي يجب أن تكون متناسقة ومتكاملة مع بعضها ومع غيرها من الأبعاد الأخرى في المنشأة لإيجاد نظام أمن معلومات متناسق ومتكامل.

وهذا المبدأ يتفق مع ما دعت إليه لجنة بازل للرقابة المصرفية بضرورة إجراء عمليات المراجعة الداخلية على إطار إدارة مخاطر العمليات، ويجب توافر إطار لتحديد وتقييم ومراقبة والتحكم في المخاطر المادية للعمليات.

المبدأ (9) إعادة التقييم (Reassessment): "ينبغي مراجعة وإعادة تقييم أمن نظم المعلومات وإجراء التعديلات المناسبة في سياسات وممارسات وتدابير وإجراءات الأمن".

يعترف هذا المبدأ بديناميكية نظم المعلومات في طبيعتها، مع العلم أن متطلبات أمن نظم المعلومات تتغير علي الدوام ولا تعتبر ثابتة في كل الأوقات، فهناك نقاط ضعف وتهديدات جديدة ومتطورة ويجب مراجعة واكتشاف تلك التهديدات باستمرار، وإعادة تقييم وتعديل كافة جوانب الأمن للتعامل مع تطور المخاطر الأمنية.

أي أن أمن نظم المعلومات يجب إعادة تقييمه دورياً، حيث أن نظم المعلومات ومتطلبات أمنها تتغير خلال الوقت، وعلي ذلك، يجب أن تمر نظم المعلومات بعملية تقييم مستمرة ودورية تتعلق بقيمتها ومدى حدوث المخاطر التي تتعرض لها.⁽²⁾

وهذا المبدأ يتفق مع ما دعت إليه لجنة بازل للرقابة المصرفية بضرورة المراقبة بانتظام على مخاطر العمليات وآلية رفع التقارير لمجلس الإدارة، ومراجعة إستراتيجية إدارة مخاطر العمليات بشكل دوري وضبطها.

2-1-5: المعايير الصادرة عن المنظمة الدولية لتوحيد المقاييس (ISO):

المنظمة الدولية لتوحيد المقاييس (ISO) هي منظمة يقع مقرها في جنيف بسويسرا، تعمل على وضع معايير موحدة وتضم هذه المنظمة ممثلين من عدة منظمات ومعاهد قومية للمعايير، تأسست هذه المنظمة في شباط (فبراير) 1947م بدعم من أكثر من (157) دولة، ويمثل اليمن فيها الهيئة اليمنية للمواصفات والمقاييس وضبط الجودة، وقد قرر أعضاء المنظمة أن يكون أيزو (ISO) الاسم الدولي للمنظمة، وأصلها من اليونانية (أيسوس/ISOS) بمعنى المساواة، وبالتالي فهي ليست اختصاراً للإنجليزية (ISO) وكذلك لم تشكل الأحرف الأولى من كلمات المنظمة بجميع اللغات ويعكس هذا الأمر هدف المنظمة وهو المساواة بين الثقافات المختلفة، وهي تصدر معايير تجارية وصناعية

(1) الهادي، محمد، (2006)، "توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية"، *cybrarians journal* - العدد (9)، أكاديمية السادات للعلوم الإدارية، القاهرة،

مصر، حزيران (يونيو) 2006، <http://www.journal.cybrarians.org>

(2) نفس المرجع السابق، <http://www.journal.cybrarians.org>

طوعية مقبولة دولياً، لها عدد من المعايير لإدارة أمن الشبكة، وتطوير البرمجيات، ومراقبة الجودة، وغيرها، وبالرغم من أنها منظمة غير حكومية ولكن قدرتها على وضع معايير تتحول عادة إلى قوانين ومعايير وطنية في معظم دول العالم تجعلها أكثر قوة من معظم المنظمات غير الحكومية، ويتحول أي إصدار لها إلى معيار دولي بموافقة 75% على الأقل من أعضائها، وهناك بلدان ذات اقتصاديات صغيرة لا تشارك في التصويت.⁽¹⁾

وقد شكلت لجنة فنية مشتركة مع اللجنة الكهروتقنية الدولية (IEC)، والتي تعتبر المصدر العالمي الرائد للمعايير الدولية للقطاع الإلكتروني ذات الصلة بالتكنولوجيا، المهمة الرئيسية للجنة الفنية المشتركة هو إعداد معايير دولية، كالمعيار ISO 27002 مثلاً.⁽²⁾

في هذا الجزء سنحاول أن نلقي نظرة على عدد من المعايير العالمية في مجال أمن المعلومات الصادرة عن هذه المنظمة، ولن نتطرق إلى نواحي تفصيلية كثيرة لأن لكل معيار تطبيقات خاصة ولكننا نحيل القارئ للمواقع الإلكترونية الخاصة بتلك المعايير للاطلاع التفصيلي.

معيار الجودة العالمية (ISO 9001)، أهم معيار من معايير الأيزو المتعلقة بنظم المعلومات، وصناعة البرمجيات، ويمكن الاستفادة منه في الوصول إلى تركيب نظم حماية الكترونية، وجدرا ن نار لحماية البيانات الهامة بالمنشأة، وخاصة البيانات المالية من أي اختراقات خارجية.

أصدرت المنظمة الدولية للمعايير أو التوحيد القياسي (ISO) مجموعة من المعايير المتعلقة بأمن وخصوصية المعلومات التي منها معيار المنظمة ISO/IEC 27005 لعام 2011م الذي يعطي المدراء والعاملين في مراكز وإدارات تكنولوجيا المعلومات إطار عمل مفصل لتنفيذ وتطبيق مدخل متكامل لإدارة المخاطر والتهديدات التي تواجههم في إدارة نظم أمن المعلومات بمنظمتهم.⁽³⁾

وبدون تطبيق مدخل وإطار إدارة المخاطر في المنشأة المتمسك بالرسوخ، فإن منشآت الأعمال والمنظمات المختلفة تعرض نفسها لأنواع كثيرة من أضرار الفضاء الخارجي الإلكتروني.

ووفقاً للجنة المسؤولة عن مجموعة معايير ISO 27000 ضمن المنظمة العالمية للمعايير فإن الأيزو يلائم استخدامات متنوعة مثل استخدامه داخل المنشآت لتشكيل الأهداف والمطالب الأمنية، وللتوافق مع التشريعات ولقوانين، وتعريف إجراءات جديدة لإدارة أمن المعلومات، كما يستخدم من قبل الإدارة لتحديد وضعية النشاطات الأمنية، ويحدد المدققين الداخليين والخارجيين من خلالها مستوى التوافق مع السياسات والإجراءات المقررة.⁽⁴⁾

المعايير والمواصفات الدولية ISO 27000 لإدارة وتشغيل المنظومة الأمنية لتكنولوجيا المعلومات

يمكن اعتبار جميع المعايير كمبادئ توجيهية لمزيد من المجالات المختلفة لضمان أمن المعلومات، وتتكون عائلة مواصفات نظم إدارة أمن المعلومات من مجموعة من المواصفات المترابطة، التي نشر بعضها بالفعل ولا يزال بعضها الآخر قيد التطوير، والتي تحتوي على عدد من المكونات الهيكلية الهامة،⁽⁵⁾ وتركز هذه المكونات على المواصفات المرجعية الموحدة لمتطلبات نظم إدارة أمن المعلومات (ISO/IEC 27001)

(1) Tofan, Dan, (2011), "Information Security Standards", **OP. Cit.**, PP: 128-135.

(2) Disterer, Georg, (2013), "ISO/IEC 27000, 27001 and 27002 for Information Security Management", **Journal of Information Security**, No.4, PP: 92-100.

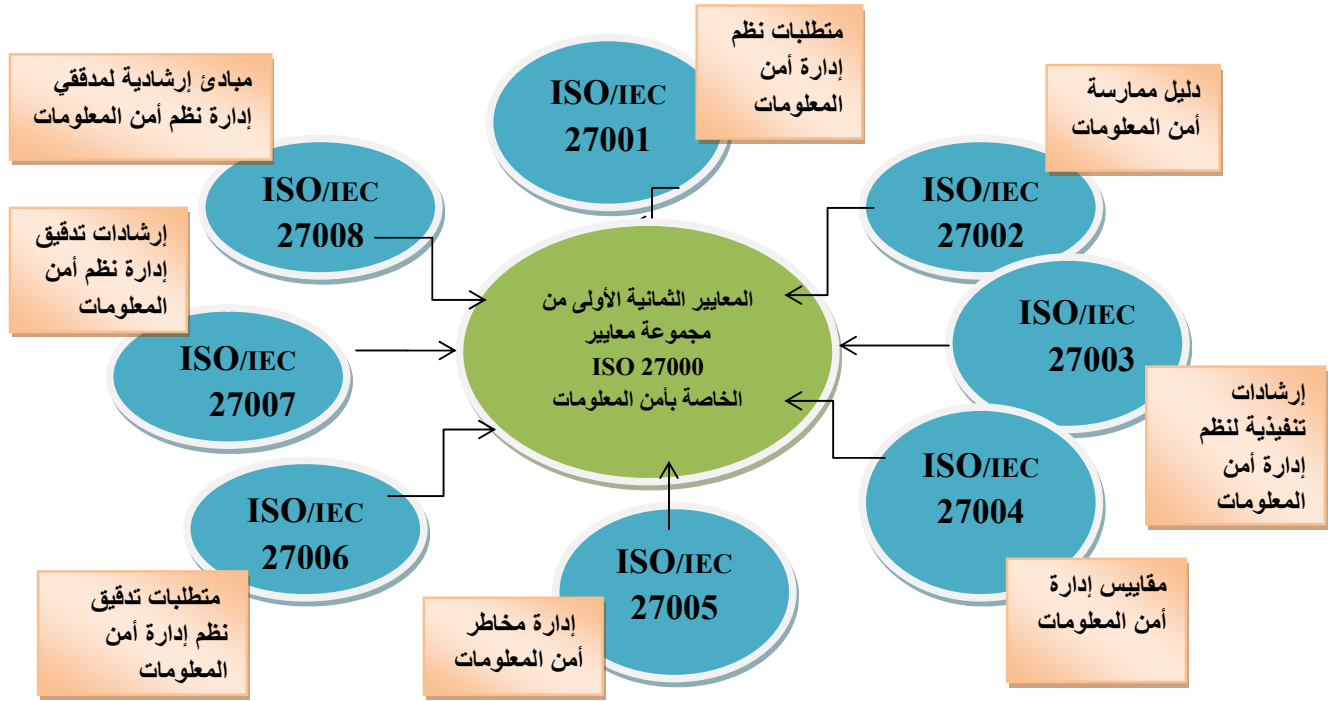
(3) الجوهر، كريمة & جاسم، أحمد، (2013)، "إجراءات حوكمة تقنية المعلومات (أنموذج مقترح في ضوء أهداف إطار COBIT)"، **المؤتمر العلمي الدولي التاسع، "الوضع الاقتصادي العربي وخيارات المستقبل"**، كلية الاقتصاد والعلوم الإدارية، جامعة الزرقاء، الأردن، للفترة 24 - 25 نيسان (أبريل) 2013م.

(4) الخطيب، محمد، (2012)، **أمن المعلومات**، مرجع سابق "ورقة عمل".

(5) Disterer, Georg, (2013), "ISO/IEC 27000, 27001 and 27002 for Information Security Management", **OP. Cit.**, PP: 92-100.

ومتطلبات جهات منح الشهادات (ISO/IEC 27006) ولجهات منح شهادات التوافق مع المواصفة (ISO/IEC 27001)، بينما تقدم مواصفات أخرى إرشادات توجيهية في العديد من جوانب تطبيق مواصفات نظم إدارة أمن المعلومات، مستهدفة العمليات العامة، والإرشادات المتعلقة بالضوابط إلى جانب الإرشادات ذات الخصوصية القطاعية.⁽¹⁾

شكل رقم (1-1-2) مجموعة معايير ISO 27K⁽²⁾



عائلة مواصفات نظم إدارة أمن المعلومات: يعكس المصنوفة التالية الموقف المعروف الحالي للمعايير التشغيلية الرئيسية في المسلسل:⁽³⁾

- ISO/IEC 27001: 2005 متطلبات نظم إدارة أمن المعلومات، ((مواصفات معيارية)).
- ISO/IEC 27002: 2007 مدونة قواعد (دليل) الممارسة لإدارة أمن المعلومات ((17799)).
- ISO/IEC 27004: 2009 قياس إدارة أمن المعلومات.
- ISO/IEC 27003:2010 إرشادات تنفيذية لإدارة نظم أمن المعلومات، ((مواصفات إرشادية)).
- ISO/IEC 27005: 2011 إدارة مخاطر أمن المعلومات.

(1) ISO/IEC 27000, (2012), "Information technology - Security techniques - Information security management systems - Overview and vocabulary", OP. Cit., Available at: <http://www.27000.org> (Accessed July 14, 2013).

(2) Disterer, Georg, (2013), "ISO/IEC 27000, 27001 and 27002 for Information Security Management", OP. Cit., PP: 92-100.

(3) The ISO 27000 Directory (2013), An Introduction to ISO 27001, ISO 27002....ISO 27008, available at: <http://www.27000.org> (Accessed July 14, 2013).

- ISO/IEC 27006: 2011 متطلبات خدمات تدقيق الحسابات وإصدار الشهادات لنظام إدارة أمن المعلومات ISMSs .
- ISO/IEC 27007: 2011 التوجيهيات الإرشادية لتدقيق إدارة نظم أمن المعلومات ISMS .
- ISO/IEC 27008: 2011 مبادئ توجيهية لمُدققي الحسابات بشأن ضوابط إدارة أمن المعلومات ISMS .

نتناول هنا ISO/IEC 27001: 2005 & ISO/IEC 27005: 2011 على النحو التالي:

- **ISO/IEC27001** : يشتهر بأنه معيار متعارف عليه دولياً لأمن المعلومات ونظم الإدارة، تحديد متطلبات هذه النظم، ويضمن الشروط الأمنية التي صقلها لمواكبة البيئة، وعلاوة على ذلك فإن المعيار (ISO/IEC27001) يعتمد خطة عمله على (PDCA)، هي اختصار للكلمات الإنكليزية (Plan-Do-Check-Act) والتي تعني خطط – نفذ – تحقق – صحح، وتمثل إحدى أهم آليات إدارة الأعمال وتطوير الجودة.
- وهذا المعيار يحدد الشروط اللازمة لتنفيذ ورصد ومراجعة وصيانة وتحسين نظم إدارة امن المعلومات،⁽¹⁾ وهذا المعيار يحدد الأهداف ومجالات نظم إدارة امن المعلومات لدى النظر في المنشآت، وطبيعة الأصول المعلوماتية والتكنولوجيات التي تمتلكها هذه المنشآت على أساس إستراتيجية معالجة المخاطر وتحديد الضوابط الأمنية المناسبة.⁽²⁾

إن التطبيق الفعّال للمعيار (ISO/IEC27001) يوفر للإدارة العليا الوسائل الكافية والمناسبة لمراقبة والسيطرة على حماية المعلومات بينما يقلل من أخطار العمل الناشئ من عدم الحصول على المعلومات بالدقة المطلوبة، كذلك خطر تسرب المعلومات، بعد تطبيق المنشأة المواصفة ستضمن حماية معلوماتها رسمياً للتواصل مع العملاء وشرعية (قانونية) المنشأة بالإضافة إلى إرضاء متطلبات أصحاب المصالح المختلفة.⁽³⁾

وعموماً ترتبط تلك المعايير بعدة ضوابط وأبعاد تخدم في تحقيق الرقابة الداخلية على أمن المعلومات وتتمثل هذه الضوابط في الأبعاد العشرة التالية:⁽⁴⁾

1. **سياسة الأمن:** يجب أن يكون هناك سياسة واضحة للأمن تؤكد على دعم إدارة المنشأة والتزامها بتحقيق أمن المعلومات.
2. **الأمن التنظيمي:** ويستلزم توفير المناخ الإداري الذي يضمن تطبيق أمن المعلومات وتحديد من يحق له الوصول إلى المعلومات.

(1) Choi, M., & Lee, C., (2015), " Information security management as a bridge in cloud systems from private to public organizations", *Sustainability*, Vol.7, No.9, PP: 12032-12051.

(2) *Ibid.*, PP: 12032-12051.

(3) الحافظ، علي عبد الستار & النعيمي، أحمد هاني، (2010)، " دور (ISO 27001:2005) في تعزيز مفهوم إدارة دورة حياة المعلومات (نموذج مقترح)"، *مجلة تكريت للعلوم الإدارية والاقتصادية*، المجلد (6)، العدد (17)، جامعة تكريت، العراق، 2010، ص ص: 56-73.

(4) الدلاهمة، سليمان مصطفى، (2008)، "أساسيات نظم المعلومات المحاسبية وتكنولوجيا المعلومات"، الطبعة الأولى، مؤسسة الوراق للنشر والتوزيع، عمان، الأردن، ص 679.

3. **تصنيف الأصول ورقابتها:** وذلك لتوفير حماية لأصول نظام المعلومات بمختلف مكوناته من برامج إلى أجهزة ونظم اتصال بتحديد المسؤولين عن تلك الأصول، كما يتم تصنيف المعلومات حسب أهميتها للمنشأة ودرجة حساسيتها لأي أحداث أمنية متوقعة ودرجة السرية والسلامة.
4. **أمن الأفراد:** ويهدف إلى تخفيض المخاطر المرتبطة بالخطأ البشري، ويتطلب إعداد برامج مستمرة لتوعية الموظفين وتعريفهم بالتهديدات والمخاطر المختلفة.
5. **الأمن المادي والبيئي:** ويشمل تأمين مكان نظام المعلومات ومن لهم حق الوصول إليه، وتأمين مصادر الطاقة للحماية من أي انقطاع للتيار الكهربائي.
6. **إدارة الاتصالات والعمليات:** وتقضي بضرورة وضع إجراءات تفصيلية موثقة توضح كيفية أداء كل مهمة من المهام الخاصة بنظم المعلومات، وتوضيح الخطوات اللازمة لاستعادة عمليات نظم المعلومات إلى وضعها الأصلي قبل وقوع أي حدث أمني، وإجراء الفصل بين المهام، واستعمال برامج الكشف عن الفيروسات وتحديثها، وعدم زيارة أي موقع غير موثوق به، وعدم فتح أية رسالة بريد الكتروني غير موثوق في مصدرها، وعدم فتح أية مرفقات للبريد الالكتروني قبل فحصها تجنباً للفيروسات.
7. **رقابة الوصول إلى المعلومات:** حيث يتم تحديد الأنشطة والمسؤوليات التي يقوم بها كل المستخدمين للنظم ثم يتم تحديد المعلومات والخدمات التي يتطلب الأمر الوصول إليها لأداء نشاطاتهم وأداء مسؤولياتهم بفعالية وكفاءة ثم يتم تحديد المعلومات والخدمات التي يصرح لكل مستخدم أو مجموعة من مستخدمي نظم المعلومات بالوصول إليها.
8. **تطوير النظم وصيانتها:** حيث يلزم عند إجراء تطوير للنظام أو عند استخدام برامج تطبيقات جديدة تحديد متطلبات عمل تلك النظم ومنها يتم التوصل لمتطلبات الأمن الواجب توافرها في تلك النظم والتي على أساسها يتم تحديد ضوابط وإجراءات أمن المعلومات التي يجب الاستعانة بها لضمان الاستمرار الكفء للنظام بعد تعديله مع إجراء اختبارات التحقق من معقولية وصحة واتساق المدخلات والمخرجات.
9. **إدارة استمرارية الأعمال:** والتي تهدف إلى منع أو تخفيف حدة التعطيل والأضرار التي قد تصيب أنشطة وعمليات المنشأة عند وقوع إحدى الكوارث أو الأحداث الأمنية الكبرى التي تضر بأمن نظم المعلومات، وتقوم على إعداد خطط استمرارية الأعمال أو خطط الاستعادة من الكوارث.
10. **الالتزام بالمتطلبات والقيود القانونية والتشريعية والتنظيمية والتعاقدية:** بهدف تجنب خرق المنشأة لأي متطلبات ناتجة عن أي من القيود السابقة بل قد يتطلب الأمر في هذه الحالة أيضاً مراعاة تشريعات وقوانين البلدان المختلفة عند تبادل البيانات.

■ **ISO/IEC 27005: 2011 إدارة مخاطر أمن المعلومات**

توفر المبادئ التوجيهية للمنظمة لتحديد نهجها لإدارة المخاطر ولمعالجة الاحتياجات في ISO / IEC 27001.

هذه هي منهجية مستقلة معيار ISO لإدارة مخاطر أمن المعلومات.

أصدرت المنظمة الدولية لتوحيد المقاييس (ISO) مجموعة من المعايير المتعلقة بأمن وخصوصية المعلومات التي منها معيار المنظمة (ISO/IEC 27005) لعام 2011م الذي يعطي المديرين والعاملين في مراكز وإدارات تكنولوجيا المعلومات إطار عمل مفصل لتنفيذ وتطبيق مدخل متكامل لإدارة المخاطر.⁽¹⁾

المعيار الدولي (ISO/IEC 27005) هو الذي ينطبق على جميع أنواع المنشآت (مثل المنشآت التجارية والوكالات الحكومية والمنشآت غير الربحية) التي تنوي إدارة المخاطر التي يمكن أن تهدد أمن نظم معلوماتها. يوفر هذا المعيار المبادئ التوجيهية لإدارة مخاطر أمن نظم المعلومات، وهو واحد من معايير نظم إدارة أمن المعلومات (ISMS) والتي تدعم المفاهيم العامة المحددة في (ISO/IEC27001)، ويهدف إلى تسهيل تنفيذ أمن نظم المعلومات على أساس منهج إدارة المخاطر، وعلاوة على ذلك فإن (ISO/IEC27005) تجرى تحليلاً للمخاطر وتحدد إستراتيجية لتخفيض المخاطر وتجنب المخاطر ونقل المخاطر من خلال الامتثال لسياسة أمن نظم المعلومات.⁽²⁾

ISO/IEC 27005 وإدارة مخاطر أمن معلومات:

إن المواصفة الدولية (ISO/IEC 27005:2008) تقدم إرشادات حول إدارة مخاطر أمن المعلومات وتدعم المفاهيم العاير المحددة في هذه المواصفة.

تم تصميم المواصفة الجديدة التي تستند إلى طريقة إدارة المخاطر ومعرفة المفاهيم والنماذج والعمليات والمصطلحات التي وضعتها المواصفة والتي تعتبر هامه للفهم الكامل لهذه المواصفة الدولية.⁽³⁾

ويقدم مبادئ توجيهية لإدارة مخاطر أمن المعلومات، وهو يدعم المفاهيم العامة المحددة في ISO / IEC 27001 ، ويهدف إلى المساعدة في تنفيذ أمن المعلومات على أساس نهج إدارة المخاطر.

إن معرفة المفاهيم والمصطلحات المذكورة في ISO / IEC 27001 و ISO / IEC 27002 من المهم للغاية بالنسبة لاستكمال فهم ISO / IEC 27005:2008، والتي تنطبق على جميع أنواع المنشآت (التجارية والحكومية وغير الربحية)، التي تنوي إدارة المخاطر التي تهدد أمن المعلومات فيها.

وقد بدأت المنشآت بجميع أنواعها بالاهتمام بشكل كبير بالتهديدات التي يمكن أن تواجه أمن نظم المعلومات وإدارتها وأصبح هذا الموضوع يحظى باهتمام أساسي من قبل أقسام تكنولوجيا المعلومات التابعة لها، وستقوم المواصفة

(1) الجوهر، كريمة & جاسم، أحمد، (2013)، " إجراءات حوكمة تقنية المعلومات (نموذج مقترح في ضوء أهداف إطار COBIT، مرجع سابق، " ورقة عمل".

(2) Choi, M., & Lee, C. (2015), "Information security management as a bridge in cloud systems from private to public organizations", *OP. Cit.*, PP: 12032-12051.

(3) ISO/IEC 27005, (2008), *Information Technology - Security Techniques -Information Security Risk Management*, OP. Cit.

الدولية الجديدة ISO/IEC 27005:2008 التي تصف عملية إدارة مخاطر أمن المعلومات والمهام المتعلقة بها بمساعدة تلك المنظمات في إدارة المخاطر ذات الصلة بموضوع هذه الدراسة.

وتعطينا المواصفة الدولية IEC/ISO27005 إرشادات توجيهية لإدارة مخاطر أمن المعلومات، بما في ذلك المشورة بشأن تقييم المخاطر، ومعالجتها، وقبولها، والتواصل بشأنها، ورصدها ومراجعتها.⁽¹⁾

ويستخدم ISO / IEC 27005 كإطار لتقييم المخاطر ومكمل لغيره من المعايير والنماذج أو الأطر الخاصة بتقييم المخاطر، بما في ذلك COSO، ITIL، ISO / IEC 27002، COBIT، وما إلى ذلك يوفر أداة يمكن استخدامها في نماذج المخاطر الأخرى لتحسين نوعية النتائج وتقييم المخاطر.⁽²⁾

المعيار الدولي الجديد ISO / IEC 27005:2011، تكنولوجيا المعلومات - تقنيات الأمن - إدارة المخاطر أمن المعلومات سوف يساعد المنشآت لإدارة أمن المعلومات وحمايتها من جميع أنواع المخاطر التي تتعرض لها على نحو أفضل. فهو يصف عملية إدارة مخاطر أمن المعلومات والإجراءات المرتبطة بها، ويدعم المفاهيم العامة المحددة في ISO / IEC 27001:2005، (تكنولوجيا المعلومات - تقنيات الأمن - نظم إدارة أمن المعلومات - المتطلبات).⁽³⁾

فذلك المعيار التقني يعطي المدراء والأفراد الموظفين في أقسام تكنولوجيا المعلومات إطاراً كافياً لتنفيذ نهج إدارة المخاطر ومساعدتها في إدارة أمن نظم المعلومات الخاصة بهم (ISMS) والمخاطر المتعلقة بها،⁽⁴⁾ ويصف بالتفصيل كيفية تطبيق تحليل عوامل مخاطر المعلومات ومنهجية أي إطار لإدارة المخاطر المحددة.⁽⁵⁾

وبالتالي نجد أن المعايير تكمل بعضها البعض في نواح كثيرة، فالمواصفة (ISO / IEC 27005) توفر إطاراً لبرنامج إدارة المخاطر، وتشمل مفاهيم مثل تطوير برنامج إدارة المخاطر والاتصال والرصد، ومعالجة المخاطر، وبالتالي فإنها توفر مبادئ توجيهية لتطوير إطار تقييم المخاطر والإبلاغ عن المخاطر، والعلاج، لكنها لا توفر منهجية محددة لتقييم تلك المخاطر (من خلال تحديد طبيعة الخطر وأثر الخطر الفعلي).⁽⁶⁾

ويرى الباحث بأن أمن نظم المعلومات المحاسبية أصبح في الصدارة، والمواصفة المذكورة لها علاقة بالأفراد الموظفين المعنيين بإدارة مخاطر أمن نظم المعلومات المحاسبية في نطاق المنشأة - وأينما كان ذلك ممكناً - غير أن المواصفة المذكورة لا تقدم أية معلومات محددة كمنهجية لإدارة المخاطر الأمنية، والأمر متروك لإدارة المنشأة لتحديد المنهج المناسب لها لتقييم وإدارة تلك المخاطر.

(1) ISO/IEC 27000, (2012), "Information technology - Security techniques -Information security management systems - Overview and vocabulary", OP.Cit., Available at: <http://www.27000.org>

(2) ISO/IEC 27005, (2008), **Information Technology - Security Techniques -Information Security Risk Management**, OP.Cit.

(3) Denis, Elizabeth Gasiorowski,(2011), "Are Information Security Risks Threatening Your Business? New and Improved ISO/IEC 27005 Standard Beefs Up Protection", http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1451

(4) Ibid., ", http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1451

(5) ISO/IEC 27005, (2008), **Information Technology - Security Techniques -Information Security Risk Management**, OP.Cit.

(6) Ibid.

2-1-6: المعايير الصادرة عن المعهد الوطني للمعايير والتكنولوجيا (NIST):

المعهد الوطني للمعايير والتكنولوجيا (NIST) التابع لوزارة التجارة في الولايات المتحدة، مسؤولة عن تطوير المعايير والمبادئ التوجيهية، بما في ذلك الحد الأدنى من المتطلبات، لتوفير أمن المعلومات الكافية لجميع الوكالات والعمليات، في منشآت القطاع العام، ولكن يمكن أن تستخدم أيضا من قبل المنشآت الخاصة غير الحكومية على أساس طوعي وغير خاضع لحقوق الطبع والنشر.

مؤخراً أصدر المعهد الوطني للمعايير والتكنولوجيا في الولايات المتحدة الأمريكية مشروعها نشر الأولي بعنوان: "معايير تصنيف أمن المعلومات ونظم المعلومات الاتحادية"، ويحدد هذا المنشور ثلاثة مستويات من المخاطر المحتملة (منخفضة، متوسطة، عالية) لكل من أهداف الأمن صرح (السرية والنزاهة والتوافر) ذات الصلة بتأمين نظم المعلومات المحوسبة، ويتم ترجيح المستويات المقترحة للخطر بشكل أكبر تجاه تأثير الخطر على أمن نظم المعلومات المحاسبية المحوسبة (CAIS) والحجم المحتمل للضرر بفقدان السرية والنزاهة والتوافر أو ما سيترتب على عمليات المنشأة (بما في ذلك رسالتها ووظائفها ومصادقيتها أو سمعتها) والأصول أو منسوبيها (خصوصية البيانات).⁽¹⁾

إن "المبادئ والممارسات الخاصة بتأمين تقنية نظم المعلومات المقبولة عموماً" تقدم الوثيقة الأساسية التي يمكن للمنشآت استخدامها لإنشاء واستعراض برامج أمن تكنولوجيا المعلومات الخاصة بهم، والتي تستخدم من قبل إدارة، والمدققين الداخليين، كما يمكن للمستخدمين ومطوري النظام، والأفراد المختصين بالأمن استخدام هذا المبدأ التوجيهي لكسب فهم أكثر لنظم تكنولوجيا المعلومات ومتطلبات الأمن الأساسية ووصف عناصر التحكم⁽²⁾

وتقييم المخاطر هو موضوع من أحدث الإصدارات الخاصة بالمعهد الوطني للمعايير والتكنولوجيا (NIST)، فالمنشور الخاص (30-800، NIST)، وأجري عليه تحديثاً عام 2002 وتم نشره بشكل واسع النطاق، وهو مصدر موثوق لتوجيهات تقييم المخاطر الشاملة لنظم المعلومات الاتحادية في الولايات المتحدة الأمريكية.⁽³⁾

كما تتناول الإرشادات العامة بشأن إدارة مخاطر لنظم المعلومات الآن في (39-800، NIST SP)، الصادر في مارس 2011م و SP 800-30 والتي تتركز الآن بشكل حصري على تقييم المخاطر، وهي واحدة من أربع خطوات لإدارة المخاطر.⁽⁴⁾

أن دليل إجراء تقييم المخاطر هو المبدأ التوجيهي الخامس والذي تم تطويره لإطار أمن المعلومات الموحد من قبل فريق العمل المشترك تحت إشراف لجنة عمل مشتركة مشكلة من وزارة الدفاع الأمريكية وأجهزة الاستخبارات التابعة لها، والمعهد الوطني للمعايير والتكنولوجيا ولجنة أنظمة الأمن القومي، واللجنة الوطنية لأمن نظم المعلومات.⁽¹⁾

(1) Abu-Musa, Ahmad A., (2006), "Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations", *OP.Cit.*, PP: 1-26.

(2) Abu-Musa A. A., (2007), "Evaluating the Security Controls of CAIS in Developing Countries an Examination of Current Research", *Information Management & Computer Security*, Vol.15, No.1&2, PP: 46-63 & PP: 128-148, PDF Copy.

(3) National Institute of Standards and Technology: NIST, (March 2011), "*Managing Information Security Risk-Organization, Mission, and Information System View*", Special Publication (SP) 800-39, 2011, Available at <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>

(4) *Ibid*, Available at <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>

ويصف دليل لإجراء تقييمات للمخاطر وكذلك كيفية تطبيق عملية تقييم المخاطر في المستويات الثلاثة من التسلسل الهرمي لإدارة المخاطر المحددة في المنشور الخاص (NIST SP 800-39) بجداول ومصفوفات تقييم العوامل الشائعة للمستخدمين على التكيف مع تقييماتها الخاصة بالمخاطر التنظيمية على أساس الغرض والنطاق والافتراضات والقيود من التقييمات.⁽²⁾

ويوفر النهج المنظم لإدارة المخاطر وفق المعايير والمبادئ التوجيهية الصادرة عن المعهد الوطني للمعايير والتكنولوجيا (NIST). دليل جديد، نيسـت SP 800-30 لمراجعة 1، ودليل لإجراء تقييمات للمخاطر، وملاحق SP 800-39، ويناقش تقييم المخاطر كجزء من نهج متكامل لإدارة المخاطر على نطاق المنشأة وهي الخامسة في سلسلة من إدارة المعلومات والمبادئ التوجيهية الأمنية لمواجهة المخاطر التي تم تطويرها من قبل لجنة المهام المشتركة وتحويل مبادرة فريق العمل المشترك، والتي كان أبرز مهامها وضع إطار لأمن المعلومات الموحدة للحكومة الاتحادية بهدف مواجهة تحديات حماية المعلومات الاتحادية ونظم المعلومات وكذلك البنية التحتية للمعلومات الحرجة.

وهناك توجه كبير بنشر تلك الأدلة بشكل موسع لتشمل مزيد من المعلومات حول مجموعة متنوعة من العوامل الأساسية لتحديد مخاطر أمن نظم المعلومات، مثل مصادر التهديد والأحداث ومواطن الضعف والظروف المهيأة، والأثر، واحتمال وقوع تهديد لحدوث المخاطر، يصف عملية من ثلاث خطوات لمساعدة المنشآت في إجراء عمليات تقييم المخاطر بنجاح والحفاظ على نتائج التقييم، ويوفر نيسـت SP 800-30 أساساً لوضع برنامج فعال لإدارة المخاطر، ويهدف إلى مساعدة المنشآت على إدارة المخاطر المتعلقة بنظم المعلومات على نحو أفضل.⁽³⁾

إن منهجية تقييم المخاطر تشمل عدة مراحل يمكن ذكرها على النحو التالي:⁽⁴⁾

1. توصيف النظام.
 2. تحديد التهديد.
 3. تحديد وجود الثغرات الأمنية.
 4. تحليل وسائل وإجراءات التحكم.
 5. تحديد الأرجحية.
 6. تحليل تأثيرات المخاطر.
 7. تحديد المخاطر.
 8. توصيات المراقبة.
 9. توثيق نتائج التقييم.
- مع ملاحظة أن الخطوات 2، و3، و4، و6، يمكن أن تُجرى بشكل متوازٍ بعد انتهاء الخطوة الأولى.

(1) *Ibid*, Available at <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>

(2) *Ibid*, Available at <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>

(3) National Institute of Standards and Technology: NIST, (2012), "Guide for Conducting Risk Assessments". OP.Cit.

(4) Pandey, Santosh K., (2012), "A Comparative Study of Risk Assessment Methodologies for Information Systems", *Buletin Teknik Elektro dan Informatika*, Vol.1, No.2, June 2012, PP: 111-122, <http://journal.uad.ac.id/index.php/EEI/index>

2-1-7: أهم التشريعات والقوانين والتعليمات المحلية الصادرة في الجمهورية اليمنية والمتعلقة بأمن نظم المعلومات:

ومن العوامل التي يجب النظر فيها عند تقييم المخاطر الأمنية المتطلبات القانونية والتعاقدية ذات الصلة، حيث صدرت عدة قوانين في الجمهورية اليمنية لها علاقة بمخاطر أمن نظم المعلومات المحاسبية - سواء بشكل مباشر أو غير مباشر - ومن أهمها: (1)

1. القانون رقم (38) لسنة 1998م بشأن البنوك التجارية.
2. القانون رقم (14) لسنة 2000م بشأن البنك المركزي اليمني.
3. القانون رقم (35) لسنة 2003م بشأن مكافحة غسيل الأموال.
4. القانون رقم (40) لسنة 2006م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية.
5. القانون رقم (1) لسنة 2010م بشأن مكافحة غسل الأموال وتمويل الإرهاب.
6. القانون رقم (13) لسنة 2012م بشأن حق الحصول على المعلومات.

الخاتمة:

الأمن هو شيء ينبغي أن تشارك فيها جميع الأطراف سواء من الإدارة العليا والعاملين في أمن المعلومات، والمحترفين في تكنولوجيا المعلومات والمستخدمين والكل منهم له دور يؤديه في تأمين أصول المنشأة، ونجاح أمن المعلومات يمكن تحقيقه من خلال التعاون الكامل على جميع مستويات المنظمة، سواء في الداخل والخارج. وبالرغم من أن هناك عدداً من معايير أمن المعلومات المتاحة، وهي منظمة ولا يمكن الاستفادة من تلك المعلومات إلا إذا تم تنفيذ هذه المعايير بشكل صحيح.

وتعتبر تلك المعايير في حقيقة الأمر بمثابة مجموعة من الإرشادات والتوصيات التي تتعلق بأمن المعلومات، وتمثل في نفس الوقت تجميعاً لأفضل ممارسات الرقابة الداخلية التي يمكن تحقيقها على أمن المعلومات في المنشآت التي تتعامل بالنظم المحوسبة.

وترتبط تلك المعايير بصفة عامة بكل من سياسة الأمن التنظيمي والإداري، وأمن الأفراد، والأمن البيئي والمادي، وأمن الأجهزة "أمن الوحدات الآلية"، وأمن الاتصالات، وأمن البرامج، وأمن العمليات والمعاملات، والتحكم في الدخول إلى النظام.

ويعتقد الاتحاد الدولي للمحاسبين أنه، من منظور دولي، فإن التحكم، وإدارة المخاطر، والرقابة الداخلية المستندة إلى مبادئ ينبغي أن تكون المبادئ توجيهية بدلاً من إلزامية فما يعمل به في بيئة وبلد معين قد لا يعمل أو قد يعمل بشكل مختلف في بلد آخر، وفي السعي من أجل التناسق العالمي، فمن المهم أن نلاحظ أن هناك اختلافات بين الناس، والهياكل، والأماكن، ووجهات النظر حول إدارة التحكم بالخطر والرقابة الداخلية، وهناك أيضاً اختلافات في التشريعات ونضج التشريعات النازمة لعمل المنشآت المختلفة وفي ولايات قضائية مختلفة.

(1) وزارة الشؤون القانونية، (القوانين الصادرة المذكورة)، صنعاء، الجمهورية اليمنية.

2-2: المبحث الثاني

طبيعة ومنهجية تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة

إن المنشآت التجارية والخدمية بشكل عام والبنوك على وجه الخصوص ينبغي أن تكون أكثر وعياً للمخاطر الأمنية المحتملة التي تهدد أمن أنظمتها وكفاءة استخدامها وذلك لتجنب هذه المخاطر والحد من الآثار السلبية إلى أقصى حد ممكن،⁽¹⁾ فالمنشآت المالية المصرفية الناجحة هي تلك التي تنقصى المخاطر في عملياتها من أجل إدارة هذه المخاطر بكفاءة عالية، بغية تخفيف أثارها، ليس تلك المنشآت المالية التي تغض الطرف عن هذه المخاطر ولا تعي أثارها.

أمن المعلومات هو الآن الساحة السياسية والاقتصادية والاجتماعية والتجارية ولم تعد المحافظة عليه تقع على عاتق خبراء التكنولوجيا وحدهم، بل هي قضية أوسع بكثير تؤثر على الجميع بدءاً بالرئيس التنفيذي، ومجلس إدارة المنشأة والمساهمين وحتى كل مستخدم وموظف من الموظفين في المنشأة، بغض النظر عن رتبهم أو دورهم الوظيفي.⁽²⁾

إن إدارة مخاطر أمن نظم المعلومات يمثل موضوع بحث ودراسة حديث نسبياً (منذ عشرين سنة) وهو تخصص علمي ينظر إليه حالياً كجزء ضروري من إدارة مخاطر المنشآت،⁽³⁾ لذلك أثارت قضية "تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة" اهتمام الباحث لدراستها وبحثها لبيان مدي تطبيقها في قطاع البنوك التجارية في الجمهورية اليمنية، فهناك حاجة ملحة لحماية هذه النظم ومخرجاتها، من التعرض للاحتيال أو التدمير أو التعديل غير المصرح به، من خلال تحديد وتقييم المخاطر المختلفة ووضع الإجراءات الرقابية الملائمة لها، لضمان نزاهة وموثوقية وسرية نظم المعلومات المحاسبية.

وبينما يجب أن تكون عملية تقييم المخاطر ديناميكية، فإن الاتجاه المتسارع للابتكار التكنولوجي الداعم للصيرفة الالكترونية واعتماد أداء بعض الخدمات المصرفية على استخدام الشبكات المفتوحة مثل الانترنت يضاعف الحاجة إلى عملية إدارة متواصلة ودقيقة للمخاطر المصاحبة لها.

وهناك مخاطر ينبغي تقييمها بهدف فهمها وكيف يمكن أن تدار وفقاً لقدرات المنشآت المختلفة⁽⁴⁾ فإدارة أمن المعلومات هي قضية إدارية في المقام الأول، حيث يتوصل فيها إلى توازن بين قيمة المعلومات للمنشأة من جهة

(1) Al Hanini, Eman, (2012), "The Risks of Using Computerized Accounting Information Systems in the Jordanian Banks: Their Reasons and Ways of Prevention", *OP. Cit.*, PP: 53-63.

(2) Humphreys, (2010), *Edward, information security risk management, handbook for ISO/IEC 27001*, British Standards Institution (BSI), Available at: <http://shop.bsigroup.com/bip0076> (Accessed May 14, 2012).

(3) Černá, Marie, (2012), "Information Risks and Their Connection With Accounting", *6th European Conference on Information Management and Evaluation*, *OP. Cit.*, PP: 375-382.

(4) Brender, Nathalie & Markov, Iliya, (2013), "Risk perception and risk management in cloud computing: Results from a case study of Swiss companies", *International Journal of Information Management*, No.33 2013, PP:726- 733, <http://www.elsevier.com/locate/ijinfomgt>

وتكلفة الأفراد والمقاييس الإدارية والتكنولوجية من جهة أخرى، وتضع مقاييس الأمن الحاجة في التوصل إلى أقل تكلفة من المخاطر أو الأضرار التي قد تسبب فقد سرية المعلومات وتحد من سلامتها وتوافرها.

إن إدارة الخطر والأمن ليست وسيلة محصورة على المنشآت العامة فقط، ولكنها أيضاً لكل الأنشطة طويلة وقصيرة الأمد، ويجب النظر للفوائد والفرص من إدارة الخطر في علاقتها بأطراف المصلحة المختلفة المتأثرة وليس فقط في علاقتها بنشاط المنشأة. (1)

إن الغرض من دراسة المخاطر هو السيطرة عليها وإدارتها بطريقة تمكن من تقليل تأثيراتها السلبية على نتيجة القرار الذي تريد أن تتخذه أي منشأة أعمال، ولذا فإن الوظيفة الرئيسية لإدارة أي منشأة مالية هي: تحديد طبيعة المخاطر الرئيسية التي تتعرض لها، وذلك لفهم مستوى المخاطر التي يمكن تجنبها، وتقرير طبيعة ومدى المخاطر التي تكون المنشأة قادرة على تحملها. (2)

ولتقييم المخاطر الأمنية لنظم المعلومات المحاسبية لا بد من تحديد أنواع تلك المخاطر ومن ثم تأثيرها على نظم المعلومات المحاسبية المحوسبة، وذلك ليس بالأمر اليسير فهناك صعوبات في عملية تقييم مخاطر تكنولوجيا المعلومات ولكنها تعد ضرورية لأنها تمكن إدارة المنشأة من التعرف على المخاطر وترتيبها حسب الأولوية لكي يسهل عملية إدارتها وبالتالي تعيين الضوابط الرقابية وصولاً إلى تحسين المزايا التي يتيحها تواجد التكنولوجيا الالكترونية في المنشآت. (3)

وفي هذا المبحث، سوف يتم مناقشة طبيعة ومنهجية وأدوات تقييم مخاطر أمن نظم المعلومات المحاسبية.

2-2-1: مفهوم تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة:

قبل التطرق لمفهوم تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة تجدر الإشارة إلى أن هناك مشكلة في استخدام المصطلح، ويعود السبب في استخدام مصطلحات متعددة للدلالة على نفس العملية إلى الترجمة الحرفية من اللغة الأجنبية إلى اللغة العربية، فهناك فرق بين تقييم المخاطر وتحليلها وإدارتها، ولمعرفة طبيعة تقييم مخاطر أمن نظم المعلومات المحوسبة لا بد من التفريق بينها وبين مفهوم إدارة تلك المخاطر وكذلك مفهوم تحليل تلك المخاطر في الأدبيات الإدارية المتاحة كما يلي:

2-2-1-1: مفهوم إدارة مخاطر أمن نظم المعلومات المحاسبية (Management Risks): إن إدارة المخاطر هي

جزء أساسي في الإدارة الإستراتيجية لأي منشأة، وهي الإجراءات التي تتبعها المنشآت بشكل منظم لمواجهة المخاطر المصاحبة لأنشطتها، بهدف تحقيق المزايا المستدامة من كل نشاط والتركيز الأساسي لإدارة المخاطر الجيدة هو التعرف على هذه المخاطر ومعالجتها.

(1) هوارى، معراج & عبيرات، "إدارة مخاطرة الأمن وشفافية المعلومات لنظم المعلومات فى ظل البيئة الرقمية"، مرجع سابق، من الموقع:

<http://www.docstoc.com/docs/145138300>

(2) Macedo, F., & Da Silva, M. M., (2016), *Comparative Study of Information Security Risk Assessment Models*, Universidad Técnica de Lisboa, Lisboa., P. 122.

(3) حوري، زينب & خضراوي، ساسية، (2013)، "معالجة مخاطر التكنولوجيا في أعمال المحاسبة والتدقيق"، مرجع سابق، ص: 379-396.

- إن مفهوم إدارة المخاطر هو مصطلح شائع بين المعنيين بأمن تكنولوجيا المعلومات، وبشكل عام فإن إدارة المخاطر يعني تقييم وتخفيف من القضايا المحتملة التي تشكل تهديداً لأحد الأعمال التجارية، أيًا كان مصدرها.⁽¹⁾
- وإدارة المخاطر هو علم يركز على عملية تحديد المخاطر التي يمكن أن يتعرض لها نظام الأمان وتحديد احتمالية حدوث أو وقوع ذلك الأثر فعلاً وتحديد وسائل الحراسة والأمان الإضافية التي يمكنها تحجيم ذلك التأثير في ظل حزمة من الظروف السائدة خلال إطار زمني معين.⁽²⁾
- وتعرف إدارة المخاطر بأنها سلسلة أفعال تتم من قبل مجلس الإدارة، والإدارة، والأفراد، من أجل وضع الاستراتيجيات لتحديد الأحداث المحتملة المؤثرة على المنشأة، وجعل المخاطر ضمن الإطار الذي يمكن التعامل معه، لتقديم تأكيد معقول حول تحقيق أهداف المنشأة.⁽³⁾
- إدارة المخاطر هي "عملية إنشاء والحفاظ على أمن نظام المعلومات داخل المنظمة والتي تهدف إلى "تحديد وقياس ومراقبة الأحداث غير المؤكدة من أجل تقليل الخسائر وتعظيم العائد على رأس المال المستثمر للأمن".⁽⁴⁾
- وهي عملية تحديد وتقييم المخاطر واتخاذ خطوات للحد منه إلى مستوى مقبول نظراً للتكاليف التي ينطوي عليها القيام بذلك، النشاط الرئيسي ضمن إدارة المخاطر هي عملية تقييم المخاطر.⁽⁵⁾
- وتتشابه إدارة المخاطر إلى حد كبير مع مفهوم الرقابة الداخلية الذي وضعته لجنة COSO) ولذلك يمكن القول إن مفهوم إدارة مخاطر يتسع في نطاقه ليشمل الرقابة الداخلية التقليدية على المعاملات والأصول والعمليات، فهي عملية منهجية لتحديد وتقييم المخاطر واتخاذ خطوات للحد منه إلى مستوى مقبول نظراً للتكاليف التي ينطوي عليها القيام بذلك.⁽⁶⁾
- إدارة مخاطر النظام هي الأساليب التي تهدف إلى تحديد، وفحص، وإزالة أو تخفيف حدوث المخاطر التي قد تؤثر على موارد النظام.⁽⁷⁾
- إدارة مخاطر نظم المعلومات هي محاولة للتوفيق بين العلاقات بين أربعة عناصر ترتبط بنظام المعلومات وهي التهديدات، والأثر (الخسائر)، والضوابط، والأصول – والقاسم المشترك بينها حدوث الخطر.⁽⁸⁾

(1) Stroe, E. R. & Rusu, A. C., (2011), "Security Risk Management - Approaches and Methodology", *OP. Cit.*, PP: 228- 240.

(2) يوسف، عبد الستار حسين، (2007)، "تقدير المخاطرة في ظل تحليل (SWOT) في المؤسسات الصناعية- دراسة تحليلية"، *المؤتمر العلمي الدولي السنوي السابع- إدارة المخاطر واقتصاد المعرفة*، كلية الاقتصاد والعلوم الإدارية، جامعة الزيتونة الأردنية، الزرقاء، الأردن، 16-18 نيسان (أبريل) 2007.

(3) Committee of Sponsoring Organization of the Tread-way Commission (COSO), (2004), *Enterprise Risk Management- Integrated Framework: Executive Summary*, OP. Cit., PP: 1-7, <http://www.coso.org/IC-Integrated Framework-summary.htm>

(4) Zhiwei, Yu & Zhongyuan, Ji, (2012), "A Survey on the Evolution of Risk Evaluation for Information Systems Security", *Energy Procedia*, Vol. 17, PP:1288-1294.

(5) Rees, Jackie & Allen, Jonathan, (2008), "The State of Risk Assessment Practices in Information Security: An Exploratory Investigation", *Journal of Organizational Computing and Electronic Commerce*, No. 18, USA, PP: 255-277.

(6) Committee of Sponsoring Organization of the Tread-way Commission (COSO), (2013), *"Internal Control-Integrated Framework"*, Tread-way Commission, New Jersey, USA, Available from http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf.

(7) Mihalache, Arsenie, (2011), "Security of the Accounting Information System Infrastructure", *Annals of the "Ovidius" University, Economic Sciences Series*, Volume XI, No.1, PP:1339-1345, <http://ideas.repec.org/a/ovi/oviste/v11y2011i1p1339-1345.html>

(8) ISO/IEC 27005, (2008), *Information Technology - Security Techniques -Information Security Risk Management*, OP. Cit..

ويرى الباحث أنه في الدول المتقدمة التي يتوفر لبنوكها قواعد بيانات إلكترونية، ونظم داخلية لقياس المخاطر وإدارتها، يمكن للباحثين من تطبيق مناهج علمية لتقييم تلك المخاطر بصورة واقعية، على عكس ما يتم في الدول النامية، التي ينقصها معايير للحوكمة، ومعايير للمحاسبة والرقابة على نظم المعلومات المحوسبة، ويجب الاستفادة من خبرات وتجارب الدول المتقدمة في مجال تقييم المخاطر، وإدارتها.

استناداً لما سبق يستطيع الباحث القول بأن إدارة المخاطر هي عبارة عن منهج أو مدخل علمي للتعامل مع المخاطر البحتة عن طريق توقع الخسائر المحتملة وتصميم وتنفيذ إجراءات من شأنها أن تقلل إمكانية حدوث الخسارة أو الأثر المالي للخسائر التي تقع إلى الحد الأدنى.

2-1-2-2: مفهوم تقييم مخاطر أمن نظم المعلومات المحاسبية (Evaluation Risks): تقييم المخاطر هو عنصر

أساسي من إدارة المخاطر وهي عملية تنطوي على تقييم التهديدات ومواطن الضعف، وتحديد المخاطر واختيار الإجراءات الأمنية للحد من المخاطر وتنفيذ ورصد مختارة تدابير لضمان أن الإجراءات فعالة وهو "تحليل موضوعي للضوابط الأمنية الحالية التي تحمي أصول المنشأة وتحديد مدى احتمال الخسائر لتلك الأصول".⁽¹⁾

■ **تقييم المخاطر بشكل عام:** وهي عملية تهدف إلى التعرف على المخاطر المرتبطة بتحقيق أهداف المنشأة، وتحليلها (تقسيمها)، وتحديد وسائل العلاج الملائمة لمواجهة تلك المخاطر.⁽²⁾

■ إن عملية تقييم المخاطر يتم من خلالها التعرف على المخاطر وتحليلها وقياسها وترتيبها وفق الأولويات ليتم التعامل معها حسب أهميتها، **وتقييم المخاطر هي عملية (Process)** وليست مجرد خطة محصورة، وهي تبدأ من التساؤل حول التهديدات ثم نقاط الضعف وأخيراً وسائل الوقاية المناسبة للتعامل مع التهديدات ووسائل منع نقاط الضعف.⁽³⁾

■ **تقييم المخاطر:** هي عملية يتم من خلالها التعرف على المخاطر وتحليلها وقياسها وترتيب هذه المخاطر وفقاً لأولويات ليتم التعامل معها حسب أهميتها.⁽⁴⁾

■ تقييم المخاطر هي عملية مقارنة تقديرات المخاطر (*Assessing Risks*) بمعايير المخاطرة السابق تحديدها لتحديد مدى أهمية تلك المخاطر ومن ثم اتخاذ إجراءات المعالجة المناسبة (أو المتناسبة مع مقدار المخاطر).⁽⁵⁾

■ **ويمكن تعريف تقييم المخاطرة** بشكل عام على أنها الظاهرة التي تحمل عاملين أساسيين هما: عدم التأكد وإمكانية الحدوث بمعنى احتمال الحدوث ونتاجها أو آثارها إذا حدثت.⁽⁶⁾

(1) Munteanu, A. & Fotache, D. & Dospinescu, O., (2008), "Information Systems Security Risk Assessment. Harmonization with International Accounting Standards", *International Conference on Innovation in Software Engineering – ISE'2008*, 10 – 12 December 2008, University of Canberra, Vienna – Austria.

(2) الدوجي، علي حسين & والخيرو، إيمان، (2013)، "تحسين فاعلية نظام الرقابة الداخلية وفق إنموذج COSO"، *مراجع سابق*، ص: 398-433.

(3) صقر، ممدوح الشحات، (2007)، "أمن المعلومات"، *ندوة أمن وحماية نظم المعلومات في المؤسسات العربية*، مرجع سابق، ص: 14.

(4) دهيرب، محمد سمير، (2012)، "تقييم أنظمة الرقابة الداخلية وفق مفهوم لجنة (COSO)"، *مجلة الكوئ للعلوم الاقتصادية والإدارية*، العدد (6)، جامعة واسط، العراق، ص: 255-278.

(5) ISO/IEC 27000, (2012), "Information technology - Security techniques - Information security management systems - Overview and vocabulary", OP. Cit., Available at: <http://www.27000.org>

(6) عبد القادر، عصماني، (2009)، "أهمية بناء أنظمة لإدارة المخاطر لمواجهة الأزمات في المؤسسات المالية"، *الملتقى العلمي الدولي – الأزمة المالية والاقتصادية الدولية والحكومة العالمية*، كلية العلوم الاقتصادية وعلوم التسيير، جامعة فرحات عباس، سطيف، الجزائر، 20-21 تشرين الأول (أكتوبر)، 2009.

- **تقييم المخاطر:** تقييم المخاطر هو العملية الأولى في منهجية إدارة المخاطر لتحديد مدى التهديد المحتملة والمخاطر المرتبطة تكنولوجيا نظم المعلومات وذلك للمساعدة على تحديد الضوابط المناسبة لخفض أو القضاء على الخطر أثناء عملية التخفيف من حدة المخاطر.⁽¹⁾
 - **تقييم المخاطر** هو إجراء منظم ومنهجي، والتي تعتمد على تحديد المخاطر وتحديد وقياس الآثار الناجمة عنها، وذلك بهدف إجراء المقارنات بين المخاطر لأغراض السيطرة عليها أو منع حدوثها.⁽²⁾
 - إن تقييم مخاطر أمن نظم المعلومات هو عملية تحديد وتحليل جميع المخاطر الموجودة في نظم معلومات منشآت الأعمال، من خلال تقييم إمكانية حدوث ثلاثة عناصر هي الخطر والتهديدات والتأثيرات السلبية، لنظم المعلومات، وخصائص أمن المعلومات، بما في ذلك السرية والنزاهة والتوافر.⁽³⁾
 - تقييم المخاطر هي عملية تحديد وتقدير، وترتيب أولويات مخاطر أمن المعلومات وبحسب الخطر كمنتج من احتمال التهديد وقيمة الأثر.⁽⁴⁾
- ويرى الباحث أن **تقييم المخاطر** يتضمن تحديد المخاطر، وقياس قيمها ومقدارها، وتحديد المناطق التي تحتاج إلى الاستعانة بضوابط حمايتها، وأخيراً تحديد تلك الضوابط بما يمكن المنشأة من إدارة تلك المخاطر، وبالتالي يتم تقييم المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة، ذلك من خلال دراسة تلك المخاطر ومعرفة جميع التهديدات المحتملة، وتحديد أسبابها وبناء تدابير مضادة لتفادي مواجهتها ومعالجة المشاكل، حيث ينطوي تقييم الأمن على دراسة الضوابط الموجودة وتقييم مدى كفايتها بالنسبة إلى التهديدات المحتملة، عن طريق تحديد أدوات وإجراءات الرقابة الداخلية اللازمة لمواجهة تلك المخاطر.

2-2-2: أهمية تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة:

برزت الحاجة إلى تقييم مخاطر نظم المعلومات المحاسبية كنتيجة طبيعية للاهتمام المتزايد من جانب المنشآت باستخدام تكنولوجيا المعلومات في إنتاج وتوليد المعلومات، تلك المعلومات التي تحتاجها العديد من الفئات سواء من داخل المنشأة أو خارجها،⁽⁵⁾ ولتوفير الحماية لنظم المعلومات المحاسبية المحوسبة ووقايتها من المخاطر فلا بد من اكتشاف تلك المخاطر التي تهدد أمن تلك النظم وتحديد درجة حدوثها إذ يعد ذلك خطوة ضرورية لوضع الأساليب الرقابية المناسبة.

وجدير بالذكر أن النظام الذي يمكن الوثوق فيه هو ذلك النظام الذي يكون قادراً على العمل بدون أخطاء، لأن المستوى المرتفع من المخاطر قد يؤدي إلى فشل بعض مشروعات نظم المعلومات، ويصبح وجود إطار لتقييم

(1) National Institute of Standards and Technology: NIST, (July 2012), "Guide for Conducting Risk Assessments", , OP. Cit..

(2) Nikolić, Božo & Ružić-Dimitrijević, Ljiljana , (2009), "Risk Assessment of Information Technology Systems", Issues in Informing Science and Information Technology, Vol. 6, PP:1-21

(3) Dai, Weihui, (2012), "Risk Management Model of Information Security in IC Manufacturing Industry", Journal of Computers, Vol. 7, No. 2, February 2012, PP: 317-324.

(4) National Institute of Standards and Technology: NIST, (July 2012), "Guide for Conducting Risk Assessments", , OP. Cit

(5) عيسي، علا & وعاشور، عصاف، (2010)، "مخاطر نظم المعلومات المحاسبية وحوكمة المنشآت ومواجهة الأزمة المالية العالمية"، مرجع سابق، ص ص: 408-434.

المخاطر يمكن أن يساعد إلى حد كبير في مواجهة تلك المخاطر، كما يعد أحد الأدوات الهامة لنجاح نظم المعلومات المحاسبية والثقة فيها.⁽¹⁾

وتعد مرحلة تقييم المخاطر اللبنة الأساس والخطوة الأولى لعملية إدارة المخاطر وحماية مصادر المعلومات، فما لا يمكن قياسه لا يمكن إدارته، فهي خطوة أولى لإدارة المخاطر.

إن تقييم المخاطر هي عملية أساسية من إدارة المخاطر وتوفير وسائل كافية للحد من هذه المخاطر، فالعملية الأكثر أهمية من إدارة المخاطر هو تقييم مخاطر أمن المعلومات،⁽²⁾ وتعتبر جوهر إدارة المخاطر، فتقييم المخاطر هو الوسيلة التي يتم من خلالها تحديد مخاطر النظم وتقييمها لتبرير الضوابط الأمنية،⁽³⁾ وتستخدم نتائج تقييم المخاطر من قبل المنشآت لوضع مسارات معينة للعمل على توفر تدابير الاستجابة الفعالة لتحديد المخاطر كجزء من عملية إدارة المخاطر على نطاق واسع.⁽⁴⁾

وبناءً على التقييمات لمستويات المخاطر لنظم المعلومات المحاسبية، يتم التوصل لنتائج يمكن استخدامها لتحسين أمن نظم المعلومات والضوابط والضمانات للحد من تلك المخاطر،⁽⁵⁾ فالهدف النهائي من تقييم المخاطر وإدارة المخاطر هو التأكد من وجود الضوابط التي تعمل على تحسين عملية اتخاذ القرارات في المنشآت وبالتالي تعزيز الأداء من وجهة نظر العديد من أصحاب المصلحة، ولا بد من إجراء تقييم المخاطر إلى فهم أفضل التدابير الأمنية المناسبة لحماية إطار أمن المعلومات: السرية والنزاهة والتوافر.⁽⁶⁾

ويوفر تقييم المخاطر أساساً لوضع السياسات المناسبة واختيار تقنيات فعالة من حيث التكلفة لتنفيذ هذه السياسات، ويقدم تقييم المخاطر وسيلة توفر لصانعي القرار المعلومات اللازمة لفهم العوامل التي يمكن أن تؤثر سلباً على العمليات والنتائج، وإصدار أحكام مستنيرة بشأن مدى الإجراءات اللازمة للتخفيف من المخاطر.⁽⁷⁾

إن تقييم المخاطر الأمنية هي الخطوة الأولى لتقييم وتحديد المخاطر والعواقب المرتبطة بنقاط الضعف، وتوفير أساس لإدارة التكلفة لإنشاء برنامج أمني فعال،⁽⁸⁾ فمن تقييم الخطر يستنتج مدير إدارة الخطر كيفية إيجاد توازن بين بين تكاليف استراتيجيات تخفيض الخطر والمزايا التي يمكن تحقيقها من وراء تنفيذ هذه الاستراتيجيات، فحجم تكاليف إدارة الخطر لتخفيض تهديد المعلومات يجب ألا تتجاوز قيمة الشيء الذي تتم حمايته من الخطر.

(1) نفس المرجع السابق، ص: 434-408.

(2) Lo, Chi-Chun & Chen, Wan-Jia (2012), " A Hybrid Information Security Risk Assessment Procedure Considering Interdependences Between Controls ", Expert Systems with Applications, No.39, PP:247-257, <http://www.elsevier.com/locate/eswa>

(3) Zhiwei, Yu & Zhongyuan, Ji,(2012),"A Survey on the Evolution of Risk Evaluation for Information Systems Security", OP.Cit, PP:1288-1294.

(4) National Institute of Standards and Technology: NIST, (July 2012), "Guide for Conducting Risk Assessments". OP. Cit.

(5) Lo, Chi-Chun & Chen, Wan-Jia,(2012), "A Hybrid Information Security Risk Assessment Procedure Considering Interdependences Between Controls", OP. Cit, PP: 247-257.

(6) Munteanu, Adrian,(2006),"Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma", Managing Information in Digital Economy: Issues & Solutions, OP. Cit, PP: 227-232.

(7) Murtaza, Mirza B. (2007),"Developing An IT Risk Assessment Framework", Review of Business Information Systems, Vol.11, No.4, Middle Tennessee State University, USA, PP:69-75.

(8) The Office of the Government Chief Information Officer, (2012),"Security Risk Assessment & Audit Guidelines", OP. Cit., P. 10.

ويوفر إطار تقييم المخاطر الأمنية هيكل شامل لتحليل المخاطر الأمنية التي من شأنها أن تساعد على كشف التهديدات ونقاط الضعف فتقييم المخاطر الأمنية هو خطوة هامة في عملية إدارة المخاطر الأمنية،⁽¹⁾ وهو جزءاً هاماً منها وضروري لفهم متطلبات أمن المعلومات، والمخاطر التي تتعرض لها أصول وأنشطة المنشأة.⁽²⁾ وتقييم المخاطر عملية تسمح لمديري تكنولوجيا المعلومات في تحقيق التوازن بين تكاليف تدابير الحماية وتحقيق مكاسب من تلك الحماية، لذلك تتجه العديد من المنشآت إلى العمل على تقييم المخاطر المرتبطة بتكنولوجيا المعلومات من خلال تحديد عوامل المخاطر لكل منطقة والتركيز على وضع الضوابط لضمان قدرتها على الاستمرارية، وبالتالي يجب أن يتم انتهاز خطوات لتقييم تلك المخاطر من أجل تحديدها وتقديرها وتخفيضها إلى أدنى حد ممكن ومقبول لديه،⁽³⁾ وتجرى عمليات تقييم المخاطر على أساس مستمر لتوفير المعلومات الهامة لصناع القرار التنظيمي للمساعدة في التوجيه والإعلام عن مخاطر أمن نظم المعلومات.

2-2-3: خطوات تقييم وإدارة مخاطر أمن نظم المعلومات المحاسبية المحوسبة:

تختلف مكونات ومراحل وخطوات تقييم وإدارة مخاطر أمن نظم المعلومات المحاسبية المحوسبة من منشأة إلى أخرى تبعاً لعوامل عديدة تتعلق بطبيعة المخاطر التي أظهرتها عملية تحليل المخاطر وما أظهرته إستراتيجيات الأمن الموضوعية في المنشأة، وتبعاً للنظام محل الحماية وما إذا كنا نتحدث عن نظم حاسوب مغلقة أم مفتوحة أو قواعد بيانات أو شبكات أو مزيج منها وما إذا كنا نتحدث عن نظام خدمة مخصص أم عن خدمات للعمامة عبر الشبكة خاصة كانت أم دولية وتبعاً لوظيفة التطبيق محل الحماية، إذ تتباين خطوات ومحتوى وعناصر خطط التعامل مع الحوادث لدى بنوك الإنترنت مثلاً عنها لدى المواقع المعلوماتية،⁽⁴⁾ ومع ذلك وبوجه عام فإن تقييم مخاطر أمن نظم المعلومات هي عملية متكاملة تتصل بأداء متواصل متدرج خاضع لقواعد محددة سلفاً ومتبعة بدقة وانضباط، وتشمل العديد من الأنشطة الرئيسية والتي تشكل إطاراً متكاملًا للتعامل مع المخاطر الأمنية ويعود متطلباً رئيسياً بالنسبة لمنشآت الأعمال كما في حالة المنشآت المالية، وهكذا، يمكن القول أن عملية تقييم المخاطر ينطوي على سلسلة من المهام موزعة على عدة مراحل،⁽⁵⁾ والتنفيذ غير الصحيح لأي مرحلة يمكن أن يؤدي ليس فقط إلى ضعف تحديد وتقييم المخاطر، ولكن أيضاً إلى فشل في خطط الأعمال التجارية في المستقبل،⁽⁶⁾ وقد تعددت آراء الباحثين المختلفين حول تحديد هذه الخطوات.

(1) Saleh, Zakaria I. & Refai, Heba & Mashhour, Ahmad, (2011), "Proposed Framework for Security Risk Assessment", *Journal of Information Security*, No.2, PP: 85-90, doi:10.4236/jis.2011.22008 Published Online April 2011, <http://www.scirp.org/journal/jis>

(2) Humphreys, Edward, (2010), *Information Security Risk Management, Handbook for ISO/IEC 27001*, OP. Cit., Available at: <http://shop.bsigroup.com/bip0076>

(3) الشرايري، عادل، (2009)، "سياسات وإجراءات التدقيق الداخلي في ظل بيئة تكنولوجيا المعلومات في البنوك الأردنية"، *مراجع سابق*، ص ص: 47-72.

(4) صقر، ممدوح الشحات، (2007)، "أمن المعلومات"، *مراجع سابق*، ص ص: 1-36.

(5) Shamala, Palaniappan & Ahmad, Rabiah & Yusoff, Mariana, (2013), "A conceptual Framework of Info Structure for Information Security Risk Assessment (ISRA)", *OP.Cit.*, PP: 45-52.

(6) Černá, Marie, (2012), "Information Risks and Their Connection With Accounting", *OP.Cit.*, PP: 375-382.

وسوف نستعرض أهم عناصر تقييم تلك المخاطر والتي تتمثل في عدة خطوات متسلسلة ومستمرة،⁽¹⁾ نذكر أهمها على النحو الآتي:⁽²⁾

2-2-3-1: توصيف أصول وعناصر النظام: يجب تحديد الأصول المهمة لكل دائرة، وهذه الأصول المهمة تشمل على: قطع الحاسوب، والبرامج، والنظم، والخدمات والتكنولوجيا المتعلقة بها وترتب تلك الأصول حسب أهميتها ودرجة حساسيتها وإمكانية الاستغناء عنها أثناء انجاز العمل، ومدة الاستغناء، ومدى فاعليتها.⁽³⁾

2-2-3-2: تحديد التهديدات ومواطن الضعف في النظام: تحديد التهديدات الأمنية ونقاط الضعف ينطوي على عملية رسمية لدراسة وتوثيق الوضع الأمني لنظم المعلومات في المنشأة، حيث تشمل عملية تقييم المخاطر تحديد أسباب ومصادر تلك المخاطر وهي تمثل العوامل والظروف التي تؤدي إلى نشأة المخاطر من مصدرها، سواء من البيئة الداخلية، أو البيئة الخارجية، ومن خلال فحص واستكشاف البيئتين الداخلية والخارجية اللتين تحكمان عمل منشآت الأعمال يمكن تحديد نقاط القوة ونقاط الضعف التي تتميز بها نظم المعلومات وكذلك التهديدات التي يمكن أن تتعرض لها،⁽⁴⁾ وبالتالي يجب معرفة الأحداث المؤثرة على مخاطر أمن نظم المعلومات واحتمال حدوثها وتكلفة تلك الأحداث وذلك من خلال إصلاح نقاط الضعف وتقييم الضوابط القائمة، ويجب على إدارة المنشآت ولاسيما المالية مثل البنوك أن تدرك مصادر التهديدات المحتملة والتي قد تستغل نقاط الضعف الموجودة للتسبب في وقوع المخاطر المختلفة، ومع ذلك يجب الأخذ في الاعتبار إن احتمال تلك التهديدات وتأثيراتها تختلف من منشأة لأخرى حسب الظروف الخاصة والمحيطية بكل منشأة.

إن تحديد مؤشرات حدوث المخاطر تمثل أحد الأعمال الهامة والضرورية والتي تتطلب مجهوداً كبيراً من المسؤولين عن إدارة المخاطر في المنشأة، ونجاح ذلك يؤدي إلى اتخاذ الخطوات اللازمة لمواجهة المخاطر المحتملة، وسيكون لذلك بلا شك نتائج طيبة على المنشأة.

إن تحليل مواطن الضعف واحتمالات تحولها إلى تهديدات حقيقية لأصول وعمليات نظم المعلومات التي تم تحديدها في الخطوة الأولى،⁽⁵⁾ والتي يمكن أن تؤثر على السرية والنزاهة أو توافر نظام المعلومات.⁽⁶⁾

ويرى الباحث أن تحديد تهديدات أمن نظم المعلومات المحاسبية يُعد الخطوة الأساسية في عملية تقييم المخاطر، وهي الخطوة الأهم لأن عدم تحديد أحد الظروف أو الأحداث السلبية المتوقعة يعني عدم تحديد المخاطر الناتجة عنها، وبالتالي عند حدوثها لن تستطيع الإدارة الاستجابة لها والتعامل معها بشكل فعال وفي الوقت المناسب.

(1) National Institute of Standards and Technology: NIST, (July 2012), "Guide for Conducting Risk Assessments", OP.Cit..

(2) Pandey, Santosh K.,(2012), "A Comparative Study of Risk Assessment Methodologies for Information Systems", OP.Cit., Vol.1, No.2, PP: 111-122.

& Lo, Chi-Chun & Chen, Wan-Jia,(2012), "A Hybrid Information Security Risk Assessment Procedure Considering Interdependences Between Controls", OP.Cit., PP: 247-257.

(3) الحسان، عطا الله أحمد، (2009)، "مدى تعامل مدققي أنظمة تكنولوجيا المعلومات بمعايير التدقيق الدولية الخاصة ببيئة أنظمة المعلومات للمحافظة على أمن وسرية المعلومات في البنوك التجارية الأردنية"، مجلة كلية بغداد للعلوم الاقتصادية، الإصدار (20)، كلية بغداد للعلوم الاقتصادية، بغداد، العراق، ص ص: 341-385.

(4) Zafar, Humayun, (2013), "Human resource information systems: Information security concerns for organizations", OP.Cit., PP: 105-113.

(5) ISO/IEC 27000, (2012), "Information technology - Security techniques -Information security management systems - Overview and vocabulary", OP.Cit., Available at: <http://www.27000.org>

(6) The Office of the Government Chief Information Officer,(2012), "Security Risk Assessment & Audit Guidelines", OP.Cit., P. 12.

2-3-2-3: تحديد المخاطر واحتمالية وأرجحية حدوثها: عرفنا فيما سبق إن المخاطر ما هي إلا حالة من عدم التأكد، فجميع عناصر المخاطر تتسم باحتمالية الحدوث، فالحدث الذي تنشأ عنه المخاطر يتسم بعدم التأكد، كما أن قيمة الخسارة التي تنتج عن تلك المخاطر محتملة وغير مؤكدة، فالخطر ينبع أساساً من عدم التأكد بسبب عدم القدرة على التنبؤ، وعدم توافر المعرفة الدقيقة اللازمة للتنبؤ، فإذا انعدم الشك وأصبح الشخص متأكداً تماماً بخصوص الظواهر المحيطة به لما كان هناك خطر على الإطلاق ولزال هذا اللفظ من الوجود، ويمكن التمييز بين المخاطر و حالة عدم التأكد أن المخاطر تتميز بالقابلية للقياس الكمي و التقدير الإحصائي على خلاف حالة عدم التأكد التي يصعب تقييم احتمالات وقوعها و تعتمد غالباً على الخبرة الشخصية، كما تتميز حالة المخاطر بتوفر بعض البيانات عن الحدث الذي يتم تقدير مخاطره في حين أن البيانات غالباً لا تكون متوفرة في حال عدم التأكد.⁽¹⁾

ومن متطلبات تقييم مخاطر أمن نظم المعلومات المحاسبية التعرف إلى أنواع المخاطر المتوقع حدوثها واحتمالية حدوثها، وطرق حدوث تلك المخاطر التي تتعرض لها تلك النظم،⁽²⁾ وتحديد المخاطر الأمنية هي مهمة معقدة، الأمر الذي يتطلب النظر في مجموعة متنوعة من العوامل، مثل مدى الثقة بالمستخدمين، وحساسية البيانات، ومدى متانة وفعالية نظام الرقابة الداخلية المستخدمة وقدرتها على منع أو اكتشاف أو معالجة تلك المخاطر،⁽³⁾ حيث يتم في هذه الخطوة تحديد المخاطر لكل الأصول التي تم حصرها كل على حده.

ويرى الباحث أن كل نوع من مخاطر نظم المعلومات المحاسبية يجب أن ينظر إليه بأبعاده الثلاثة وهي حجمه (جسامة نتائجه)، ومدته (تكرارية حدوثه)، واحتمالية حدوثه (*Probability*)، ولذلك فإن القياس الصحيح للمخاطر والذي يتم في الوقت المناسب يعتبر أمراً بالغ الأهمية في عملية تقييم المخاطر.

2-3-2-4: تحليل أثر حدوث المخاطر: وهي عبارة عن النتائج الملازمة لوقوع أحد المخاطر، فبعد التعرف على المخاطر المحتملة يجب أن تجرى عملية تقييم لها من حيث شدتها في إحداث الخسائر، وتحديد مستوى الأثر (*Impact*) الذي يمكن أن تحدثه التهديدات والثغرات الأمنية الخاصة بخطر معين، وخاصة تركيز الاهتمام على الجوانب الثلاثة وهي سرية وسلامة وتوافر نظم المعلومات،⁽⁴⁾ ويتم التركيز دائماً على المخاطر التي سيكون لها - في نهاية المطاف - تأثير اقتصادي سلبي وينتج عنها خسائر بسبب الإخلال باتفاقيات و فقدان السرية، والنزاهة، والخصوصية، أو إتاحة المعلومات لأفراد أو جهات لم يكن من المسموح لهم الاطلاع عليها، والأثر قد يكون إما ملموس مثل الأثر المالي أو غير ملموس مثل تأثير السمعة وتأثير كفاءة العمل،⁽⁵⁾ ولذلك يكون من السهل قياس هذه

(1) الشحادة، عبدالرزاق & العاصي، سعد، (2009)، "إطار متكامل لتقييم كفاءة نظم المعلومات المحاسبية في المؤسسات المصرفية في ظل الأزمة المالية العالمية - دراسة ميدانية على المصارف العاملة بمدينة حلب"، *مجلة كلية بغداد للعلوم الاقتصادية*، العدد (20)، كلية بغداد للعلوم الاقتصادية، ص: 15-48.

(2) الساكني، سعد & العواودة، حنان، (2012)، "مخاطر استخدام تكنولوجيا المعلومات وأثرها على أداء نظم المعلومات المحاسبية - دراسة تطبيقية لعينة من الشركات المساهمة المدرجة في بورصة عمان للأوراق المالية"، *مرجع سابق*، ص: 207-257.

(3) Khambhammettu, Hemanth, et al., (2013), "A framework for risk assessment in access control systems", *OP.Cit.*, PP: 1-18.

(4) The Office of the Government Chief Information Officer, (2012), "*Security Risk Assessment & Audit Guidelines*", Version: 5.0, The Government of the Hong Kong Special Administrative Region, September 2012, P. 12.

(5) NASTASE, Pavel & UNCHIAȘU, Simona, (2013), "Implications of the Operational Risk Practices Applied in the Banking Sector on the Information Systems Area", *OP. Cit.*, PP: 101-117.

التأثيرات وأحياناً أخرى يتعذر قياسها فتقييم شدة النتائج عادةً ما يكون صعب في حالة الموجودات غير المادية، ولكن يمكن تحليل وتقييم المخاطر مادياً وذلك بهدف اتخاذ القرار اللازم بخصوصها، ويتم الاستفادة من هذه الخطوة في خطوة أخرى مهمة هي ترتيب المخاطر من حيث أولويتها والذي بناء عليه يتم اتخاذ القرارات المناسبة لتخصيص المصادر المالية وغيرها حتى يتسنى تفاديها حسب الإمكانيات.⁽¹⁾

ويرى الباحث إن المخاطر المرتفعة تؤدي إلى قرارات منخفضة القيمة، حيث إن ارتفاع نسبة المخاطر في دورات نظام المعلومات المحاسبي سوف تخفض من قيمة البيانات وقيمة القرارات التي تعتمد عليها، وهذا يؤثر على مركز المنشأة المالي ويفقدها حصتها السوقية وميزتها التنافسية وترتفع تكاليفها التشغيلية.

وتعتبر نظم المعلومات المحاسبية المحوسبة من النظم الحرجة والأكثر حساسية والتي تعتمد عليه المنشأة في تلبية احتياجاتها وتتأثر به جميع أنشطة المنشأة، ومطلباً أساسياً للنظم الأخرى، ويؤدي توقفها إلى نتائج غير مرغوب فيها، ويتم حساب شدة تأثير المخاطر كما هو مبين أدناه:

شدة تأثير الخطر = قيمة الأصل X شدة التهديد X شدة ضعف إجراءات ووسائل الحماية

ويمكن استخدام جداول تحليل المخاطر والتي تظهر بالشكل التالي رقم (2-2-1) والتي تربط احتمال حدوث الخطر بالأثر الناجم عنه مع استغلال طرق أخرى لتقييم المخاطر كمياً.

لقد أظهرت الدراسات أن مرحلة تقييم المخاطر كمياً ضرورية في دورة تحليل وإدارة المخاطر وإن كانت تعتمد على فرضيات كثيرة ولكنها تؤدي إلى نتائج مناسبة.⁽²⁾

شكل رقم (2-2-1) تحليل أثر حدوث المخاطر

احتمال حصول الخطر			
	مرتفع	متوسط	متدني
	مرتفع	مرتفع	متدني
	مرتفع	متوسط	متدني
	متوسط	متوسط	متدني

الأثر المتوقع حدوثه

(1) أبو شنب، عماد، (2009)، "تحليل المخاطر لمشاريع أنظمة المعلومات"، مرجع سابق، ص5.

(2) نفس المرجع السابق، ص5.

2-2-3-5: تحديد الإجراءات الرقابية المطبقة حالياً: يتحقق أمن نظم المعلومات من خلال تنفيذ مجموعة من الضوابط - الفنية وغير الفنية - القابلة للتطبيق، والتي تشمل على السياسات والعمليات والإجراءات والهياكل التنظيمية والبرامج والأجهزة لحماية الأصول المعلوماتية التي سبق تحديدها،⁽¹⁾ فالضوابط الفنية هي الضمانات التي يتم دمجها في أجهزة الحاسوب والبرمجيات، أو البرامج الثابتة والضوابط غير التقنية هي الضوابط الإدارية والتشغيلية، ولذلك ينبغي تقييم الضوابط الأمنية لتحديد ما إذا كان يتم تنفيذ الرقابة بشكل صحيح، وهل تعمل على النحو المنشود، لتلبية الاحتياجات الأمنية للنظام.⁽²⁾

وتلك الضوابط يجب أن تكون متطورة بشكل مستمر بما يواكب مستجدات التطور التقني من خلال مراقبة المخاطر المفترضة والمتوقعة وابتكار حلول لها، فلا يوجد نظام معلومات آمن بشكل مطلق إذا لم يكن هناك مواكبة واستمرارية في التطوير لتقليل واحتواء المخاطر المفترضة أو المتوقعة.⁽³⁾

ويرى الباحث أن هذه الخطوة تنطوي على تحديد وسرد جميع الإجراءات والسياسات المتبعة والمعمول بها حالياً ويتم ذلك من خلال إجراء مقابلات واستخدام استبيانات أو استطلاعات مع الموظفين الرئيسيين لجمع المعلومات ذات الصلة عن الحالة الراهنة لتلك النظم، ويجب على المقيم اخذ هذه المعلومات والإجراءات بعين الاعتبار إذ عليه تضمينها لأنه وبدون تضمينها قد يأخذ فترة من الوقت لتحليل كل ما سبق والوصول لإجراء معين، قد يكون هو نفسه الإجراء المتبع.

2-2-3-6: ربط الضوابط الرقابية بالمخاطر: يتم خلال هذه المرحلة ربط المخاطر بالإجراءات الرقابية المطبقة للتعرف على المخاطر حسب درجة السيطرة عليها وتخفيف حدتها حيث يتم إعطاء كل إجراء رقابي يخفف من المخاطر درجة معينة من (1-5) بناءً على نوع الإجراء الرقابي وقدرته على تخفيف الخطر، وعند الانتهاء من ربط كافة المخاطر بالإجراءات الرقابية يمكننا احتساب الفجوة الرقابية والتي تمثل الفرق بين البيئة الحقيقية (ما هو كائن) والبيئة المستهدفة (ما يجب أن يكون)، كنسبة مئوية.

تقييم المخاطر يتضمن مدى المخاطر التي يمكن تحملها وبالتالي مستوى إجراءات السيطرة الأمنية المضادة التي يمكن تحملها فبعد تحديد المخاطر يجب اتخاذ الإجراءات الملائمة لمواجهة تلك المخاطر وتحديد مجموعة الأنظمة الرقابية التي تمنع الخسائر المترتبة عنها،⁽⁴⁾ وهي الحد الأدنى من متطلبات الأمن التي يجب أن تطبق على نظم المعلومات من أجل تحقيق الأمن الكافي، وهو الأمن الذي يتناسب مع خطورة وأهمية الضرر الناتج عن حدوث المخاطر وذلك يتطلب إجراء تقييم سنوي لنظام المعلومات ومدى الامتثال للمعايير والضوابط المطلوبة.⁽⁵⁾

(1) ISO/IEC 27000, (2012), "Information technology - Security techniques -Information security management systems - Overview and vocabulary", OP.Cit., Available at: <http://www.27000.org>

(2) Vacca, John R.,(2009), Computer and Information Security Handbook, OP.Cit , P.260.

(3) Van Niekerk, J.F. & Von Solms, R.,(2010), "Information security culture: A management perspective", Computer & Security, Vol.29, No.4., PP: 476-486.

(4) Committee of Sponsoring Organization of the Tread-way Commission (COSO), (2013), "Internal Control-Integrated Framework", OP.Cit., Available from http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf

(5) Hulitt, Elaine & Vaughn, Rayford B., (2010), Information system security compliance to FISMA standard: a quantitative measure, Telecomm un Syst , No. 45, PP: 139-152.

وخلال عمليات تقييم المخاطر يجب ترتيب المخاطر حسب درجة الخطورة وتحديد وسائل الأمان المعتمدة وتحديد وتقييم وسائل الأمان الجديدة أو الإضافية وتحديد مستوياتها بدرجة تتناسب مع التهديدات المتصورة بحيث تؤدي إلى وقاية نظام المعلومات بدرجة مقبولة،⁽¹⁾ فالحل الأمني الذي تقدمه التقنيات الحديثة يعتمد على العديد من العوامل منها مدى التهديدات والمخاطر التي يواجهها النظام الحالي للمنشآت أو حتى الأفراد، والحالة التقنية المتوفرة حالياً لحماية النظام ومدى قوتها لصدّ ومنع الخطر.⁽²⁾

وفي اعتقاد الباحث أن الضوابط الرقابية بالنسبة لبيئة نظم المعلومات المحاسبية يجب أن لا يتولد عنها تكاليف غير مباشرة أو يتولد عنها تأثير على الأداء أو القدرة الاستيعابية أو الوظيفية، وأن الوسيلة الأفضل لمواجهة المخاطر هي الأقل تكلفة، فليس من المتصور أن تتعدى تكلفة مواجهة المخاطر ما قد تسفر عنه المخاطر من خسائر، ولا بديل لتخفيض التهديدات سوى إجراءات الرقابة التي سوف تحد من المخاطر المتأتية من هذه التهديدات المحتملة.

بعد تنفيذ هذه الخطوات يتم الخلوص إلى تقرير يتضمن توصيات تعتمد على قابلية المنشأة للتعرض للخطر وعلى درجة الخطر التي تتعرض له حيث يتم تصنيف هذه الإجراءات حسب الشكل أدناه والذي يقيس علاقة القابلية بأثر الخطر، ونتائج التقرير تتراوح بين إجراء تحليلات مكثفة لدرجة المخاطر التي تتعرض له المنشأة إلى الإبقاء على وسائل وإجراءات حماية نظم المعلومات كما هي.⁽³⁾

شكل رقم (2-2-2) العلاقة بين مدى قابلية المنشأة للتعرض للمخاطر والأثر الناتج عن التهديدات



(1) Dai, Weihui, (2012), "Risk Management Model of Information Security in IC Manufacturing Industry", *OP. Cit.*, PP: 317-324.

(2) الطبطي، خضر مصباح (إسماعيل)، (2010)، "أساسيات أمن المعلومات والحاسوب"، مرجع سابق، ص 20.

(3) أبو شنب، عماد، (2009)، "إدارة وتحليل مخاطر أمن المعلومات"، *مؤتمر أمن المعلومات والحكومة الإلكترونية*، مرجع سابق، "ورقة عمل".

2-2-3-7: وضع استراتيجيات لضبط المخاطر: هي خطة على مستوى عال في المنشأة لحماية نظم المعلومات وهي مجموعة من القواعد التي تضعها المنشأة والتي يجب أن يطبقها المعنيون لدى التعامل مع التقنية والمعلومات داخل المنشأة وتتصل بشؤون الدخول إلى المعلومات والعمل على تنظيمها وإدارتها،⁽¹⁾ ويجب على المنشآت وضع تدابير كافية لضمان حماية أمن نظم المعلومات من خلال سياسة فعالة، وضوابط وإجراءات موحدة وهذا من شأنه ضمان تخفيض التهديدات،⁽²⁾ فمن الضروري للمنشآت أن تخطط للمستقبل ضد المخاطر الأمنية، من خلال مجموعة واسعة من الحماية التقنية أو تشفير جدار الحماية ومع ذلك، فمن المهم أن ندرك أن استخدام هذه التقنيات يتطلب تخطيطاً دقيقاً ومنهجية، وهذا يؤدي إلى أن تكون قادرة على تنفيذ الضوابط المناسبة داخل المنشأة،⁽³⁾ فإذا تم تحديد مصادر الخطر ومسبباته ثم تحليل الخطر وقياسه يمكن اقتراح وتطبيق استراتيجيات معينة لتخفيض درجة الخطورة، فإذا أظهر تحليل الخطر ارتفاع مستوى درجة الخطورة من حيث حجم الخسارة المتوقعة وكذلك احتمال حدوث الخسارة يصبح من الضروري اتخاذ كافة الإجراءات اللازمة والسياسات الممكنة لمنع حدوث ذلك الخطر، وتتضمن استراتيجيات ضبط المخاطر أخذ قرارات تتعلق باختيار مجموعة الطرق والأساليب التي ستتبع للتعامل مع المخاطر، وكل قرار يجب أن يسجل ويوافق عليه من قبل المستوى الإداري المناسب، وعلى الخطة أن تقترح وسائل تحكم أمنية تكون منطقية وقابلة للتطبيق من أجل إدارة المخاطر حيث تقوم إدارة المنشأة باختيار الاستجابات للمخاطر - التجنب، القبول، التخفيض، أو المشاركة - تطوير مجموعة من التصرفات للمخاطر القائمة مع المخاطر المحتملة والقابلية للمخاطر في المنشأة.

وتشمل إستراتيجية حماية أمن نظم المعلومات مستويين رئيسيين هما مستويات الأمن العامة، كالأمن المادي والأمن الشخصي للأفراد والأمن الإداري والأمن الإعلامي (أو الإعلان)، كما تشمل مستويات أمن التطبيقات، كأمن المدخلات وأمن المعالجة وأمن المخرجات وأمن التخزين وأمن التبادل، ويتعين أن تكون نظم الأمن التطبيقية متكاملة مع بعضها البعض ومع نظم الأمن العامة حتى تحقق الوقاية المطلوبة لأنها بالعموم تتطوي أيضاً على اتصال وارتباط بمستويات الأمن العامة، ويمكن تجميع استراتيجيات الاستجابة في أربع مجموعات عريضة وهي:

1. تجنب أو تفادى المخاطر (Avoidance): (تأثير أعلى ، إحصائية أعلى): وهو أكثر الدرجات فاعلية لأنه يهدف إلى منع وجود الخطر، وفي بعض الأحيان يتعذر تحقيق هذا الهدف بشكل عملي لأنه يتطلب الكثير من المال والأفراد لتطبيق الإجراءات المطلوبة وفي هذه الحالة لابد أن تدرس المنشأة المنفعة والعائد ، لأن ذلك قد يكلف المنشأة الكثير، فإذا أظهر تحليل الخطر ارتفاع مستوى درجة الخطر من حيث حجم الخسارة المتوقعة وكذلك

(1) الخضيري، سليمان، (2013)، الشامل، مرجع سابق، ص: 16-18.

(2) Muhrtala, Tijani & Ogundeji, Mathias, (2013), "Computerized Accounting Information Systems and Perceived Security Threats in Developing Economies: The Nigerian Case", *OP. Cit.*, PP: 9-18.

(3) Maram, Venkata et al., (2012), "A Study of Risk Management of an Information System by Assessing Threat, Vulnerability and Countermeasure", *OP. Cit.*, PP: 51-53.

احتمال حدوث الخسارة يصبح من الضروري اتخاذ كافة الإجراءات اللازمة والسياسات الممكنة لمنع حدوث ذلك الخطر.⁽¹⁾

2. **تخفيف المخاطر (Reduction):** وهذا يعني تمكين المختصين في إدارة المخاطر من السيطرة وتخفيض الدرجة الاحتمالية للخطر باتخاذ إجراءات وقائية مناسبة ومدروسة مثل تركيب أجهزة الإنذار واستخدام الحراس الليليين وتركيب أجهزة مكافحة الحرائق، وتلجأ إليه المنشأة لتقليل معدل حدث الخطر أو الخسائر المالية في حالة حدوثه، وبعض المخاطر لا يمكن القضاء عليها تماماً، وبالتالي تحتاج إلى تخفيضها لمستويات مقبولة، من خلال عمل كل الاحتياطات لعدم حدوث الخطر أو معالجة آثاره في حال حدوثها، بتنفيذ ضوابط التخفيف من المخاطر.⁽²⁾

3. **نقل ومشاركة المخاطر (Transfer & Sharing):** (تأثيرها كبير، واحتمالية منخفضة): إذا كانت قيمة الخطر مرتفعة من حيث حجم الخسارة المتوقعة ولكن احتمال حدوثها منخفض عندها ينصح القيام بإجراءات التأمين، ويمكن أيضاً أن يتم نقل جزء من المخاطر من طرف إلى طرف آخر أفضل تجهيزاً أو أكثر استعداداً لتحمل ذلك، وهي وسائل تساعد على قبول الخطر من قبل طرف آخر، من خلال توزيع المخاطر بنقلها إلى طرف آخر، والتي تستهدف خطر محدد، فبعض المخاطر لا يمكن منعها أو اكتشافها، فيتم تخفيض تأثيرها بتحويلها أو بمشاركة جزء منها، من خلال شراء بوليصة التأمين أو الاستعانة بمصادر خارجية أو كفالات وضمانات الموردين أو الحكومة.⁽³⁾

4. **قبول المخاطر (Acceptance):** (تأثير أدنى، احتمالية أدنى): تشير المخاطر المتبقية إلى مستوى المخاطر التي تبقى بعد اتخاذ التدابير الكافية ومن المستحيل أن يكون هناك نظام أو بيئة آمنة 100 % وبالتالي يجب أن يكون هناك مستوى مقبول من المخاطر، حيث ترى بعض المنشآت الاحتفاظ بالخطر الاحتمالي وتحمل عبء الخسارة بكاملها في حال حدوثه، ويقبل احتمال وتأثير المخاطر من خلال عدم التحرك لمنع الخطر أو تخفيف حدته رغم إدراك المنشأة لذلك الخطر، وتعني قبول عبء الخسائر عند حدوثها من خلال عدم عمل أي تصرف لتخفيض احتمالية المخاطر أو تأثيرها وتعايش المنشأة معها، وهذا يتم عندما تكون الإدارة مضطرة إلى قبول مستوى معين من المخاطر ويكون ذلك في الحالات التي تكون آثار المخاطر السلبية فيها قليلة، ولكن كلفة معالجتها عالية.⁽⁴⁾

ويضيف الباحث أنه ليس من الممكن تحديد جميع المخاطر، كما أنه ليس من الممكن القضاء على كل المخاطر وما تبقى من مخاطر يسمى المخاطر المتبقية، وإدارة المخاطر المتبقية هي جوهر إدارة المخاطر، ويجب أن يتم مراجعة ظروف و بيئة المخاطر بصورة دورية، لفترة لا تزيد عن عام من تاريخ قرار قبول المخاطر وتحديد هل المخاطر لازالت موجودة، و ما إذا كان بالإمكان التخفيف منها بتطبيق الضوابط المقترحة.

(1) Vacca, John R.,(2009), *Computer and Information Security Handbook*, OP. Cit., P. 8.

(2) Dahbur, Kamal & Mohammad, Bassil & Tarakji, Ahmad,(2011), "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing", *OP. Cit.*

(3) الدلاهمة، سليمان مصطفى، (2008)، "أساسيات نظم المعلومات المحاسبية وتكنولوجيا المعلومات"، مرجع سابق، ص ص 664-665.

(4) Vacca, John R.,(2009), *Computer and Information Security Handbook*, OP. Cit., P. 8.

2-2-3-8: الرصد والمتابعة (*Monitoring Risks*) :

استشارة الطبيب للحصول على التشخيص بدون الحصول على دواء ولذلك هناك خطوة تكون متوازية من بداية أول خطوة إلى انتهاء آخر خطوة في التقييم وهي خطوة تتمثل في رصد ومتابعة المخاطر من خلال متابعة الأنشطة والوسائل الرقابية وتحديثها كلما تطلب الأمر ذلك، وتلك العمليات يجب أن تكون متطورة بشكل مستمر بما يواكب مستجدات التطور التقني من خلال مراقبة المخاطر المفترضة والمتوقعة وابتكار حلول لها، فلا يوجد نظام معلومات آمن بشكل مطلق إذا لم يكن هناك مواكبة واستمرارية في التطوير لتقليل واحتواء المخاطر المفترضة أو المتوقعة.⁽¹⁾

2-2-3-9: تقرير المخاطر (*Reporting Risks*):

التقرير النهائي لتقييم المخاطر والنتائج الواردة فيه لمعالجة نقاط الضعف ومساعدة المنشأة في إدارة مخاطرها، من خلال توثيق وتسجيل نتائج تقييم المخاطر بشكل يبين تفاصيل طريقة التقييم، وذلك لتتمكن إدارة المنشأة من ترتيب وتصنيف المخاطر حسب درجة أهميتها وخطورتها على أعمال المنشأة، بحيث تستطيع الإدارة معالجة المخاطر حسب الأولوية والأهمية وفي الوقت المناسب، أو عدم معالجتها في حالة المخاطر غير الهامة.⁽²⁾

إن النتائج وثيقة من وثائق تحليل المخاطر ولذلك، فإننا يفترض أنها سوف تعزز تحليل مخاطر الأمن الشامل،⁽³⁾ وإن تقديم تقارير دورية عن الوضع الأمني في النظام مسؤولية تنظيمية وعلى المنشآت أن تعمل على إيجاد نظام معلومات قادر على تحديد وقياس مخاطر المعلومات بدقة، وبنفس الوقت والأهمية أن يكون قادر على مراقبة التغيرات المهمة في وضع المخاطر لديها، فالرقابة على المخاطر تعني تطور أنظمة التقارير في المنشأة التي تبين التغيرات المعاكسة في المخاطر التي تواجهها المنشأة وبالتالي تحديد الإجراءات والاستعدادات المتوفرة لدى البنك للتعامل مع هذه التغيرات، حيث يشتمل التقرير المذكور الناتج عن تقييم التهديدات والمخاطر على ما يلي:⁽⁴⁾

1. وصف للخطر الذي درسته، ومصدر الخطر، ودرجة الخطورة (يمكن استعمال مقياس متدرج).
2. وسائل وإجراءات الحماية التي تم توظيفها وتطبيقها (الضوابط الحالية)، والجهة المعنية بذلك.
3. ما هي التوصيات الخاصة بالتعامل مع الخطر في حالات مماثلة (الضوابط المقررة).
4. المدة الزمنية التي تتطلبها عملية التعامل معه (والتي يمكن أن تشمل إزالته، أو التخفيف من تأثيره أو تحييده)
5. ما الذي تم فعله للتخلص من الخطر لاستخدامه في حالات مماثلة.

(1) Van Niekerk, J.F. & Von Solms, R., (2010), "Information security culture: A management perspective", *OP. Cit.*, PP: 476-486.

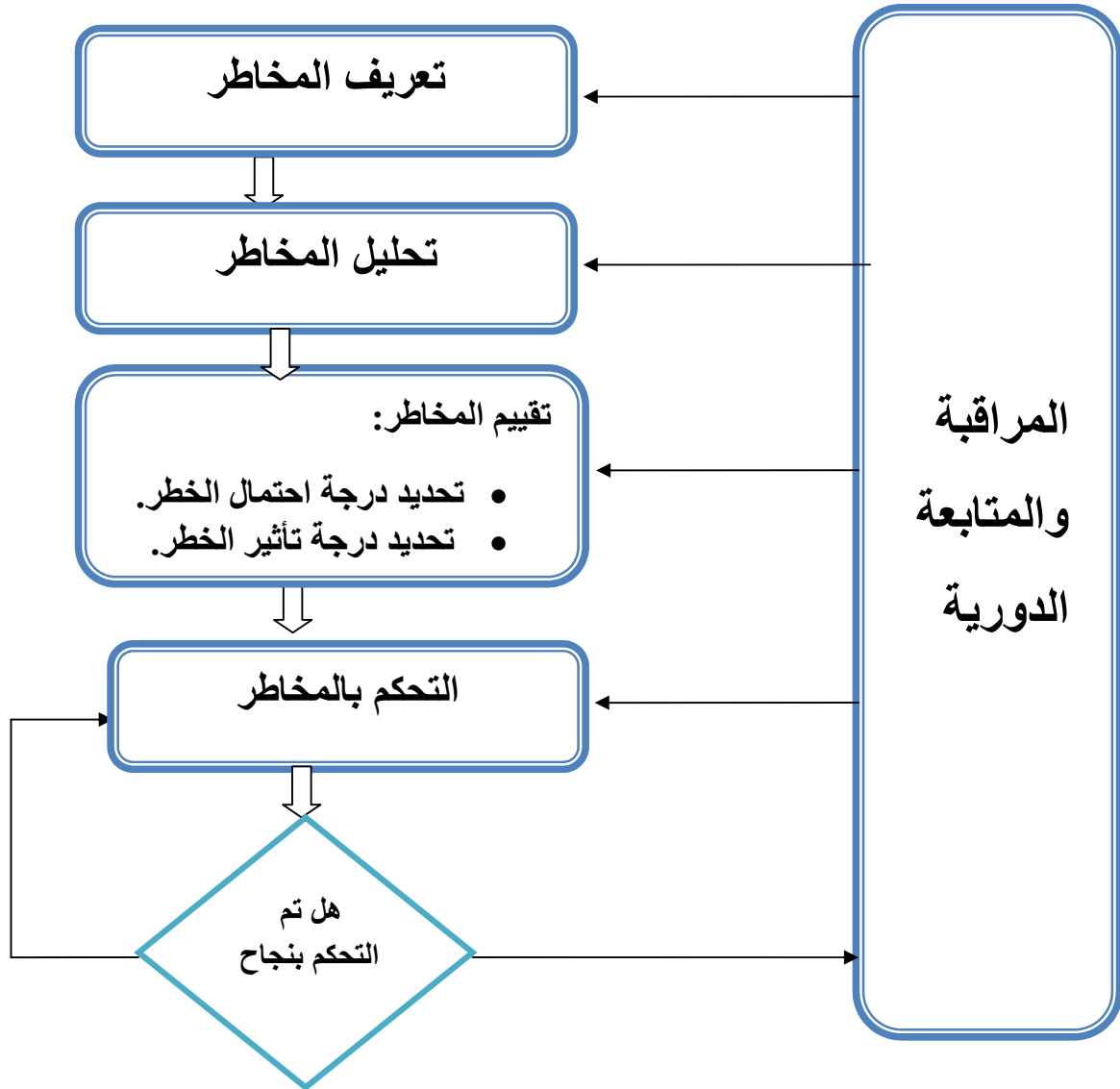
(2) National Institute of Standards and Technology: NIST, (July 2012), "*OP. Cit.*", Revision. 1.

(3) Zafar, Humayun, (2013), "Human resource information systems: Information security concerns for organizations", *OP. Cit.*, PP: 105-113.

(4) The Office of the Government Chief Information Officer, (2012), "*Security Risk Assessment & Audit Guidelines*", *OP. Cit.*, P. 34.

ويمكن تلخيص مراحل تقييم وإدارة مخاطر أمن نظم المعلومات المحاسبية كما في الشكل التالي:

شكل رقم (3-2-2) مراحل تقييم وإدارة مخاطر أمن نظم المعلومات المحاسبية ⁽¹⁾



(1) عاطف، عبد المنعم & الكاشف، محمد & سيد، كاسب، (2008)، "تقييم وإدارة المخاطر"، الطبعة الأولى، مركز تطوير الدراسات العليا والبحوث، جامعة القاهرة، مصر، ص7.

2-2-4: أدوات تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة:

يجب على المنشآت في البداية أن تتعرف على كل التهديدات والمخاطر التي يمكن أن تواجهها وبالتالي تقرر الآلية المناسبة لاختيار أفضل الأدوات التي تلائمها من أجل ضمان أمن وسلامة نظم معلوماتها وعملائها⁽¹⁾، على الإدارة العليا في أي منشأة أن تقرر الأسلوب والمنهج الأمثل في إدارة المخاطر ومدى تكثيف الأساليب⁽²⁾. ولكي يتم تحقيق هذا الهدف لا بد من تحديد أدوات وتقنيات ووضع وسائل ذات كفاءة عالية للرقابة والسيطرة على النظام ككل وذلك من أجل حمايته أمنياً ووظيفياً⁽³⁾ ومن تلك الأدوات ما يلي:

1. **قائمة الاستقصاء:** وهي مجموعة من الأسئلة المكتوبة والتي تتعلق بكافة المجالات من حيث المخاطر وأسبابها وآثارها والأنشطة الخاصة بالرقابة الداخلية، فيتم توجيه الأسئلة وتكون الإجابة بنعم أو لا وعند توفر الإجراء الرقابي تكون الإجابة بنعم وإذا لم يتوفر الإجراء تكون الإجابة بلا، ورغم سهولة الاستقصاء كوسيلة لفهم النظام وسهولة الرجوع إليها وشموليتها على تفاصيل كثيرة إلا أنه يغاب عليها أنها تتعلق بأجزاء من النظام ولا تظهر النظام كوحدة واحدة مترابطة، ويجب على أسئلة الاستقصاء أن تكون شاملة عن جميع المخاطر المتوقعة والمحتملة في الكشف عن كافة الحالات المعنية في التحليل⁽⁴⁾.
 2. **المقابلات الشخصية:** يتم إجراء تقييم نوعي غير كمي من خلال مقابلات مع موظفي دعم نظام تكنولوجيا المعلومات وإدارة شؤون الموظفين يمكن تمكين الأفراد القائمين بتقييم المخاطر لجمع معلومات مفيدة حول نظم تكنولوجيا المعلومات (على سبيل المثال، كيف يتم تشغيل نظم المعلومات وإدارتها)⁽⁵⁾.
 3. **مصفوفة درجات شدة المخاطر:** وهناك العديد من الطرق الإحصائية التي يمكن بواسطتها تقييم درجة المخاطر لكن أبسطها وأكثرها فعالية هو وصف درجة المخاطر بأنها عالية جداً، عالية، متوسطة، منخفضة، منخفضة جداً، وتقييم درجة المخاطر تعتمد على خاصيتين هما درجة احتمال حدوث الخطر ودرجة تأثير الخطر⁽⁶⁾ ويصنف كلا من حدوث الخطر وتأثيره بأنه عالي ومتوسط ومنخفض، ويجب أن تُقيم المخاطر بطريقة وصفية (Qualitative) وبصورة منتظمة وحيثما أمكن يتم التقييم بطريقة كمية (Quantitative) ويجب أن يأخذ تقييم المخاطر في الحسبان تأثير الأحداث المتوقعة وغير المتوقعة.
- وحتى تستطيع الإدارة تقييم المخاطر بالشكل الصحيح لابد من توفر هيكلية واضحة لكل من احتمال حدوث الظروف والأحداث المسببة للمخاطر من جهة، ودرجة التأثير من جهة أخرى.

(1) الطيطي، خضر مصباح إسماعيل، (2010)، "أساسيات أمن المعلومات والحاسوب"، مرجع سابق، ص52.
 (2) Osunmuyiwa, Olufolabi, (2013), "Online Banking and the Risks Involved", *Research Journal of Information Technology*, Vol. 5, No. (2), June 2013, PP: 50-54.
 (3) ياسين، سعد غالب، (2010)، *تحليل وتصميم نظم المعلومات*، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان، الأردن ص233.
 (4) Munteanu, A. & Fotache, D. & Dospinescu, O., (2008), "Information Systems Security Risk Assessment. Harmonization with International Accounting Standards", *OP. Cit.*
 (5) National Institute of Standards and Technology (NIST), (2006), "*Risk Management Guide for Information Technology Systems*", Special Publication (SP) 800-30, USA.
 (6) عاطف، عبد المنعم & الكاشف، محمد & سيد، كاسب، (2008)، "*تقييم وإدارة المخاطر*"، مرجع سابق، ص 13.

وهناك شكل يشبه المصفوفة الثلاثية البسيطة بإشارة المرور حيث أن الأحداث التي تقع ضمن منطقة الضوء الأحمر والبرتقالي تعبر عن مخاطر تأثيرها السلبي واحتمال حدوثها كبير، بينما التي تقع ضمن منطقة الضوء الأصفر تعبر عن درجة متوسطة لتأثير المخاطر واحتمال وقوعها، وأحداث منطقة اللون الأخضر والأزرق للمخاطر الخفيفة، ويوضح ذلك الشكل التالي:

الشكل رقم (2-2-4) مصفوفة تقييم شدة المخاطر

تأثير الخطر / الخطر	مرتفع (H) HIGH	متوسط (M) MEDIUM	منخفض (L) LOW
مرتفع (H) HIGH	مرتفع جداً	مرتفع	متوسط
متوسط (M) MEDIUM	مرتفع	متوسط	منخفض
منخفض (L) LOW	متوسط	منخفض	منخفض جداً

4. التقييم الآلي بواسطة النظم الخبيرة: يتم ذلك عن طريق تحليل البيانات ووضع التوصيات من خلال مرحلتين رئيسيتين هما: (1)

1. مرحلة جمع بيانات: الأنشطة الأولية تشمل الضوابط الحالية وتحديد الخسارة المحتملة.

2. مرحلة التحليل: تشمل قياس أي ثغرات بين مدى كفاية الضوابط الحالية على النحو المستمد من إجابات الاستقصاء، والسياسات المطلوبة وإنشاء تطبيقات وتوصيات أمنية إضافية.

ويمكن إجراء التقييم الكمي أو التقييم النوعي باستخدام برمجيات مخصصة لتحسين أمن نظم المعلومات المحاسبية، ولكن ليس تقييم المخاطر الكاملة لنظام المعلومات. (2)

التقييمات الآلية كأداة للحصول على معلومات الامتثال للسياسة الأمنية تصبح أكثر استخداماً على نطاق واسع، ويمكن توقع أن المعلومات التي تم جمعها سيتم جنباً إلى جنب مع البيانات التي تم جمعها بواسطة نظم رصد أحداث

(1) Jaisingh, Jeevan & Rees, Jackie, (2001), "Value at Risk: A Methodology for Information Security Risk Assessment", Krannert Graduate School of Management, Purdue University, West Lafayette, PP:3-4,

https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/bibtex_archive/2001-127.pdf

(2) Munteanu, A. & Fotache, D. & Dospinescu, O., (2008), "Information Systems Security Risk Assessment. Harmonization with International Accounting Standards", OP. Cit.

الأمان (أنظمة كشف التسلل، الجدران النارية للحماية، وما إلى ذلك)، ومن المتوقع يوماً ما أن تدرج هذه الأدوات ضمن نماذج جديدة لتحليل التهديد بشكل كمي، مما يعني أن عملية التقييم ستصبح مؤتمتة بالكامل.⁽¹⁾

الخاتمة:

من خلال ما سبق عرضه يتبين لنا أن كل منشأة اقتصادية قائمة حالياً تواجه مخاطر على نشاطها من مختلف الأنواع سواء أكانت تنافسية، تكنولوجية، اقتصادية، أو تغيرات بيئية في ظل العولمة والعالم سريع التغير والنمو والتطور وبالتالي إن المنشآت الاقتصادية يتحتم عليها إجراء الفحص البيئي المستمر الداخلي والخارجي لتحديد نقاط قوتها والعمل على دعمها وزيادتها وتحديد نقاط ضعفها والعمل على تقليصها وكذلك تحديد الفرص المتاحة للمنشأة التي يمكن اقتناصها وقبل أن يختطفها المنافسون وإيجاد الوسائل الفعالة للفوز بها وكذلك تحديد التهديدات التي يمكن أن تتعرض لها المنشأة من البيئة الخارجية وما هي خطط الطوارئ المعدة لمواجهة مثل تلك المخاطر إن وقعت.

إن الدقة في تحديد نقاط القوة ونقاط الضعف والفرص والتهديدات أمر حيوي، في ظل الظروف السائدة الآن، لضمان سلامة نظم أي منشأة وديمومتها وهذه الدقة تعتمد أساساً على الطرق والأساليب المتبعة لفحص البيئتين الداخلية والخارجية ومستوى استمرارية هذا الفحص وفترته الزمنية والفريق الذي يقوم به ومستوى تأهيله وكفاءته.⁽²⁾

ولذلك يرى الباحث بأن على البنوك التجارية أن تعمل على تقييم كافة مخاطر أمن نظم المعلومات المحاسبية المحوسبة لديها باستمرار، من خلال تحديد المخاطر وتحليلها وقياسها وترتيبها وفق الأولويات ليتم التعامل معها حسب أهميتها، ويفضل أن يكون التقييم مبني على تحليل كمي قدر الإمكان، وفي جميع الأحوال لا بد من وضع سياسات وآليات وطرق واضحة لإدارة تلك المخاطر، على أن تختبر جودة تلك السياسات والطرق، ليكون لدى إدارات تلك البنوك صورة واضحة عن كيفية التعامل معها بشكل كفء وفعل في الوقت المناسب.

(1) Bonnette, Cynthia A., (2006), *"Assessing Threats to Information Security in Financial Institutions"*, SANS Technology Institute, 31 May 2006, USA, PP.7- 12.

(2) يوسف، عبد الستار حسين، (2007)، "تقدير المخاطرة في ظل تحليل (SWOT) في المؤسسات الصناعية- دراسة تحليلية"، المؤتمر العلمي الدولي السنوي السابع- إدارة المخاطر واقتصاد المعرفة، مرجع سابق، "ورقة عمل".

2-3: المبحث الثالث: تأثيرات حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة

إن أمن نظم المعلومات المحاسبية المحوسبة يجب أن يكون مبنياً على المكونات الأساسية والتي يعتمد عليها كل نظام للحاسوب وأهمها السرية وسلامة البيانات وإتاحة البيانات، فكل منشأة بحاجة إلى تنظيم وتنسيق ووضع قوانين صارمة للحفاظ على سرية وسلامة وإتاحة البيانات للمستخدمين الشرعيين وهذا يحتاج إلى إدارة ناجحة وإستراتيجية متينة وقوية يتم تطبيقها من أجل الوصول إلى مرحلة من النضج في نظام أمن الحاسوب.⁽¹⁾

وقد عرفنا أن نظم المعلومات المحاسبية تتعرض للعديد من المخاطر والتي تشغل بال معظم المنشآت المتطورة في العالم والتي تعتمد على التكنولوجيا المتقدمة في تعاملها مع الأطراف المختلفة،⁽²⁾ سواء كانت تلك المخاطر نتيجة تهديدات داخلية من داخل المنشأة ذاتها، أو بسبب تهديدات خارجية تتعلق بالبيئة التي تعمل بها المنشأة، ولا شك أن تلك المخاطر من شأنها أن تنعكس وتؤثر سلبياً على كفاءة وفعالية نظام المعلومات المحاسبية، وعلى جودة المعلومات التي يفرزها النظام وعلى موثوقية البيانات المخزنة،⁽³⁾ فتطور وسائل تكنولوجيا المعلومات والاتصالات وتزايد استخدامها في نظم المعلومات المحاسبية، سهّل بشكل كبير خزن واسترجاع وتعديل ونسخ المعلومات والوصول إليها، مما جعل تلك النظم عرضة للعديد من التهديدات الداخلية والخارجية والتي تسبب مخاطر تؤثر على سرية وموثوقية وسلامة محتوى وتكامل وتوافر المعلومات المحاسبية.

إن المخاطر والضوابط المستخدمة في نظم المعلومات المحاسبية تؤثر تأثيراً كبيراً على نوعية نظام المعلومات المحاسبية،⁽⁴⁾ وتكمن خطورة مشاكل أمن المعلومات في عدة جوانب منها تقليل أداء الأنظمة الحاسوبية، أو تخريبها بالكامل؛ مما يؤدي إلى تعطيل الخدمات الحيوية للمنشأة، أما الجانب الآخر فيشمل سرية وتكامل المعلومات حيث قد يؤدي الاطلاع والتصنت على المعلومات السرية أو تغييرها إلى خسائر مادية أو معنوية كبيرة،⁽⁵⁾ فمخاطر نظم المعلومات المحاسبية قد يكون لها أثراً مالياً أو أثراً على السمعة أو أثراً قانونية أو أثراً على العملاء أو أثراً على المنافسة،⁽⁶⁾ والخطوة الرئيسية في قياس مستوى المخاطر هو تحديد الآثار السلبية الناجمة عن ممارسة التهديدات ناجحة لوجود ثغرات أمنية،⁽⁷⁾ وبصفة عامة تؤثر المخاطر تأثيراً سلبياً

(1) الطيطي، خضر مصباح إسماعيل، (2010)، "أساسيات أمن المعلومات والحاسوب"، مرجع سابق، ص 22.

(2) Zainol, Zaini & Nelson, Sherliza & Malami, AbuBakar, (2012), "Internal Human Based Threats and Security Controls in Computerized Banking Systems: Evidence from Malaysia", *OP. Cit.*, PP: 199 –204.

(3) Gerić, Sandro & Hutinski, Željko, (2007), Information System Security Threats Classifications, *OP. Cit.*, PP: 59-60.

(4) Wahyudi, Ilham, (2016), "Do Risk Controls and User's Competence Affecting Accounting Information System Quality?." *IJA B.E.R.*, Vol. 14, No. 3, Pp: 1561-1569

(5) Al Hanini, Eman, (2012), "The Risks of Using Computerized Accounting Information Systems in the Jordanian Banks: Their Reasons and Ways of Prevention", *OP. Cit.*, PP: 53-63.

(6) عيسى، علا & عاشور، عصاف، (2010)، "مخاطر نظم المعلومات المحاسبية وحوكمة الشركات ومواجهة الأزمة المالية العالمية"، مرجع سابق، ص 434-408.

(7) National Institute of Standards and Technology: NIST, (July 2012), "*Guide for Conducting Risk Assessments*", *OP. Cit.*, Revision. 1.

على أمن نظم المعلومات وبالأخص في ثلاثة جوانب أساسية هي إتاحة النظام وسرية وسلامة البيانات والمعلومات المحاسبية وتكاملها.⁽¹⁾

فنظم المعلومات المحاسبية في المنشآت الاقتصادية المختلفة تتعرض كغيرها من النظم في عصر التطور التكنولوجي للعديد من المخاطر التي قد تؤدي إلى توقفها عن العمل فترات قد تقصر أو تطول، وقد تؤدي إلى ضياع البيانات والمعلومات المخزنة بها، وربما تؤدي بعض المخاطر إلى تلف البنية التحتية لنظم المعلومات المحاسبية، وهذا من شأنه أن يؤدي إلى توقف المنشآت عن القيام بأعمالها، أو تعطيل تلك الأعمال لفترة طويلة مما سينتج عنه خسائر كبيرة قد تؤدي أحياناً إلى خروج المنشآت التي تتعرض نظمها المحاسبية للكوارث من السوق بالإعلان عن إفلاسها خلال فترات غير طويلة.

حيث تتأثر سرية النظام وسلامته وتكامله وكذلك إتاحتها أو توافره بالإضافة إلى عدم الرفض والاعتمادية، وذلك بشكل عام يؤثر سلباً على تحقيق أهداف المنشأة،⁽²⁾ وكلما زاد اعتماد المنشآت على التكنولوجيا في تنفيذ أنشطتها فإن السرية والدقة لنظم المعلومات المحوسبة ستكون مقلقة وحرجه والنظام غير الموثوق به يصدر سلسلة من الأحداث ذات التأثير السلبي على المنشأة وزبائنها ومجهزيها والأطراف ذات العلاقة بها.⁽³⁾

وقد صاحب اعتماد المنشآت المصرفية على النظم المحوسبة، وشبكات المعلومات، تخوف من قدرة البنوك في الحفاظ على سرية المعلومات المخزونة بأجهزتها ودقتها وسلامتها، وعدم تسريبها أو تغييرها أو حذفها نتيجة للمخاطر التي تتعرض لها هذه الأجهزة والنظم من قبل المتسللين عبر الشبكات، والعابثين من داخل المنشآت المصرفية، وفي المقابل أيضاً - نشأت مشكلة أخرى متمثلة في عمليات توثيق الحركات المالية، المتعلقة بالعملاء، لنكران بعضهم ورفضهم لبعض العمليات والحركات المالية التي تنشأ منهم عبر الشبكات.

وسوف ننطلق في مناقشتنا لكيفية تأثير المخاطر التي تتعرض لها نظم المعلومات المحاسبية من المبادئ الخمسة السابق ذكرها لتحقيق أمن وموثوقية نظم المعلومات ال، فمن أهم الطرق الشائعة لعرض تأثيرات المخاطر على أمن نظم المعلومات هي فقدان السلامة والتكامل أو فقدان الإتاحة والتوافر أو فقدان السرية والخصوصية أو مزيج من فقدان وتدهور عناصر الأمن.⁽⁴⁾

وفي هذا المبحث سيتم التطرق لأهم التأثيرات التي يمكن أن تحصل نتيجة حدوث التهديدات والمخاطر السابق ذكرها على أمن نظم المعلومات المحاسبية وذلك على النحو التالي:

(1) Brandas, C. & Stirbu, D. & Didraga, O., (2013), "Integrated Approach Model of Risk, Control and Auditing of Accounting Information Systems", OP. Cit., PP: 87-95.

(2) Drtil, Jan, . (2013) "Impact of Information Security Incidents - Theory and Reality", Journal of Systems Integration, NO.1, University of Economics, Prague, Czech Republic, PP: 44-52.

(3) الجوهر، كريمة & البلداوي، شاكر & البلياتي، محمود جلال، (2011)، "دور المدقق الداخلي والخارجي في إدارة مخاطر التكنولوجيا - دراسة تحليلية مقارنة"، مرجع سابق، ص ص: 22-35.

(4) Abu-Musa, Ahmad A., (2010), "Investigating Adequacy of Security Controls in Saudi Banking Sector: An Empirical Study", OP. Cit., PP: 1-41.

2-3-1: تأثير المخاطر على إتاحة نظم المعلومات المحاسبية المحوسبة:

يعني إتاحة المعلومات أنها متوفرة ومتاحة (*Availability*)، ويمكن الاستفادة منها والحصول عليها دون أن يتم الاعتراض أو الامتناع عن إعطائها بالكامل أو حذف جزء منها، حيث تعتمد المنشآت في عصرنا في ممارسة أنشطتها على استخدام الحاسوب وهو ما يتطلب جعله متاحاً لمستخدميه طيلة الوقت، ولكن في حال حدوث المخاطر التي تتعرض لها نظم المعلومات المحاسبية وخاصة الناتجة عن الزلازل والفيضانات والحروب وفشل البرامج والمعدات وما تحدثه الفيروسات من مشكلات والاحتيايل بصوره المختلفة، فإن ذلك يعني توقف النظام، والذي يؤدي إلى توقف نشاط المنشأة ذاته، وعدم استمراريته،⁽¹⁾ فالنظام الذي لا يتوفر عند الحاجة إليه لا يمكن الاعتماد عليه، وعليه فإنه لا يمكن أن يكون النظام آمناً وموثوقاً منه ويعتمد به فالنظم الآمنة والموثوقة تكون متوفرة عند احتياجها في أي وقت،⁽²⁾ وتكون توقعات العملاء بالحصول على خدمة سريعة مستمرة مأمونة (24) ساعة و(7) أيام في الأسبوع، لكن تلك المخاطر تؤدي إلى ببطء الأنظمة التشغيلية ومن ثم توقفها بشكل مفاجئ ومتكرر.⁽³⁾

2-3-1-1: تعرض نظام المعلومات المحاسبية بالبنك للتعطيل بسبب المخاطر يؤثر على استرجاع البيانات والمعلومات ويترتب على ذلك خسائر مالية كبيرة، وقد يؤدي ذلك إلى خروج البنك من السوق وإفلاسه:

هناك تأثير اقتصادي سلبي لتلك المخاطر على المنشأة حيث تنتج خسائر في الإيرادات بسبب الإخلال ببعض الاتفاقيات وفقدان السرية والخصوصية والنزاهة أو إتاحة المعلومات لأفراد أو جهات لم يكن من المسموح لهم الاطلاع عليها، وفقد ثقة العملاء و الجمهور في المنشأة.⁽⁴⁾ فسوء الاستخدام المقصود للنظام والوصول غير المصرح به، بغرض الاطلاع أو الشروع في الأذى وتعتمد التخريب والتدمير والاحتيايل أو السرقة تعتبر مخاطر وتهديدات خطيرة تؤثر سلباً على نظم المعلومات المحاسبية، كما تؤثر على قدرة المنشأة في البقاء والتواجد داخل بيئة الأعمال، مما يؤدي إلى خسائر كبيرة على المنشأة، فمثلاً يعتبر إغراق نظام المعلومات المحاسبية بطلبات تبادل البيانات يؤدي إلى إعاقة وصول المستخدمين الطبيعيين للنظام، وبالتالي يؤدي فقد هذا الاتصال إلى إمكانية فقد فرص نشاط حقيقية للمنشأة.

وقد تؤدي تلك المخاطر إلى تعطل عمل التجهيزات وتوقفها لفترة طويلة نسبياً لإجراء الإصلاحات اللازمة واسترداد البرمجيات وقواعد البيانات،⁽⁵⁾ وربما تؤدي بعض المخاطر إلى تلف البنية التحتية لنظم المعلومات المحاسبية، وهذا من شأنه أن يؤدي إلى توقف المنشآت عن القيام بأعمالها، أو تعطيل تلك الأعمال لفترة طويلة

(1) حجر، عبد الملك إسماعيل، "نظم المعلومات المحاسبية"، مرجع سابق، ص 445.

(2) Romney, Marshall B. & Steinbart, Paul J., (2015), "Accounting Information Systems", OP. Cit., P. 157.

(3) Basel Committee on Banking Supervision (BCBS), (2011), "Sound Practices for the Management and Supervision of Operational Risk", Bank for International Settlement (BIS), Basel, Switzerland, February 2011, PP: 6-22, www.bis.org

(4) عبيد، أحمد يوسف (2008) "إدارة مخاطر أمن المعلومات"، مقالة علمية متاحة على:

<http://www.secureminds.net/Pages/articleRiskManagement.asp> تم الدخول بتاريخ 23 / 2 / 2011م الساعة 25 : 09 صباحاً.

(5) رملي، فياض حمزة، (2011)، "نظم المعلومات المحاسبية المحوسبة - مدخل معاصر لأغراض ترشيده القرارات الإدارية"، مرجع سابق، ص 110.

مما سينتج عنه خسائر كبيرة قد تؤدي أحياناً إلى خروج المنشآت التي تتعرض نظمها المحاسبية للكوارث من السوق بالإعلان عن إفلاسها خلال فترات غير طويلة.

وينتج عن ذلك أعطال كبيرة تؤدي إلى توقف العمل، أو إبطاء العمل بصفة دائمة أو تقلل قيمة النظام وتضعف خدماته، وتعطل نظام المنشأة لبعض الوقت قد يؤدي إلى إحداث خلل لنظم معلومات بعض عملائها مما يفقدون الثقة بها، ويتجنبوا التعامل معها مستقبلاً،⁽¹⁾ فإذا تمكن أحد القراصنة من تعطيل نظام معلومات المنشأة عن العمل لفترة معينة (ساعات أو أيام قليلة)، فإن ذلك سوف يحرمها من ممارسة أعمالها وبالتالي فقد إيراد يمكن تحقيقه، والأخطر من ذلك هو فقدانها لثقة عملائها وإحجامهم عن التعامل معها، فضلاً عن تحملها تكلفة ووقت تعطل أعمالها لمجرد الشك في إمكانية وجود اختراق لأمن نظم معلوماتها وأيضاً يؤدي ذلك إلى تعطل أعمال العملاء وخسائرهم.⁽²⁾ فمثلاً في يناير 2001 قام بنك Egg بإيقاف الدخول مؤقتاً إلى الحسابات المصرفية من خلال الخط المباشر، وذلك بدون إنذار مسبق أو أبداء تفسير إلى عملائه ونشأت صعوبات بالنسبة للعملاء في الدخول إلى حساباتهم المصرفية و إلى بياناتهم الشخصية لعدة أيام، ولقد كان الأمر غير مقبول للعملاء بأن لا يتم إخطارهم لتلك الفترة الزمنية، وربما حدث تأثير ضار طويل الأمد على الأداء المصرفي من خلال الخط المباشر للبنك، وفي مثل هذه الحالة فإن العملاء يصيبهم الضيق ولا يرتاحون لأن تظل أموالهم أو تصريح شؤون أعمالهم لدى نظام ينكر عليهم مجرد الإخطار، وفي كوريا الجنوبية تعرضت لـ 40 ألف حالة هجوم إلكتروني في عام 2012 فقط، تعرض عدد من خوادم النت مؤخراً إلى هجوم إلكتروني خبيث، مما أدى إلى تعطل مواقع الكترونية وشبكات عدد من البنوك، إضافة إلى وسائل الإعلام في البلاد،⁽³⁾ وذلك يؤدي إلى خسائر حتمية للمنشأة، فحجم الخسائر الاقتصادية السنوية في الولايات المتحدة الأمريكية تبلغ بليون دولار تقريباً بسبب التهديدات والمخاطر التي تتعرض لها نظم المعلومات المحاسبية المحوسبة في المنشآت المختلفة،⁽⁴⁾ وقد بينت إحدى الدراسات أن 50 % - 90 % من الشركات الأمريكية فقدت أموالاً نتيجة وجود جرائم تتعلق بالحاسوب فيها، وأن القضايا التي يعلن عنها ليست هي جميع القضايا التي تحصل وذلك لأن كثير من منشآت الأعمال تمتنع عن ذلك لعدة أسباب.⁽⁵⁾

ولا شك أن وجود المخاطر السابقة التي تهدد أمن وسلامة المعلومات في ظل بيئة تكنولوجيا المعلومات يترتب عليها إلحاق العديد من الخسائر المالية للمنشأة، فعلى سبيل المثال في حالة تمكن أحد القراصنة من تعطيل نظام المعلومات المحاسبي لفترة معينة، فإن ذلك سيؤدي إلى عدم إمكانية ممارسة المنشأة لنشاطها، خاصة إذا كانت المنشأة تعتمد في تعاملاتها على التجارة الإلكترونية، بالإضافة إلى الخسائر الناتجة عن سرقة معلومات

(1) National Institute of Standards and Technology: NIST, (July 2012), "Guide for Conducting Risk Assessments", OP. Cit. Revision. I.

(2) Arens, Alvin A., Elder, Randal J., & Beasley, Mark S., (2014), *Auditing & Assurance Services: An Integrated Approach*, OP. Cit., PP: 740-742.

(3) عبدالرحيم، شريفة، (2013)، *سياق القط والفار بين البنوك والهاكرز*، جريدة الاهرام الاقتصادي، القاهرة، مصر، 16 أيلول (سبتمبر)، 14:24، <http://economic.ahram.org.eg>

(4) Romney, Marshall B. & Steinbart, Paul J., (2015), "Accounting Information Systems", OP. Cit. , P. 145.

(5) أحمر، إسماعيل، (2006)، "أسباب ضعف الإجراءات الرقابية في نظم المعلومات المحاسبية - دراسة تحليلية"، *مراجع سابق*، ص ص: 21-42.

المنشأة، واختراق سريتها، وفي هذه الحالة يجب مراعاة توقيتات الأعطال والتشويش الذي يتعرض له النظام عند التخطيط لأمن المعلومات من البداية.

2-1-3-2: تدمير البنية التحتية لنظم المعلومات المحاسبية وتوقفها لفترات طويلة يؤدي إلى إعاقة وصول

المستخدمين والأطراف المستفيدة، مما يفقد المنشأة فرص نشاط حقيقية: تؤدي المخاطر على اختلاف أنواعها ومسبباتها إلى تدمير شامل أو جزئي لكافة محتويات النظم المحاسبية مما يشكل تهديداً حقيقياً يترتب عليه خسائر قد تكلف الكثير من الجهد والأموال وعادة ما تكون هذه الخسائر قاتلة لعدم وجود التخطيط المسبق لمواجهة الطوارئ والتعامل معها، فقد تؤدي المخاطر التي تتعرض لها النظم الآلية إلى تدمير كافة سجلات المنشأة وبذلك فهي أشد خطورة على النظم الآلية من النظم اليدوية، وسواء كانت المخاطر ناتجة عن كوارث طبيعية أم غير طبيعية فإنها قد تؤثر على عمل نظم المعلومات المحاسبية، وقد تؤدي إلى تعطل عمل التجهيزات وتوقفها لفترات طويلة مما يؤثر على أمن وسلامة وإتاحة نظم المعلومات المحاسبية.

2-1-3-3: حالات التعطيل والتوقف المفاجئ لنظام المعلومات المحاسبية للمنشأة لبعض الوقت يؤدي إلى

اهتزاز مكانة المنشأة أمام عملائه وتكبد المنشأة خسائر تجارية ومالية كبيرة: إن حدوث أي من التهديدات والمخاطر يمكن أن يؤدي إلى توقف نظم المعلومات المحاسبية لأي منشأة لبعض الوقت والتوقف هو الفترة الزمنية التي تصبح فيه العمليات التجارية غير قادرة على العمل، وبالتالي قد يؤدي ذلك لفقدان الثقة بالمنشأة من قبل بعض عملائها وتجنب التعامل معها مستقبلاً،⁽¹⁾ وقد يصل الضرر في بعض المنشآت التجارية والصناعية إلى تكبد خسائر مادية قد تصل إلى مبالغ كبيرة، وعلى سبيل المثال وصلت الأضرار المادية إلى ملياري دولار أمريكي، حيث ينتج عنها توقف أعمال بعض تلك المنشآت نتيجة إتلاف قواعد بياناتها،⁽²⁾ الأمر الذي قد يؤدي إلى فقد بعض الإيرادات و حدوث خسائر مالية قد تصل إلى حد كبير لدرجة يصعب تخيلها خصوصاً إذا كانت المنشأة تعتمد على التجارة الإلكترونية، وبالتالي تتحمل المنشأة خسائر إصلاح الأضرار الناتجة عن حدوث تلك التهديدات والمخاطر، وخسائر التوقف التي تواجهها المنشأة تتمثل في المبالغ المستثمرة في التقنيات الأمنية لتفادي الهجمات، أو لإصلاح الفشل بسبب الهجمات، وتنويع البرامج للحد من المخاطر الأمنية.⁽³⁾

ولتحقيق متطلبات أمن وحماية نظم المعلومات المحاسبية فلا بد للمنشأة من إتباع عدة إجراءات للحماية ومنها إجراءات ضمان استمرارية عمل وجاهزية نظم المعلومات في شتى الظروف والأزمات والمخاطر التي قد تواجه النظم، مثل تعطل أو توقف النظم المعلوماتية عن العمل، ولذلك لا بد من جعل النظام متاحاً للمنشأة ولكافة

(1) Benaroch, Michel & Chernobai, Anna & Goldstein, James,(2012),"An Internal Control Perspective on the Market Value Consequences of IT Operational Risk Events", *OP. Cit.*, PP:357- 381.

(2) Feng, Nan & Wang, Harry & Li, Minqiang,(2013), "A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis", *OP. Cit.*, PP: 1-17.

(3) Chen, Pei-yu et al.,(2011),"Correlated Failures, Diversification and Information Security Risk Management", *MIS Quarterly* , Vol. 35 No. 2, June 2011, U.S.A., PP: 397-422

مستخدميه من الأطراف ذات العلاقة بصورة مستمرة وهو ما يتحقق من خلال تبني المنشآت خطط لمواجهة الكوارث المختلفة، بما يكفل الاستمرار في ممارسة العمل واستئناف النشاط بصورة سريعة.⁽¹⁾

وهناك منشآت - ومنها البنوك التجارية - لا يسمح طبيعتها نشاطها بالتوقف حتى لفترة وجيزة وبالتالي هناك حاجة إلى نظام حماية يعمل على استعادة النشاط مباشرة بمجرد توقف النظام الأساسي، وذلك من خلال ربط نظم معلوماتها بصورة مستمرة بالإنترنت بحيث يكون لديها أكثر من موقع يشتمل كل موقع على البرامج والبيانات والوثائق بصورة كاملة، ويتم تحديث مختلف المواقع بصورة مباشرة في آن واحد، وبالتالي فإن أي ظرف يحدث للموقع الرئيسي فإن الموقع الثانوي يقوم باستئناف النشاط، وأحياناً تلقائياً وبدون أن يدرك أحد ذلك وبدون حدوث أي تأخير، وهناك منشآت تتعاقد مع مكاتب متخصصة تقدّم هذه الخدمة، من خلال نقل بيانات المنشأة وأي تعديلات بها أوتوماتيكياً عبر الإنترنت إلى سيرفر خارجي يديره مكتب تقديم الخدمة، وتتم استعادة البيانات من المخزن الإلكتروني لذلك المكتب (طرف خارجي).⁽²⁾

2-3-3: تأثير المخاطر على سلامة وتكامل تجهيز البيانات في نظم المعلومات المحاسبية المحوسبة:

إن نظم المعلومات المحاسبية المحوسبة يمكنها إنتاج تقارير ومخرجات على قدر من الأهمية في حالة كون البيانات التي تغذي النظام تتمتع بالسلامة والملائمة،⁽³⁾ ويقصد بسلامة وتكامل تجهيز البيانات ضمان أن أصول تكنولوجيا المعلومات، بما في ذلك البيانات والمعلومات وعمليات تدفقها هي أصيلة (أي حقيقية وجديرة بالثقة) وصحيحة (أي الحفاظ عليها دون فساد)، وتكامل تشغيل نظام المعلومات، يركز على أن المعلومات المحاسبية محصنة ضد أي تغيير من الداخل أو من الخارج.⁽⁴⁾

ولكن توجد الكثير من المخاطر التي تهدد سلامة المعلومات وتكاملها، فتجعل برامج النظام لا تعمل بشكل جيد ومتربط فيما بينها، فتحتوي البرامج على أخطاء، ولا يتم الحصول على النتائج المطلوبة بشكل دقيق في الوقت المناسب، فالتحدي الحقيقي لنظم المعلومات هو التأكد من أن المعلومات هي من أعلى مستويات الجودة من حيث توقيتها واكتمالها ودقتها، والسرية والموثوقية وسهولة القراءة والملاءمة كما تواجه المنظمات مستويات عالية غير مقبولة من الانتهاكات الأمنية فإنها نادراً ما تقدم موارد المعلومات عالية الجودة باستمرار لتلبية متطلبات الإدارة.⁽⁵⁾

(1) حجر، عبد الملك إسماعيل، (2009)، "نظم المعلومات المحاسبية"، مرجع سابق، ص 441.

(2) حجر، عبد الملك إسماعيل، (2009)، "نفس المرجع"، ص 447.

(3) محمد، حيدر صاحب، (2011)، "مسؤولية مراقب الحسابات في تحديد و تقييم مخاطر تكنولوجيا نظم المعلومات المحاسبية لرفع جودة أدائه"، مرجع سابق، ص: 86

(4) Benaroch, Michel & Chernobai, Anna & Goldstein, James, (2012), "An Internal Control Perspective on the Market Value Consequences of IT Operational Risk Events", *OP. Cit.*, PP: 357- 381.

(5) Parakkattu, Sindhuja & Kunnathur, Anand. S., (2010), "A Framework for Research in Information Security Management", *OP. Cit.*, PP: 318-323.

كما أن الفشل في الحفاظ على سلامة البيانات والمعلومات الخاصة بالمعاملات يمكن أن تعرض البنوك لخسائر مالية فادحة فضلاً عن المخاطر القانونية والسمعة.⁽¹⁾

وبالتالي يتضح تأثير المخاطر على سلامة وتكامل تجهيز البيانات في نظم المعلومات المحاسبية كما يلي:

2-3-2: حدوث مخاطر أمن نظم المعلومات المحاسبية يؤثر على سلامة تجهيز البيانات وعمليات التشغيل والمخرجات، بالدقة والشمولية المطلوبة وفي الوقت المناسب:

من الآثار الهامة للمخاطر التي تواجه نظم المعلومات المحاسبية المحوسبة إن الوصول للنظام بطريقة غير مصرح بها يمكن أن يؤدي إلى إدخال فيروسات تعمل على إتلاف أو تدمير البيانات من الملفات والبرامج ونظم التشغيل وبالتالي تفريغ المحتوى المعلوماتي للنظام، وقد يؤدي ذلك إلى اتخاذ إدارة المنشأة لقرارات خاطئة، ولا شك أن التمكن من الدخول غير المصرح به إلى قاعدة البيانات والتلاعب بها يضعف من قدرة نظام المعلومات المحاسبي على تقديم المعلومات الموضوعية إلى الأطراف ذات العلاقة،⁽²⁾ ويمكن أن تتغير سلامة البيانات في قواعد البيانات وسلامة أجهزة النظام عند حدوث انقطاع مفاجئ للكهرباء التي تغذي جهاز الخادم، أو عند عدم إقبال قاعدة البيانات بشكل صحيح، أو حذف المعلومة بطريقة الخطأ من قبل أحد الموظفين، أو حصول خلل بسبب فيروس،⁽³⁾ كما أن إدخال بيانات غير صحيحة سواء متعمدة أو غير متعمدة سوف ينعكس فوراً بشكل سلبي على حسابات وقواعد بيانات المنشأة، وبشكل خاص عند تكامل النظم الفرعية للنظام مع بعضها البعض، على مستوى الأقسام والفروع، وبالتالي تأثير مثل تلك المخاطر يمكن أن يترك أثر على المستثمر الحذر لتأثيرها السلبي المباشر على موثوقية المعلومات المالية المنشورة، وإلى حد ما تؤدي إلى أضرار مالية حادة ومسؤوليات قانونية على المنشأة،⁽⁴⁾ مما يزيد في النفقات ويسبب تأخير الأعمال وعدم تكامل البيانات وبالإضافة إلى ذلك فإن السماح باستمرار الوضع الراهن يحد من النمو المستقبلي ويؤخر المنشآت بالحق بعصر المعلومات والمعرفة المستهدفة.⁽⁵⁾

ويرى الباحث إن ارتفاع نسبة التهديدات التي يتعرض لها نظام المعلومات المحاسبي في أنظمتها الفرعية المختلفة سوف تخفض من قيمة البيانات والمعلومات التي تحصل عليها المنشأة من هذا النظام ومن ثم الوصول إلى قرارات سيئة لا تضيف قيمة للمنشأة وربما تفقدها حصتها السوقية وميزتها التنافسية وترفع من تكاليفها، فمثلاً دخول الفيروسات إلى النظام نتيجة لضعف إجراءات الحماية المضادة لتلك الفيروسات يؤدي إلى خسائر فادحة وتشويه لسمعة المنشأة نتيجة توافر رأي عام سلبي تجاهها، وأيضاً قد يربك عملية اتخاذ القرارات الضرورية.

(1) Rafique, Rajia & Mehmood, Furhan, (2010), "Management of Operational Risks Related to Information Security in Financial Organizations", *OP. Cit.*, P.5.

(2) Beard, Deborah & Wen, H. Joseph, (2007), "Reducing the Threat Levels for Accounting Information System, Challenge for Management, Accountants and Academicians", *OP. Cit.*, PP: 34-42.

(3) Ashenden, Debi, (2008), "Information Security management: A human challenge?", *OP. Cit.*, PP: 195 – 201, P 197.

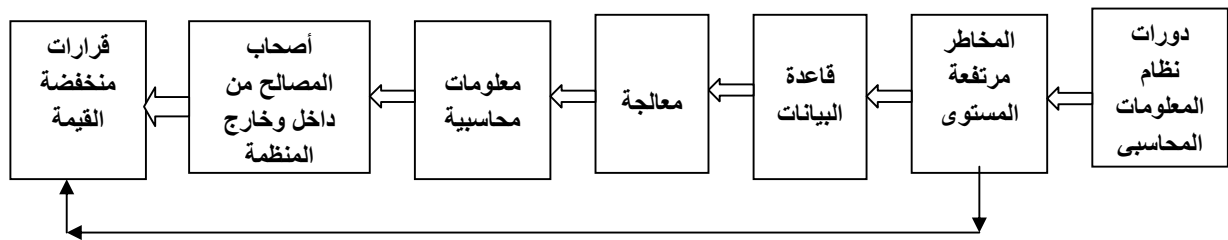
(4) Tarmidi, M., et al., (2013), "Computerized Accounting Systems Threats in Malaysian Public Services", *OP. Cit.*, PP: 109-113.

(5) Abu-Musa, Ahmad A., (2006), "Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations", *OP. Cit.*, PP: 1-26.

2-2-3-2: تشغيل النظام بشكل خاطئ وباستخدام برامج غير ملائمة يؤدي إلى حصول المنشأة لمخرجات غير دقيقة وغير سليمة، يؤثر على صحتها ومصداقيتها:

من الآثار الهامة للمخاطر التي تواجه نظم المعلومات المحاسبية المحوسبة كتشغيل النظام بشكل خاطئ وباستخدام برامج غير ملائمة أو فشل أداء المعدات وانقطاع التيار الكهربائي أو تذبذبه وتعرضه للفيروسات،... الخ يؤدي إلى تحريف بيانات النظام وتشويهها،⁽¹⁾ وبالتالي حصول المنشأة على مخرجات ونتائج غير سليمة، مما يؤدي إلى تقديم معلومات للإدارة تقودها إلى اتخاذ قرارات خاطئة أو غير رشيدة أو إلى تضليل جوهري في القوائم المالية وذلك يساهم في إضعاف أداء المنشأة وفقدان حصتها السوقية وميزتها التنافسية وارتفاع تكاليفها التشغيلية،⁽²⁾ ويتضح ذلك كما بالشكل التالي:

شكل رقم (2-3-1) المخاطر المرتفعة تؤدي إلى قرارات منخفضة القيمة⁽³⁾



وفي رأي الباحث إن تخفيض أو إزالة تهديدات ومخاطر أمن نظم المعلومات المحاسبية سوف يحسن من أداء المنشأة بشكل عام لأن المعلومات المحاسبية التي تفرزها دورات نظم المعلومات المحاسبية تشكل جوهر عمل أي منشأة وإن اختلفت طبيعة العمل من منشأة إلى أخرى وذلك يتطلب الاهتمام الجدي بوضع أطار للرقابة الداخلية من خلال وضع إجراءات رقابة ووقائية واستكشافية وتصحيحية وبالشكل الذي يكفل دقة وسلامة البيانات المستلمة والمرسلة، وضمان إنتاج المعلومات محاسبية جديرة بالثقة وأمانة، وبما من شأنه إن يخفض من تلك المخاطر والتهديدات المحتملة التي تتعرض لها نظم المعلومات المحاسبية المحوسبة من أجل الحصول على بيانات ومعلومات محاسبية على درجة من الموثوقية يمكن الاعتماد عليها في ترشيد اتخاذ القرارات التشغيلية والإستراتيجية للمنشأة من خلال ترشيد اتخاذ قرارات أصحاب المصالح المختلفة المرتبطة بالمنشأة.

2-3-3-2: تعرض نظم المعلومات المحاسبية المحوسبة بالمنشأة إلى أي خطر يخفض من تكامل تلك النظم مع بعضها البعض على مستوى الأقسام والفروع، ففوق خطأ ما يؤدي إلى وقوع سلسلة من الأخطاء نتيجة التحديث الفوري للملفات.

تعتبر سلامة البيانات جزء مهم من المكونات الأمنية للمعاملات المصرفية الالكترونية، خاصة في ظل اعتماد نظم المعلومات المحاسبية الفرعية على بعضها البعض بدرجة كبيرة حيث أن أي خطأ أو تلاعب في نظام

(1) National Institute of Standards and Technology: NIST, (2012), "Guide for Conducting Risk Assessments", OP. Cit., Revision 1.
 (2) الذبيبة، زياد & الرمحي، نضال & الجعدي، عمر، (2011)، "نظم المعلومات في الرقابة والتدقيق"، مرجع سابق، ص 60.
 (3) الشكل من إعداد الباحث.

معلومات فرعى سيؤدي إلى آثار سيئة على النظام ككل على سبيل المثال : خطأ غير مكتشف في تطبيقات نظام المدفوعات النقدية قد يؤثر عكسياً على التدفقات النقدية للشركة وثقة عملائها ومورديها في نظام معلوماتها، وتعرض نظام المعلومات إلى أي تهديد لا بد ضمنياً من أن يفقد أو يخفض من تكامل النظام، وبالتالي فإن إجراء أي نوع من أنواع الحماية واستخدام سياسة أمنية يساهم في تحقيق أو زيادة تكاملية النظام، ولذلك يتعين على المنشآت إرساء إجراءات تحكم فعالة تضمن كفاءة إدارة الارتباط والعلاقات بين الأنظمة داخل هذه المنشآت وكذلك مع الأطراف والمؤسسات الأخرى والعملاء.

2-3-3: تأثير المخاطر على سرية المعلومات الناتجة عن نظم المعلومات المحاسبية المحوسبة:

السرية هو ضمان الوصول للبيانات الهامة كالأسرار التجارية والخطط الإستراتيجية، ومشاركتها مع شركاء العمل كالأشخاص أو النظم أو المنشآت المرخص لها فقط.⁽¹⁾ بمعنى أن المعلومات الحساسة تكون محمية من أن تكون مكشوفة لغير المخولين، وغالبية البيانات التي تعرضت لعملية اختراق أمني حسب ما أكد معظم خبراء أمن تكنولوجيا المعلومات كانت بيانات شخصية لعملاء إضافة للمعلومات المالية التي تخص المنشأة، فهناك تحديات ومخاطر كبيرة نتيجة استخدام تكنولوجيا المعلومات، تنصب في أغلبها على سرية المعلومات، من خلال إطلاع العابثين على المعلومات، بعدة وسائل، فالقرصنة لديهم القدرة على الحصول على كلمات سر المستخدم للوصول إلى المعلومات المخزنة في قواعد بيانات نظم المعلومات، كما أن انتشار كلمات الدخول إلى النظام بين أفراد المنشأة من غير المخولين والفشل في الحفاظ على ملفات النسخ الاحتياطي بطريقة سليمة، يؤدي إلى فقدان لسرية بياناتها وبرامجها وخطتها ويسهل على الدخلاء إباحة نشاطات المنشأة،⁽²⁾ والمساس بسرية المعلومات خطير للغاية من حيث الأضرار الناجمة بسبب الخسائر المالية وتعطيل العمليات الداخلية والاتصالات للمنشأة، وفقدان الإيرادات المحتملة، وفقدان الميزة التنافسية، وهدر للوقت والجهد للقوى العاملة وكذلك الإضرار بسمعة علاقات حسن النية والثقة بين المنشأة والأطراف المتعاملة معها.⁽³⁾

ولا شك في أن إدارة المنشأة ستكون حريصة على أن تكون البيانات والمعلومات الخاصة بعملائها وموظفيها غير متاحة للجميع ولذلك يتم المحافظة على سرية المعلومات من خلال منع الوصول إليها من غير المصرح لهم، وتشفيرها عند تراسلها إلكترونياً، وتقليل أو منع الأضرار الناجمة عن محاولات الاعتداء على هذه المعلومات.

(1) Benaroch, Michel & Chernobai, Anna & Goldstein, James, (2012), "An Internal Control Perspective on the Market Value Consequences of IT Operational Risk Events", *OP. Cit.*, PP: 357- 381.

(2) Beard, Deborah & Wen, H. Joseph, (2007), "Reducing the Threat Levels for Accounting Information System, Challenge for Management, Accountants, Auditors and Academicians", *OP. Cit.*, PP: 34-42.

(3) Parakkattu, Sindhuja & Kunnathur, Anand. S., (2010), "A Framework for Research in Information Security Management", *OP. Cit.*, PP: 318-323.

ويتضح تأثير المخاطر الأمنية على سرية المعلومات المحاسبية من خلال النقاط التالية:

2-3-3-1: إن اقتحام نظام المعلومات المحاسبي من أطراف غير مخولة بالدخول، يؤدي إلى إمكانية سرقة أو

تسرب معلومات هامة على درجة عالية من السرية لجهات غير مرغوب فيها:

من الآثار الهامة للتهديدات والمخاطر التي تواجه نظم المعلومات المحاسبية المحوسبة اقتحام نظام المعلومات المحاسبي من أطراف داخلية أو خارجية ليس لهم حق دخول النظام مما يؤدي إلى إمكانية سرقة معلومات هامة قد تكون على درجة عالية من السرية، وهذا يشمل معلومات حول إستراتيجية المنشأة والمعلومات المالية ومعلومات العملاء وأي معلومات أخرى حساسة يمكن أن يسبب سرقتها دمار للمنشأة ولسمعتها في السوق.⁽¹⁾

2-3-3-2: إن حدوث مخاطر أمن نظم المعلومات المحاسبية يؤدي إلى إطلاع المنافسين على المعلومات المرتبطة

بالمنشأة والتي قد يترتب عليها الإضرار بالموقف التنافسي:

وتكمن تأثيرات مخاطر أمن المعلومات في عدة جوانب منها تقليل أداء نظم المعلومات المحوسبة أو تخريبها بالكامل، مما يؤدي إلى تعطل الخدمات الحيوية للمنشأة، أما الجانب الآخر فيشمل سرية وتكامل المعلومات حيث قد يؤدي الإطلاع والتصنت على المعلومات السرية التي ما كان ينبغي الإطلاع عليها إلى خسائر مادية أو معنوية كبيرة،⁽²⁾ فحدث أي من التهديدات والمخاطر السابقة لنظم المعلومات المحاسبية للمنشأة أو لموقعها على الانترنت يؤدي إلى التعرف على أرقام بطاقات الائتمان الخاصة بالعملاء والسطو على حساباتهم، ووصول أطراف خارجية ليس لها علاقة بأعمال المنشأة، إلى البيانات الخاصة بالمنشأة والمخزنة في نظم معلوماتها المحاسبية، وقد يصل المنافسون إلى تلك البيانات وبالتالي قد يمكنهم من التعرف على خطط التشغيل المستقبلية للمنشأة، والمنتجات أو الخدمات الجديدة ومواصفاتها وربحياتها، وقوائم وأرصدة العملاء، والمستندات القانونية الخاصة بالمنشأة، مما يضر بالموقف التنافسي للمنشأة ويقلل من ميزتها التنافسية، وينتج عن ذلك خسائر كبيرة للمنشأة نتيجة إفشاء معلومات هامة على درجة عالية من السرية وكشفها للمنافسين.

ولذلك يرى الباحث أن الوصول غير المخول إلى نظم المعلومات المحاسبية المحوسبة يؤدي إلى سرقة المعلومات المحاسبية للمنشأة أو التلاعب بها الأمر الذي يؤثر سلباً على مركزها المالي ويضر بسمعتها ويسرب بيانات أنشطتها إلى منافسيها، وبالتالي يجب أن توفر تلك النظم حماية سرية المعلومات الخاصة بالمنشأة والغير مصرح بالإفصاح عنها.

(1) French, Aaron M., (2012), " A Case Study on E-Banking Security – When Security Becomes Too Sophisticated for the User to Access Their Information", OP. Cit., PP: 1-15.

(2) الذبيبة، زياد & الرمحي، نضال & الجعدي، عمر، " نظم المعلومات في الرقابة والتدقيق"، مرجع سابق، ص 64.

2-3-3: إن حدوث المخاطر يؤدي إلى عدم قدرة نظام المعلومات المحاسبي في المنشأة على التعامل مع

الأطراف المستفيدة المختلفة وفقاً لأصول السرية والفائدة المرجوة: فتطبيقات نظم المعلومات المحاسبية

المحوسبة الموجودة على شبكات الحاسبات معرضة للهجمات الضارة أو للفشل فيما يتصل بسرية معلوماتها أو عدم حفظ خصوصية بيانات المنشأة والمتعاملين معها أو التأخير في توافرها في الوقت الملائم لمن يحتاجها بسرعة، وينشأ نتيجة ذلك مخاطر على سمعة المنشأة لتوفر رأى عام سلبي تجاه المنشأة، الأمر الذي قد يمتد إلى التأثير على منشآت أخرى، نتيجة عدم مقدرة المنشأة على إدارة أنظمتها بكفاءة أو حدوث اختراق مؤثر لها.

وإذا فقدت المعلومات السرية المخزنة على جهاز الحاسوب فإن المنشأة تتعرض لخطر فقدان عملائها بواسطة جهات أخرى أو إلى تخريب وتحريف تلك المعلومات وكذلك عمليات التخريب بواسطة الفيروسات أو حصان طروادة، مما يؤدي إلى انخفاض في الربحية وفقدان الأمن الوظيفي لجميع العاملين.

ومن المحتمل إن يكون الرد على المخاطر الأمنية له إبعاد وتأثيرات اقتصادية هامة على المنشأة لأن ذلك لا يؤثر على أمن المنشأة فحسب لكنه يؤثر أيضاً على تعاملها التجاري وأحد مواردها الاقتصادية فمثلاً قد يتطلب الأمر إيقاف خدمة التجارة الالكترونية لفترة معينة،⁽¹⁾ وبالتالي يمكن أن يؤدي تحقيق أي من مخاطر أمن نظم المعلومات المحاسبية إلى تحمل المنشأة لبعض أو كل التكاليف والخسائر التالية:

1. التكلفة المباشرة المتمثلة في تكاليف إصلاح الأضرار الناتجة عن تحقيق أحد التهديدات، وسرقة بعض الأموال من حسابات المنشأة، والغرامات والتعويضات، والجزاءات التي قد تفرض على المنشأة.
2. تكلفة الوقت الضائع والإيرادات المفقودة بسبب توقف نظم المعلومات المحاسبية عن العمل لبعض الوقت.
3. تكلفة إفشاء معلومات المنشأة السرية وإطلاع المنافسين عليها.
4. تكلفة الخسائر التي تصيب عملاء المنشأة نتيجة تعطل أعمالهم، أو الاستيلاء على أرقام بطاقات الائتمان الخاصة بهم، وكشف بياناتهم الشخصية، وبالتالي تتأثر سمعة المنشأة وموقف العملاء منها.
5. الأثر السلبي على سمعة المنشأة وفقدان ثقة العملاء فيها وتجنبهم التعامل معها، وقد يؤدي ذلك إلى إفلاس المنشأة وانهارها خاصة إذا كانت تعتمد على المعاملات الالكترونية في أعمالها.

2-3-4: تأثير المخاطر على خصوصية بيانات الأطراف المتعاملة مع المنشأة:

الخصوصية (Privacy): وتعني حقوق والتزامات الأطراف المتعاملة من الأفراد والمنشآت فيما يتعلق بجمع واستخدام والإفصاح والاحتفاظ بالمعلومات الشخصية (كالأسماء والعناوين والسن والوظيفة والدخل السنوي والحالة الصحية وغير ذلك) وتحويل تلك المعلومات إلى معلومات رقمية بهدف حمايتها، وبكل الأحوال فإن هذه

(1) Romney, Marshall B. & Steinbart, Paul J., (2015), "Accounting Information Systems", OP. Cit., P. 262.

المعلومات الشخصية يجب إن تكون محمية من الوصول غير المخول لها،⁽¹⁾ ولا شك إن وصول بعض الدخلاء لتلك المعلومات يشكل خرقاً لخصوصية العملاء وما ينتج عن ذلك من آثار سلبية بالنسبة للعميل والمنشأة،⁽²⁾ فالمعلومات الشخصية هي ملكية خاصة ومطلقة للمتلين لها، ولذلك يجب العناية بحفظ الدقة والاكتمال لها أثناء تجميعها واستعمالها والإفصاح عنها وصيانتها بطريقة مناسبة بما يتفق مع سياسات وإجراءات الخصوصية للمنشأة.⁽³⁾

إن المخاطر الأمنية الناتجة عن التعامل المباشر عبر شبكة الانترنت لا يمس المنشآت المتعاملة بوسائل إلكترونية فقط وإنما يتجاوز ذلك ليصل إلى الأفراد المتعاملين عبر هذه الشبكة، ومن أكثر المخاطر أهمية هو إفشاء المعلومات الخاصة كتعرض العملاء للنصب والاحتيال خاصة بالسطو على المعلومات الخاصة ببطاقات الائتمان العائدة إليه ومن ثم استغلالها بصورة غير شرعية أو سحب ما فيها من أرصدة.

فالكثير من المنشآت الكبرى تجمع عن الأفراد بيانات عديدة ومفصلة تتعلق بالوضع المادي أو الصحي أو التعليمي أو العائلي أو العادات الاجتماعية أو العمل.. الخ، وتستخدم الحاسبات وشبكات الاتصال في خزنها ومعالجتها وتحليلها والربط بينها واسترجاعها ومقارنتها ونقلها، وهو ما يجعل فرص الوصول إلى هذه البيانات على نحو غير مصرح به أو بطريق التحايل أكثر من ذي قبل، ويفتح مجالاً أوسع لإساءة استخدامها أو توجيهها توجيهاً منحرفاً أو خاطئاً أو مراقبة الأفراد وتعرية خصوصياتهم أو الحكم عليهم حكماً خفياً من واقع سجلات البيانات الشخصية المخزنة، فقد مكنت تكنولوجيا المعلومات من سهولة خزن واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات والدوائر والوكالات الحكومية ومن قبل الشركات الخاصة، وأكثر من هذا فإنه يمكن مقارنة المعلومات المخزنة في ملف بمعلومات في قاعدة بيانات أخرى، ويمكن نقلها عبر البلد في ثوانٍ وبتكاليف منخفضة نسبياً، إن هذا بوضوح يكشف إلى أي مدى يمكن أن يكون تهديد الخصوصية.

ويرى الباحث أن الخصوصية تركز على حماية المعلومات الشخصية الخاصة بالمتعاملين مع المنشأة أكثر من بيانات المنشأة نفسها، وهنا الفرق بين تناول الباحث لتأثير المخاطر على سرية المعلومات، وتأثيرها على خصوصية المعلومات.

(1) Beard, Deborah & Wen, H. Joseph, (2007), "Reducing the Threat Levels for Accounting Information System, Challenge for Management, Accountants, Auditors and Academicians", *OP. Cit.*, PP: 34-42.

(2) Arens, Alvin A., Elder, Randal J., & Beasley, Mark S., (2014), *Auditing and Assurance Services: An Integrated Approach*, *OP. Cit.*, PP: 740-742.

(3) الهادي، محمد، (2006)، "توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية"، *مرجع سابق*، من الموقع: <http://www.journal.cybrarians.org>

ويتضح تأثير المخاطر الأمنية على خصوصية بيانات الأطراف المتعاملة مع المنشأة في النقاط التالية:

2-3-4-1: إن حدوث مخاطر أمن نظم المعلومات المحاسبية يؤدي إلى ضعف قدرة المنشأة في حماية خصوصيات وأسرار عملائه، نتيجة سرقة أو كشف المعلومات الشخصية لهم والتي يتم جمعها واستخدامها والاحتفاظ بها من قبل نظام المعلومات المحاسبي للمنشأة: فهناك مخاطر تتعرض لها المنشآت الإلكترونية وأعلى تلك المخاطر درجة هي اختراق الخصوصية والاطلاع على المعلومات السرية والتي تكون عادة غي مرحلة نقل البيانات بحيث تمر على أوساط ومواقع عديدة قبل وصولها إلى مقرها النهائي وذلك يسمح لذوي النوايا السيئة بقراءة المعلومات السرية والهامة وبالتالي الاستفادة منها،⁽¹⁾ ولسرية معظم البيانات الشخصية فإن وقوعها في أيدي غير أمينة يفسد العلاقة مع العملاء ويسبب إلى سمعة المنشأة واحتمال المطالبات بالتعويض عن الأضرار، ولذلك من الضروري حماية البنك بوسائل الأمن وإجراءات الرقابة الكافية، وبالرغم من التقدم الكبير على هذا الصعيد إلا أن أحدث تقارير الخصوصية تشير إلى أنه ما تزال حياة الأفراد وأسرارهم في بيئة النقل الرقمي معرضة للاعتداء في ظل عدم تكامل حلقات الحماية (التنظيمية و التقنية و القانونية).

ويجب تقييم درجة المخاطر مقابل مستوى الأمن وتأثير الخسائر على المنشأة، أو تقييم مستوى الرقابة مقابل درجة المخاطر وتأثير الخسائر على الأمن، فالحفاظ على المعلومات السرية للعملاء هي مسؤولية رئيسية للمنشأة لأن الكشف غير المصرح به لبيانات العملاء السرية يعرض المنشأة للمساءلة القانونية بالإضافة لمخاطر السمعة.⁽²⁾

2-3-4-2: إن تعرض المنشأة لمخاطر أمن نظم المعلومات المحاسبية يهدد سمعته نتيجة فقدان الثقة وفشل المنشأة في تحقيق متطلبات العملاء بتقديم خدمة إلكترونية متطورة وآمنة: إن التخوف من التعامل مع المنشآت الإلكترونية ناتج من عدم الثقة وتهديد أمن وحماية المعلومات الخاصة بهم أو نتيجة عدم الوعي الثقافي لدى فئة كبيرة من مستخدمي الإنترنت،⁽³⁾ وتعتبر التعاملات الإلكترونية التي تتم بين المنشأة وعملائها ذات طابع معلوماتي هام جداً، حيث تحفظ تلك المعلومات على ذاكرة النظام الرقمية وهي معلومات قيمة للغاية، وبالتالي إن تمكن أحد من معرفتها أو حتى تتبعها كنتيجة أرقام بطاقات الائتمان الخاصة بالعملاء، فسيشعر العملاء أن خصوصيتهم قد تم اختراقها وبالتالي يفقدوا ثقتهم بالمنشآت التي يتعاملوا معها من منطلق أنها لم تتمكن من حماية خصوصياتهم.

(1) القري، ميسون محمد، (2007)، "أمن المعلومات المحاسبية"، مرجع سابق، من الموقع: www.maysoon.ws/archives/420
(2) Basel Committee on Banking Supervision (BCBS), (2012), "Core Principles for Effective Banking Supervision", Bank for International Settlement (BIS), Basel, Switzerland, September 2012, PP: 1-85, www.bis.org
& Basel Committee on Banking Supervision (BCBS), (2003), "Risk Management Principles for Electronic Banking", Bank for International Settlement (BIS), Basel, Switzerland, July 2003, PP: 6-22. www.bis.org
(3) وادي، رشدي عبد اللطيف، (2008)، "أهمية ومزايا البنوك الإلكترونية في قطاع غزة بفلسطين ومعوقات انتشارها"، مرجع سابق، ص: 855-893.

2-3-4-3: إن حدوث مخاطر أمن نظم المعلومات المحاسبية يؤدي إلى عدم إتاحة الفرصة للعملاء للوصول إلى المعلومات المخزنة الشخصية لتعديلها أو إلغائها.

يجب على المنشأة منح جميع عملائها المحتملين الفرصة للوصول للمعلومات كلما لزم الأمر وهذا ينبغي أن يكون ممزوجاً مع بدائل مختلفة من الاختيارات كما ينبغي السعي للحصول على إذن العميل قبل نشر أي معلومات خاصة به للأطراف الخارجية.⁽¹⁾

إن من أهم المخاطر التي تهدد أمن نظم المعلومات المحاسبية في ظل التجارة الإلكترونية هو اختراق خصوصية المعلومات الشخصية، فالعقبة الرئيسية في تطبيقات التجارة الإلكترونية هي مشكلة أمنية لكل المستخدمين والمستهلكين في جميع أنحاء العالم، وهي مخاوف مشروعة فيما يتعلق بالخصوصية والثقة لا تزال تشكل عائقاً أمام نمو على كل من الأفراد والمنشآت، وتحتاج المنشآت إلى تحديد وفهم كيف يمكن أن تؤثر مخاطر نظام المعلومات المحاسبية على قرارات المديرين التنفيذيين للانخراط في تطبيقات التجارة الإلكترونية على شبكة الإنترنت.⁽²⁾

ورغم أن بعض المنشآت استطاعت الحد من الخسائر المالية، ولكنها لم تستطع منع الغير من الاطلاع على المعلومات الشخصية الخاصة بعملائها، فبعض العملاء يعتبر حماية عنوانه الشخصي ورقم هاتفه أهم من حماية بطاقة اعتماده.

وعلى المنشأة اتخاذ الخطوات المنطقية لحماية المعلومات الخاصة بالعملاء من الضياع أو من اطلاع الأفراد الآخرين غير المصرح لهم بالاطلاع عليها، وفي بعض الأحيان تكون الأمور متعلقة بالتخلص من أجهزة الكمبيوتر، حيث أن المعلومات المخزنة على ذاكرة الحاسوب (*Hard Disk Drive*) يصعب مسحها وضمان عدم إمكانية استرجاعها وعليه يفضل أتلأفها عند الرغبة بالتخلص منها بدلاً من بيعها.⁽³⁾

2-3-5: تأثير المخاطر على إثبات تصرفات الأطراف المتعاملة مع المنشأة خلال تبادل البيانات إلكترونياً:

عدم الإنكار أو عدم التنصل هو القدرة على إثبات وقوع حدث مزعوم أو إجراء ما والكيانات المنشأة له، بغرض حل الخلافات حول وقوع أو عدم وقوع الحدث، أو الإجراء، واشتراك الكيانات فيه.⁽⁴⁾ ويتم إنكار الخدمة من خلال القيام بأنشطة تمنع المستخدم الشرعي من الوصول إلى المعلومات أو الحصول على الخدمة وأبرز أنماط إنكار الخدمة إرسال كمية كبيرة من رسائل البريد الإلكتروني دفعة واحدة إلى

(1) Osunmuyiwa, Olufolabi, (2013), "Online Banking and the Risks Involved", *OP. Cit.*, PP: 50-54.

(2) Belkhamza, Zakariya & Wafa, Syed Azizi, (April 2009), "The Effect of Perceived Risk on the Intention to Use E-commerce: The Case of Algeria", *Journal of Internet Banking and Commerce*, Vol. 14, No.1., PP:1-9, available at <http://www.arraydev.com/commerce/jibc>

(3) Romney, Marshall B. & Steinbart, Paul J., (2015), "*Accounting Information Systems*", *OP. Cit.*, P. 168.

(4) ISO/IEC 27000, (2012), "*Information technology - Security techniques - Information security management systems - Overview and vocabulary*", *OP. Cit.*, Available at: <http://www.27000.org>

موقع معين بهدف إسقاط النظام المستقبل لعدم قدرته على احتمالها أو توجيه عدد كبير من عناوين الإنترنت على نحو لا يتيح عملية تجزئة حزم المواد المرسله فتؤدي إلى اكتظاظ الخادم وعدم قدرته على التعامل معه.⁽¹⁾

2-3-5-1: حدوث المخاطر يؤدي إلى تهرب بعض أطراف المعاملات الإلكترونية من الالتزامات، عن طريق إنكار وقوع أحداث وقعت أو ادعاء وقوع أحداث لم تقع، وقد يؤدي ذلك إلى تحمل المنشأة لخسائر مالية وفقدان الثقة في مخرجات نظم المعلومات المحاسبية.

يشير إنكار الالتزامات في المعاملات الإلكترونية إلى محاولة أحد أطراف تلك المعاملات التهرب من الالتزامات الواقعة عليه عن طريق إنكار وقوع أحداث وقعت بالفعل، أو ادعاء وقوع أحداث لم تقع، وقد يؤدي ذلك إلى تحمل المنشأة لخسائر مالية وفقدان الثقة في المعلومات التي تقدمها نظم معلوماتها المحاسبية. ونتيجة عدم وجود مستندات ورقية والاعتماد على التبادل الإلكتروني للبيانات، وبالتالي فقدان الدليل الإلكتروني الذي يمكن من خلاله إثبات الحقوق والالتزامات، وترتب على ذلك مخاطر إنكار الالتزامات من خلال إنكار أحد أطراف العملية لحدوثها، وعدم التأكد من هوية العميل، مما أدى إلى كثرة الشكاوي من العملاء وإنكارهم إتمام الصفقة والمعاملات وحدث خسائر للمنشآت.⁽²⁾

ويتمثل هذا الخطر في عدم إقرار الشخص المرسل أو المرسل إليه بالتصرف الذي صدر عنه، كأن ينكر أنه هو شخصياً الذي قام بإرسال طلب شراء سلعة أو حصول على خدمة عبر الإنترنت.⁽³⁾ لا تحتوي بروتوكولات الشبكات اللاسلكية على آلية للتأكيد على أن مرسل البيانات قد حصل على إثبات لتسلم المستقبل لرسالته أو على أن المستقبل قد حصل على إثبات لهوية المرسل، لذلك يجب إعداد المسؤولية ضمن بروتوكولات نقل البيانات عبر شبكات، وهناك وسائل تضمن عدم قدرة المستخدم من إنكار أنه هو الذي قام بالتصرف، وهي وسائل ذات أهمية بالغة في بيئة الأعمال الإلكترونية والتعاقدات على الخط، وترتكز هذه الوسائل حالياً على تقنيات التوقيع الإلكتروني وشهادات التوثيق الصادرة عن طرف ثالث.⁽⁴⁾

2-3-5-2: رفض بعض الجهات الحكومية لحجية مخرجات نظم المعلومات المحاسبية المحوسبة استناداً لنصوص تشريعية، كالقانون التجاري وقانون البنوك.

كان معهد بونيمون (Ponemon Institute) قد أجرى استطلاعاً بين المديرين التنفيذيين في عشرات المنشآت في خمس دول في عام 2012، وتوصل إلى أن متوسط إنفاق المنشآت لمكافحة الهجمات الإلكترونية بلغ (9.8) مليون دولار في الولايات المتحدة، و(2.3) مليون في بريطانيا، و(6) ملايين في ألمانيا، و(1.5) مليون في اليابان والخسائر تتراوح بين سرقة بيانات مهمة مثل الأسرار التجارية وبيانات بطاقات ائتمان، إضافة

(1) المري، عايض، (2011)، "أمن المعلومات ماهيتها وعناصرها واستراتيجياتها"، مرجع سابق، من الموقع:

http://www.dralmarri.com/show.asp?field=res_a&id=205

(2) وادي، رشدي عبد اللطيف، (2008)، "أهمية ومزايا البنوك الإلكترونية في قطاع غزة بفلسطين ومعوقات انتشارها"، مرجع سابق، ص: 855-893.

(3) النجار، فايز جمعه، (2010)، "نظم المعلومات الإدارية: منظور إداري"، مرجع سابق، ص: 272.

(4) صقر، ممدوح الشحات، (2007)، "أمن المعلومات"، مرجع سابق، ص: 23.

إلى الخسائر غير المباشرة مثل الضرر الذي يلحق بسمعة المنشأة، حيث أسهم بجعل المنشأة تتأثر سلباً في حال الإعلان عن تعرضها للاختراق الإلكتروني.⁽¹⁾

خاتمة المبحث:

يمكن القول من كل ما تقدم في هذا المبحث، أن جميع المنشآت الاقتصادية - ومنها البنوك التجارية - تعتمد على نظم المعلومات لأداء معظم عملياتها التجارية، وقد أدى الاعتماد المتزايد على نظم المعلومات إلى زيادة نسبية في تأثير مخاطر أمن نظم المعلومات المحاسبية حيث يتضح أن البيئة الاقتصادية الحالية تجلب طائفة جديدة من مخاطر تكنولوجيا المعلومات ذات الصلة، مثل الاحتيال، والكشف عن البيانات السرية، وعدم توافر الخدمات بسبب تعطل الأنظمة، ومخاطر أمن نظم المعلومات لها تأثيرات سلبية تتمثل في تقليل أداء نظم المعلومات المحوسبة أو تخريبها بالكامل أو تعطيل تقديم الخدمات الإلكترونية أو إفشاء المعلومات السرية.

إن مخاطر أمن نظم المعلومات المحاسبية التي يعاني منها القطاع المصرفي تتسبب في خسائر مالية فادحة للبنوك التجارية الأمر الذي سيكون له في نهاية المطاف أثر سلبي على الاقتصاد ككل، ولذلك يجب حماية سلامة ودقة البيانات، وكذلك المحافظة على خصوصية البيانات وسريتها، وتحدد استجابة الأطراف الداخلية لمثل هذه التهديدات بجملة من الإجراءات التي تقوم بها الإدارة والتي هي جزء من مسؤوليتها القانونية أو التعاقدية، فضلاً عن مسؤوليتها الأخلاقية تجاه حملة الأسهم والدائنون لتخفيض اثر التهديدات والمخاطر إلى الحد الأدنى، لذلك ينبغي على المنشآت أن تقوم بتطوير أنظمة الحماية الملائمة وإدارة أنظمتها الداخلية وبما يتناسب والمعايير والقواعد المعمول بها دولياً على أصعدة التأكد من هوية الزبائن وشرعية التوقيع الإلكتروني والتشفير وغيرها، وهذا ما سوف يتم التركيز عليه في المبحث التالي والذي يتناول إجراءات ووسائل الحماية.

(1) عبدالرحيم، شريفة، (2013)، سياق القط والفار بين البنوك والهاكرز، مرجع سابق، من الموقع: <http://economic.ahram.org.eg>

4-2: المبحث الرابع

إجراءات ووسائل الحماية الداخلية لأمن نظم المعلومات المحاسبية المحوسبة

مقدمة:

من خلال المباحث السابقة يتبين للباحث وجود تهديدات ومخاطر مؤثرة سلباً على أمن نظم لمعلومات المحاسبية المحوسبة، حيث تتعرض عملية إدخال البيانات وتجهيزها ونقلها وتوزيعها وحفظها للمعلومات لمخاطر عديدة، وخاصة في المنشآت التي تعمل في مجال التجارة الالكترونية وتستخدم وسائل الاتصالات وشبكات المعلومات في إنجاز أعمالها، وهو ما يستدعي أخذ كافة الوسائل المتاحة والممكنة لتعزيز أمن نظم المعلومات المحاسبية وحمايتها، ومن هنا تظهر الأهمية الكبرى في معرفة سبل حماية نظم المعلومات والقدرة على تقليل التهديدات والمخاطر التي تواجهها.

فإذا ما تم تحديد المخاطر المحدقة بأصول المعلومات وتقييمها، نحتاج إلى اختيار الضوابط المناسبة ووضعها موضع التنفيذ لضمان خفض المخاطر إلى المستوى المقبول لدى المنظمة، ويمكن اختيار عناصر الضبط من بين تلك الواردة في المواصفة الدولية ISO/IEC 27002، أو من غيرها من الضوابط ذات العلاقة، أو من بين الضوابط الجديدة المصممة لتلبية الاحتياجات المحددة حسب الحاجة.⁽¹⁾

وإذا كانت نظم المعلومات المحاسبية المحوسبة هي جزء لا يتجزأ من نظم المعلومات الموجودة بالمنشآت التجارية فإنه ينبغي توفير الحماية المناسبة لهذه النظم حتى تتفادى المنشآت الخسائر التي يمكن أن تحدث نتيجة للمخاطر التي تواجهها هذه النظم، فالوسائل الرقابية وأساليب الحماية المستخدمة في نظم المعلومات بصفة عامة ونظم المعلومات المحاسبية بصفة خاصة تقلل من حدوث هذه المخاطر وتعمل على تلافيها ومعالجتها قبل أن تتسبب في تعطل النظام بشكل كامل.⁽²⁾

وتعرف الضوابط الداخلية لأمن نظم المعلومات على أنها الممارسات والإجراءات والسياسات وهياكل المسؤولية المستخدمة في المنشأة والتي تساعد في إدارة المخاطر وحماية أصول المعلومات، فهي وسيلة لإدارة مخاطر أمن نظم المعلومات بما في ذلك السياسات والإجراءات والمبادئ التوجيهية والممارسات، أو الهياكل التنظيمية والتي يمكن أن تكون ذات طبيعة إدارية أو تقنية أو قانونية،⁽³⁾ فهي مزيج من المقاييس اليدوية

(1) ISO/IEC 27000, (2012), "Information technology - Security techniques -Information security management systems - Overview and vocabulary", OP. Cit., Available at: <http://www.27000.org>

(2) Teru, S. P., & Hla, D. T. (2015). Appraisal of Accounting Information System and Internal Control Frameworks. *International Journal of Scientific and Research Publications*, Volume 5, Issue 9, ISSN 2250-3153, www.ijsrp.org

& Fang, J., & Shu, L. (2016). Modern Accounting Information System Security (AISS) Research Based on IT Technology, *Advanced Science and Technology Letters*, Vol.121 (AST 2016)

(3) Saleh, Mohamed & Alfantooh, Abdulkader, (2011), "A New Comprehensive Framework for Enterprise Information Security Risk Management", *Applied Computing and Informatics*, Vol. 9, King Saud University, Riyadh, Saudi, PP:107-118, <http://www.sciencedirect.com/science/journal/22108327>

والمحوسبة والتي تحمي نظم المعلومات وتتألف من جميع الوسائل والسياسات والإجراءات التي تضمن سلامة موجودات المنشأة، ودقة وموثوقية سجلاتها المحاسبية.⁽¹⁾

إن الرقابة الداخلية هي جزء لا يتجزأ من إدارة المخاطر في أي منشأة وبالتالي فإن نجاح السلطات الإدارية والأجهزة الرقابية في تحقيق أهدافها في إدارة المخاطر والتهديدات الرقابية الناتجة عن الأنشطة والعمليات المصرفية المحوسبة يستلزم تطوير وتكييف إجراءات الرقابة وأدواتها لإحكام السيطرة على المخاطر التي تفرضها استخدام نظم المعلومات المحاسبية المحوسبة في الصناعة المصرفية بسبب خصائص وطبيعة أنشطتها كما يتطلب توفر مجموعة من الخصائص الأساسية في نظم تكنولوجيا المعلومات والاتصالات التي تشكل البنية التحتية للنشاط المصرفي ونظم الرقابة الداخلية،⁽²⁾ ولذلك فإن تطوير وتكييف إجراءات الرقابة الداخلية لمواجهة المخاطر التي تفرضها استخدام تكنولوجيا المعلومات في نظم المعلومات المحاسبية المحوسبة للبنوك أمر ضروري، من خلال تدابير وقواعد معينة يترتب عليها تطوير أساليب السيطرة على إدخال البيانات، وتشغيلها والسيطرة على مخرجاتها،⁽³⁾ وعلى الرغم من أن أي منشأة لا يمكن أن تكون واثقة 100% أن أصولها محمية باستمرار على مدار الساعة 24/7، ولكن الهدف هو الحصول على مستوى معقول من الاطمئنان⁽⁴⁾ ويمكن أن تؤخذ الضوابط الأمنية في نظم المعلومات كمعايير لتقييم المخاطر اعتماداً على الاحتياجات والممارسات المتفاوتة لكل منشأة لأنه من الصعب جداً إجراء تقييمات مع معايير بأكملها.⁽⁵⁾

وفي هذا المبحث سوف يتم التركيز على أبرز الأساليب والوسائل والمعدات التي تساهم في تخفيض المخاطر والتهديدات الداخلية والخارجية التي تهدد أمن نظم المعلومات المحاسبية المحوسبة، وللوصول إلى نظام معلوماتي آمن وفعل يضمن أمن وسلامة البيانات المتضمنة فيه لابد من تصنيف ومعالجة القضايا الأمنية المتعلقة بحمايتها من خلال عدد من المحاور المتعلقة بحماية نظام المعلومات المحاسبية المحوسبة ويمكن تحديد هذه المحاور بمحور حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية المحوسبة، ومحور حماية الأمن المادي لتلك النظم، ومحور حماية أمن الوصول البرمجي لقواعد البيانات، ومحور حماية أمن التخزين غير المتصل بقاعدة البيانات، ومحور حماية أمن المدخلات، ومحور حماية أمن عمليات التشغيل البرمجي، ومحور حماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة، ومحور حماية أمن البيانات والمعلومات المنقولة عبر الشبكات، ومحور حماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة، وسوف يتم تناول هذه المحاور بالتفصيل في هذا المبحث.

(1) Laudon Kenneth C. & Laudon Jane P., (2011), *"Management Information Systems- Managing The Digital Firm"*, OP. Cit., P. 531.

(2) القطناني، خالد محمود، (2007)، "أثر خصائص البيئة التقنية وتكنولوجيا المعلومات في مخاطر الرقابة التشغيلية- دراسة تحليلية في المصارف الأردنية"، مرجع سابق، ص 9-39.

(3) Al-Laith, Ali, (2012), "Adaptation of the Internal Control Systems with the Use of Information Technology and its Effects on the Financial Statements Reliability: An Applied Study on Commercial Banks", *International Management Review*, Vol. 8, No. 1, 2012, PP: 12-19.

(4) Bagranoff, Nancy A. & Simkin, Mark G. & Norman, Carolyn Strand, (2010), *Core Concepts of Accounting Information Systems*, 11th Edition, John Wiley & Sons, INC., U.S.A., P. 378.

(5) Lo, Chi-Chun & Chen, Wan-Jia (2012), "A Hybrid Information Security Risk Assessment Procedure Considering Interdependences Between Controls", *OP. Cit.* PP:247-257.

2-4-1: طبيعة الرقابة الداخلية لنظم المعلومات المحاسبية المحوسبة:

لمعرفة طبيعة نظم الرقابة الداخلية في ظل نظم المعلومات المحوسبة لا بد من معرفة كلاً من مفهومها وأهدافها ومحدداتها وكذلك أنواعها الرئيسية كما يلي:

2-4-1-1: مفهوم نظم الرقابة الداخلية (Internal Control Systems):

تدريجياً متكيفاً مع التطورات السريعة والمتلاحقة في الحياة الاقتصادية، وتعرف الرقابة الداخلية بأنها خطة المنشأة وإجراءاتها وقيودها المتعلقة بالمحافظة على الأصول والثقة في القيود المالية وعرفت الرقابة الداخلية بأنها العملية المصممة والمنفذة من قبل أولئك المكلفين بالرقابة والإدارة والموظفين الآخرين لتوفير تأكيد معقول بشأن تحقيق أهداف المنشأة فيما يتعلق بموثوقية تقديم التقارير المالية وفعالية وكفاءة العمليات والامتثال للقوانين والأنظمة المطبقة، وهي عملية ديناميكية لا تتجزأ فيتم تكيفها باستمرار مع التغيرات التي تواجهها المنشأة، وعلى الإدارة العليا إشراك الأفراد العاملين في جميع المستويات الإدارية بالمنشأة في هذه العملية للتصدي للمخاطر ولتقديم ضمانات معقولة لتحقيق الأهداف العامة للمنشأة.⁽¹⁾

وعليه يرى الباحث أن نظم الرقابة الداخلية هي عبارة عن كافة الوسائل والإجراءات والخطط التي تتبناها إدارة المنشأة لتمكينها من استغلال مواردها بكفاءة، ومساعدتها في تحقيق أهدافها الرئيسية بفعالية، من خلال التأكد من سلامة وكفاءة تنفيذ أعمالها الجارية، وتطبيق سياساتها المتعلقة بحماية الأصول من الضياع والغش وسوء الاستخدام، وضبط البيانات المحاسبية والتأكد من دقتها واكتمالها ومدى الاعتماد عليها، ومنع الأخطاء واكتشافها فور وقوعها وتصحيحها، وتنمية الكفاءة التشغيلية، وتشجيع العاملين على الالتزام بتنفيذ السياسات والتعليمات الإدارية، وبما ضمن حسن سير عمل المنشأة وتحقيق أهدافها بكفاءة عالية.

2-4-2: أهمية وأهداف نظم الرقابة الداخلية في ظل نظم المعلومات المحاسبية المحوسبة:

هناك أهمية متزايدة لوجود نظام كفء وفعال للرقابة الداخلية في ظل استخدام تكنولوجيا المعلومات، فامتلاك المنشأة لإطار عمل جيد لنظم للرقابة الداخلية - كأحد الأدوات المكونة للنظام المحاسبي في بيئة تكنولوجيا المعلومات - سوف يحقق لها كثير من المزايا منها زيادة في فاعلية وكفاءة العمليات التشغيلية،⁽²⁾ والحصول على تقارير مالية ذات درجة عالية من الموثوقية وإمكانية الاعتماد عليها، وحماية الأصول ورفع الكفاءة الإنتاجية، وكذلك الامتثال للقوانين واللوائح المعمول بها، والالتزام بالبرامج التي تؤدي إلى قيادة المنشأة للقطاع

(1) Soudani, Siamak, (2013), "The Impact of Implementation of E-Accounting System on Financial Performance with Effects of Internal Control Systems", *Research Journal of Finance and Accounting*, Vol.4, No.11, PP: 17-27, <http://www.iiste.org>
Hamdan, M. N., & Hosban, A. (2015). The Role of the Auditor in Planning and Reduce the Risk of IT Environment in Commercial Jordanian Banks. *International Journal of Economics and Finance*, 7(11), 222.

(2) Rubino, M., et. Al., (2017), "How IT controls improve the control environment", *Management Research Review*, Vol.40, No.2, PP: 218-234.

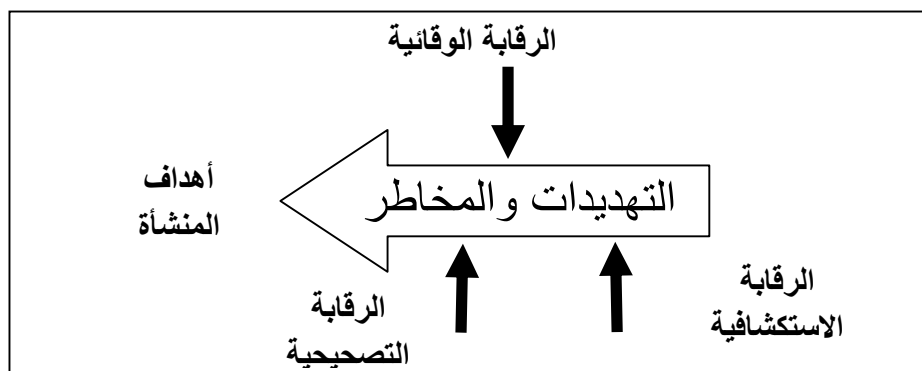
الذي تعمل فيه،⁽¹⁾ حيث لم يعد موضوع أمن وسلامة نظم المعلومات المحاسبية موضوعاً محلياً بل يؤثر أيضاً على الأطراف الخارجية، فقد يشكل خطراً على المنشأة إذ أشار شركاؤها الحاليين أو المحتملين إلى أن هذه المنشأة غير آمنة فيما يتعلق بحماية المعلومات وهو ما يطلق عليه مخاطر السمعة، وبالتالي يجب أن تكون الضوابط الداخلية موحدة مع النظم الإلكترونية في ضوء التطور الكبير في تكنولوجيا المعلومات، كي تلعب دوراً هاماً في الوقاية والكشف عن الغش، وضمان إعداد التقارير المالية موثوق بها وفعالة، وضمان كفاءة وفعالية العمليات، وكذلك الامتثال للقوانين واللوائح المعمول بها.⁽²⁾

ويرى الباحث بما أن أمن نظم المعلومات المحاسبية يتطلب بالضرورة توفير الحماية للمكونات المادية للنظام الذي يقوم بإنتاج هذه المعلومات فإن المسؤولية تقع على عاتق نظام الرقابة الداخلية في سبيل تحقيق ذلك، فوجود نظام للرقابة الداخلية يعتبر أمراً ضرورياً ومحتملاً من خلال قدرته على تقليل مخاطر أمن نظم المعلومات أو الحد منها وبما يؤدي إلى المساهمة في تحقيق الهدف العام للمنشأة التي يعمل في نطاقها.

إن نظم الرقابة الداخلية هي واحدة من الوسائل الرئيسية التي من خلالها يمكن إدارة المخاطر، فهي تستخدم كدرع يحمي أصول المنشأة من العديد من الأحداث غير المرغوب فيها والمخاطر التي تتعرض لها المنشأة، ويطلق على غياب أو ضعف عنصر التحكم بالتعرض، والتي هي بمثابة ثغرات أو ثغوب في درع التحكم،⁽³⁾ حيث ينصب اهتمام نظام الرقابة الداخلية على المخاطر المختلفة والتي تمت الإشارة إليها وعلى حماية موارد المنشأة والمحافظة عليها والتأكد من دقة وصحة البيانات المحاسبية.⁽⁴⁾

إن أهداف المنشأة والبيئة التي تعمل فيها تتطور باستمرار، ولذلك فإن المخاطر التي تواجهها أيضاً تتغير، وهناك ترابط بين أمن نظم المعلومات المحاسبية ونظم الرقابة الداخلية وجودة التقارير المالية.⁽⁵⁾

الشكل رقم (2-4-1) يبين دور الرقابة الداخلية في تحقيق أهداف المنشأة.⁽⁶⁾



(1) Samukri, (2015), Influence Effectiveness of Internal Control System and Implementation of Financial Accounting Information System on the Quality of Accounting Information, *Research Journal of Finance and Accounting*, Vol.6, No.11, (Online) www.iiste.org

(2) Soudani, Siamak, (2013), "The Impact of Implementation of E-Accounting System on Financial Performance with Effects of Internal Control Systems", *Research Journal of Finance and Accounting*, Vol.4, No.11, PP: 17-27, <http://www.iiste.org>

(3) Hall, James A., (2013), *Accounting Information Systems*, 8th Edition, Thomson, South-Western, Lehigh University, Pennsylvania, U.S.A., P.111.

(4) الساكني، سعد & العواودة، حنان، (2012)، "مخاطر استخدام تكنولوجيا المعلومات وأثرها على أداء نظم المعلومات المحاسبية - دراسة تطبيقية لعينة من الشركات المساهمة المدرجة في بورصة عمان للأوراق المالية"، *مراجع سابق*، ص ص: 257-207.

(5) Beard, Deborah & Wen, H. Joseph, (2007), "Reducing the Threat Levels for Accounting Information System, Challenge for Management, Accountants, Auditors and Academicians", *OP. Cit.*, P. 8.

(6) الشكل من إعداد الباحث.

وللرقابة على نظم المعلومات أهمية قصوى لتأثيرها المباشر على كفاءة وفعالية أداء وعمل النظام، بالإضافة إلى حماية أمن وسلامة النظام بمكوناته وموارده من البيانات والمعلومات والملفات التي تحتويها والبرامج التي تقوم بتخزينها وإدارتها وتشغيلها،⁽¹⁾ فوجود نظام رقابة داخلي سليم يعتبر دليل على انتظام الدفاتر والسجلات والعمليات المالية فكلما كانت الأنظمة المطبقة سليمة ودقيقة كلما كانت مكوناتها وعناصرها سليمة والعكس بالعكس، وهناك دراسات حديثة أثبتت أنه يتم الإبلاغ عن الأخطاء والغش في نظم الرقابة الداخلية الضعيفة أكثر مما هو عليه في نظم الرقابة الداخلية القوية، وبالتالي يتوقف نجاح نظم المعلومات المحاسبية على مدى فعالية نظم الرقابة الداخلية، والتي لها تأثير كبير ومباشر على فعالية عمليات إدخال البيانات المحاسبية، وتقنيات تجهيزها وتشغيلها، وأساليب تخزينها، ودقة المعلومات المحاسبية المنتجة، فنظم الرقابة الداخلية مصممة لمراقبة والحفاظ على جودة وأمن أنشطة نظم المعلومات المحاسبية في تنفيذ المدخلات، وعمليات التشغيل، والإخراج، وبالتالي فإن تلك النظم تساعد إدارة المنشأة في المحافظة على دقة البيانات المالية، وحماية أصولها من الخسائر والاختلاس بمنعها أو تقليل احتمال وقوعها.⁽²⁾

3-4-2: أنواع إجراءات ووسائل الحماية الداخلية في نظم المعلومات المحاسبية:

إن أنواع المخاطر والتهديدات الداخلية والخارجية التي تتعرض لها نظم المعلومات المحاسبية، تتطلب تضافر الجهود الفنية المتمثلة بوسائل التكنولوجيا الحديثة للحاسبات بشقيها البرمجي والمادي، وتلك الضوابط قد تتراوح من إجراءات بسيطة إلى إجراءات معقدة تنطوي عادة على مزيج من الأجهزة والبرمجيات، وينبغي لجميع هذه التدابير العمل معاً لتأمين نظم المعلومات المحاسبية بما يحويه من بيانات هامة ومعلومات حساسة.⁽³⁾

ولا شك أن تحقيق ذلك يتطلب أن تشتمل نظم الرقابة الداخلية عند تصميمها على السياسات والإجراءات والآليات الكفوءة والفعالة التي تضمن القيام بإجراءات معالجة المخاطر الأمنية لمنع حدوثها، أو اكتشافها عند أقرب نقطة في دورة تشغيل البيانات، وكذلك تصحيح ومعالجة الآثار المترتبة عليها.⁽⁴⁾

وتهدف الرقابة بشكل عام إلى حماية أصول المنشأة بما في ذلك نظم معلوماتها المحاسبية، لذلك ينبغي تصميم الضوابط والأدوات الرقابية في نظم المعلومات المحاسبية، وتقييم تلك الضوابط بشتى أنواعها للتخفيف أو اللحد من تأثير المخاطر المختلفة، وتتكون إجراءات الرقابة في ظل تكنولوجيا المعلومات من خليط من الأدوات والوسائل اليدوية والآلية التي تتوافق بالفعل مع استخدام الحاسوب،⁽⁵⁾ وتلك الضوابط عموماً يمكن تصنيفها حسب

(1) ياسين، سعد غالب، (2010)، تحليل وتصميم نظم المعلومات، مرجع سابق، ص. 285.

(2) Fardinal, (2013), "The Quality of Accounting Information and The Accounting Information System through The Internal Control Systems: A Study on Ministry and State Agencies of The Republic of Indonesia", OP. Cit., PP: 156-161.

(3) National Institute of Standards and Technology: NIST, (July 2012), "Guide for Conducting Risk Assessments", OP. Cit., Revision. 1.

(4) Brandas, C. & Stirbu, D. & Didraga, O., (2013), "Integrated Approach Model of Risk, Control and Auditing of Accounting Information Systems", OP. Cit., PP: 87-95.

(5) Al-Laith, Ali, (2012), "Adaptation of the Internal Control Systems with the Use of Information Technology and its Effects on the Financial Statements Reliability: An Applied Study on Commercial Banks", OP. Cit., PP: 12-19.

طبيعتها إلى إجراءات إدارية أو تقنية أو مادية، كما يمكن تصنيفها حسب توقيتها الزمني لوقوع الخطر إلى إجراءات وقائية (مانعة) أو اكتشافية (تحذيرية) أو تصحيحية (لاحقة).⁽¹⁾

2-4-3-1: أساليب الرقابة الداخلية على المخاطر وفق غرضها وتوقيتها بالنسبة لحدوث الخطر: تقسم إجراءات وضوابط حماية أمن نظم المعلومات المحاسبية وفقاً لذلك المعيار إلى ثلاثة أنواع رئيسية من عناصر التحكم أو الضوابط الرقابية، تعمل بالتعاقب وفق ثلاثة خطوط أو مستويات دفاعية لمواجهة التهديدات والمخاطر التي تتعرض لها نظام المعلومات المحاسبية، ويمكن النظر إلى هذه الأساليب على أنها عبارة عن حلقات تتضمن مستويات مختلفة للرقابة حيث إذا ما أخفق أحد هذه المستويات في درء الخطر انتقلنا إلى مستوى آخر من الرقابة، وهذه المستويات أو الخطوط الدفاعية الثلاثة يطلق عليها الرقابة الوقائية والرقابة الاستكشافية والرقابة التصحيحية على التوالي،⁽²⁾ والتي تلعب دوراً هاماً في الحد من التهديدات والمخاطر الأمنية التي يتعرض لها أمن نظم المعلومات المحاسبية من خلال منعها أو اكتشافها بعد حدوثها أو من خلال تصحيح تأثير تلك المخاطر، ويمكن تلخيص هذه المستويات على النحو التالي:⁽³⁾

1. الرقابة المانعة أو الوقائية (السابقة لحدوث المخاطر) (Preventive Control): هي مجموعة من الضوابط والآليات وأساليب الحماية التي يتم تصميمها وتستخدم كخط دفاع أول لمنع حدوث مخاطر أمن نظم المعلومات المحاسبية قبل وأثناء وقوعها للحد منها بشكل كامل،⁽⁴⁾ وتنتم من خلال أداتين مهمتين هما رقابة التحقق من صحة الوصول المادي والمنطقي إلى نظم المعلومات المحاسبية، ورقابة التخويل لمن له حق الوصول إلى تلك النظم،⁽⁵⁾ ويعتبر إتباع منهجيات الحماية المسبقة مهماً على صعيد أمن أنظمة المعلومات، والقيمة التي تضيفها الرقابة الوقائية بمنعها التهديدات والمخاطر تفوق كثيراً تلك التي تضيفها الرقابة الاستكشافية والتصحيحية، لاسيما وأنه بات من المعروف الآن بأن المنهجيات القائمة على رد الفعل قد تكون فاشلة في صد بعض المخاطر، ولكن يصعب تنفيذها فلا يمكن منع حدوث جميع المخاطر، لأنه لا يمكن القول بأن هناك حماية (100%) لنظم المعلومات المحاسبية، لكثرة تكاليف الاحتياطات الخاصة بها إذ عندما يتوفر الوقت والموارد الكافية يمكن وضع رقابة وافية،⁽⁶⁾ وإدارة وتقييم المخاطر في المنشأة - التي نوقشت في مبحث سابق- تساعد إدارة المنشأة على تحديد المجالات التي ينبغي أن تكون الضوابط الوقائية ملائمة، ومن أمثلة هذه الضوابط استخدام رجال الحراسة، والنسخ الاحتياطي، ومنظم الطاقة الكهربائية (UPS)، والفصل بين المهام والواجبات، والحماية من الفيروسات، والجدران النارية، ونظم كشف التسلل، وإدارة كلمات المرور، ومنع إقفال الدفاتر والسجلات في حال وجود خطأ، وغيرها.

(1) خليل، عطا الله وزّاد، (2011)، " آليات أمن المعلومات في ظل الانفتاح المعلوماتي "، مرجع سابق، ص: 589 – 641.

(2) Hall, James A., (2013), *Accounting Information Systems*, OP. Cit., P. 108.

(3) محمد، طارق مختار، (2011)، "تفعيل دور الرقابة الداخلية في الأنشطة المصرفية في ظل نظام المعلومات المحاسبية الإلكترونية"، *المجلة العلمية للاقتصاد والتجارة*، العدد (1)، كلية التجارة، جامعة عين شمس، القاهرة، مصر، ص: 578-665.

(4) Bagranof, Nancy A. & Simkin, Mark G. & Norman, Carolyn S. (2010). *Accounting Information Systems*, OP. Cit., P. 356.

(5) Romney, Marshall B. & Steinbart, Paul J., (2015), *"Accounting Information Systems"*, OP. Cit., P. 171 & P. 243.

(6) Turner, Leslie & Weickgenannt, Andrea, (2013), *Accounting Information Systems: Controls And Processes*, 2nd Edition , John Wiley & Sons, New Jersey, USA, 2013, <http://my.safaribooksonline.com/book/accounting/9781118162309>

2. الرقابة الاستكشافية أو التحذيرية (المتزامنة مع حدوث المخاطر) *(Detective Control)*: هي مجموعة من

الضوابط والآليات وأساليب الحماية التي يتم تصميمها في نظم المعلومات لتستخدم كخط دفاع ثاني بهدف تحذير الإدارة والعاملين أثناء حدوث تهديدات ومخاطر أمن نظم المعلومات المحاسبية التي لم تستطع الرقابة الوقائية من النجاح في منعها، فمن غير الممكن منع جميع المخاطر قبل حدوثها بشكل تام ومطلق، وهناك مخاطر لا يمكن مراقبتها بشكل مسبق، لذلك يتم اللجوء لاستخدام تلك الرقابة التشخيصية المصممة لاكتشاف المخاطر عند حدوثها، إذ تعمل الرقابة الاستكشافية على تحسين أمن نظم المعلومات من خلال مراقبة مدى كفاية الرقابة الوقائية، واكتشاف التحايل على الرقابة الوقائية في حالة حدوثها، وتهدف إلى مراقبة المخاطر المختلفة المحتمل أن تتعرض لها النظم الالكترونية والتقرير عنها للمسؤولين لاتخاذ كافة الإجراءات اللازمة،⁽¹⁾ ومنطق عمل هذا النوع من الرقابة يعتمد على المقارنة بين الإحداث التي تحصل وبين ما هو معياري لها وعند ذلك نكتشف الأخطاء والتزوير والتلاعب، وتعد الرقابة الاستكشافية أهم من الرقابة التصحيحية، ولكنها ليست بمستوى أهمية الرقابة الوقائية، ومن أمثلة لضوابط الاستكشافية أو التحذيرية استخدام مسارات التدقيق ومطابقة سجلات جرد النقدية، ومصادقات العملاء بأرصدتهم، وبرامج الكشف عن الفيروسات، ووضع كاميرات وشاشات المراقبة، وتقارير وسجلات كشف التسلل وتحليل الدخول، واختبارات الاختراق الدورية، وغيرها.⁽²⁾

3. الرقابة التصحيحية أو العلاجية (رقابة لاحقة بعد حدوث الخطر) *(Corrective Control)*: وهي الضوابط

والإجراءات التي يتم تصميمها في النظام لتصحيح الثغرات ونقاط الضعف بعد حدوث المخاطر أو الكوارث الطبيعية وتخفيض أو الحد من التأثيرات الناتجة عن حدوثها،⁽³⁾ وهذه الضوابط تتعامل مع المخاطر بعد اكتشافها، حيث أن كشف المخاطر أمر مهم ولكن لا جدوى منه إذا لم تتبعه إجراءات تصحيحية وبصفة مستمرة وفي الواقع يتوفر معياران في هذا الصدد هما ردة الفعل تجاه تلك المخاطر، واتخاذ إجراء تصحيحي في الوقت المناسب.⁽⁴⁾ وحتى تكون هذه الضوابط ذات كفاءة على الإدارة وضع نظام يسلط الضوء على المخاطر ومتابعتها لحين تصحيحها وعدم السماح بتكرار حدوثها، وهذه الضوابط مكملية للأنواع السابقة حيث إنها تقوم بمعالجة المخاطر التي تجاوزت الضوابط الوقائية وتم اكتشافها من خلال الضوابط الكاشفة.

وتعد الخط الدفاعي الثالث والأخير، فالرقابة الاستكشافية ينحصر دورها بتحديد التهديدات والمخاطر وجلب الانتباه إليها، إما الرقابة التصحيحية فأنها تقوم بالإصلاح والمعالجة للتهديدات والمخاطر التي لم تستطع الرقابة الوقائية منعها، ولم تستطع الرقابة الاستكشافية معالجتها، لأن هناك الكثير من التهديدات والمخاطر التي تكتشف وتصح تلقائياً، مثال على هذا النوع من الإجراءات التصحيحية تحديث البرامج الأمنية والتشغيلية مع الأخذ في الاعتبار نقاط الضعف المكتشفة، وإنشاء نسخ احتياطية من الملفات الرئيسية والتطبيقات الهامة ووضعها في مكان

(1) محمد ، طارق مختار، (2011)، "تفعيل دور الرقابة الداخلية في الأنشطة المصرفية في ظل نظام المعلومات المحاسبية الإلكترونية"، مرجع سابق، ص: 578-665.

(2) Tayeh, A., (2008), "Effectiveness of Information Security Management at the Palestinian Information Technology Companies", OP. Cit., P. 46.

(3) محمد ، طارق مختار، (2011)، "تفعيل دور الرقابة الداخلية في الأنشطة المصرفية في ظل نظام المعلومات المحاسبية الإلكترونية"، مرجع سابق، ص: 578-665.

(4) Romney, Marshall B. & Steinbart, Paul J., (2015), "Accounting Information Systems", OP. Cit., P. 171.

أمن، ووضع خطط طوارئ للاستمرار بالعمل ومواجهة الكوارث والأحداث الطارئة التي تتعرض لها النظم، وتعيين مدير تنفيذي أو جهاز تنظيمي مسؤول عن أمن نظم المعلومات من واجباته تقييم البيئة التي تعمل بها تلك النظم، وتحليل وتقييم المخاطر التي تهددها، عن طريق القيام بإجراء تحريات دقيقة والتحقيق من الظروف التي أدت إلى حدوث هذه المخاطر وبصفة عامة فإن المعلومات التي يتم الحصول عليها من خلال هذه التحريات يمكن استخدامها عند تخطيط سياسة الأمن المتعلقة بالأنظمة الإلكترونية، ويجب أن لا تعامل إجراءات الرقابة الوقائية والاستكشافية والتصحيحية بشكل منفصل بل يجب أن تكون تلك الإجراءات والضوابط وفق منظومة عمل متكاملة للحماية والأمن في نظم الرقابة الداخلية لنظم المعلومات المحاسبية.⁽¹⁾

وفي رأي الباحث عندما تفشل جميع إجراءات الأمن في التغلب على تهديد معين، فإن الوسيلة الوحيدة الباقية هي إعادة تصميم النظام مرة أخرى مع اتخاذ الإجراءات الأمنية الجديدة التي تعمل على منع مثل هذا التهديد.

2-3-4-2: أساليب الرقابة الداخلية على المخاطر الأمنية وفق هيكل الإطار العام لنظم الرقابة الداخلية: لا تختلف

مقاييس الرقابة والأمان في بيئة نظم المعلومات المحاسبية المحوسبة عنها في البيئة التقليدية ولكنها تختلف عنها في آليات التنفيذ، حيث اتجهت معظم منشآت الأعمال إلى تصحيح نظم معلوماتها المحاسبية وبنائها بمواصفات محددة بهدف السيطرة على الكم الهائل من المعلومات الضرورية وضمان موثوقية كبيرة لها، ونتيجة لظهور الإدارة العلمية الحديثة بمفاهيمها وأساليبها المتطورة في المنشأة الاقتصادية والازدياد الهائل في كمية البيانات والمعلومات المحاسبية أوجب توفر ضوابط رقابية تتضمن جودة تلك البيانات والمعلومات.⁽²⁾

ومن أجل تحقيق تلك الأهداف كان لا بد من تصميم ضوابط رقابية في هذه النظم تتضمن عنصرين الأول يهتم بوضع السياسات العامة والثاني يهتم بمجموعة الإجراءات التي تبين كيف يتم تنفيذ تلك السياسات، ولذلك هناك مجموعتان من الضوابط والإجراءات الرقابية الخاصة بنظم المعلومات المحاسبية المحوسبة، هما الضوابط الرقابية العامة وضوابط الرقابة على التطبيقات.⁽³⁾

وقد اعتمدت لجنة بازل للإشراف المصرفي هذا التقسيم للضوابط الرقابية والتي يجب تصميمها في النظم المحاسبية للمنشآت المصرفية عند تحديدها للإطار العام لنظم الرقابة الداخلية في المنشآت المصرفية حيث أشارت إلى ضرورة أن تتضمن نظم المعلومات كل من الرقابة العامة والرقابة التطبيقية.⁽⁴⁾

1. الضوابط الرقابية العامة (General controls): وهي ضوابط لا تتعلق مباشرة بالعمليات المحاسبية ولكنها ذات أهمية عالية لنظم المعلومات المحاسبية المحوسبة، كونها تمثل سياسات رقابية إدارية وتنظيمية يتم تطبيقها على إدارة نظم المعلومات، حيث أنه يوجد هناك ضوابط رقابية لا تتعلق مباشرة بالعمليات المحاسبية، بل لها

(1) Bagranof, Nancy A. & Simkin, Mark G. & Norman, Carolyn S. (2010), *Accounting Information Systems*. OP. Cit., P. 3567.

(2) Christopher, Joe; Sarens, Gerrit; Leung, Philomena. (2009), "A critical analysis of the independence of the internal audit function: evidence from Australia", *Accounting, Auditing & Accountability Journal*, Vol. 22 Issue 2: P 200-220, P.204.

(3) Anomah, Sampson & Agyabeng, Owusu. (2013), "Evaluating internal controls in a computerized works environment – a risk to audit professionals and a challenge to accountancy training providers", *OP. Cit.*, PP: 132- 143.

(4) محمد، حيدر صاحب، (2011)، "مسؤولية مراقب الحسابات في تحديد وتقييم مخاطر تكنولوجيا نظم المعلومات المحاسبية لرفع جودة أدائه"، *مراجع سابق*، ص: 72.

منفعة ملحوظة لنظم المعلومات المحاسبية ويطلق على هذه الضوابط الرقابية مصطلح أساليب الرقابة العامة، وهي تمثل المعايير والتوجيهات التي يلتزم بإتباعها المختصون بوظائف جمع المعلومات وتبويبها وتلخيصها.⁽¹⁾ وتعني السياسات والإجراءات التي تتعلق بالعديد من التطبيقات وتدعم العمل الفعّال لعناصر رقابة التطبيق، ولذلك فإن الأساس الذي تقوم عليه الضوابط العامة هو ضمان أن يتم إجراء معالجة المعلومات بناء على عناصر معقولة من السيطرة والتحكم وكذلك وفق بيئة متسقة،⁽²⁾ وذلك من خلال المساعدة في ضمان التشغيل الصحيح المستمر لنظم المعلومات والتأكد من أن النظم مستقرة وآمنة وتدار بشكل جيد، وتشمل عناصر الرقابة العامة لتكنولوجيا المعلومات عناصر الرقابة على مركز البيانات وعمليات الشبكة وامتلاك وتغيير وصيانة برامج الأنظمة وأمن الوصول وامتلاك نظم التطبيق وتطويرها وصيانتها وتعدد الأنشطة الرقابية التي تتعلق ببيئة معالجة المعلومات الشاملة،⁽³⁾ فهي رقابة إجمالية تؤسس هيكل عام لمراقبة التصميم والأمن، واستخدام برامج الحاسوب من خلال المنشأة،⁽⁴⁾ وهي ضوابط إدارية أو منطقية أو تقنية تعمل وفق منهجية تكاملية وهي ضرورية وتدعم عدة تطبيقات في آن واحد وتعد من أهم متطلبات فعّالية الضوابط التطبيقية، حيث تعدّ الرقابة العامة الأساس المناسب لوضع الرقابة على التطبيقات حيث أن ضمان نجاح الرقابة العامة تؤدي إلى تحقيق نجاح الرقابة على التطبيقات ولذلك يكون لأي موطن ضعف في أساليب الرقابة العامة آثار بالغة على كافة عمليات معالجة البيانات.

وتطبق ضوابط الرقابة العامة على كافة مكونات نظم المعلومات المحاسبية من الأجهزة والشبكات والبرامج والبيانات والأفراد،⁽⁵⁾ ومن أهم أهداف الرقابة العامة في نظم المعلومات المحاسبية تطوير خطة أمن تلك النظم بما فيها التخطيط للكوارث التي تهددها، والحماية المادية للأصول، وتدريب الأفراد مع الفصل بين المهام المتعارضة، والرقابة المنطقية على الوصول إلى البيانات، وتنفيذ معايير توثيق وتطوير تلك النظم، ويتم تحقيق ذلك من خلال توفير مجموعة من الأساليب تتعلق بكل من: أمن الأفراد، أمن الأجهزة والمعدات، أمن البرمجيات، أمن نظام الاتصالات، ولذلك تنقسم الضوابط الرقابية العامة في نظم المعلومات المحاسبية المحوسبة إلى ضوابط تنظيمية وإدارية، وضوابط تطوير وتعديل النظم وتوثيقها، وضوابط مادية على أمن الأجهزة والمعدات، وضوابط الوصول لنظم المعلومات المحاسبية.⁽⁶⁾

2. الضوابط الرقابية على التطبيقات (Application Controls): وهي الإجراءات الرقابية المحوسبة واليدوية المطبقة على دورات تشغيل البيانات في نظم المعلومات المحاسبية بداية من تسجيل العمليات المالية ومروراً

(1) البجيصي، عصام، (2014)، "مدى فعالية نظام الرقابة الداخلية في ظل نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على البنوك العاملة في قطاع غزة"، مجلة جامعة فلسطين للأبحاث والدراسات - العدد (6)، غزة، فلسطين، ص: 78-95.

(2) Bodnar, George H. & Hopwood, William S., (2012), Accounting Information Systems, OP. Cit., P.149.

(3) IFAC, IAASB, (2009), Handbook of International Auditing, Assurance, and Ethics pronouncements, International Federation of Accountants, New York, USA, P. 315.

(4) النجار، فايز جمعه، (2010)، "نظم المعلومات الإدارية : منظور إداري"، مرجع سابق، ص 258.

(5) Davis, Chris & Schiller, Mike & Wheeler, Kevin, (2011), "IT Auditing: Using Controls to Protect Information Assets", 2nd Edition, Mc Graw Hill, Network Pro Library, New York, USA., P. 178.

(6) حمادة، رشاء، (2010)، "أثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية في زيادة موثوقية المعلومات المحاسبية"، دراسة ميدانية، مرجع سابق، ص: 305-334.

بمعالجتها وحتى التقرير عنها،⁽¹⁾ فهي مصممة ضمن برامج التطبيقات لضمان توفير درجة معقولة من سلامة وصحة واكتمال عمليات تسجيل ومعالجة البيانات وإعداد التقارير المحاسبية.⁽²⁾

وتعتبر خط الدفاع الأول وأحد أجهزة الإنذار المبكر لمنع وصد وتحجيم المخاطر التي يمكن أن تتعرض لها نظم المعلومات المحاسبية من خلال تلك الضوابط التي تعمل على التأكد من صحة ودقة وسلامة البيانات والمعلومات المحاسبية خاصة في ظل العمليات المصرفية الالكترونية، فبينما ترتبط ضوابط الرقابة العامة بكافة تطبيقات نظم المعلومات المحاسبية فإن ضوابط الرقابة على التطبيقات تقتصر على تطبيقات محددة في نظم المعلومات المحاسبية دون غيرها، لأن الهدف من الرقابة على التطبيقات التأكد بدرجة مقبولة من أن التسجيل، والتشغيل، والتقرير عن المعلومات المحاسبية والمالية التي قام بها الحاسوب قد تم تنفيذها بصورة ملائمة.⁽³⁾

وفي الأغلب تقسم الضوابط الرقابية التطبيقية في بيئة نظم المعلومات المحاسبية المحوسبة إلى ثلاثة أقسام هي الضوابط الرقابية على المدخلات، والضوابط الرقابية على معالجة وتشغيل البيانات، والضوابط الرقابية على المخرجات، وضوابط التطبيق تعنى الدقة والاكتمال وصلاحيات التفويض في إدخال البيانات وتجهيزها وتخزينها إلى نظم أخرى.⁽⁴⁾

الجدير بالذكر أن الأساليب الرقابية التطبيقية كذلك تشمل أساليب رقابية وقائية (Preventive)، وأساليب رقابة اكتشافية (Detective)، وأساليب رقابة تصحيحية (Corrective)، ولكن معظم إجراءات تلك الأساليب بطبيعتها وقائية أو استكشافية لأنها تعمل على منع أو كشف أنواع متعددة من التحريفات في كافة مراحل التطبيق،⁽⁵⁾ وغالبية تلك الأساليب تتجه نحو الرقابة الوقائية أكثر من اتجاهها نحو الرقابة بالتغذية العكسية (الراجعة)، كما أن العديد من هذه الأساليب يهدف إلى اكتشاف الأخطاء التي يصعب اكتشافها في غياب مثل هذه الأساليب.⁽⁶⁾

ويرى الباحث إن إتباع هذه المراحل سوف يساهم في سلامة وصحة نظام المعلومات المحاسبي المحوسب وبياناته وذلك من خلال تخفيض الآثار والمخاطر التي يمكن أن يتعرض لها النظام إلى أقل حد ممكن، مع الأخذ في الاعتبار أن هذه الضوابط لا تمثل متطلبات مطلقة أو أفضل ممارسة رقابية يجب الالتزام بها وإنما تمثل إرشادات ومعايير متعارف عليها تهدف إلى تكوين إطار عام لتحقيق الرقابة الداخلية، وإن اعتبارها ضوابط مطلقة سيؤدي إلى إعاقة تطويرها وتحديثها خصوصاً مع ارتفاع وتيرة التطور في مجال تكنولوجيا المعلومات والاتصالات.

(1) Bodnar, George H. & Hoop-wood, William S. (2010). *Accounting Information Systems*, 10th Ed. NJ: Prentice Hall, P.151.

(2) Davis, Chris & Schiller, Mike & Wheeler, Kevin, (2011), "IT Auditing: Using Controls to Protect Information Assets", 2nd Ed., Mc Graw Hill, Network Pro Library, New York, USA, 2011, P.

(3) Anomah, Sampson & Agyabeng. Owusu, (2013), "Evaluating internal controls in a computerized works environment – a risk to audit professionals and a challenge to accountancy training providers", *OP. Cit.*, PP: 132- 143. , www.iiste.org

(4) Bafghi, A. A. S. T., (2014), "Status and Security of Accounting Information Systems in Iranian Organizations", *International Journal of Economy, Management and Social Sciences*, Vol. 3, No. 12, PP: 71-76.

(5) Arens, Alvin A., Elder, Randal J., & Beasley, Mark S., (2014), *Auditing & Assurance Services: An Integrated Approach*, OP. Cit., P.695.

(6) فاضل، عبدالكريم محمد يحيى، (2012)، "مدى تأثير استخدام الصيرفة الإلكترونية على فاعلية الرقابة التطبيقية لنظم المعلومات المحاسبية المحوسبة - دراسة ميدانية لدى البنوك التجارية اليمنية"، *مرجع سابق*، "بحث مقبول للنشر".

وهناك علاقة وثيقة بين الرقابة العامة والرقابة على التطبيقات في بيئة الحاسوب، فالرقابة العامة تدعم فعالية أداء الرقابة على التطبيقات، وهناك حاجة إلى كليهما لضمان المعالجة الكاملة والصحيحة للمعلومات، فإذا كانت الإجراءات الرقابية العامة غير فعّالة، فإن الرقابة على التطبيقات قد لا تكون ملائمة ويمكن تجاوزها، ومن الضروري تطوير الإجراءات الرقابية كي تكون فعّالة ومواكبة للتغير السريع في تكنولوجيا المعلومات، والذي حتماً سيؤدي إلى تغيير في الأنشطة الرقابية، وكيفية تطبيقها، مع عدم تغير المتطلبات الأساسية للرقابة.

2-4-4: حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية المحوسبة:

إن الرقابة التنظيمية للأفراد العاملين في نظم المعلومات المحاسبية تتمثل في تحديد صلاحيات تنفيذ العمليات، وفصل المسؤوليات للعمليات والمهام المختلفة، وتحديد مهمة الإشراف على عمليات النظام ومهامه، وتحديد السجلات المحاسبية المستخدمة يدوياً أو إلكترونياً، وطريقة الوصول إلى المعلومات ومدى صلاحيتها، والاستقلالية في التحقق من عمليات النظام ومهامه.⁽¹⁾

وأمن الأفراد يشمل تعيين موظفين جدد من ذوي المؤهلات العلمية والخبرة العملية، فضلاً عن تدريب العاملين ورفع كفاءتهم وزجهم بدورات متخصصة في مجال الرقابة الداخلية ونظم المعلومات المحاسبية وأمن وتكنولوجيا المعلومات.

وفي رأي الباحث فإن الأمن التنظيمي للأفراد يركز على تقسيم العمل داخل وخارج دوائر نظم المعلومات المحاسبية بهدف تخفيض المخاطر التي تهدد أمن تلك النظم.

وكما عرفنا سابقاً في المبحث الثالث من الفصل الأول إن أفراد المنشأة يشكلوا مصدر تهديد كبير على المنشأة سواء عن طريق الإهمال أو التصرفات المتعمدة التي قد تصل إلى حد تحقيق مكاسب مادية من وراء بيع معلومات المنشأة، مما يتطلب إعطاء أهمية كبيرة لرقابة وحماية أمن الأفراد العاملين في نظم المعلومات المحاسبية المحوسبة.⁽²⁾

ويرى الباحث أن العنصر البشري هو العنصر الأهم القادر على توفير وتطوير الجدار الأمني لنظم المعلومات المحاسبية، حيث ترتبط محاولات الاختراق بالتطور مما يوجب حالة عالية من المرونة في بناء الأنظمة الأمنية والتي يمكن تحقيقها عبر التأهيل البشري المستمر للكوادر البشرية، وإن النظام الرقابي لأمن نظم المعلومات المحاسبية مهما بلغت نزاهته ومصداقيته لن يتفوق على نزاهة ومصداقية من أوجده ومن يقوم على صيانته، وأفضل طريقة لنقل رسالة السلوك الأخلاقي داخل المنشأة تكون من خلال أفعال الإدارة باعتبارها قدوة لبقية أفراد المنشأة، لذلك على الإدارة تبني رسالة مفادها عدم التنازل عن النزاهة والقيم الأخلاقية، وإيصال هذه الرسالة للموظفين وإدراكهم لمضمونها والالتزام بها قولاً وفعلاً وبشكل مستمر بأعلى المعايير الأخلاقية أثناء تعاملها مع الأطراف كافة.

(1) Hall, James A., (2013), *Accounting Information Systems*, OP. Cit., PP152-155.

(2) حسين، أماني حسين، (2006)، " إطار مقترح لتقييم الرقابة الداخلية لأنشطة التجارة الإلكترونية"، *أطروحة دكتوراه غير منشورة*، جامعة حلوان، حلوان، مصر، ص: 99-100.

2-4-5: حماية الأمن المادي لنظم المعلومات المحاسبية المحوسبة:

ويمثل الأمن المادي الضوابط والتدابير المادية والبيئية الملموسة والمترابطة والمتداخلة مع تنفيذ السياسة الأمنية وهي ضوابط تتخذ لكشف أو ردع التدخلات والمخاطر المادية من سرقة أو إساءة استخدام النظم من منظور مادي وبالتالي منع الخسارة أو الضرر أو تعطل وتوقف أنشطة الأعمال وبما يؤدي إلى حسن أداء التجهيزات المحوسبة ومصادر الطاقة وإاحتها بشكل دائم ومستمر وبما يضمن إدانة العمليات وعدم توقفها.

ويتم الأمن المادي من خلال الإجراءات المصممة لإحكام السيطرة على الوصول المادي للأجهزة كلها، ومن هذه الإجراءات وضع أجهزة الحاسوب في أماكن آمنة ومناسبة، وعدم السماح بالدخول إلى غرفة الحاسب المحصنة إلا للأشخاص المخولين بموجب تفويض رسمي واستخدام الأقفال والحواجز وأجهزة التنبيه وأجهزة الإنذار للإعلان عن الوصول غير المصرح به، واستخدام منظمات التيار وأجهزة عدم الانقطاع لضمان استمرارية التيار الكهربائي،⁽¹⁾ كما تشتمل على جميع الأشكال والمتطلبات اللازمة لحمايتها من الاختراقات ومن حسن استخدامها وسلامتها وصيانتها كلما تطلب ذلك، مع وجود أجهزة بديلة لاستخدامها في الحالات التي تتعرض فيها الأجهزة العاملة للعبث أو الخراب، بالإضافة إلى وجود تعليمات محددة للتعامل مع هذه الأجهزة، وتطبيقها بالشكل السليم الموضوع من أجله.⁽²⁾

إن الهدف من الأمن المادي لنظم المعلومات المحوسبة لا يتعلق فقط بحماية البيانات والمعلومات، لكنها تتعلق أيضاً بجوانب أخرى، كحماية سلامة الكيانات البرمجية والمادية لتلك النظم، وضمان استمرارية خدمات النظم المحوسبة،⁽³⁾ فالأمن المادي الفعال هو جزء لا يتجزأ من برنامج الأمن الشامل الذي يشمل كل العناصر المكونة لنظم المعلومات المحاسبية، ولذلك يعد الأمن المادي من الوسائل المهمة جداً لتوفير الحماية المادية لنظام المعلومات المحاسبية بمكوناتها المختلفة من التخريب والسرقة والأعطال المقصودة وغير المقصودة،⁽⁴⁾ ومن الناحية العملية ليس هناك حاجة إلى وقاية هذه الأجهزة والمعدات ضد المخاطر العرضية غير المقصودة نظراً لمتانة هذه الأجهزة وقدرتها على تحمل الظروف التشغيلية مهما بلغت شدتها، ولذلك يتركز الجهد الكبير في الوقت الحاضر على حماية أجهزة الحاسوب ضد مخاطر محاولات التخريب المقصودة، أو المخاطر الناتجة عن الكوارث البيئية، التي سبق تناولها في الفصل الأول من هذه الأطروحة.

(1) Romney, Marshall B. & Steinbart, Paul J., (2015), "Accounting Information Systems", OP. Cit., P. 247.

(2) قاسم، عبدالرزاق & الردايدة، مراد، (2010)، "أمن البيانات ونظم المعلومات المحاسبية في بيئة تكنولوجيا المعلومات في البنوك الأردنية - دراسة ميدانية"، مرجع سابق، ص: 91-111.

(3) Joseph, Rhoda & Jeffers, Patrick, (2009), "E-Government in the Caribbean Nations", Journal of Global Information Technology Management, Vol. 12, No. 1, PP: 52-71.

(4) Romney, Marshall B. & Steinbart, Paul J., (2015), "Accounting Information Systems", OP. Cit., P. 243.

2-4-6: حماية أمن الوصول البرمجي لقواعد بيانات نظم المعلومات المحاسبية المحوسبة:

يتم تخزين البيانات في قاعدة بيانات مرتبطة بنظام المعلومات المحاسبي، حيث تخزن كافة البيانات والمعلومات التي يتداولها النظام على تلك القواعد، فهي تمثل وعاء لكافة تعاملات النظام، وتتكون من مجموعة الملفات المرتبطة مع بعضها البعض بصورة منطقية ومخزنة بشكل منظم بحيث يسهل وصول البرامج التطبيقية إليها، ولا يمكن اعتبار النظم محمية ما لم يكن هناك تكاملاً أمنياً يشمل الأجهزة والبرمجيات على حد سواء وهنا لا بد من وجود تعليمات مركزية بشأن كتابة البرامج خصوصاً تلك التي تمس أمن نظم المعلومات، لذلك لابد من وضع نظام لحماية قاعدة البيانات من المخاطر التي قد تتعرض لها، وتزداد خطورتها في ظل التشغيل المباشر للبيانات عنه في ظل التشغيل الجماعي، لأن التشغيل المباشر يتم من خلال قاعدة البيانات حيث تمكن معظم المنشآت المستخدمين والعملاء والموردين من الوصول المباشر إلى نظم معلوماتها عن بعد عبر الانترنت عن طريق استخدام أجهزة المودم.⁽¹⁾

والتحكم في الوصول البرمجي (*Access Control*): يشير إلى عمليات السيطرة على الوصول للنظم والشبكات استناداً إلى نظم معلومات الأعمال وبما يتوافق مع المتطلبات والسياسات الأمنية للمنشأة،⁽²⁾ وهي واحدة من الضوابط المنطقية والفنية أو التقنية التي يمكن استخدامها في الأجهزة والبرامج على نطاق واسع لتحقيق ضمان معقول بعدم الوصول غير المصرح به والمحافظة على نظم معلومات آمنة ومتسقة،⁽³⁾ وهي وسائل مستخدمة وإجراءات مصممة ومنفذة لمنع أي شخص غير مخول له بالوصول إلى المكونات المنطقية للنظام وقواعد البيانات عن طريق وضع العوائق أمام هذا الوصول غير المشروع للبيانات سواء من داخل المنشأة أو من خارجها.⁽⁴⁾

ولكي يتحقق أمن نظم المعلومات المحاسبية فإنه لا بد من تناول الوسائل والإجراءات المختلفة لحماية أمن الوصول البرمجي لقواعد بيانات تلك النظم، وتهدف هذه الوسائل إلى حماية البيانات من الانكشاف للأشخاص غير المخولين، سواء عن قصد أو غير قصد،⁽⁵⁾ وتتباين هذه الوسائل بدرجة فاعليتها وتعقيدها وذلك حسب البرامج المصممة لهذا الغرض، ومن أهم تلك الوسائل والإجراءات: طرق تحديد الهوية كإدارة واستخدام كلمات السر، ومصفوفة الرقابة على الوصول، والبرامج المضادة للفيروسات، وتشفير البيانات والمعلومات، وبرامج الجدران النارية، ونظم التوثيق ومنع الاختراق، واختبارات فحص الاختراق، وحماية الخوادم الرئيسية.

(1) الجواد، دلال صادق & الفتال، حميد ناصر، (2008)، "أمن المعلومات"، مرجع سابق، ص 103.

(2) Ojha, Vibha & Sharma, Neha, (2011), "Security Threats for Organization Information Systems", *International Journal of Computer - Electronics & Electrical Engineering*, Vol.2, No.3, PP:7-10, www.ijceee.org

(3) Rafique, Rajia & Mehmood, Furhan (2010), "Management of Operational Risks Related to Information Security in Financial Organizations", *OP. Cit.*, P.6.

(4) Beard, Deborah & Wen, H. Joseph, (2007), "Reducing the Threat Levels for Accounting Information System, Challenge for Management, Accountants, Auditors and Academicians", *OP. Cit.*, PP: 34-42.

(5) الداهمة، سليمان مصطفى، (2008)، "أساسيات نظم المعلومات المحاسبية وتكنولوجيا المعلومات"، مرجع سابق، ص 668.

2-4-7: حماية أمن التخزين غير المتصل بقاعدة البيانات في نظم المعلومات المحاسبية:

المقصود بتأمين البيانات هو حماية البيانات من الفقد أو التلف أو سوء الاستخدام ثم تأمين استعادة هذه البيانات إذا فشلت إجراءات تأمينها لسبب ما، وهناك مسائل متصلة بوسائل التخزين خارج النظام من حيث تحديد وسائل التخزين المستخدمة وتبويبها وحفظها والوصول إليها وتبادلها وإتلافها،⁽¹⁾ وهنا سوف نناقش متطلبات التعامل مع الوسائل الممغنطة،⁽²⁾ حيث يمثل وقت الحفظ، وحماية النسخ الاحتياطية، ونظام الترقية والتبويب، وآلية الاسترجاع والاستخدام، ومكان الحفظ وأمنه، وتشفير النسخ التي تحتوي معطيات خاصة وسرية، مسائل رئيسية يتعين اتخاذ معايير واضحة ومحددة بشأنها،⁽³⁾ وفي هذا الصدد يتم التركيز على عمل نسخ احتياطية للبيانات (Data Back-Up) وتشفير النسخ الاحتياطية من البيانات (Data Back-Up Encryption)، وفحص وسائل التخزين باستمرار والتخلص من وسائل التخزين.

2-4-8: حماية أمن مدخلات نظم المعلومات المحاسبية المحوسبة (Input Security):

ويمكن تقسيم الرقابة التطبيقية في نظم المعلومات المحاسبية المحوسبة إلى الرقابة على المدخلات، والرقابة على معالجة البيانات، والرقابة على المخرجات.

والرقابة على المدخلات: تتمثل في إجراءات فحص مدخلات النظام لضمان درجة عالية من الدقة والثبات في جودة وأمن البيانات عند دخول النظام،⁽⁴⁾ وهي الإجراءات المبرمجة الروتينية التي تقوم بإجراء الاختبارات على البيانات للتأكد من خلوها من الأخطاء، وينبغي أن تصمم إجراءات مراقبة المدخلات في النظام عند نقاط مختلفة، اعتماداً على ما إذا كان معالجة المعاملات تتم في الوقت الحقيقي بشكل مباشر أو دفعة واحدة،⁽⁵⁾ وقد صممت ضوابط الإدخال، لمنع أو اكتشاف الأخطاء في مرحلة الإدخال ومعالجة البيانات،⁽⁶⁾ وينبغي أن تحدد هذه الضوابط على أساس الاحتياجات الأمنية وتقييم المخاطر،⁽⁷⁾ وتهدف إلى توفير درجة تأكد معقولة من صحة اعتماد البيانات التي يتسلمها قسم معالجة البيانات ومن سلامة تحويلها بصورة تساعد الحاسوب على التعرف عليها، وعدم فقدانها أو الإضافة إليها أو حذف جزء منها أو طبع صورة منها أو عمل أي تعديلات غير مصرح بها، كما تشمل رفض وتصحيح وإعادة إدخال البيانات التي سبق رفضها،⁽⁸⁾ وتعد هذه الرقابة هامة جداً لأن الجزء الأكبر من الأخطاء في نظم الحاسوب ينتج عند نقطة أخطاء المدخلات.⁽⁹⁾

(1) المري، عليز، (2011)، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها، **مرجع سابق**،

http://www.dralmarri.com/show.asp?field=res_a&id=205

(2) خالد، أبو ذر عثمان، (2011)، "سياسات أمن المعلومات"، مرجع سابق، ص 71.

(3) صقر، ممدوح الشحات، (2007)، "أمن المعلومات"، **مرجع سابق**، ص 10.

(4) النجار، فايز جمعه، (2010)، "نظم المعلومات الإدارية : منظور إداري"، مرجع سابق، ص 260.

(5) Hall, James A., (2013), *Accounting Information Systems*, OP. Cit., P. 741.

(6) Bodnar , George H. & Hopwood, William S., (2012), *Accounting Information Systems*, 11th Edition, Prentice Hall, New Jersey, USA., P.151.

(7) ISO/IEC 27002, (2005), *Information Technology – Security Techniques - Code of Practice for Information Security Management International*, OP. Cit.

(8) صيام، وليد زكريا، (2010)، "الرقابة الداخلية على تطبيقات نظم المعلومات المحاسبية الالكترونية"، **مرجع سابق**، ص ص: 17- 19.

(9) Arens, Alvin A., Elder, Randal J., & Beasley, Mark S., (2014), *Auditing & Assurance Services: An Integrated Approach*, OP. Cit., P.696.

ويرى الباحث أن إعداد المدخلات مرحلة هامة وتمثل أساساً لما بعدها من المراحل، ويعتبر التحقق من دقة وسلامة المدخلات عنصراً حيوياً للوقاية من حدوث الأخطاء ومنع الوقوع في المشكلات ومواجهة الصعوبات من خلال الرقابة على مصدر البيانات (*Source data Control*) والرقابة على إدخال البيانات (*Data Entry Control*) وتتبع أخطاء إدخال البيانات (*Data Error Control*) ومراجعة البيانات (*Data Audit*).

9-4-2: حماية أمن عمليات التشغيل البرمجي (*Processing control*) لنظم المعلومات المحاسبية:

وتهدف أساليب الرقابة على معالجة البيانات إلى توفير درجة تأكد معقولة حول تنفيذ عمليات معالجة البيانات إلكترونياً تمت بدقة وبشكل كامل طبقاً للتطبيقات المحددة، من خلال معالجة وتتبع كافة العمليات كما صرح بها وعدم إغفال معالجة عمليات صرح بها وعدم معالجة أية عمليات لم يصرح بها،⁽¹⁾ والتأكد من أن البرنامج المطلوب المطلوب والمناسب لعملية المعالجة هو البرنامج الذي تم استدعائه، وأن الملفات التي يجب معالجتها هي تلك التي تمت عليها عملية المعالجة، ووجود ضوابط رقابية في برنامج المعالجة لمنع حدوث الأخطاء أثناء عمليات المعالجة،⁽²⁾ لذلك يجب التأكد من صحة البرامج والقواعد المستخدمة في عمليات المعالجة، وتحديد صلاحية المستخدمين، والرقابة المدمجة داخل النظام، وتصحيح أخطاء المعالجة ومعالجة البيانات كاملاً عند حد الانقطاع وتوقيف عمل التطبيقات المحاسبية إجبارياً نهاية الدوام.

10-4-2: حماية أمن مخرجات نظم المعلومات المحاسبية (*Out-Pout Control*):

إن وجود نظم معلومات محاسبية موثوق بها أمراً ضرورياً من أجل الإدارة الفاعلة وتعتبر نظم المعلومات وما تفرزه من مخرجات ذو أهمية لكافة المستخدمين، فمحورية دورها يستلزم دراسة كافة المستجدات التي تعمل على تطويرها لتحسين المخرجات وفق متطلبات مستخدميها وارتباطاً بالمتغيرات المحيطة للبيئة المعلوماتية، فأهداف أي نظام معلومات هو إنتاج مخرجات معلومات متكاملة وآمنة ومحدثة لأقصى حد يمكن الوصول إليها في أي ظرف بكل سهوله ويسر، لذلك أول مرحلة من مراحل التحليل هو تحليل مدى تحقيق المخرجات لكل متطلبات النظام ومدى الوصول إليها،⁽³⁾ وبعد فحص مخرجات نظام المعلومات المحاسبي بعناية أداة مهمة لتزويد المنشأة برقابة إضافية تؤكد سلامة معالجة البيانات، وذلك لضمان جودة المخرجات من حيث الدقة والموثوقية والتوقيت والشكل المناسب،⁽⁴⁾ ويعتبر الالتزام بهذه الإجراءات أساساً موضوعياً لضمان سلامة المعلومات المحاسبية التي ينتجها النظام المحاسبي، وفي هذا الصدد يجب حصر أنواع المعلومات وتصنيفها (*Information classification*)، والرقابة على توزيع المخرجات (*Information Distribution Control*)، ووجود صيانة دائمة لوسائل الإخراج، وعمل نسخ مطبوعة لبعض المعلومات المحاسبية الهامة، وتتبع مسار معين لمراجعة سير المعاملات وإتلاف المخرجات المهمة.

(1) الذبيبة، زياد & الرمحي، نضال & الجعدي، عمر، (2011)، "نظم المعلومات في الرقابة والتدقيق"، مرجع سابق، ص75.
(2) محمد، طارق مختار، (2011)، "تفعيل دور الرقابة الداخلية في الأنشطة المصرفية في ظل نظام المعلومات المحاسبية الإلكترونية"، مرجع سابق، ص: 578-665.

(3) Bagranof, Nancy A. & Simkin, Mark G. & Norman, Carolyn S., (2010), *Accounting Information Systems*, OP. Cit., P.397.

(4) Anomah, Sampson & Agyabeng, Owusu, (2013), "Evaluating internal controls in a computerized works environment – a risk to audit professionals and a challenge to accountancy training providers", *OP. Cit.*, PP: 132- 143. , www.iiste.org

وعليه يتضح للباحث أن الهدف الرئيسي للرقابة الداخلية التطبيقية هو تأكيد صحة وشمولية عمليات معالجة البيانات المحاسبية، والتأكد من عدم توزيع المخرجات للأفراد غير المصرح لهم بتداولها، وغالبية تلك الأساليب تتجه نحو الرقابة الوقائية أكثر من اتجاهها نحو الرقابة بالتغذية العكسية (الراجعة)، وأن العديد من هذه الأساليب تهدف إلى اكتشاف الأخطاء التي يصعب اكتشافها في حال غياب مثل تلك الأساليب.

4-2-11: حماية أمن البيانات المنقولة عبر الشبكات في نظم المعلومات المحاسبية المحوسبة:

بالإضافة للثلاث الوظائف الرقابية التطبيقية السابق ذكرها فإن هناك وظيفة رقابية هامة لها ارتباط بالرقابة التطبيقية لنظم المعلومات المحاسبية تتمثل في الرقابة على البيانات المنقولة عبر الشبكات، حيث أن المعاملات المالية في العالم أجمع تحولت إلى تعاملات إلكترونية، بعدما أصبح بإمكانك الشراء والبيع وتحويل أموال من خلال ضغط زر واحدة، فكان لزاماً على المنشآت المالية مواكبة هذه التقنيات لأن التعاملات الخارجية حتمت الأمر، وفرضته مع غياب الوعي بخطورة نظم المعلومات، إذا ما أحكمت السيطرة عليها، ولذا يجب إعادة هيكلة النظم المصرفية، وإحكام نظم الأمان فيها، حتى لا تتكرر عمليات السرقات الإلكترونية التي شهدتها السنوات الماضية.

وتتضمن خدمات أمن المعلومات كثير من التعقيدات بسبب تنوع الشبكات الكبيرة والمفتوحة وتعرضها لهجمات وتهديدات كبيرة نتيجة لتطور التقنيات المستخدمة في هذه الشبكات بشكل مستمر،⁽¹⁾ ولابد من العمل على تحقيق أمن الإنترنت⁽²⁾ واعتباره أحد الموجودات المادية التي يقع على عاتق نظم المعلومات المحاسبية صيانتها وتدقيقها والمحافظة عليها،⁽³⁾ ويُعدُّ الأمان من المتطلبات الأساسية التي يستند إليها التعامل التجاري عبر الإنترنت، لذلك من الضروري وجود نظام يسمح بحماية المعلومات والمعاملات على الإنترنت، وخاصة أن هذه الشبكة عالمية ومفتوحة لجميع المنشآت والأفراد، وبالتالي فإن التعامل المباشر على شبكة الانترنت وما يتصل به من تحويل للمعلومات يجعل من إقامة بنية أمنية مشددة هدفاً رئيسياً تسعى المصارف إلى تحقيقه، فتوفير الحماية والأمان لعملائها فيما يتعلق بأموالهم وبياناتهم وجميع المعلومات الخاصة بهم والمسجلة إلكترونياً على صفحات البنك الرقمية لا يقل أهمية عن تقديم منتجات وخدمات مصرفية بجودة عالية وتكلفة أقل، ولهذا تسعى البنوك التجارية إلى التحسين في نظم الحماية كنوع من الحرص غير المتناهي على الحفاظ على علاقتها بعملائها والمبنية على الثقة وحسن الخدمة،⁽⁴⁾ ويشير الواقع العملي إلى زيادة استخدام شبكة المعلومات الدولية (الانترنت) في مجال تبادل السلع والخدمات والمعلومات، وقد أدى التطور السريع والمذهل في مجال التجارة الإلكترونية إلى ضرورة الاهتمام بأمن نظام

(1) الدباغ، راند & وزيل، بشرى، (2012)، "فاعلية التدريب في تحقيق نجاح أمن نظم المعلومات دراسة استطلاعية لآراء عينة من العاملين في نظم المعلومات بجامعة الموصل"، *تسمية الراغبين*، مجلد ٣٤، ملحق العدد ١١، كلية الإدارة والاقتصاد، جامعة الموصل، العراق، ص: 123-140.

(2) تستند الشبكة العالمية للمعلومات (الانترنت) على ثلاثة مفاهيم:
أ. بروتوكول نقل النص الواسع النطاق (HTTP) Hyper Text Transfer Protocol الذي يمكن وحدات خدمة الشبكة ومستخدميها من الاتصال.
ب. محدد مواضع المصادر العامة (URL) Universal Resource Locator، الذي يعطي عنوان مصدر الإنترنت أو وصلاتها.
ج. وثائق لغة تحديد علامات النص الواسع النطاق (HTML) Hyper Text Markup Language وهي اللغة التي يستخدمها الحاسب لإبلاغ متصفح الشبكة بكيفية إظهار المعلومات على شاشة الحاسب.

(3) رشيد، ناظم حسن، (2011)، "دور مراقب الحسابات في إضفاء الثقة بالبيانات المحاسبية المنشورة على الإنترنت في بيئة التجارة الإلكترونية"، *مجلة تكريت للعلوم الإدارية والاقتصادية*، المجلد (7)، العدد (23)، كلية الإدارة والاقتصاد، جامعة تكريت، العراق، 2011، ص: 173-197.

(4) زيدان، محمد & حمود، محمد، (2010)، "متطلبات أمن المعلومات المصرفية في بيئة الانترنت"، *مراجع سابق*، "ورقة عمل".

المعلومات لمواجهة كافة التهديدات والمخاطر بصفة عامة، وحتى يمكن تحقيق الهدف من نظام المعلومات بأكبر قدر ممكن من الكفاءة والفعالية.⁽¹⁾

إن حماية التبادل الإلكتروني للبيانات هي في غاية الأهمية وتصبح أكثر أهمية في المنشآت التي تستخدم تبادل البيانات الإلكترونية أو الإرسال الإلكتروني للأموال، فتحقيق أمن المعاملات المالية أمر حتمي للحصول على ثقة الزبائن بمواقع التجارة الإلكترونية يعتمد أمن المعاملات المالية على قدرة المنشأة على ضمان الخصوصية، والتحقق من هوية المستخدم، ومنع الاختراقات غير المرغوبة، ولذلك كان لا بد من الرقابة على البيانات المنقولة عبر الشبكات لتوفير درجة تأكيد معقولة من أن البيانات المنقولة عبر شبكات النظام محمية من كافة المخاطر التي قد تتعرض لها، والتحقق من أن الرسالة قد أرسلت أو استلمت من قبل الطرف المعني، والتحقق من توافر الرقابة الكافية في مختلف مراحل التبادل الإلكتروني للبيانات، والتحقق من الحماية والرقابة على برامج الحاسوب والشبكات، ويمكن التحقق مما سبق والوصول إلى رقابة داخلية عالية في بيئة كذلك بإتباع العديد من الإجراءات والوسائل الرقابية وفي هذا الصدد لا بد من استخدام الجدران النارية (Fire-Walls) وعلى ذلك يرى الباحث بأن الجدران النارية تقدم حلاً شاملاً حيث توفر الأجهزة والبرامج الخاصة بحماية وأمن المعلومات فعن طريقها يتم تبادل المعلومات بين نظم المعلومات المحاسبية سواء داخل المنشآت نفسها أو مع بعضها البعض وذلك بدرجة كبيرة من الدقة مع الحفاظ على خصوصيتها وسلامتها والتأكد من هوية مستخدمي هذه النظم.

كما يجب الاهتمام بوسيلة التشفير (Encryption): من أجل تأمين السرية والأمان للاتصالات الإلكترونية لنظم المعلومات المحاسبية والتأكد من عدم عبث أحد بمحتوى الرسالة الإلكترونية أثناء انتقالها بين المستخدمين، ويعزز التشفير التحقق من هوية المستخدمين والتأكد من صحة التبادل الإلكتروني للبيانات كما أن عملية التشفير تمنع القرصنة من الوصول إلى البيانات أثناء نقلها إلكترونياً عبر شبكات الاتصال، أو حفظها في قواعد البيانات،⁽²⁾ كما يجب التركيز على التوقيع الرقمي (Digital Signature): وتعتبر أنظمة تبادل المعلومات الكترونياً المعتمدة على الانترنت أقل كفاءة وأقل أمناً من الشبكات الخاصة، إلا أنها من ناحية أخرى تكون أكثر سهولة في الاستخدام وأكثر قدرة على التفاعل مع المستخدم وتتاح لمدى واسع من المستخدمين، ومع تطور سبل التحقيق من شخصية المستخدمين للحفاظ على أمن وسرية التعاملات سيزيد اتجاه استخدام بديل تبادل المعلومات الكترونياً عبر الإنترنت،⁽³⁾ فإذا تحقق كل طرف من أطراف تبادل المعاملات الإلكترونية من هوية الشخص الآخر فإن ذلك يعزز من موثوقية البيانات، وتزداد مصداقية التوقيع الإلكتروني، إذا ارتبط استخدامه بتدخل جهة محايدة مؤمنة للتصديق على توقيع صاحب رسالة البيانات الإلكترونية، وإصدار شهادة بما يفيد صحة وسلامة مضمونه وأنه لم يحدث أي تلاعب أو تحريف أو تعديل فيه،⁽⁴⁾ فالشهادة الرقمية (Digital Certificates) هي عبارة عن وثيقة الكترونية تم إعدادها والتوقيع عليها رقمياً من قبل طرف ثالث موضع ثقة، يشهد في تلك الوثيقة بهوية مالك المفتاح العام الذي يظهر اسمه في تلك الشهادة،⁽⁵⁾ كما ينبغي استخدام بروتوكولات

(1) الدلاهمة، سليمان مصطفى، (2008)، "أساسيات نظم المعلومات المحاسبية وتكنولوجيا المعلومات"، مرجع سابق، ص 677.

(2) الريبيدي، محمد علي، "حماية المعلومات المحاسبية في ظل مخاطر التكنولوجيا للعمليات المصرفية الإلكترونية: دراسة ميدانية في البنوك العاملة في اليمن"، مجلة كلية التجارة والاقتصاد، العدد (33)، كلية التجارة والاقتصاد، جامعة صنعاء، صنعاء، اليمن، مارس 2010، ص: 1-46. ص 18.

(3) الدوغجي، علي حسين، (2008)، " دور مراقب الحسابات في ظل تكنولوجيا المعلومات المعقدة ومخاطر التدقيق"، مجلة العلوم الاقتصادية والإدارية، المجلد (14)، العدد (52)، كلية الإدارة والاقتصاد، جامعة بغداد، العراق، ص: 285-304.

(4) Hall, James A., (2013), Accounting Information Systems, OP. Cit., P.711.

(5) حجر، عبد الملك إسماعيل، (2009)، " نظم المعلومات المحاسبية"، مرجع سابق، ص 430.

التبادل الآمن للمعلومات، فتبادل المعلومات بين الأفراد والمنشآت المالية غير آمن بما فيه الكفاية وهذا قد يؤدي إلى تسرب البيانات، ويُعد هذا الخطر من المخاطر الحرجة للمنشأة لأن الإفصاح عن المعلومات المالية الشخصية والاعتبارية قد يكون لها عواقب قانونية وجلب ضرر لسمعة المنشأة وبالتالي لا بد من توفير بروتوكول لأمن المعاملات المالية عبر الانترنت.⁽¹⁾

2-4-12: حماية أمن تعديل وتطوير نظم المعلومات المحاسبية (Systems Development controls):

وهي ضوابط مصممة لتوفير تأكيد معقول بأن النظم قد تم ويتم تطويرها وصيانتها بطريقة رسمية وناجحة، وهي أيضا مصممة نموذجياً للرقابة على اختبار تحويل وتنفيذ وتوثيق النظم الجديدة أو المعدلة، والرقابة على التغييرات في النظم التطبيقية، وحصر تداول البرامج وتوثيقها على الموظفين المختصين، والرقابة على حيازة نظم التطبيقات من أطراف ثالثة،⁽²⁾ وبالتالي لا بد من التأكد من أن أي تغييرات لا تؤثر سلباً على موثوقية نظم المعلومات المحاسبية، ومن الضروري تعديل إجراءات الرقابة المتعلقة بمبادئ الأمن لإبقاء فعاليتها بعد تطبيق التغييرات الجديدة والقيام بإجراءات التشغيل.⁽³⁾

وفي هذا الصدد ينبغي توفر معايير وإجراءات للتطوير: من متطلبات نجاح العملية الرقابية المتعلقة بأمن الأنظمة والبرامج توفير إجراءات واضحة وموثقة مكتوبة لاعتماد الأنظمة الجديدة ولاعتماد التعديلات التي تتم على الأنظمة المعتمدة ولتوضح آلية تعديل وفحص البرامج والأنظمة من مرحلة التكليف بالتعديل وحتى مرحلة اعتماد البرامج ووضعها موضع التطبيق، ويجب أن يكون هناك فريق متخصص لتعديل وتطوير نظام المعلومات المحاسبي من داخل المنشأة، وتشرف إدارة المنشأة على تعديل وتطوير النظام، مع فحص كل التغييرات التي تمت على الأجهزة والبرامج في بيئة غير منتجة قبل وضعها في بيئة حية، والتأكد من أن هناك خطة بديلة لكل تغيير لا يعمل بشكل ملائم، لأنه من الممكن للأنظمة الحرجة أن لا تعمل أو يمكن أن تعمل بشكل خاطئ في حال سحب أي تغيير.⁽⁴⁾ فلا تتم أية تعديلات في برمج النظام بدون حصول المبرمجين المختصين على موافقات رسمية من الإدارات المعنية المخولة، فنظم المعلومات المحاسبية المحوسبة عرضة للتغيير والتحديث المستمر، لذلك يجب أن تخضع عمليات التغيير بما فيها التغييرات الطارئة إلى إجراءات رسمية مصرح بها.⁽⁵⁾

ويرى الباحث أن إدارة المنشأة يجب عليها تنفيذ الرقابة المشددة واختبار النظم والبرامج الجديدة من أجل تقليل مخاطر حدوث تغييرات غير مصرح بها للنظم كأن تقوم باختبار تطبيق النظام الجديد في جزء من المنشأة مع الاستمرار في تطبيق النظام القديم في بقية أجزاء المنشأة، ويجب أن يستمر العمل بالنظام القديم و النظام الجديد بخط متوازي على الأقل لمرة واحدة و مقارنة النتائج لكلا النظامين لتحديد أي تناقضات قد تظهر بينهما.

(1) Brender, Nathalie & Markov, Iliya, (2013), "Risk perception and risk management in cloud computing: Results from a case study of Swiss companies", *OP. Cit.*, PP:726- 733, <http://www.elsevier.com/locate/ijinfomgt>

(2) Vaassen, Eddy H. J., (2005), *Accounting Information System- A managerial Approach*, John Wiley & Sons Ltd, Chichester, England, PP: 128- 131

(3) Romney, Marshal B. & Steinbart, Paul John, (2015), *Accounting Information Systems*, *OP. Cit.*, P. 297.

(4) *Ibid.*, P. 297..

(5) Hall, James A., (2013), *"Accounting Information Systems"*, *OP. Cit.*, P.734.

الخلاصة: بناءً على ما تقدم في هذا المبحث توصل الباحث إلى نتائج هامة وأساسية، ومنها إن نظام الرقابة الداخلية مهما بلغ من جودة في مجال التصميم والتنفيذ، فإنه يمكن أن يقدم ضمان معقول فقط بأن أهداف الرقابة سوف تتحقق ولا يمكن لأي رقابة داخلية إن تقدم ضمان مطلق بأن كل أهداف الرقابة الداخلية سوف تتحقق، وذلك لأسباب وعوامل تتعلق بالأخطاء البشرية وبمحددات تتعلق بالموازنة بين الكلفة والمنفعة، فأمن البيانات ليس في وضع الإجراءات المحكمة لتأمين البيانات فحسب وإنما المهم أن تكون هذه الإجراءات عملية وممكنة التطبيق دون أن تؤثر على فعالية وكفاءة قاعدة بيانات نظم المعلومات المحاسبية.

وينبغي تنفيذ متطلبات نظم المعلومات المحاسبية الفعالة في البيئة الرقمية لتوفير تأكيد معقول بأن نظم المعلومات المحاسبية سوف تنتج المعلومات ذات الصلة ويمكن الاعتماد عليها لتلبية احتياجات الأطراف الداخلية والخارجية ذات العلاقة بالمنشأة، لأن الحماية الكاملة من المخاطر يصعب تنفيذها في الواقع العملي، لأنها تتطلب مجهود وتكاليف ضخمة يصعب توفيرها في ظل تحليل المنافع والتكاليف المرتبطة بأمن وسلامة نظم المعلومات.

ويرى الباحث كذلك أن الوسيلة المناسبة للحد من هذه المخاطر وسواها يكمن في اعتماد إجراءات الرقابة الوقائية والاستكشافية والتصحيحية فضلاً عن التركيز على الكادر وتدريبه وتطويره وتعزيز ولائه الوظيفي للمنظمة والعمل على الحد من التهديدات والمخاطر التي تواجه أمن نظم المعلومات المحاسبية.

وبناءً على ذلك يرى الباحث إن زيادة فاعلية الرقابة الداخلية من خلال تحسينها وتطويرها بشكل مستمر بما يتواءم مع التغيير في بيئة العمل وتكنولوجيا المعلومات سوف يساعد المنشآت على انجاز أهدافها وتحقيق أرباحها المتوقعة ومنع خسارة الموارد وكذلك يساعد في توفير ضمان بان القوائم المالية يمكن الاعتماد عليها، ويتم الالتزام بالقوانين والأنظمة عند أعدادها وبعبارة أخرى أن الهدف من تحسين الرقابة الداخلية يؤدي إلى إضافة قيمة للمنشأة والزبون فضلاً عن مساعدة المنشأة في تجنب فقدان القيمة.

وفي كافة الأحوال فإنه يجب أن يتضمن النظام الرقابي لنظم المعلومات المحاسبية مجموعة كافية من الأدوات والضوابط الرقابية التي تتناسب مع حجم وطبيعة الأعمال التي يمارسها بحيث يحقق مستوى معقول من الرقابة. وأهم ما يعيب أدوات ووسائل الحماية البرمجية عموماً عن غيرها من أدوات ووسائل حماية نظم المعلومات هو كونها الأكثر التصاقاً بالعامل الزمني، أي أن استخدام هذه الأدوات دون الالتفات للتحديثات تبقى دائماً محدثة ومتطورة يعني أنها ستكون دون جدوى وفعالية ولن تحقق المستوى الأمني المطلوب، فإجراءات الحماية عموماً عمليات مستمرة تتطلب استمرارية في التطوير ومتابعة للمستجدات، واستمرار في مراقبة وافترض المخاطر وابتكار الحلول لها، ولهذا فالمنشآت لا توصف بأن لها نظام معلوماتي أمني حقيقي وفعال حتى تحقق نظام متطور وبشكل مستمر للعمليات الأمنية والبشرية والتقنية من أجل تقليل واحتواء المخاطر المفترضة أو المتوقعة.

وبالتالي فإن المنشآت تولي نظم معلوماتها اهتماماً كبيراً، ليس فقط في تطويرها وإنما في العمل على حمايتها من مختلف المخاطر والتهديدات التي قد تواجهها، من خلال الإنفاق على نظم الحماية المتطورة المطابقة لمعايير الهيئات العالمية، وإن التركيز على حماية البيانات والهيكل العام لتكنولوجيا المعلومات سوف يستمر في النمو في المستقبل المنظور.

الفصل الثالث

الدراسة التطبيقية لدى البنوك التجارية في الجمهورية اليمنية

الفصل الثالث: الدراسة التطبيقية

مقدمة:

تم في الفصلين السابقين تناول الخلفية النظرية للدراسة من خلال الرجوع لأدبيات الدراسة المختلفة، وفي محاولة لربط الجانب النظري بالتطبيق العملي فقد جاء هذا الفصل ليسلط الضوء على مناهج وأساليب الدراسة الذي أتبعه الباحث عند جمع وتحليل البيانات والاختبارات التمهيدية، ويوضح مجتمع الدراسة وعينة الدراسة وحدودها، ثم عرضاً لكيفية بناء أداة الدراسة لجمع المعلومات اللازمة للدراسة، والإجراءات العلمية المستخدمة التي تم إتباعها للتأكد من صدقها وثباتها، وأساليب المعالجة الإحصائية التي تم استخدامها في معالجات البيانات التي تم الحصول عليها.

ثم يتناول الواقع الميداني في البنوك التجارية العاملة في الجمهورية اليمنية، ويتطرق لدراسة الحالة العملية المقارنة التي قام بها الباحث لمجموعة من البنوك التجارية العاملة داخل بيئة الأعمال اليمنية بقطاعاتها المختلفة العامة والخاصة والمختلطة.

كما يتناول هذا الفصل تحليل البيانات واختبار الفرضيات الخاصة بالدراسة، وأخيراً سيتناول هذا الفصل مناقشة نتائج الدراسة التي توصلت إليها واستنتاجاتها، ومن ثم التوصيات والمقترحات التي أوصت بها، والدراسات المستقبلية التي أقترحها الباحث كامتداد لموضوع هذه الدراسة.

ويختتم الباحث أطروحته بالمصادر والمراجع والملاحق التي استقت منها هذه الدراسة بجانبها النظري ومن ثم العملي.

وبناءً على ما تقدم فقد تم تقسيم هذا الفصل إلى خمسة مباحث على النحو التالي:

المبحث الأول: مناهج وأساليب جمع وتحليل البيانات والاختبارات التمهيدية.

المبحث الثاني: دراسة الحالة العملية لتقييم مخاطر نظم المعلومات المحاسبية المحوسبة.

المبحث الثالث: تحليل البيانات.

المبحث الرابع: اختبار الفرضيات.

المبحث الخامس: النتائج والتوصيات والمقترحات.

1-3: المبحث الأول

مناهج وأساليب جمع وتحليل البيانات والاختبارات التمهيدية

يتضمن هذا المبحث على أهم الجوانب العملية التي استند إليها الباحث عند إجراء الدراسة العملية، فقد تم توضيح آلية اختيار وتحديد كل من مجتمع الدراسة وعينتها، وبيان خصائصهما، ووصف أداة الدراسة (قائمة الاستقصاء)، والتعريف القياسي لمتغيرات الدراسة، ثم اختبار ثبات وصلاحيّة أدوات القياس، ويبرز هذا المبحث آلية وإجراءات التحليل المتبعة لمعالجة البيانات، والأساليب والمقاييس التحليلية الإحصائية المستخدمة والمناسبة لتحليل البيانات واختبار الفرضيات وخصوصاً ما يتعلق بالجانب التطبيقي الخاص بهذه الدراسة، وذلك على النحو الآتي:

3-1-1: مناهج الدراسة والإجراءات المتبعة:

إن اختيار المنهجية المناسبة عملية ليست بالسهلة لعدم وجود منهجية مثالية بشكل دائم لجميع الدراسات والبحوث، ولو كانت موجودة لكننا استخدمناها دوماً، حيث تمتلك معظم المنشآت معايير وسياسات خاصة بها ترشدها لاختيار المنهجية المناسبة.⁽¹⁾

ولتحقيق أهداف الدراسة فقد اعتمدت الباحثة على المنهج الوصفي التحليلي، فبعد أن قام بالاطلاع على الدراسات السابقة، وعلى الخلفية النظرية للدراسة، قام بإجراء دراسة حالة عملية لدى ثلاثة بنوك تجارية تمثل القطاعات الاقتصادية المختلفة (العامة والخاصة والمختلطة)، من خلال بيانات عملية تم استخراجها بواسطة المقابلات والملاحظات، وتم تعزيز ذلك بدراسة مسحية شاملة لجميع البنوك التجارية العاملة في الجمهورية اليمنية، من خلال تصميم وتطوير قائمة استقصاء علمية محكمة، وقد تم تحليل البيانات واختبار الفرضيات باستخدام الأساليب التحليلية المناسبة، اعتماداً على الرزمة الإحصائية للعلوم الاجتماعية (SPSS).

كما اعتمدت الباحثة نظرياً وعملياً على منهجين كلاً منهما مكمل للآخر وهما منهجي الاستقراء والاستنباط، حيث اعتمدت المنهج الاستقرائي من أجل تحليل واقع البيئة الحالية في البنوك التجارية في الجمهورية اليمنية بشأن تقييم مخاطر أمن نظم المعلومات المحاسبية، كما اعتمدت المنهج الاستنباطي من أجل استنباط الحلول والمقترحات اللازمة لمعالجة تلك المخاطر، وعلى النحو التالي:

1. في الجانب النظري والوصفي: لجأ الباحث للمنهج الاستقرائي من خلال الاطلاع على مجموعة من المراجع العلمية الرائدة في مجال نظم المعلومات المحاسبية وخاصة فيما يتعلق بتحديد تلك المخاطر وبيان التهديدات المسببة لها، ومدى تأثير تلك المخاطر على أمن نظم المعلومات، وأساليب وإجراءات الحماية والتحوطات المتبعة لحماية تلك النظم، كما قام الباحث باستقراء المعايير الدولية والمهنية الصادرة عن المعاهد والجمعيات المهنية والدولية الصادرة وكذلك الدراسات السابقة ذات العلاقة بهدف التوصل إلى ما أتفق عليه الكثير من الباحثين في هذا الموضوع، ثم تحول الباحث للمنهج الاستنباطي من أجل بلورة الأسس والمنطلقات التي يقوم عليها بناء الإطار المفاهيمي والنظري لهذه الدراسة، وذلك لتأطير الأفكار والمفاهيم الحديثة والمطلوبة لهذه الدراسة والتي تعتبر بمثابة المقدمات التي شكلت الأساس لحل مشكلة الدراسة والذي ينبغي تطبيقها من قبل البنوك التجارية في الجمهورية اليمنية، وهو ما ساعد الباحث في تحديد المعالم الرئيسية للاتجاهات المستقبلية للظاهرة محل الدراسة، وقد تجلّى ذلك في الجانب النظري في الفصلين الأول والثاني.

2. في الجانب العملي التطبيقي: اتبع الباحث كذلك منهجاً استقرائياً بني على دراسة حالة عملية شملت ثلاثة بنوك تجارية رائدة ضمن القطاع المصرفي في الجمهورية اليمنية، بالإضافة إلى دراسة مسحية لجميع جوانب التقييم لدى جميع البنوك التجارية في الجمهورية اليمنية، والذي يركز على جمع البيانات الأساسية اللازمة والفعلية والمتعلقة بتقييم الوضع الحالي لمخاطر أمن نظم المعلومات المحاسبية لدى تلك البنوك، والتي لا يمكن توفيرها عن طريق الدراسة النظرية، حيث تم إجراء المقابلات الشخصية المباشرة بالمسؤولين الإداريين والتقنيين في

(1) Dennis, Alan (2012), *Systems Analysis and Design with UML*, 5th Ed., John-Wiley & Sons, Inc. USA, P. 15.

تلك البنوك والمعنيين بهذه الدراسة لمعرفة أهم المخاطر المهددة لأمن نظم المعلومات المحاسبية ، وأهم أسبابها وتأثيراتها، وسبل مواجهتها، بناءً على أسس علمية ونتائج موضوعية وفي ضوء الإطار النظري ونتائج الدراسات السابقة ذات الصلة بمتغيرات الدراسة، لاستقراء الواقع الحالي، وبما يضيفي الثقة على نتائج الدراسة وتعميمها، ثم تحول الباحث إلى المنهج الاستنباطي، الذي يعتمد على التفكير المنطقي الاستنتاجي، بربط ما تم التوصل إليه من نتائج عملية بالمقدمات التي تم بناؤها في الجانب النظري لمحاولة بلورة توصيات ومقترحات علمية سليمة لتقييم ومعالجة مخاطر أمن نظم المعلومات المحاسبية تعمل على الحد من أو تخفيف تلك المخاطر، ويمكن تطبيقها والعمل بها في البنوك التجارية في الجمهورية اليمنية، وقد تجلى ذلك في الفصل الثالث من هذه الدراسة.

2-1-3: مجتمع الدراسة وعينتها:

3-1-2-1: مجتمع الدراسة: يتكون مجتمع الدراسة من كافة البنوك التجارية العاملة في الجمهورية اليمنية، سواء تلك التي تتبع القطاع العام أو الخاص أو المختلط، والبالغ عددها (16 بنكاً تجارياً)⁽¹⁾، [منها (12) بنكاً محلياً، و(4) بنوك تمثل فروع لبنوك عربية وأجنبية إدارتها الرئيسية خارج الجمهورية اليمنية]، وقد تم اختيار البنوك التجارية كمجال للدراسة كونها تفي بمتطلبات هذه الدراسة فهي أكثر المنشآت استجابة لاستخدام نظم المعلومات المحاسبية المحوسبة في كافة عملياتها، ومن أهم المنشآت مواكبةً لتكنولوجيا المعلومات وتحديث هياكلها وقدرتها على التكيف مع البيئة المحيطة، وتعتمد بشكل كامل في غالبية تعاملاتها المصرفية على استخدام وسائل تكنولوجيا متعددة. ومن أجل تحقيق أهداف هذه الدراسة، تم التوجه للمسؤولين الذين لديهم القدرة والمعرفة اللازمة بموضوع هذه الدراسة، وأولئك الأفراد المقصودين يتمثلوا في المختصين في إدارة تكنولوجيا المعلومات (رؤساء أقسام الحاسوب ومبرمجي ومشغلي نظم المعلومات المحاسبية)، والمدراء الماليين ورؤساء أقسام الحسابات، ومدراء إدارة المخاطر، والمدققين الداخليين والخارجيين، ومفتشي البنك المركزي، كونهم المعنيين برقابة وتقييم المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى تلك البنوك، حيث بلغ عدد أولئك الأفراد من العاملين في المراكز الرئيسية للبنوك التجارية في الجمهورية اليمنية وفروعها في العاصمة صنعاء (1445) فرداً⁽²⁾، وقد تم اللجوء إليهم بهدف الحصول على إجابات تكون أكثر مصداقية ويمكن الاعتماد عليها لاختبار فرضيات الدراسة والتوصل إلى النتائج.

3-1-2-1: عينة الدراسة: قام الباحث باختيار عينة عشوائية قصدية طبقية من الأفراد المهنيين العاملين لدى البنوك التجارية في الجمهورية اليمنية، وذلك طبقاً لعدد الأفراد بكل بنك إلى إجمالي عدد الأفراد بالبنوك ككل، حيث لجأ الباحث إلى اختيار (210) فرداً⁽³⁾ من الأفراد المستهدفين في هذه الدراسة والبالغ عددهم (1445) فرداً، وبالتالي فإن العينة تمثل ما نسبته (14.5%) من أفراد مجتمع الدراسة، وعليه يرى الباحث أن العينة تعكس صورة مقبولة عن مجتمع

(1) البنك المركزي اليمني، (2012-2016)، الإدارة العامة للبحوث والإحصاء، **مجموعة تقارير ربع سنوية عن الأعوام : 2012-2016م**، الإدارة العامة للبحوث والإحصاء، مطبع اليمن العصرية، صنعاء، اليمن & جمعية البنوك اليمنية، (2012)، **مجلة المصارف**، العدد(6)، 2012م، صنعاء، اليمن، ص 76.
(2) منشورات وسجلات **إدارات الموارد البشرية** لدى البنوك التجارية محل الدراسة حتى نهاية كانون الأول (ديسمبر) 2012م.
(3) أنظر ملحق الدراسة رقم (3)، وسيتم بيان آلية اختيار عينة الدراسة من المجتمع في هذا المبحث.

الدراسة، الجدير بالذكر أن الباحث قد عزز دراسته التطبيقية القائمة على الاستقصاء في جميع تلك البنوك بأجراء مقابلات شخصية مباشرة مع المسؤولين الإداريين والتقنيين في ثلاثة بنوك تجارية رائدة في الجمهورية اليمنية، البنك الأول (ع) يمثل بنك تجاري من بنوك القطاع العام، والبنك الثاني (خ) يمثل بنك تجاري من بنوك القطاع الخاص، والبنك الثالث (م) يمثل بنك تجاري من بنوك القطاع المختلط، كما أجرى الباحث ملاحظاته الشخصية في تلك البنوك مدعماً بالوثائق التنظيمية فيها لتقييم مخاطر أمن نظم المعلومات المحاسبية فيها، والتحقيق فيما إذا كان هناك أي اختلاف بين تلك البنوك، فيما يخص المخاطر والتهديدات ووسائل الحماية.

3-1-3: مصادر جمع البيانات والمعلومات:

استندت هذه الدراسة في تغطية جانبها النظري والعملي إلى مجموعتين من المصادر هما:

1. **المصادر الثانوية:** وتتمثل في الإطار النظري لهذه الدراسة والذي تم جمعه من خلال مطالعة ومراجعة الكتب، والمقالات، والأبحاث المنشورة في الدوريات والمجلات العلمية المتخصصة، وأطروحات الدكتوراه، ورسائل الماجستير، وأوراق المؤتمرات العلمية، والقرارات والقوانين والأنظمة ذات الصلة بموضوع الدراسة، والمعايير الدولية ذات العلاقة، والمواقع العلمية الالكترونية العربية والأجنبية على شبكة الإنترنت وخاصة المتعلقة بمخاطر أمن نظم المعلومات، وذلك لتغطية وصياغة الجانب النظري في هذه الدراسة، مع شرح ونقد للمفاهيم والأفكار كلما كان ذلك ضرورياً.
2. **المصادر الأولية:** وتتمثل في البيانات التي تم جمعها من خلال مجموعة من الأساليب النوعية (أسلوب الملاحظة والمقابلة وتحليل الوثائق الإجرائية)، والكمية (أسلوب الاستقصاء)، حيث يعتبر أسلوب المقابلة المباشرة مع الأفراد الخبراء واستخدام قائمة الاستقصاء من أنسب المداخل لإجراء مثل هذه الدراسة للحصول على صورة شاملة للموضوع محل الدراسة وتتمثل تلك الأساليب في:
 - أ. **أسلوب الملاحظة الشخصية:** اتبع الباحث هذا الأسلوب بما أتيح له من زيارات ميدانية للبنوك موضع الدراسة، مدعماً ذلك بتحليل الوثائق التنظيمية والتشريعية وتقارير مدققي الحسابات الخاصة بالمخاطر والضوابط الأمنية المستخدمة لحماية أمن نظم المعلومات المحاسبية.
 - ب. **أسلوب المقابلة الشخصية المباشرة:** وذلك من خلال إجراء الباحث للمقابلات الشخصية المهيكلية والمنظمة بطريقة شبه موحدة، مع الأفراد الخبراء المعنيين ذوي العلاقة بالموضوع محل الاهتمام، وخاصة كبار مدراء تكنولوجيا المعلومات ومدراء التدقيق الداخلي ومدراء إدارة المخاطر لدى تلك البنوك، وذلك لجمع البيانات النوعية والتفصيلية الخاصة بمعرفة أهم المخاطر المهددة لنظم المعلومات المحاسبية، وسبل مواجهتها، ومدى تطبيق المعايير الدولية المتعارف عليها بهذا الخصوص، حيث تعاون بعض المدراء في تلك البنوك بضمان أن هوياتهم ستكون محمية وقد تكلموا بشفافية عن قضاياهم واهتماماتهم الخاصة بأمن نظم المعلومات المحاسبية، والمخاطر التي تهددها.
 - ج. **أسلوب الاستقصاء:** واتبع الباحث هذا الأسلوب من خلال تصميم قائمة استقصاء (ملحق الدراسة رقم 1)، تضمنت مجموعة من الأسئلة غطت كافة أبعاد ومتغيرات الدراسة، وتم توزيعها باليد على الجهات ذات العلاقة بموضوع الدراسة ممثلة بالأفراد المعنيين في الإدارات الرئيسية لكل البنوك التجارية في اليمن، وذلك مكن الباحث من تنفيذ

التحليل الكمي حيث تم تحويل البيانات الوصفية إلى بيانات كمية لاختبار الفرضيات والتوصل إلى النتائج وتعميمها على مجتمع الدراسة، وكذلك استخلاص الاستنتاجات وصياغة التوصيات والمقترحات المناسبة.

3-1-4: آلية اختيار مجتمع الدراسة وعينتها إحصائياً:

إن اختيار عينة الدراسة بشكل دقيق وغير متحيز أهم خطوة نحو نجاح الدراسة، ولذلك قام الباحث بإجراء هذه الدراسة التطبيقية في جميع البنوك التجارية العاملة في الجمهورية اليمنية والتي طُبِّقَتْ عليها الدراسة، والبالغ عددها (16) بنكاً تجارياً حتى شهر كانون الأول (ديسمبر) 2012م،⁽¹⁾ وقد قام الباحث بتحديد وحدة المعاينة الخاصة بالدراسة في كل بنك في ضوء عدد العاملين بالإدارة المالية وإدارة نظم وتكنولوجيا المعلومات (IT)، وإدارة المخاطر والتدقيق الداخلي، وفقاً للهيكل التنظيمية لتلك البنوك، وبالتالي فإن وحدة المعاينة تتكون من العاملين في تلك الإدارات بالإضافة إلى المراجعين الخارجيين، ومفتشي البنك المركزي، وقد بلغ إجمالي عدد أفراد مجتمع الدراسة المستهدفين (1445) فرداً، يعملوا في الدوائر المستهدفة لدى المراكز الرئيسية للبنوك التجارية وفروعها في العاصمة صنعاء،⁽²⁾ ونظراً لكبر حجم مجتمع الدراسة، وفي ظل الإمكانيات المتواضعة للباحث، ولضرورة جمع البيانات اللازمة لاختبار فرضيات الدراسة والتوصل إلى نتائج واقعية، فقد تم أخذ عينة عشوائية طبقية قوامها (210) فرداً من أصل (1445) فرداً، أي أن العينة تشكل ما نسبته (14.5%) من مجتمع الدراسة، وحدد حجم العينة في هذه الدراسة باستخدام القانون التالي:⁽³⁾

$$n = \frac{P (1 - P)}{\frac{P (1 - P)}{N} + \frac{E^2}{SD^2}}$$

حيث يتم التعبير عن تلك الرموز على النحو التالي:

- (n): حجم عينة الدراسة المطلوب تحديدها.
 - (N): حجم مجتمع الدراسة وهو إجمالي عدد العاملين المستهدفين في هذه الدراسة والبالغ (1445) فرداً.
 - (P): نسبة الحد الأقصى للخصائص المطلوب دراستها في أي مجتمع وقد اعتبرها الباحث 80%.
 - (E): نسبة الخطأ المسموح به في هذه الدراسة والبالغة (5%) عند معامل ثقة (95%).
 - (SD): الدرجة المعيارية المقابلة لمعامل الثقة الذي اختاره الباحث وهو (95%) وتساوي (1.96) درجة.
- وبالتعويض في قانون العينة أعلاه، نجد أن حجم العينة قد بلغ (210) أفراد من مجتمع الدراسة البالغ عدده (1445) فرداً، ويتضح ذلك على النحو الآتي:

(1) البنك المركزي اليمني، (2016-2012)، الإدارة العامة للبحوث والإحصاء، مجموعة تقارير ربع سنوية عن الأعوام : 2012-2016م، مرجع سابق & جمعية البنوك اليمنية، (2012)،

مجلة المصارف، مرجع سابق، ص 76.

(2) وفقاً لمنشورات وسجلات إدارات الموارد البشرية لدى تلك البنوك محل الدراسة حتى نهاية كانون الأول (ديسمبر) 2012م.

(3) الزعبي، محمد بلال & الطلاقحة، عباس، (2004)، النظام الإحصائي SPSS- فهم وتحليل البيانات الإحصائية، الطبعة السادسة، دار وائل للنشر والتوزيع، عمان، الأردن، صفحات متعددة.

$$n = \frac{0.80 (1 - 0.80)}{\frac{0.80 (1 - 0.80)}{1445} + \frac{(0.05)^2}{(1.96)^2}} = 210$$

وقام الباحث بتوزيع تلك العينة على البنوك التجارية في الجمهورية اليمنية بالطريقة العشوائية التطبيقية بأسلوب التخصيص المتناسب على أساس نسبة عدد الأفراد المستهدفين في كل بنك إلى العدد الإجمالي المستهدف في تلك البنوك (حجم المجتمع الأصلي)، وبالتالي يصبح مجتمع البحث وعينته موزعة حسب عدد الأفراد المستهدفين بكل بنك، كما هو موضح في الجدول الآتي:

جدول رقم (3-1-1) البنوك التجارية في الجمهورية اليمنية
مرتبة وفقاً لسنة التأسيس موضحاً فيه مجتمع الدراسة وحجم العينة المختارة *

م	إسم البنك	جنسية البنك	سنة التأسيس	نوع الشركة	حجم مجتمع الدراسة المستهدف		حجم عينة الدراسة	
					عدد	نسبة %	عدد	نسبة %
1	البنك اليمني للإنشاء والتعمير	يمني	1962	مختلطة	198	13.71	29	13.81
2	البنك الأهلي اليمني	يمني	1969	عامة	65	4.50	9	4.29
3	يونايتد بنك ليمنتد	أجنبي	1971	مساهمة مقفلة	26	1.80	4	1.90
4	البنك العربي	عربي	1972	مساهمة مقفلة	50	3.46	7	3.33
5	بنك اليمن والكويت للتجارة والاستثمار.	يمني	1977	مساهمة مقفلة	119	8.24	17	8.10
6	بنك اليمن الدولي.	يمني	1979	مساهمة مقفلة	79	5.47	11	5.24
7	مصرف الرافدين.	عربي	1982	عامة	25	1.73	4	1.90
8	بنك التسليف التعاوني والزراعي	يمني	1982	مختلطة	138	9.55	20	9.52
9	البنك التجاري اليمني	يمني	1993	مساهمة مقفلة	97	6.71	14	6.67
10	البنك الإسلامي اليمني	يمني	1996	مساهمة مقفلة	66	4.57	10	4.76
11	بنك التضامن الإسلامي الدولي	يمني	1995	مساهمة مقفلة	145	10.03	21	10.00
12	بنك سبأ الإسلامي	يمني	1997	مساهمة مقفلة	152	10.51	22	10.47
13	بنك اليمن والخليج	يمني	2001	مساهمة مقفلة	73	5.05	11	5.24
14	مصرف اليمن البحرين الشامل	يمني	2002	مساهمة مقفلة	113	7.82	16	7.63
15	بنك قطر الوطني	عربي	2007	مساهمة مقفلة	53	3.67	8	3.81
16	مصرف الكريمي للتمويل	يمني	2010	مساهمة مقفلة	46	3.18	7	3.33
	الإجمالي				1445	%100	210	%100

* الجدول أعلاه من إعداد الباحث معتمداً على:

- البنك المركزي اليمني، مجموعة تقارير ربع سنوية عن الأعوام 2012م-2016م، الإدارة العامة للبحوث والإحصاء، صنعاء، اليمن، www.ybrd.com.ye
- جمعية البنوك اليمنية، مجلة المصارف، العدد (6)، صنعاء، اليمن، كانون الأول (ديسمبر) 2012.
- منشورات وسجلات إدارات الموارد البشرية لدى تلك البنوك محل الدراسة حتى نهاية كانون الأول (ديسمبر) 2012م..
- النخبة للعلاقات العامة والإعلان، (2010)، النليل المصرفي اليمني وشركات التأمين، صنعاء، اليمن، صفحات متفرقة.

3-1-5: أداة الدراسة - مكوناتها وآلية توزيعها واستردادها:

اعتمد الباحث في دراسته للحالة العملية على ملاحظاته وعلى البيانات التي حصل عليها بعد إجراء المقابلات الشخصية لمسؤولي نظم المعلومات المحاسبية في ثلاثة بنوك تجارية رائدة في الجمهورية اليمنية تمثل القطاع العام والقطاع الخاص والقطاع المختلط، وضمن إطار أخلاقيات البحث العلمي، وما تحمله المعلومات التفصيلية من خصوصيات لا تكشف عنها التحليلات الإجمالية، ولذلك تتحفظ الدراسة عن ذكر أسماء تلك البنوك وبياناتها التفصيلية - كإجراء احترازي- حفاظاً على أسرارها، وجزء من إجراءات الحماية التي تتبعها.

كما قام الباحث بتصميم أداة الدراسة وهي عبارة عن قائمة استقصاء (ملحق الدراسة رقم 1)، ليتم جمع البيانات من أكبر عدد من المختصين بموضوع الدراسة لدى المنشآت المعنية، وبما يسمح للباحث بتنفيذ التحليل الكمي لاختبار فرضيات الدراسة، وإمكانية تعميم النتائج، حيث تعد أداة الاستقصاء مصدراً مهماً للحصول على البيانات اللازمة لأنها تغطي معظم أبعاد متغيرات الدراسة واختبار فرضياتها، وتعد أداة إحصائية مناسبة وشائعة الاستعمال لهذا النوع من الدراسات.⁽¹⁾

ويتكون الاستقصاء من ثلاثة أجزاء، بالإضافة إلى توطئة بسيطة موجهة إلى المستجيبين توضح الفكرة التي يدور حولها الاستقصاء، ومقدمة توضيحية لبعض المفاهيم والمصطلحات الأساسية الواردة فيها، وفيما يلي شرح موجز لهذه الأجزاء:

الجزء الأول: خُصص لجمع البيانات المتعلقة بالخصائص الشخصية لأفراد عينة الدراسة.

الجزء الثاني: هدفه معرفة بعض المعلومات الأساسية العامة عن البنوك من وجهة نظر المبحوثين (أفراد العينة).

الجزء الثالث: خُصص لقياس متغيرات الدراسة وفقاً لمقياس ليكرت (Likert) خماسي الدرجات، من خلال (150) فقرة تم توزيعها على خمسة محاور، مكونة من عدة فقرات رئيسية وفرعية، فالمحور الأول تضمن (30) فقرة لقياس المخاطر التي من المحتمل أن تهدد أمن نظم المعلومات المحاسبية المحوسبة، أما المحور الثاني فشمّل (29) فقرة لمعرفة التهديدات الداخلية التي من الممكن أن تؤدي إلى حدوث تلك المخاطر، بينما المحور الثالث شمل (17) فقرة لمعرفة التهديدات الخارجية التي من الممكن أن تؤدي إلى حدوث تلك المخاطر، أما المحور الرابع فتضمن (14) فقرة لمعرفة مدى تأثير حدوث تلك المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة، وأخيراً المحور الخامس تضمن (60) فقرة لمعرفة مدى كفاية إجراءات الحماية المتبعة لمواجهة تلك المخاطر، وتم إرفاق خطاب رسمي من الأمانة العامة لجامعتي دمشق وعمران للتعاون مع الباحث، ويلاحظ أن البنك اليمني للإنشاء والتعمير، وبنك سبأ الإسلامي، وبنك التضامن الإسلامي الدولي، كانت أكبر البنوك حجماً من

(1) Shamszadeh, Bagher & Sharif, Abolfazl Azizi, (2012), "Computerized Accounting Information Systems (CAIS) Versus Security Threats", *OP. Cit.*, PP: 69-80.

حيث الاستقصاءات الموزعة والمستلمة، والخاضعة للتحليل، والجدول الآتي يوضح الاستقصاءات الموزعة والمستردة والمستبعدة والخاضعة للتحليل، على مستوى كل بنك.

جدول (2-1-3) الاستقصاءات الموزعة والمستردة والمستبعدة والخاضعة للتحليل مصنفة وفقاً لاسم البنك *

م	اسم البنك	الاستقصاءات الموزعة (العينة)		الاستقصاءات المستردة		نسبة الاستجابة من العينة %	الاستقصاءات المستبعدة (غير صالحة)		الاستقصاءات الخاضعة للتحليل		نسبة الخاضع للتحليل من العينة %
		عدد	نسبة %	عدد	نسبة %		عدد	نسبة %	عدد	نسبة %	
1	البنك اليمني للإنشاء والتعمير	29	13.81	19	12.34	65.52	5	15.62	14	11.48	48.28
2	البنك الأهلي اليمني.	9	4.29	7	4.55	77.78	1	3.13	6	4.92	66.67
3	يوناييتد بنك ليمتد	4	1.90	4	2.60	100.00	2	6.25	2	1.64	50.00
4	البنك العربي	7	3.33	7	4.55	100.00	2	6.25	5	4.10	71.43
5	بنك السيمن والكويست للتجارة والاستثمار.	17	8.10	12	7.79	70.59	2	6.25	10	8.20	58.82
6	بنك اليمن الدولي.	11	5.24	9	5.84	81.82	2	6.25	7	5.74	63.64
7	مصرف الرافدين.	4	1.90	3	1.95	75.00	1	3.13	2	1.64	50.00
8	بنك التسليف التعاوني والزراعي.	20	9.52	13	8.44	65.00	1	3.13	12	9.84	60.00
9	البنك التجاري اليمني.	14	6.67	8	5.19	57.14	2	6.25	6	4.92	42.86
10	البنك الإسلامي اليمني للتمويل والاستثمار.	10	4.76	8	5.19	80.00	3	9.37	5	4.10	50.00
11	بنك التضامن الإسلامي الدولي.	21	10.00	17	11.04	80.95	3	9.37	14	11.48	66.67
12	بنك سبا الإسلامي.	22	10.47	16	10.39	72.73	2	6.25	14	11.48	63.64
13	بنك اليمن والخليج.	11	5.24	9	5.84	81.82	2	6.25	7	5.74	63.64
14	مصرف اليمن والبحرين الشامل.	16	7.63	11	7.14	68.75	1	3.13	10	8.20	62.50
15	بنك قطر الوطني	8	3.81	6	3.90	75.00	1	3.13	5	4.10	62.50
16	مصرف الكريمي للتمويل الأصغر الإسلامي.	7	3.33	5	3.25	71.43	2	6.25	3	2.46	42.86
الإجمالي		210	%100	154	%100	73.33	32	%100	122	%100	58.10

* الجدول من إعداد الباحث.

وباستقراء الجدول السابق يتضح بأنه قد تم توزيع (210) قائمة استقصاء باليد على الأفراد العاملين المستهدفين لدى البنوك التجارية في الجمهورية اليمنية، واسترد منها (154) استقصاء بما نسبته (73.33%) من قوائم الاستقصاء الموزعة، واستبعد (32) استقصاء لعدم صلاحيتها بسبب عدم استيفائها وبعضها مستوفى بطريقة خاطئة، ولذلك فقد تم إخضاع (122) قائمة استقصاء سليمة وصالحة للتحليل تشكل ما نسبته (58.10%) من قوائم الاستقصاء الموزعة، وتلك النسبة كافية إلى حد ما ومناسبة لإجراء التحليلات الإحصائية اللازمة، والخروج بنتائج واقعية وخصوصاً لهذا النوع من الدراسات.

3-1-6: آلية وإجراءات تحليل ومعالجة بيانات الاستقصاء:

في سبيل تسهيل إجراءات التحليل الإحصائي للبيانات فقد قام الباحث بتحويل البيانات الوصفية إلى صيغ كمية رقمية يمكن قياسها، بإعطاء خمسة أوزان للإجابة عن كل فقرة، وتم قياسها باستخدام مقياس فنوي هو مقياس ليكرت خماسي الدرجات (Five Point Likert Scale)، حيث تم تحديد الأرقام (1، 2، 3، 4، 5) لتمثل أوزاناً لتلك الإجابات كما بالجدول الآتي: ⁽¹⁾

جدول (3-1-3) درجات الموافقة والنسب المئوية المقابلة لها والصيغة الكمية المقابلة لها ⁽²⁾

درجات الموافقة للصيغة الوصفية	عالية جداً	مرتفعة	متوسطة	منخفضة	منخفضة جداً
النسبة المئوية للموافقة	80% فأكثر	من 60% إلى أقل من 80%	من 40% إلى أقل من 60%	من 20% إلى أقل من 40%	أقل من 20%
الوزن النسبي (الصيغة الكمية)	(5)	(4)	(3)	(2)	(1)

ونظراً لعدم وجود توزيع معياري يعتمد عليه فقد لجأ الباحث إلى توزيع المدى (4=1-5) على (5) مستويات حسب مقياس ليكرت خماسي الدرجات، أي $0.8 = 5 \div 4$ ، وبالتالي تم تصنيف المتوسطات الحسابية لإجابات الأفراد إلى خمسة مستويات رئيسية يرى الباحث أنها ملائمة للدراسة، كما بالجدول التالي:

جدول (4-1-3) مستويات الأهمية النسبية لإجابات عينة الدراسة وفقاً للمتوسط الحسابي ⁽³⁾

مستوى الموافقة	مرتفع جداً	مرتفع	متوسط	منخفض	منخفض جداً
المتوسط الحسابي	(4.2) فأكثر	من (3.4) إلى أقل من (4.2)	من (2.6) إلى أقل من (3.4)	من (1.8) إلى أقل من (2.6)	أقل من (1.8)
الأهمية النسبية	(84%) فأكثر	من (68%) إلى أقل من (84%)	من (52%) إلى أقل من (68%)	من (36%) إلى أقل من (52%)	أقل من (36%)

فإذا كان المتوسط الحسابي لإجابات أفراد عينة الدراسة ما دون (1.8) فهذا يدل على أنهم غير موافقين بشدة ويكون مستوى موافقتهم منخفض جداً، أما إذا كان المتوسط الحسابي يقع بين (1.8) وما دون (2.6) فإن هذا يدل على أنهم غير موافقين ويكون مستوى موافقتهم منخفض، أما إذا كان المتوسط الحسابي يقع بين (2.6) وما دون (3.4) فإن هذا يدل على أن إجابة أفراد عينة الدراسة تتأرجح بين الموافقة والرفض وبالتالي فيعتبر مستوى موافقتهم عندئذٍ متوسط، أما إذا كان المتوسط الحسابي يقع بين (3.4) وما دون (4.2) فإن هذا يدل على أنهم

(1) Sekaran, Uma, (2003), "Research Methods for Business: A Skill-Building Approach", 4th Edition, John Wiley & Sons Inc., New York, USA, P.294

⁽²⁾ الجدول من إعداد الباحث.
⁽³⁾ الجدول من إعداد الباحث.

موافقين ويكون مستوى موافقتهم مرتفع، أما إذا كان المتوسط الحسابي أكبر من (4.2) فإن ذلك يدل على أن أفراد عينة الدراسة موافقين وبمستوى مرتفع جداً.

وبشكل عام كلما كان المتوسط الحسابي أكثر من (3) فإن ذلك يدل على أن اتجاهات عينة الدراسة إيجابية نحو الفقرات المختلفة، إذ يمثل نسبة موافقة تزيد عن (60%)، وبالتالي تكون الموافقة إيجابية على درجة مخاطر أمن نظم المعلومات المحاسبية المحوسبة أو وجود التهديدات الداخلية والخارجية وحدث تلك المخاطر، ومدى تطبيق إجراءات الحماية المتبعة لمواجهة حدوث تلك المخاطر، حيث تعكس اتفاق من قبل الأفراد المجيبين على الفقرات المختلفة للاستقصاء، وتكون العبارة مرفوضة إذا كان المتوسط الحسابي أقل من (3) والذي يمثل نسبة موافقة تقل عن (60%)، ولذلك حدد الباحث المتوسط الفرضي المعياري ب(3)، والذي يمثل متوسط الوزن النسبي للإجابات $5/(1+2+3+4+5)$.

وبعد قياس مستوى المخاطر وإجراءات الحماية المقابلة لها، يتم قياس الفجوة بين مستوى تطبيق وسائل وإجراءات الحماية ومستوى حدوث المخاطر التي تهدد أمن نظم المعلومات المحاسبية، فإذا كانت الفجوة موجبة فإن ذلك يعني أن نطاق إجراءات الرقابية والحماية فعالة وتفي أو تزيد عن مستوى الرقابة المطلوبة وإذا كانت الفجوة سالبة فإن نطاق إجراءات الرقابية والحماية غير فعالة.

3-1-7: المقاييس والأساليب التحليلية الإحصائية المستخدمة في معالجة البيانات:

لغرض تحليل البيانات التي تم الحصول عليها، تمت الاستفادة من الإصدار رقم (18.1) للبرنامج الإحصائي والذي يُعرف بالحزمة الإحصائية للعلوم الاجتماعية، (SPSS: Win 18.1)، حيث جرى الاستعانة بعدة مقاييس إحصائية وصفية وتحليلية من أجل توظيف البيانات التي تم جمعها لخدمة أغراض هذه الدراسة وتحقيق أهدافها، وأهم تلك المقاييس تتمثل في: (1)

3-1-7-1: مقاييس الإحصاء الوصفية: تم استخدام التحليلات الوصفية لوصف خصائص أفراد العينة واستخراج التكرارات والنسب المئوية، وللإجابة على تساؤلات الدراسة تم استخدام المتوسطات الحسابية والانحرافات المعيارية، ومعاملات الاختلاف.

3-1-7-2: مقاييس الإحصاء التحليلي الاستدلالي: فضلاً عما قدمه الإحصاء الوصفي من أوساط حسابية وانحرافات معيارية ومعاملات اختلاف للمتغيرات المستقلة والمتغير التابع، فإن الإحصاء الاستدلالي سيبيّن معنوية ودلالة الفروق للأوساط الحسابية لمتغيرات الدراسة، وكذلك تأثيرات وعلاقات المتغيرات المستقلة بالمتغير التابع من حيث طبيعة التأثيرات والعلاقات واتجاهها ودرجات المعنوية، ولذلك فقد تم استخدام عدد من الأساليب الإحصائية التحليلية الاستدلالية لتحقيق أهداف الدراسة، وتم اعتماد مستوى الدلالة الإحصائية (5%) الذي يقابله مستوى ثقة

(1) منسي، محمود & الشريف، خالد (2014)، *التحليل الإحصائي للبيانات باستخدام برنامج SPSS - الجزء الأول*، دار الجامعة الجديدة، الإسكندرية، مصر.
& البياتي، محمود مهدي (2005)، *تحليل البيانات الإحصائية باستخدام البرنامج الإحصائي SPSS*، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، الأردن، ص: 81-98

(95%) لتفسير نتائج الاختبارات التي أجراها الباحث وفيما يلي أهم الأساليب الإحصائية التحليلية الاستدلالية التي تم استخدامها:

1. **اختبار ثبات الأداة (Reliability Test):** لقياس مقدار الاتساق الداخلي للأداة، ومدى الاعتماد عليها، ودرجة مصداقية فقراتها، تم احتساب معامل كرونباخ ألفا (Cronbach's Alpha)، وتفسر ألفا بأنها معامل الثبات الداخلي بين الإجابات، ولذا فإن القيمة المقبولة إحصائياً لهذا المعامل هي (60%) فأكثر، لتعميم النتائج.⁽¹⁾
2. **اختبار التوزيع الطبيعي (Kolmogorove- Smirnov : K-S):** لمعرفة فيما إذا كانت البيانات موزعة توزيعاً طبيعياً (توزيع غوس)، وهو التوزيع الذي يفترض فيه أن تتساوى قيم الوسط الحسابي والوسيط والمنوال وأن يكون شكله متناظر كشرط لتطبيق أسلوب الانحدار والارتباط الخطيين، ومن ثم إمكانية تعميم النتائج على مجتمع الدراسة.
3. **تحليل الارتباط الخطي (Linear Correlation Analysis):** تم استخدام معامل ارتباط بيرسون للتأكد من قوة النموذج، وقوة واتجاه الارتباط (التوافق) بين متغيرات الدراسة، حيث تم استخدام اختبار بيرسون لاختبار الفرضيات وقياس قوة العلاقة بين المتغيرات المستقلة والمتغير التابع، فإذا كانت القيمة المعنوية المحسوبة (Sig) أقل من مستوى الدلالة (0.05)، ترفض الفرضية العدمية وتقبل الفرضية البديلة.
4. **اختبار (T) للعينة الواحدة (One Sample T-Test):** يستخدم لاختبار فرضية تتعلق بالمتوسط الحسابي، لفحص ما إذا كان متوسط متغير ما لعينة واحدة يساوي قيمة ثابتة⁽²⁾، حيث يستخدم لتحديد اتجاه الفروق بين آراء أفراد عينة الدراسة من خلال التحقق من أن متوسط كل فقرة من الفقرات الواردة في الاستقصاء أقل أو أكبر من المتوسط الفرضي المعياري لأداة القياس (3) وفق مقياس ليكرت الخماسي، بدرجة جوهرية معنوية إحصائياً وليست ناتجة عن الصدفة، ويكون معيار القبول أو الرفض للفرضيات هو قيمة المتوسط الحسابي والقيمة المعنوية المحسوبة (P. Value=Sig) لمعاملات (T) عند مستوى الدلالة الإحصائية المعيارية (5%).
5. **تحليل الانحدار الخطي البسيط (Simple Regression Analysis):** لفحص أثر المتغير المستقل بشكل منفرد (التهديدات الداخلية أو التهديدات الخارجية أو إجراءات الحماية المطبقة لدى البنوك التجارية في الجمهورية اليمنية)، على المتغير التابع (المخاطر التي تهدد نظم المعلومات المحاسبية في تلك البنوك) ومعرفة مدى تفسير كل متغير مستقل للتغير في حركة المتغير التابع، حيث يتضمن هذا التحليل:
 - معامل ارتباط بيرسون (R) لقياس شدة واتجاه العلاقة بين المتغير المستقل والمتغير التابع، وتقع قيم معاملات ارتباط بيرسون بين (-1) و(+1) وبناءً عليه تكون العلاقة بين المتغيرات ضعيفة إذا كان المعامل أقل من (0.30)، ومتوسطة إذا كان بين (0.30) و(0.70)، وقوية إذا كان أكبر من (0.70).
 - معامل التحديد (R^2) ويساوي مربع معامل الارتباط (R)، ويستخدم لقياس المساهمة النسبية للمتغير المستقل في تفسير التباين في المتغير التابع.

(1) Sekaran, Uma, (2003), "Research Methods for Business: A Skill-Building Approach", OP. Cit., P.291.

(2) الزعبي، محمد بلال & والطلافة، عباس، (2004)، "النظام الإحصائي SPSS- فهم وتحليل البيانات الإحصائية"، مرجع سابق، ص 154.

■ معامل الانحدار (B)، ويستخدم لقياس التغير في المتغير التابع عندما يزداد المتغير المستقل بدرجة واحدة. وفي جميع الأحوال يكون معيار قبول أو رفض الفرضية المتعلقة بالعلاقة أو التأثير هو قيمة مستوى الدلالة المحسوب ($P. Value$) لمعاملات (F) أو (T) ومقارنتها بمستوى الدلالة المعنوية (5%).

6. **تحليل التباين الأحادي ($One-Way Analysis of ANOVA - F$):** للتعرف على مدى وجود فروقات ذات دلالة إحصائية بين إجابات عينة الدراسة تعزى لبعض الخصائص الخاصة بالمحيط أو البنك الذي ينتمي له، حيث تم الاعتماد على مستوى قيمة (F)، ومقارنتها بقيمة الدلالة الإحصائية (0.05) المعتمدة لقبول، أو رفض الفرضيات.

8-1-3: التحقق من صدق أداة الدراسة واختبار موثوقيتها وثباتها ($Validity \& Reliability$):

■ 1-8-1-3: اختبار الصدق الظاهري التحكيمي ($Validity$):

للتحقق من سلامة وصدق فقرات الاستقصاء، والتأكد من دقتها ووضوحها وملاءمتها لموضوع الدراسة، وقدرتها على قياس المتغيرات المراد قياسها، قام الباحث بصياغة الفقرات بشكل يتوافق مع الجانب النظري، بالإضافة إلى تحكيم الاستقصاء في صورته الأولية من قبل بعض السادة الأفاضل من أعضاء هيئة التدريس المتخصصين في كلية الاقتصاد بجامعة دمشق وكلية التجارة والاقتصاد بجامعة صنعاء وعمران⁽¹⁾، حيث قاموا مشكورين بتحكيم قائمة الاستقصاء وتم الاستفادة من ملاحظاتهم القيمة، وإجراء التعديلات المطلوبة بشكل دقيق يحقق التوازن بين مضامين الاستقصاء في فقراته، وبالحد الذي يضمن الاحتفاظ بشمولية الاستقصاء وصدق محتواه، حيث تم إعادة صياغة بعض الفقرات، وتم إلغاء بعض منها لإخراج الاستقصاء في صورته النهائية⁽²⁾.

■ 2-8-1-3: اختبار ثبات أداة الدراسة ($Reliability$):

لاختبار مدى توفر الثبات للبيانات الواردة في الاستقصاء ومدى الحصول على نفس النتائج أو نتائج قريبة منها فيما لو كررت الدراسة تحت نفس الظروف أو في ظروف مشابهة، تم احتساب معاملات الاتساق الداخلي حسب معامل ثبات ألفا كرونباخ ($Cronbach's Alpha$)، والذي يعبر عن متوسط الارتباط الداخلي بين الفقرات التي يقيسها، وتتراوح قيمته ما بين (صفر) و (1)، وتعتبر القيمة المقبولة له (0.60) فأكثر، حيث يعتبر المقياس ضعيفاً إذا كان أقل من (0.60)، ومقبولاً إذا كان يقع بين (0.60-0.70)، وجيداً إذا كان يقع بين (0.70-0.80)، وممتازاً إذا كان أكبر من (0.80)⁽³⁾، وكلما اقتربت قيمته من الواحد الصحيح كلما ارتفعت درجة ثبات الأداة وصلاحياتها للاستخدام، وقد كانت النتائج كما في الجدول الآتي:

(1) انظر الملحق رقم (2) أسماء المحكمين للاستقصاء.

(2) انظر الملحق رقم (1) قائمة الاستقصاء.

(3) Sekaran, Uma, (2003), "Research Methods for Business: A Skill-Building Approach", OP. Cit., P.291.

جدول (3-1-5) يبين نتائج اختبار معامل ألفا كرونباخ
للتحقق من درجة ثبات البيانات الواردة في الاستقصاء

م	محاور ومتغيرات الدراسة	عدد الفقرات	قيمة معامل الثبات (Cronbach's Alpha)	النتيجة
1	مخاطر أمن نظم المعلومات المحاسبية (30-1)	30	0.897	مقبولة
2	التحديات الداخلية لأمن نظم المعلومات المحاسبية (31-59)	29	0.928	مقبولة
3	التحديات الخارجية لأمن نظم المعلومات المحاسبية (60-76)	17	0.818	مقبولة
4	مدى تأثير مخاطر أمن نظم المعلومات المحاسبية (77-90)	14	0.897	مقبولة
5	مدى كفاية إجراءات ووسائل الحماية المطبقة (91-150)	60	0.963	مقبولة
	أداة الاستقصاء ككل (1-150)	150	0.913	مقبولة بدرجة عالية جداً

الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS).

ومن الجدول يتضح أن قيم معاملات الثبات لجميع الأبعاد بمتغيرات الدراسة كانت عالية ومقبولة إحصائياً، فقد تراوحت بين (0.818 - 0.963) لمتغيرات الدراسة المختلفة، و(0.913) للأداة الكلية (باستثناء الأسئلة الخاصة بخصائص الأفراد والبنوك)، وذلك يُعدُّ مؤشراً جيداً لأنه يعني توفر درجة عالية جداً من الثبات الداخلي للبيانات، وأنه لو تم إعادة توزيع الاستقصاء مرة أخرى على نفس مجتمع الدراسة فسوف نحصل على نفس النتائج وبنسبة لا تقل عن (81.8%)، وبالتالي يمكن الاعتماد على البيانات التي جمعت بواسطة الاستقصاء كمصدر أولي للدراسة لتحقيق أهدافها، وتعميم نتائجها على مجتمع الدراسة الكلي لدى البنوك التجارية في الجمهورية اليمنية.

3-1-9: اختبار التوزيع الطبيعي لبيانات متغيرات الدراسة (Tests of Normality):

قام الباحث بإجراء بعض الاختبارات وذلك من أجل ضمان ملائمة البيانات لافتراضات تحليل الانحدار، وتطبيق الاختبارات المعلمية لاختبار فرضيات الدراسة، وتعميم النتائج على مجتمع الدراسة⁽¹⁾، حيث تم استخدام اختبار كولمجروف سميرونوف ($K-S = Kolmogorov-Smirnov Test$) لدراسة مدى إتباع بيانات متغيرات الدراسة للتوزيع الطبيعي، إذ تتبع البيانات التوزيع الطبيعي عندما تكون القيمة المعنوية ($Level of Significance$) أكبر من مستوى الدلالة الإحصائية (0.05)، ويوضح الجدول الآتي نتيجة هذا الاختبار:

(¹) الزعبي، محمد بلال & الطلافحة، عباس، (2004)، "النظام الإحصائي SPSS- فهم وتحليل البيانات الإحصائية"، مرجع سابق، ص 246.

جدول (3-1-6) يبين نتيجة اختبار (K-S) حول إتباع بيانات الدراسة للتوزيع الطبيعي (توزيع غوس)

م	متغيرات الدراسة	عدد الفقرات	قيمة (Z) المحسوبة	القيمة المعنوية Sig.	دلالة الفروق عن التوزيع الطبيعي	النتيجة
1	مخاطر أمن نظم المعلومات المحاسبية (30-1)	30	0.078	0.200	لا توجد فروق دالة	يتبع التوزيع الطبيعي
2	التحديات الداخلية لأمن نظم المعلومات المحاسبية (31-59)	29	0.063	0.200	لا توجد فروق دالة	يتبع التوزيع الطبيعي
3	التحديات الخارجية لأمن نظم المعلومات المحاسبية (60-76)	17	0.070	0.200	لا توجد فروق دالة	يتبع التوزيع الطبيعي
4	مدى تأثير مخاطر أمن نظم المعلومات المحاسبية (77-90)	14	0.076	0.084	لا توجد فروق دالة	يتبع التوزيع الطبيعي
5	مدى كفاية إجراءات ووسائل الحماية المطبقة (91-150)	60	0.067	0.200	لا توجد فروق دالة	يتبع التوزيع الطبيعي
	أداة الدراسة ككل (1-150)	150	0.064	0.200	لا توجد فروق دالة	يتبع التوزيع الطبيعي

الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS)، N=122، df=121، قيمة (Z) الجدولية = 1.96، مستوى الدلالة (α) = 0.05

نلاحظ من الجدول السابق أعلاه أن القيم المعنوية لجميع متغيرات الدراسة أكبر من مستوى الدلالة الإحصائية (0.05)، أي أنه عند مستوى الثقة 95% لا توجد فروق دالة إحصائية في توزيع قيم متغيرات الدراسة عن التوزيع الطبيعي، فضلاً عن أن القيمة المعنوية لأداة الدراسة ككل بلغت (0.200) وهي أكبر من مستوى الدلالة 0.05 وبالتالي لا توجد فروق دالة إحصائية، كما أن قيمة (Z) المعيارية المحسوبة لكل مقياس كانت أصغر من قيمة (Z) المعيارية الجدولية 1.96 عند مستوى دلالة أقل من (0.05)، بما يؤكد إتباع بيانات مقاييس الدراسة الخمسة للتوزيع الطبيعي (غوس)، وبالتالي فإنه يمكن استخدام الاختبارات الإحصائية المعلمية (البارامترية) عليها، والسماح بتعميم النتائج على مجتمع الدراسة، وعلى ضوء ذلك يمكن استخدام اختبار (T) لعينة الدراسة، بالإضافة إلى تطبيق تحليل الانحدار للتعرف على مدى تأثير وعلاقة أي من المتغيرات المستقلة على المتغير التابع في هذه الدراسة.

3-1-10: اختبار قوة نموذج الدراسة (Multicollinearity):

للتأكد من الاتساق الداخلي (Internal Consistency) لمتغيرات الدراسة وأن أسئلة كل فرضية لا تصلح إلا لها فقط ولا تصلح لغيرها من الفرضيات، بحيث لا يوجد تداخل فيما بينها فقد تم استخراج مصفوفة معاملات الارتباط الخطي لبيرسون (Pearson Correlation) للتحقق من مدى اتساق كل فقرة من فقرات الاستقصاء مع المجال الذي تنتمي إليه، حيث يقصد بمدى الاتساق الداخلي قوة الارتباط بين درجات كل مجال ودرجات أسئلة الاستقصاء الكلية، أما تحليل الصدق فهو مدى اتساق كل فقرة من مع المجال الذي تنتمي إليه تلك الفقرات⁽¹⁾، ومن أجل ضمان ملائمة البيانات لافتراضات تحليل الانحدار، قام الباحث بإجراء اختبار معامل التباين التضخمي (Variance Inflationary Factors) لمتغيرات الدراسة، ويكون نموذج الدراسة قوي عندما يكون معامل التباين التضخمي أصغر من (5) درجات ويتم حسابه بتعويض أكبر معامل ارتباط للمتغيرات المستقلة للدراسة فيما بينها بمعادلة معامل تضخم التباين R^2 (-1) / VIF = 1 ويوضح ذلك الجدول التالي:

(1) عبد الفتاح، محمد نجيب، وآخرون، (2009)، التحليل المعقد للبيانات باستخدام حزمة البرامج الجاهزة (SPSS)، جامعة الدول العربية، القاهرة، مصر، ص ص: 211 - 213.

جدول (3-1-7) مصفوفة معاملات ارتباط (بيرسون) بين متغيرات الدراسة

متغيرات الدراسة	معامل الارتباط ومستوى الدلالة	مخاطر أمن نظم المعلومات المحاسبية	التهديدات الداخلية لأمن نظم المعلومات المحاسبية	التهديدات الخارجية لأمن نظم المعلومات المحاسبية	مدى تأثير المخاطر على أمن نظم المعلومات المحاسبية	مدى كفاية إجراءات وسائل الحماية المطبقة
مخاطر أمن نظم المعلومات المحاسبية	معامل الارتباط مستوى الدلالة	1 0.000	**0.570 0.000	**0.386 0.000	*0.220 0.015	- **0.498 0.000
التهديدات الداخلية لأمن نظم المعلومات المحاسبية	معامل الارتباط مستوى الدلالة	**0.570 0.000	1 0.000	**0.581 0.000	**0.476 0.000	- **0.347 0.000
التهديدات الخارجية لأمن نظم المعلومات المحاسبية	معامل الارتباط مستوى الدلالة	**0.386 0.000	*0.581 0.000	1 0.000	**0.627 0.000	- **0.274 0.002
مدى تأثير المخاطر على أمن نظم المعلومات المحاسبية	معامل الارتباط مستوى الدلالة	*0.220 0.004	**0.476 0.000	*0.627 0.000	1 0.692	- 0.036 0.692
مدى كفاية إجراءات وسائل الحماية المطبقة	معامل الارتباط مستوى الدلالة	- **0.498 0.000	- **0.347 0.000	- **0.274 0.002	- 0.036 0.692	1 0.692

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS).
• ** ذات دلالة إحصائية عند مستوى الدلالة الإحصائية (0.01 = α)، * ذات دلالة إحصائية عند مستوى الدلالة الإحصائية (0.05 = α).

وتشير بيانات الجدول السابق أن أكبر قيمة للارتباط بين العوامل المستقلة ببعضها كانت بين التهديدات الخارجية لأمن نظم المعلومات، وتأثيرات المخاطر على أمن نظم المعلومات، حيث بلغ معامل الارتباط (0.627)، وبتعويض هذه القيمة في معادلة التباين التضخمي تبين أن:

$$VIF = 1/(R^2 - 1) = 1/\{(0.627)^2 - 1\} = 1.648$$

وبما أن قيمة (VIF) بلغت (1.648) وهي أقل من (5) فإن ذلك يعني عدم وجود تداخل بين متغيراته المستقلة مما يعكس قوة نموذج الدراسة، وبالتالي يمكن للباحث استخدام أسلوب الانحدار في اختبار بعض فرضيات هذه الدراسة.

2-3: المبحث الثاني: دراسة الحالة العملية

مقدمة:

يهدف أخذ صورة مبدئية لتقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية العاملة في الجمهورية اليمنية، فقد تم إجراء دراسة حالة عملية من خلال تصميم مجموعة من الأسئلة أعدت خصيصاً لهذا الغرض والتي تم استخلاصها من الأدبيات السابقة المتعلقة لإجراء المقابلات الشخصية شبه المنظمة مع مدراء أقسام تكنولوجيا المعلومات ومساعدتهم ومدراء إدارة المخاطر، في (3) بنوك مختارة تمثل القطاعات الثلاثة العامة والخاصة والمختلطة وباعتبار أن هذه البنوك تقدم التشكيلة الأوسع من الخدمات المصرفية الإلكترونية، والتي يتم من خلالها الوقوف على أهمية كل من المتغيرات المرشحة للتحليل والتقييم التي وردت في المحاور التي تناولتها الدراسة.

والجزء الثاني في هذا المبحث عبارة عن تسليط الضوء لبعض الملاحظات التي أكتشفها الباحث أثناء إجرائه للدراسة الاستكشافية في تلك البنوك الثلاثة وذلك لمعرفة نقاط الضعف وجوانب الخلل في الإجراءات المتخذة في نظم الرقابة الداخلية لنظام المعلومات المحاسبية والمخاطر الأمنية التي قد تحدث، وتقديم التوصيات المناسبة حتى تأخذ البنوك التحوطات الأمنية اللازمة أو تعديل إجراءات الرقابة الداخلية عندها حتى لا تحدث مثل تلك المخاطر، سواء من خلال توفر سياسات وإجراءات لإدارة هذا النوع من المخاطر أو توفر الكفاءات الإدارية المؤهلة للتعامل معها، وذلك انسجاماً مع الممارسات السليمة في مراقبة وإدارة مخاطر أمن نظم المعلومات المحاسبية المحوسبة.

2-3-1: هيكل البنوك التجارية العاملة في الجمهورية اليمنية:

يضم القطاع المصرفي في اليمن (16) بنكاً تجارياً رئيسياً تدير شبكة كبيرة من الفروع التي تعمل داخل الجمهورية اليمنية حتى نهاية عام 2016م، وتنقسم البنوك الرئيسية إلى عدد (12) بنكاً محلياً وطنياً، - منها عدد (9) بنوك قطاع خاص و(3) بنوك قطاع عام ومختلط - و(4) بنوك عربية وأجنبية منها بنك واحد قطاع عام والبقية بنوك تنتمي للقطاع الخاص.

وتمثل البنوك التجارية الحكومية (القطاع العام) الجزء الأعظم من القطاع المصرفي اليمني بنسبة تصل إلى حوالي (57.3%) من إجمالي البنوك العاملة في اليمن، حيث تقدم خدماتها المصرفية في معظم المحافظات اليمنية الرئيسية والثانوية بعدد فروع تصل إلى أكثر من (120) فرعاً، بينما يقتصر نشاط البنوك الأخرى (القطاع الخاص الوطني والأجنبي) على بعض المدن الرئيسية فقط بعدد فروع تصل إلى حوالي (81) فرعاً، الأمر الذي يعني اقتران التنافس في تقديم الخدمات المصرفية على المدن الرئيسية وهي ست مدن: صنعاء (العاصمة السياسية)،

عدن (العاصمة التجارية)، تعز، الحديدة، المكلا، إب، وبيبين الجدول رقم (3-2-1) البنوك التجارية العاملة في الجمهورية اليمنية ونوعها كما يلي:

جدول رقم (3-2-1) البنوك التجارية في الجمهورية اليمنية مرتبة وفقاً لسنة التأسيس

م	إسم البنك	جنسية البنك	سنة التأسيس	نوع الشركة	رأس المال (بملايين الريالات)	نسب ملكية رأس المال %			عدد الفروع	عدد الصرافات الآلية
						عام يمني	خاص يمني	خاص خارجي		
1	البنك اليمني للإنشاء والتعمير.	يمني	1962	مختلطة	15000	51	49		44	41
2	البنك الأهلي اليمني.	يمني	1969	عامة	10000	100			34	9
3	يوناييتد بنك ليمتد	أجنبي	1971	مساهمة مقفلة	6016			100	3	—
4	البنك العربي	عربي	1972	مساهمة مقفلة	6000			100	10	—
5	بنك اليمن والكويت للتجارة والاستثمار.	يمني	1977	مساهمة مقفلة	6000		100		17	—
6	بنك اليمن الدولي.	يمني	1979	مساهمة مقفلة	15000		85	15	23	250
7	مصرف الرافدين.	عربي	1982	عامة	6500			100	1	—
8	بنك التسليف التعاوني والزراعي	يمني	1982	مختلطة	17000	99	1		56	189
9	البنك التجاري اليمني	يمني	1993	مساهمة مقفلة	7900	10	90		18	42
10	البنك الإسلامي اليمني للتمويل والاستثمار	يمني	1996	مساهمة مقفلة	4394	5	74	21	5	—
11	بنك التضامن الإسلامي الدولي	يمني	1995	مساهمة مقفلة	20000		97	3	24	150
12	بنك سبأ الإسلامي	يمني	1997	مساهمة مقفلة	10119		85	15	14	100
13	بنك اليمن والخليج	يمني	2001	مساهمة مقفلة	1250	1	77	22	2	—
14	مصرف اليمن البحرين الشامل	يمني	2002	مساهمة مقفلة	6000		53	47	10	—
15	بنك قطر الوطني	عربي	2007	مساهمة مقفلة	6000			100	1	—
16	مصرف الكريمي للتمويل الأصغر الإسلامي	يمني	2010	مساهمة مقفلة	6000		100		87	—

المصدر: من إعداد الباحث بالاعتماد على البنك المركزي اليمني، التقرير السنوي، أعداد متفرقة، سعر الصرف 215 ريال/ دولار خلال العام 2012 م.

3-2-2: الخدمات المصرفية التقليدية للبنوك التجارية العاملة في الجمهورية اليمنية

لا شك أن قيام أي بنك تجاري يعني قيامه بمجموعة من الخدمات البنكية لعملائه بالإضافة إلى دوره في دعم الاقتصاد الوطني والمساهمة في عملية التنمية الاقتصادية، وتأخذ البنوك التجارية في الجمهورية اليمنية بأسلوب التطوير الشامل فلسفة ومنهجاً، وتهدف أساساً إلى تلبية احتياجات العملاء بأسلوب يفوق توقعاتهم، سواءً أكان ذلك من حيث جودة ودقة الخدمة وتشكيلة المنتجات، ومن أهم أهداف البنك التجاري سعيه للحصول على عائد، ومساهمته في دعم الاقتصاد الوطني، ولتحقيق ذلك لابد من أداء مجموعة من الوظائف، ويصعب حصر وتحديد تلك الوظائف باعتبار أن البنوك التجارية تقوم بخدمات متنوعة ومتجددة، ولم تعد تدور حول عمليات مارستها منذ مئات السنين، كقبول الودائع ومنح القروض، بل تعدتها إلى ما توصلت إليه العقليّة المصرفية من أساليب ووسائل ابتكرتها تلبيةً لرغبة وحاجة عملائها فهي تخضع لعمليات التطوير باستمرار، فلا يوجد حد يمكن أن تقف عنده البنوك سوى مستوى تخيل إدارة البنك والتشريعات والقوانين الخاصة بدولة معينة والتي يمارس البنك أعماله في حدودها، وقد حدد المشرع اليمني مجموعة من الوظائف اوجب على كل بنك مرخص يزاول أعماله المصرفية داخل اليمن القيام بها وتتمثل في الأعمال المصرفية التالية:⁽¹⁾

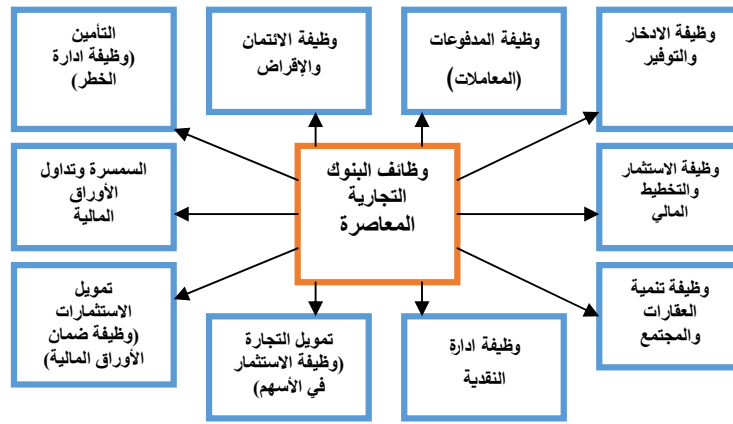
1. قبول الودائع النقدية القابلة للدفع عند الطلب أو حسب ترتيبات أخرى والقابلة للسحب بالشيك أو الحوالة أو أمر الصرف ومنح القروض والتسهيلات الائتمانية.
 2. بيع وخصم الكمبيالات والحوالات والكوبونات والسندات للأغراض التجارية.
 3. إجراءات المعاملات المصرفية مع المراسلين والحصول على التسهيلات المصرفية.
 4. شراء وبيع العملات الأجنبية والسبائك والنقود الذهبية والفضية والأسهم والسندات.
 5. إصدار وخصم خطابات الضمان، وفتح الاعتمادات المستندية وتحصيل مستندات الشحن.
 6. تحصيل الشيكات والسندات والحوالات، وشراء وبيع سندات الدولة والحوالات الحكومية.
 7. القيام بأعمال الوكيل أو الأمين بصفة مراسل أو وكيل للمؤسسات المصرفية والمالية.
 8. التأجير التمويلي، ويتضمن إيجار أصول ثابتة لمدة معينة مقابل اجر محدد مع وعد بالبيع عند نهاية المدة وبشروط لتحويل الإيجار إلى بيع أو التنازل عن ملكية الشيء المؤجر إلى المستأجر.
- وعلاوة على تلك الوظائف التي أوردتها المشرع اليمني فقد أضاف الكثير من الكتاب الوظائف التالية:

1. شراء الشيكات العادية والسياحية، وإصدار بطاقات الائتمان والفيزا للعملاء.
2. تقديم الخدمات الاستشارية المالية للعملاء.
3. المساهمة في إنشاء أو دعم المشاريع الاقتصادية، وكذلك تنمية المدخرات والاستثمارات المالية لخدمة الاقتصاد الوطني.

(¹) الجمهورية اليمنية، وزارة الشؤون القانونية، قانون رقم 38 لعام 1998 بشأن البنوك، الجريدة الرسمية، العدد 24، ج 2 المادة 2، الفقرة هـ & قانون رقم 14 لعام 2000 بشأن البنك المركزي اليمني، الجريدة الرسمية، العدد 12، ج 2، المادة 2، الفقرة (ز).

4. إيجاد وسائل حديثه تحل محل التعامل بالنقد الفعلي، مثل الشيكات المصرفية وبوالص التحصيل.
 5. الاحتفاظ بسجلات صحيحة عن الخدمات المقدمة للعملاء، بما يتيح فحص ومراجعة حساباتهم.
 6. صرف الرواتب الشهرية لموظفي الشركات العامة أو الخاصة والمتعاقدة مع البنك على ذلك.
 7. تحصيل فواتير الكهرباء والمياه من العملاء وتسجيلها لحساب الدوائر المختصة.
 8. تأجير الخزائن الحديدية الآمنة لحفظ المجوهرات والمستندات الهامة لعملائها.
- كما أنها توفر مجالاً واسعاً من الوظائف المالية لأي منشأة تعمل في ميدان الاقتصاد، مما أدى إلى وجود بنوك وخدمات مالية عالمية ذات جودة عالية، ويوضح الشكل رقم (3-1-1) وظائف البنوك التجارية المعاصرة.

الشكل رقم (3-2-1) وظائف البنوك التجارية المعاصرة (1)



ولا شك أن البنوك تقوم بأعمال مهمة ونافعة للمجتمع ولكن في نفس الوقت لها أعمال محرمة شرعاً لما فيه من الابتزاز والضرر بضعفاء المجتمع، وبالتالي فإن البنوك التجارية الإسلامية لا تختلف في وظائفها عن البنوك التجارية التقليدية إلا في عدم استعمالها للفائدة الربوية.

3-2-3: الخدمات المصرفية الإلكترونية للبنوك التجارية في الجمهورية اليمنية:

أدى التقدم التكنولوجي إلى ظهور تغيرات جوهرية في طبيعة عمل القطاع المصرفي، وبالتالي ظهور خدمات مصرفية متطورة ومتنوعة و ذلك بالاعتماد على ما أنتجته تلك التكنولوجيا من وسائل وأدوات حديثة ومتطورة أدت إلى استبدال أو تطوير بعض الخدمات التقليدية بخدمات إلكترونية،⁽²⁾ ويستطيع البنوك من خلال استخدام التكنولوجيا تذليل الصعوبات وتطوير خدمات مصرفية إضافية جديدة لأسواقها الحالية والمستقبلية، فتقدم البنوك الإلكترونية كافة الخدمات المصرفية التقليدية، وإلى جانبها خدمات أكثر تطوراً تميزها عن الأداء التقليدي من خلال قيامها بتطوير عدة تطبيقات جديدة للخدمات المصرفية الحالية التي تقدمها لعملائها وتحسين نوعية الخدمات المصرفية.⁽³⁾

(1) Rose, Peter S. (2002), "Commercial Bank Management", 5th Edition, McGraw-Hill, Companies, Inc., Boston, USA, P.8.

(2) Daru, M. U. (2015). Role of computerized accounting in banking sector. *OP. Cit.*, PP: 26-34.

(3) القاسم، عبد الرزاق & العلي، أحمد، "أثر تقنية المعلومات في تطوير نظم عمليات المصارف العامة في سوريا"، *مجلة جامعة دمشق*، مجلد (28)، العدد (1)، 2012، ص ص: 301-326.

إن الأعمال الإلكترونية هي كل العمليات والنشاطات التي يتم عقدها أو تنفيذها أو الترويج لها بوسائل إلكترونية كالهاتف والحاسوب والصراف الآلي والانترنت وغيرها، وكذلك العمليات التي تجريها المؤسسات التي تصدر بطاقات الدفع أو الائتمان الإلكترونية، والتي تتعاطى التحويلات النقدية إلكترونياً ولها مواقع للعرض والشراء والبيع،⁽¹⁾ والبنوك التجارية في الجمهورية اليمنية تقوم بتطوير المصارف الإلكترونية في الأنظمة الخاصة بها، ومع ذلك فإن هذا التطوير يمكن النظر إليه كخطوات أساسية نحو تنمية المصارف الإلكترونية، استجابة لثورة المعلومات، وخاصة مع اعتماد سياسة الباب المفتوح وإفساح المجال أمام البنوك الأجنبية لتعزيز المنافسة، وقد انعكس هذا في الغالب في حوسبة نظم المعلومات المحاسبية والإدارية والابتكار الجديد في تقديم الخدمات المتخصصة اعتماداً على مرافق الحاسوب، وإنشاء مراكز المعلومات والإدارات المتخصصة في تكنولوجيا المعلومات مع تطعيم تلك المراكز بالكوادر البشرية المؤهلة وإعطائهم دورات تدريبية داخل اليمن وخارجها لزيادة قدراتهم وكفاءاتهم.

وتعدّ البنوك التجارية في الجمهورية اليمنية أحد أهم المنشآت الرائدة والتي استفادت من تكنولوجيا الاتصالات والمعلومات، حيث انتقلت من مرحلة استخدام تقنيات الحاسوب وفق الأسلوب التقليدي من تخزين واسترجاع البيانات والمعلومات إلى تقديم الخدمات بقالب جديد واستحداث خدمات مصرفية جديدة وبعده وسائل والتي من أهمها شبكات الصرف الآلية (ATM)،⁽²⁾ وكذلك البنك الناطق (Tele Bank)، واستخدام نظام السويفت (SWIFT)، وشبكة المدفوعات الإلكترونية في إنجاز التحويلات المصرفية محلياً ودولياً، وتقديم الخدمات المصرفية من خلال مواقع البنوك على شبكة الإنترنت أو ما يطلق عليه الإنترنت المصرفي (Internet Banking) والذي يعد بدوره أحد أسرع تطبيقات الإنترنت انتشاراً على مستوى العالم.

ومن الخدمات الإلكترونية التي تقدمها البنوك خدمات بطاقات الصراف الآلي التي تقدمها أغلب البنوك اليمنية، كما أن بعض البنوك تقدم سقف متدني لعمليات السحب عبر الصراف الآلي ولا يتجاوز هذا السقف 100 ألف ريال يمني لدى أغلب البنوك العاملة في السوق المصرفي اليمني.

ومن البنوك التي تقدم خدمات بنكية عبر الرسائل القصيرة بنك التسليف التعاوني (كاك بنك) ومصرف الكريمي الذي يتيح للعملاء إرسال الحوالات عبر الجوال بسعر مخفّض رغم سوء الخدمات التي يقدمها مصرف الكريمي حيث يفرض رسوم على كل عملية إيداع أو سحب من الحساب في غير الفرع الذي تم فتح الحساب فيه وهو ما دفع العملاء للإحجام عن افتتاح حسابات لهم لدى ذلك المصرف، إلى جانب الخدمات عبر المواقع الإلكترونية هناك خدمات عبر الجوال تمكن المشترك من الاستعلام عن رصيده وإجراء تعاملات بنكية والتحويل من حساب إلى آخر عبر الرسائل القصيرة.

وفي الجانب الآخر ما تزال بعض البنوك التي تقدم خدمات إلكترونية ترفض تقديمها إلا للشركات فقط ولا تقدمها للعميل العادي، كما أن هناك عدد من البنوك التجارية اليمنية ما تزال خارج المنافسة وما تزال غير قادرة على مواكبة التطور الحاصل في عالم الخدمات البنكية الإلكترونية.

(1) الحداد، وسيم وآخرون، (2011)، "الخدمات المصرفية الإلكترونية"، دار المسيرة للنشر والتوزيع والطباعة، عمان، الأردن، ص 38.

(2) الربيدي، محمد علي، (2010)، "حماية المعلومات المحاسبية في ظل مخاطر التكنولوجيا للعمليات المصرفية الإلكترونية: دراسة ميدانية في البنوك العاملة في اليمن"، مرجع سابق، ص: 1-46.

وبشكل عام تقوم البنوك التجارية في اليمن بتقديم خدمات مصرفية واستثمارية متكاملة، أهمها ما يأتي: (1)

1. **الحسابات الجارية:** وهي حسابات مصرفية تتميز بمرونة السحب والإيداع، وتسهيل القيام بعدد غير محدود من المعاملات المصرفية، وفقاً لأحكام الشريعة الإسلامية.
2. **حسابات التوفير:** وهي حسابات مصرفية تمنح أرباحاً وتتميز بمرونة السحب والإيداع، وإنجاز عدد غير محدود من المعاملات المصرفية، ومتوافقاً مع أحكام الشريعة الإسلامية.
3. **حسابات الودائع الاستثمارية:** وهي حسابات مصرفية يُخول المودع فيها المصرف باستثمار أمواله وفقاً لأحكام الشريعة الإسلامية.
4. **خدمات الفيزا إلكترون:** وتتيح للعميل عملية السحب النقدي، ودفع قيمة مشترياته من حسابه الجاري، أو حساب التوفير، وفي حدود رصيده المتاح.
5. **بطاقة الفيزا كارد:** وتعد إحدى وسائل الدفع، لسداد المشتريات من السلع والخدمات التي يوفرها المصرف.
6. **بطاقة الإنترنت:** وهي بطاقة مسبقة الدفع يتمكن حاملها من استخدامها للتسوق عبر شبكة الإنترنت لدى المواقع التجارية للشراء، أو وضع الخدمات أو الاشتراك في المواقع الأكاديمية.
7. **بطاقة الصراف الآلي:** وهي بطاقة يستطيع العميل من خلالها القيام بعمليات السحب النقدي، ودفع قيمة مشترياته من حسابه الجاري، أو حساب التوفير في حدود رصيده المتاح.
8. **خدمة المصرف الناطق:** وهي خدمة تقدمها المصارف لتوفير الراحة لجميع عملاء المصرف، بتقديم العديد من العمليات المصرفية التي تغني العميل عن مراجعة الفرع.
9. **خدمة الرسائل القصيرة:** تقدم المصارف خدمة الرسائل القصيرة (SMS)، وذلك للخدمات التالية: وصول رسالة قصيرة عند حدوث أي عملية على حساب العميل، الاستعلام عن الرصيد، الاستعلام عن أسعار العملات، والاستعلام عن آخر ثلاث عمليات تمت على حساب العميل.
10. **الحوالات (المحلية، والدولية):** بالإضافة للخدمات المصرفية الخاصة مثل خدمة صرف المراتب.

وعلى الرغم من اختلاف المسميات لمفاهيم الصيرفة الإلكترونية لكنها تصب في مفهوم واحد هو البنوك التي تعمل عن طريق شبكة المعلومات الدولية (الإنترنت)، حيث تشير كلها إلى إمكانية قيام العميل بإدارة حساباته وإنجاز أعماله المتصلة بالبنك من أي مكان وفي أي وقت يرغب به لإجراء مختلف التعاملات المصرفية، بعبور الحدود الجغرافية عبر شبكة المعلومات الدولية (الإنترنت) أو أي شبكة أخرى يستخدمها البنك، وعلى أساس تزويد البنك للعميل بحزمة البرمجيات الشخصية لتقديم خدماته المالية عن بعد. (2)

(1) الجمهورية اليمنية، (2016)، **منشورات وبيروشورات مختلفة**، البنوك التجارية العاملة في الجمهورية اليمنية، صنعاء، اليمن.
(2) مريم، بن الشريف، (2011)، "الأعمال المصرفية الإلكترونية: الرهانات والتحديات وإشكالية الإشراف والرقابة المصرفية"، **مراجع سابق**، " ورقة عمل".

والجدول التالي يوضح مدى انتشار خدمات الصيرفة الإلكترونية لدى البنوك التجارية في اليمن:

جدول رقم (2-3) الخدمات المصرفية الإلكترونية في البنوك التجارية في الجمهورية اليمنية⁽¹⁾

م	البنك	الصراف الآلي	الإنترنت المصرفي	البنك الخليوي	البنك الفوري	البنك الناطق	بنك المنزل	سيارة صراف آلي متنقل	الرسائل المصرفية القصيرة
1	البنك اليمني للإنشاء والتعمير.	✓	X	X	X	X	X	X	X
2	البنك الأهلي اليمني.	✓	X	X	X	X	X	X	X
3	يوناييتد بنك ليمنتد	✓	X	X	X	X	X	X	X
4	البنك العربي	✓	✓	✓	✓	✓	X	X	✓
5	بنك اليمن والكوييت للتجارة والاستثمار.	✓	✓	✓	✓	X	X	X	✓
6	بنك اليمن الدولي.	✓	✓	X	X	✓	✓	X	✓
7	مصرف الرافدين.	X	X	X	X	X	X	X	X
8	بنك التسليف التعاوني والزراعي	✓	X	✓	✓	X	X	X	✓
9	البنك التجاري اليمني	✓	✓	✓	✓	✓	X	✓	✓
10	البنك الإسلامي اليمني للتمويل والاستثمار	✓	✓	✓	✓	✓	X	X	✓
11	بنك التضامن الإسلامي الدولي	✓	X	✓	X	✓	X	X	✓
12	بنك سبأ الإسلامي	✓	X	✓	X	X	X	X	✓
13	بنك اليمن والخليج	✓	✓	✓	X	✓	X	X	✓
14	مصرف اليمن البحرين الشامل	✓	✓	✓	✓	X	X	X	✓

(1) الجدول من إعداد الباحث بالاعتماد على منشورات وبروشورات مختلف البنوك التجارية العاملة في الجمهورية اليمنية خلال العام 2016 م.

م	البنك	الصراف الآلي	الإنترنت المصرفي	البنك الخليوي	البنك الفوري	البنك الناطق	بنك المنزل	سيارة صراف آلي متنقل	الرسائل المصرفية القصيرة
15	بنك قطر الوطني	✓	✓	✓	X	X	X	X	✓
16	مصرف الكريمي	✓	X	X	X	X	X	X	X
عدد البنوك المقدمة للخدمة		15	8	10	6	6	1	1	11

الجدول من إعداد الباحث بالاعتماد على منشورات وبروشورات مختلفة للبنوك التجارية العاملة في الجمهورية اليمنية خلال العام 2016 م.

وهنا تقتضي الضرورة الإشارة إلى أن معظم مواقع البنوك التجارية العاملة في اليمن على الشبكة العالمية للمعلومات (الانترنت) على حد سواء الوطنية منها والأجنبية لا تعدو أن تكون مواقع تعريفية فقيرة المحتوى وأغلبها لم يتغير فحواه منذ فترة طويلة.

ويلاحظ من الجدول السابق رقم (3-2-2) مدى الانتشار الواسع لشبكات وأجهزة الصراف الآلي كأهم قناة إلكترونية بين البنوك ووجود فروقات كبيرة بين البنوك في حجم انتشار القنوات الإلكترونية الأخرى فمثلاً البنك الناطق يقدم من خلال (6) بنوك فقط من أصل (16) بنكاً تجارياً، وقناة البنك الفوري، تقدم بشكل متكامل لجميع العملاء في (3) بنوك، حيث يستطيع العميل من خلالها الحصول على العديد من الخدمات المصرفية. إن انخفاض عدد المتعاملين الذين يقومون باستخدام تلك الخدمات تعد دليلاً قاطعاً على مدى الثقة في الخدمات الإلكترونية التي تقدمها البنوك التجارية العاملة في اليمن، والتي سوف تزداد أكثر وأكثر في ظل بيئة مصرفية مشجعة محاطة بتشريعات منظمة ورقابة قوية.

ويرى الباحث أنه نظراً لما يصاحب إجراء العمليات المصرفية الإلكترونية وإصدار وسائل دفع لنقود الكترونية من مخاطر فإن الأمر يستلزم وضع الأسس للإدارة الحسنة لهذه المخاطر والتحديد الدقيق لمسؤوليات مختلف الجهات ذات العلاقة بها.

الجدير بالذكر هنا أن البنك المركزي اليمني قام منذ وقت مبكر بدراسة وتقييم هذه الوسائل والتطبيقات الحديثة في الصناعة المصرفية، وتنظيماً لهذه العملية قام بإصدار قانون العمليات المصرفية الإلكترونية رقم (40) لسنة 2006م⁽¹⁾ والذي يتضمن الكثير من المواد التي تنظم العمليات المصرفية الإلكترونية، وتساهم في رقابتها من أجل تحقيق الاستفادة العالية من هذه الوسائل والتطبيقات الحديثة والحد من مخاطرها.

(1) الجمهورية اليمنية، (2006)، القانون رقم (40) لعام 2006م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية، وزارة الشؤون القانونية، الجريدة الرسمية، العدد (24)، ديسمبر 2006، صنعاء، اليمن.

وعملية الرقابة هي في الأساس عملية مشتركة بين البنك المركزي وجميع البنوك باعتبارهم المعنيين بها والمستهدفين من مخرجاتها، وبالتالي فإنه يتوجب على البنوك وضع السياسات والإجراءات التي تتيح لها إدارة المخاطر التي تصاحب تقديم العمليات المصرفية الالكترونية من خلال تقييمها والرقابة عليها ومتابعتها.⁽¹⁾

ويتفق رجال المصارف والمؤسسات ورجال الرقابة على ان المبادئ الرقابية التي تطبق على الصيرفة التقليدية هي ذاتها قابلة للتطبيق على الصيرفة الالكترونية ونتيجة التغيرات السريعة في التكنولوجيا والخدمات غالباً ما تعدل وتضاعف حجم المخاطر التقليدية وتشير بعض الدراسات التي قامت بها جهات رقابية دولية في أوروبا وآسيا وأمريكا الشمالية إلى أن هناك حاجة للمزيد من التوجيه الرقابي في ميادين مختارة من اجل تحسين الإطار العام لإدارة المخاطر بالنسبة للعمليات المصرفية الالكترونية.⁽²⁾

3-2-4: معلومات أساسية عن بعض البنوك التجارية الخاضعة لدراسة الحالة العملية:

تم اللجوء إلى (3) بنوك مختارة تمثل القطاعات الثلاثة العامة والخاصة والمختلطة وباعتبار أن هذه البنوك تقدم التشكيلة الأوسع من الخدمات المصرفية الإلكترونية، مع الحرص على عدم ذكر اسم هذه البنوك كجزء من الاحتياطات الأمنية لتلك البنوك للحفاظ على سريتها والمحافظة على سمعتها، وهذه نبذة مختصرة لكلاً منها على النحو التالي:

3-2-4-1: البنك (ع): تأسس البنك في مطلع الثمانينات كشركة عامة للقيام بتمويل القطاعات الاقتصادية والإنتاجية، وقد اعتبر شخصاً اعتبارياً عاماً ومؤسسة مصرفية حكومية تتمتع بالاستقلال المالي والإداري، وتشارك في تنمية الاقتصاد الوطني، وتمارس عملاً ذا طابع اقتصادي، حيث قدم خدمات تمويلية ومصرفية بنجاح منذ تأسيسه حتى نهاية العام 2003م، وفي بداية 2004م وانطلاقاً من برامج الإصلاح الاقتصادي التي انتهجتها الحكومة اليمنية بما يتماشى مع متطلبات العصر بالانفتاح نحو الاقتصاد العالمي وتشجيع البنوك على الانفتاح والتطور ليُطابق في التزامه وتطوره وتنوع خدماته قواعد ومواصفات العمل المصرفي العالمي، ولذلك توجه البنك للعمل المصرفي الشامل وولج سوق الصناعات المصرفية مقدماً أفضل الخدمات المصرفية فأنفرد بامتلاكها على نظرائه في الساحة المصرفية المحلية، كما واكب البنك التطورات العالمية الخاصة بالمنشآت المالية والمصرفية والتي ضمنت له دخول عالم التنافس لمصرفي بجدارة باعتباره الرائد الأول في مراتب الصدارة المالية للأعوام الماضية على التوالي ولديه أكبر شبكة مصرفية محلية فضلاً عن تواجده في دول الخليج العربي والقرن الأفريقي وتربطه شراكة مصرفية متميزة مع شبكة البنوك المراسلة.

(1) قطينة، عدنان، (2016)، "الخدمات المصرفية الالكترونية في اليمن والرقابة عليها"، دراسات وأفكار، بتاريخ 2016/6/30، 5:14 مساءً،

<http://adnanqatinah.blogspot.com/2010/06/electronic-banking-services-in-yemen.html>

(2) البواب، احمد إسماعيل، (2016)، "البنوك اليمنية ومواكبها للعمليات المصرفية الالكترونية"، تاريخ الاطلاع 2016/8/20م الساعة 7:33 صباحاً، من الموقع الالكتروني لصحيفة 26 سبتمبر، <http://www.26sep.net/newsweekarticle.php?sid=6526>

ولدى البنك نظام مصرفي متكامل يمنح العميل إمكانية تنفيذ العديد من الخدمات المصرفية من أي مكان في العالم وفي أي وقت وذلك عبر شبكة الانترنت، وتتيح له خدمة فتح الاعتمادات المستندية من أي مكان في العالم، وتنفيذ الحوالات الخارجية، وخدمة فتح الضمانات الخارجية والمحلية في أي وقت، وخدمة التحويل من حساب إلى حساب آخر لنفس العميل، خدمة سداد جميع فواتير الكهرباء والماء والهاتف الأرضي والمحمول، خدمة استعراض كشوفات الحساب والاستعلام عن أسعار صرف العملات، خدمة استعراض السقف الائتماني وفتح الحسابات الجارية، وتم تطبيق تقنية تشفير البيانات المرسله من العميل بحيث يقوم برنامج متطور معتمد من شركة (VeriSign) البريطانية بتشفير تلك البيانات حتى وصولها إلى السيرفر (الخادم)، وبحيث لا يمكن اختراقها أو اعتراضها.

ولأن البنك يدرك قيمة الوقت ويحرص على توفير الخدمات المصرفية الحديثة التي تلبي رغبات وتطلعات عملائه فقد وضع خدمة الصراف الآلي لعملائه الراغبين في الحصول على خدمات مصرفية آلية فورية متنوعة، فالخدمة متاحة على مدار الساعة بما في ذلك أيام الجمع والعطل والأعياد وفي مواقع متميزة حيث بلغ عددها في العام 2013م (147) صراف آلي، توفر الكثير من الوقت والجهد ومن أهم خدماتها السحب النقدي، الاستفسار عن الرصيد، الحصول على كشف فوري للحساب، سحب مرتبات شهرية بمجرد تحويلها للبنك، الحصول على نقد فوري لحملة بطاقة الفيزا والماستر كارد الصادرة عن البنك أو أي بنك آخر محلي أو دولي.

وفي مجال تطبيق الحماية المحلية والعالمية تم استحداث نظم ومعدات شبكية متطورة لمضاعفة أمان الشبكة المعلوماتية للبنك، بالإضافة إلى استخدام البنك أفضل الأنظمة في العالم فيما يتعلق بالمدفوعات الالكترونية من نظام البطاقات (Power Card)، والطابعات لطباعة البطاقات بمختلف أنواعها محلية ودولية وبأحدث الطرق التكنولوجية في العالم (EMV).

3-2-4-2: البنك (خ): هو شركة مساهمة يمنية مقفلة أنشئ بموجب قرار البنك المركزي اليمني ومنح الترخيص التجاري بمزاولة العمل من وزارة التموين والتجارة وهو أول بنك تجاري يمني أنشئ بعد إعلان الوحدة اليمنية المباركة، ويقدم جميع الخدمات المصرفية لعملائه من الأفراد والشركات بمستوى عالٍ من الكفاءة والأداء محتلاً بذلك موقعاً متميزاً في السوق المصرفي اليمني ومصدراً أساسياً لعملية البناء الاقتصادي في اليمن حيث ساهم البنك وبشكل مباشر في عملية التنمية الاقتصادية باعتباره من أكبر البنوك تمويلياً لمشاريع التنمية الاقتصادية.

حيث باشر انطلاقة مصرفية متميزة وحديثة تمثلت هذه الانطلاقة في تنفيذ عملية شاملة ممكنة لأنظمتها وعملياته المصرفية وتطبيق خدمات الربط الشبكي الآلي والفوري بين الفروع، الأمر الذي أحدث نقلة نوعية في مستوى وكفاءة الأداء في تقديم الخدمات المصرفية.

ومما تجدر الإشارة إليه فإنه قد تم تنويجه للسنة السادسة على التوالي كأفضل بنك في اليمن لعام 2012م من قبل مجلة المصرفي (*The Banker*) البريطانية المتخصصة في تقييم الأداء المصرفي العالمي وذلك تقديراً لأدائه المتميز وقدرته على تطوير إستراتيجيته في العمل المشهود له خلال السنوات الماضية.

3-4-2-3: البنك (م): هو البنك الأول في اليمن ويمتلك تاريخاً جيداً ويتميز بالخصوصية، تأسس في صنعاء كشركة مساهمة عامة، برأس مال محلي قدره (10) مليون ريال يمني بملكية مختلطة بين حكومة الجمهورية اليمنية بنسبة 51 % والقطاع الخاص بنسبة 49 % من رأس المال المدفوع لكل منهما.

وهو البنك التجاري الأول في اليمن ويعتبر رائد التنمية الأول وبدون منافس وعميد السلك المصرفي اليمني وكل ما نراه اليوم من إمبراطوريات تجاربه خاصة وعامه ومؤسسات وشركات كان أساسها، فكان ولا يزال حتى اليوم البنك المصرفي الشامل لكافة المجالات والقطاعات وهو ما نستنبطه من خلال النظر لشعاره والذي يدل دلالة واضحة لما قام به البنك من أعمال فقد قام بإعمال البنك التجاري والبنك الصناعي والزراعي والإسكان و كان سفير اليمن الأول و نافذته للعالم التجاري الخارجي من خلال شبكة واسعة من المراسلين وفي أكثر من دولة في العالم.

قام البنك ومنذ إنشائه في مطلع الستينات بكافة المهام والمسؤوليات المتعلقة بالبنك المركزي، حتى تم إنشاء وتأسيس البنك المركزي اليمني.

يمارس البنك أعماله المصرفية من المركز الرئيسي للبنك (الإدارة العامة) في مدينة صنعاء ومن خلال 44 فرعاً منتشرة في أنحاء الجمهورية اليمنية حتى نهاية 2013م، وتتبع هذه الفروع إشرافياً (6) مناطق هي (صنعاء، عدن، تعز، الحديدة، إب، ذمار)، ويحتفظ بشبكة واسعة من المراسلين في الخارج، ويوفر البنك خدمات مصرفية ومالية مميزة، وساهم البنك في التنمية الاقتصادية مساهمة فعالة مما أدى إلى ترسيخ سمعة البنك داخلياً وخارجياً.

هذا هو باختصار والحديث عنه حديث طويل وذو شجون ولا يتسع المجال هنا لذكرها نظراً لضخامة الانجازات التي حققها خلال مرحلة عمره المصرفي الطويل التي وصلت إلي يوبيلها الذهبي لفترة الخمسون عاماً ولا يزال يحقق النجاحات عاماً بعد عام ويتمتع بميزة مالية ومركز مالي قوي جعله محل ثقة جميع اليمنيين.

3-2-5: تقييم المخاطر التي تهدد أمن نظم المعلومات المحاسبية

- تم قياس جميع متغيرات المخاطر بناءً على عدة مؤشرات لحدوث تلك المخاطر وتكرارها مرة على الأقل أسبوعياً وعلى النحو التالي:

3-2-5-1: تقييم مخاطر أمن الأفراد العاملين في نظم المعلومات المحاسبية: تم التقييم بناءً على عدة مؤشرات لحدوث مخاطر أمن الأفراد أهمها:

1. استغلال الصلاحيات من قبل بعض الأفراد لتحقيق أغراض شخصية.
2. انتحال صلاحيات الأفراد المخولين.
3. استخدام كلمات مرور مشتركة.
4. تبادل كلمات المرور فيما بين العاملين المخولين.
5. ضعف الخبرات والمهارات الذاتية للأفراد العاملين.
6. عدم وجود خبراء من خارج البنك.
7. انخفاض معدل الدوران الوظيفي.
8. الإهمال وقلة الوعي لدى الأفراد العاملين.
9. الثقة المتبادلة بين الأفراد العاملين.
10. ضعف الفصل الوظيفي.

- وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجدول الآتي:

جدول رقم (3-2-3) مصفوفة تقييم مخاطر أمن الأفراد العاملين في نظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	0	1	0	1	1	1	1	1	1	0	7
2	البنك (خ)	0	0	0	1	0	1	0	0	1	0	3
3	البنك (م)	0	0	0	1	1	1	1	1	1	0	6
	الإجمالي	0	1	0	3	2	3	2	2	3	0	16

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-2-5-2: تقييم مخاطر الأمن المادي لنظم المعلومات المحاسبية: تم التقييم بناءً على عدة مؤشرات لحدوث مخاطر الأمن المادي أهمها:

1. تلف جزئي للأجهزة بشكل متعمد.
2. تلف جزئي للأجهزة بشكل غير متعمد.
3. أعطال في المكونات البرمجية.
4. تلف كلي للأجهزة نتيجة الكوارث الطبيعية.
5. تلف كلي للأجهزة والبرامج نتيجة كوارث غير طبيعية.
6. أعطال في المكونات المادية.
7. سرقة الأجهزة والمعدات.
8. تشغيل الأجهزة في أغراض خاصة لا علاقة لها بالعمل.
9. استغلال برامج نظم المعلومات لأغراض شخصية.
10. فقد وتسرب الأفراد الخبراء العاملين بالنظام سواء بالاستقالة أو الموت.

- وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-4) مصفوفة تقييم مخاطر الأمن المادي لنظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	0	1	0	1	0	1	1	1	0	0	5
2	البنك (خ)	0	1	1	0	0	0	0	0	0	1	3
3	البنك (م)	0	1	0	0	1	0	1	0	1	0	4
	الإجمالي	0	3	1	2	0	2	1	1	1	1	12

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-5-2-3: تقييم مخاطر أمن الوصول البرمجي لقواعد بيانات نظم المعلومات المحاسبية: تم

التقييم بناءً على عدة مؤشرات لحدوث تلك المخاطر أهمها:

1. الوصول البرمجي غير المصرح به إلى برامج النظام والملفات في قاعدة البيانات بواسطة أفراد من داخل البنك بقصد تدمير البرامج أو البيانات.
2. الوصول البرمجي غير المصرح به إلى برامج النظام والملفات في قاعدة البيانات بواسطة أفراد من داخل البنك بقصد تعديل البرامج والبيانات.
3. الوصول البرمجي غير المصرح به إلى برامج النظام والملفات في قاعدة البيانات بواسطة أفراد من داخل البنك بقصد التجسس على البرامج أو البيانات.
4. الوصول البرمجي، غير المصرح به إلى برامج النظام والملفات في قاعدة البيانات بواسطة أفراد أو جهات من خارج البنك، لتعديل البرامج أو البيانات بطريقة غير مشروعة.
5. الوصول البرمجي، غير المصرح به إلى برامج النظام والملفات في قاعدة البيانات بواسطة أفراد أو جهات من خارج البنك، لتدمير البرامج والبيانات بطريقة غير مشروعة.
6. الوصول البرمجي، غير المصرح به إلى برامج النظام والملفات في قاعدة البيانات بواسطة أفراد أو جهات من خارج البنك، للكشف عن البيانات بطريقة غير مشروعة.
7. الوصول البرمجي، غير المصرح به إلى برامج النظام والملفات في قاعدة البيانات بواسطة أفراد أو جهات من خارج البنك، لنسخ وسرقة البرامج أو البيانات بطريقة غير مشروعة.
8. الوصول البرمجي، غير المصرح به إلى برامج النظام والملفات في قاعدة البيانات بواسطة أفراد أو جهات من خارج البنك، لاستخدام البرامج أو البيانات بطريقة غير مشروعة.
9. تلف بعض ملفات البيانات والبرامج ونظم التشغيل نتيجة تعرض قاعدة البيانات لنظام المعلومات المحاسبي المحوسب للإصابة بفيروسات الحاسوب.
10. تلف بعض ملفات البيانات والبرامج ونظم التشغيل نتيجة تعرض قاعدة البيانات لنظام المعلومات المحاسبي المحوسب لبرامج التجسس.

- وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-5) مصفوفة تقييم مخاطر الوصول البرمجي لقواعد نظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	0	1	1	0	1	0	0	1	1	1	6
2	البنك (خ)	0	1	1	0	0	0	0	1	1	0	4
3	البنك (م)	0	1	1	0	1	0	0	0	1	1	5
	الإجمالي	0	3	3	0	2	0	0	2	3	2	15

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

4-5-2-3: تقييم مخاطر أمن النسخ في وسائط غير متصلة بقواعد بيانات نظم المعلومات

المحاسبية: تم التقييم بناءً على عدة مؤشرات لحدوث تلك المخاطر أهمها:

1. سرقة وسائط تخزين البيانات والبرامج الاحتياطية غير المتصلة بقاعدة بيانات نظام المعلومات المحاسبي المحوسب.
2. ضياع وسائط تخزين البيانات والبرامج الاحتياطية غير المتصلة بقاعدة بيانات نظام المعلومات المحاسبي المحوسب.
3. الوصول غير المصرح به للبيانات والبرامج المخزنة في وسائط غير متصلة بنظام المعلومات المحاسبي المحوسب من أفراد داخل البنك بغرض تعديل المحتوى.
4. الوصول غير المصرح به للبيانات والبرامج المخزنة في وسائط غير متصلة بنظام المعلومات المحاسبي المحوسب من أفراد داخل البنك بغرض الكشف عنها.
5. الوصول غير المصرح به للبيانات والبرامج المخزنة في وسائط غير متصلة بنظام المعلومات المحاسبي المحوسب من جهات أو أفراد خارج البنك.

- وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-6) مصفوفة تقييم مخاطر أمن النسخ في وسائط غير متصلة بقواعد بيانات نظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	المجموع
1	البنك (ع)	0	0	2	2	0	4
2	البنك (خ)	0	0	0	2	0	2
3	البنك (م)	0	0	0	2	0	2
	الإجمالي	0	0	2	6	0	8

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-2-5-5: تقييم مخاطر أمن عمليات مدخلات نظم المعلومات المحاسبية: تم التقييم بناءً على عدة مؤشرات لحدوث تلك المخاطر أهمها:

1. الحذف المتعمد لمصادر بيانات مدخلات صحيحة بواسطة الأفراد المخولين والعاملين في نظام المعلومات المحاسبي.
2. الحذف المتعمد لمصادر بيانات مدخلات صحيحة بواسطة أفراد أو جهات خارجية غير مخولة.
3. الحذف غير المتعمد لمصادر بيانات مدخلات صحيحة بواسطة الأفراد المخولين والعاملين في نظام المعلومات المحاسبي.
4. التعديل المتعمد لمصادر بيانات مدخلات صحيحة بواسطة الأفراد العاملين في نظام المعلومات المحاسبي.
5. التعديل المتعمد لمصادر بيانات مدخلات صحيحة بواسطة أفراد أو جهات خارجية غير مخولة.
6. التعديل غير المتعمد لمصادر بيانات مدخلات صحيحة بواسطة الأفراد العاملين في نظام المعلومات المحاسبي.
7. الإدخال غير المتعمد لبيانات غير سليمة أو مكررة من قبل العاملين في نظام المعلومات المحاسبي، نتيجة السهو.
8. الإدخال غير المتعمد لبيانات غير سليمة أو مكررة من قبل العاملين في نظام المعلومات المحاسبي، نتيجة عدم المعرفة وقلة الخبرة.
9. التأخير المقصود في إدخال بعض البيانات بواسطة العاملين في نظام المعلومات المحاسبي.
10. التأخير غير المقصود في إدخال بعض البيانات بواسطة العاملين في نظام المعلومات المحاسبي.

■ وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-7) مصفوفة تقييم مخاطر أمن عمليات مدخلات نظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	0	0	1	1	0	1	1	1	1	1	7
2	البنك (خ)	0	0	1	0	0	1	0	1	0	1	4
3	البنك (م)	0	0	1	1	0	1	1	1	0	1	6
	الإجمالي	0	0	3	2	0	3	2	3	1	3	17

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-2-5-6: تقييم مخاطر أمن عمليات تشغيل نظم المعلومات المحاسبية: تم التقييم بناءً على عدة مؤشرات لحدوث تلك المخاطر أهمها:

1. إهدار وسرقة وقت تشغيل بعض أجهزة الحاسوب المستخدمة في نظام المعلومات المحاسبي من خلال استغلالها في الأغراض الشخصية.
 2. تعديل البيانات بطريقة مقصودة نتيجة حدوث احتيال وغش من قبل مستخدم نظام المعلومات المحاسبي أثناء عمليات التشغيل.
 3. حذف البيانات بطريقة مقصودة نتيجة حدوث احتيال وغش من قبل مستخدم نظام المعلومات المحاسبي أثناء عمليات التشغيل.
 4. تعديل البيانات بطريقة غير مقصودة نتيجة حدوث أخطاء من قبل مستخدم نظام المعلومات المحاسبي أثناء عمليات التشغيل بسبب الإهمال.
 5. تعديل البيانات بطريقة غير مقصودة نتيجة حدوث أخطاء من قبل مستخدم نظام المعلومات المحاسبي أثناء عمليات التشغيل بسبب عدم الإدراك ضعف الخبرة.
 6. حذف البيانات بطريقة غير مقصودة نتيجة حدوث أخطاء من قبل مستخدم نظام المعلومات المحاسبي أثناء عمليات التشغيل بسبب الإهمال.
 7. حذف البيانات بطريقة غير مقصودة نتيجة حدوث أخطاء من قبل مستخدم نظام المعلومات المحاسبي أثناء عمليات التشغيل بسبب عدم الإدراك وضعف الخبرة.
 8. حدوث عمليات تشغيلية غير مكتملة لبيانات محاسبية تم إدخالها لأسباب فنية داخلية.
 9. حدوث عمليات تشغيلية غير مكتملة لبيانات محاسبية تم إدخالها لأسباب فنية خارجية.
 10. حدوث عمليات تشغيلية غير مكتملة لبيانات محاسبية تم إدخالها لأسباب بشرية.
- وبناءً على ذلك تم تفرغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-8) مصفوفة تقييم مخاطر أمن عمليات تشغيل نظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	1	1	0	1	1	1	0	1	0	0	6
2	البنك (خ)	1	0	0	1	0	0	1	0	0	0	3
3	البنك (م)	1	0	0	1	1	1	0	1	0	0	5
	الإجمالي	3	1	0	3	2	2	1	2	0	0	14

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الالكترونية للبنوك موضع دراسة الحالة.

3-2-5-7: تقييم مخاطر أمن مخرجات نظم المعلومات المحاسبية: تم التقييم بناءً على عدة مؤشرات لحدوث تلك المخاطر أهمها:

1. حذف وإخفاء بنود معينة من مخرجات نظام المعلومات المحاسبي لإنتاج مخرجات مظلة غير سليمة.
2. الكشف غير المخول به للمعلومات المحاسبية أثناء عرضها على الشاشات.
3. الكشف غير المخول به للمعلومات المحاسبية أثناء طباعتها على الورق.
4. الكشف غير المخول به للمعلومات المحاسبية أثناء التخلص منها بعد استخدامها.
5. توجيه وتوزيع وتسليم بعض البيانات والمعلومات المحاسبية لأشخاص غير مخولين باستلام نسخة منها.
6. توجيه وتوزيع وتسليم بعض البيانات والمعلومات لأشخاص لا تتوفر فيهم الأمانة.
7. سوء استخدام المعلومات من قبل القائمين على النظام واستغلالها في أغراض شخصية.
8. سرقة المعلومات المحاسبية من قبل القائمين على النظام واستغلالها في أغراض شخصية، ومنع الوصول إليها من قبل المخولين على الاطلاع عليها.
9. سرقة المعلومات المحاسبية من قبل أفراد من داخل البنك غير مخولين بالاطلاع عليها.
10. سرقة المعلومات المحاسبية من قبل أفراد أو جهات خارج البنك.

■ وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-9) مصفوفة تقييم مخاطر أمن مخرجات نظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	0	1	0	1	1	1	1	0	1	0	5
2	البنك (خ)	0	0	1	0	1	0	1	0	1	0	4
3	البنك (م)	0	1	0	0	1	0	1	0	1	0	4
	الإجمالي	0	2	1	1	3	1	2	0	3	0	13

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الالكترونية للبنوك موضع دراسة الحالة.

3-2-5-8: تقييم مخاطر أمن تبادل البيانات عبر شبكات نظم المعلومات المحاسبية: تم التقييم بناءً على عدة مؤشرات لحدوث تلك المخاطر أهمها:

1. انقطاع وتوقف تدفق البيانات والمعلومات المحولة إلكترونياً عبر شبكات الحاسوب من المركز الرئيسي للبنك إلى الفروع.
2. انقطاع وتوقف تدفق البيانات والمعلومات المحولة إلكترونياً عبر شبكات الحاسوب من الفروع إلى المركز الرئيسي.
3. اعتراض وصول البيانات المرسله عبر الشبكات من أجهزة الخوادم لأجهزة المستخدمين، وتعرضها للكشف.

4. اعتراض وصول البيانات المرسله عبر الشبكات من أجهزة الخوادم لأجهزة المستخدمين، وتعرضها للتعديل.
 5. اعتراض وصول البيانات المرسله عبر الشبكات من أجهزة الخوادم لأجهزة المستخدمين، وتعرضها للسرقة.
 6. اختراق مواقع الويب الخاص ببيانات البنك.
 7. التجسس على خطوط الاتصالات الخاصة بنقل البيانات.
 8. إنكار بعض الأطراف المتعاملة مع البنك للبيانات والمعلومات المحاسبية المتبادلة إلكترونياً.
 9. حدوث أخطاء غير مقصودة أثناء نقل البيانات كإرسال بيانات أو معلومات عن طريق الخطأ إلى موقع آخر.
 10. حدوث أخطاء مقصودة أثناء نقل البيانات من قبل المخولين كإرسال بيانات أو معلومات مظللة.
- وبناءً على ذلك تم تفرغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (10-2-3) مصفوفة تقييم مخاطر أمن تبادل البيانات عبر شبكات نظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	0	1	0	0	0	1	0	0	1	0	3
2	البنك (خ)	0	0	1	0	0	1	1	1	1	0	5
3	البنك (م)	0	1	0	0	0	0	1	0	1	0	3
	الإجمالي	0	2	1	0	0	2	2	1	3	0	11

الجدول من إعداد الباحث بناء على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-2-5-9: قياس مخاطر أمن تعديل وتطوير نظم المعلومات المحاسبية: تم التقييم بناءً على عدة مؤشرات لحدوث تلك المخاطر أهمها:

1. حدوث أخطاء غير مقصودة في عدم استكمال التعديلات المطلوبة أثناء عمليات التعديل.
2. حدوث أخطاء غير مقصودة في عدم استكمال التحديثات المطلوبة أثناء عمليات التطوير.
3. يتم إجراء تغييرات للنظام وبرامجه بطريقة غير مسموح بها، من قبل أشخاص مخولين بذلك، للقيام بعمليات تلاعب واحتيال لاحقة.
4. يتم إجراء تغييرات للنظام وبرامجه بطريقة غير مسموح بها، من قبل أشخاص غير مخولين بذلك من داخل البنك، للقيام بعمليات تلاعب واحتيال لاحقة.
5. يتم إجراء تغييرات للنظام وبرامجه بطريقة غير مسموح بها، من قبل أشخاص أو جهات خارجية غير مخولة بذلك، للقيام بعمليات تلاعب واحتيال لاحقة.

- وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-11) مصفوفة تقييم مخاطر أمن تعديل وتطوير نظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	المجموع
1	البنك (ع)	2	2	2	0	0	6
2	البنك (خ)	2	0	0	0	0	2
3	البنك (م)	2	2	0	0	0	4
	الإجمالي	6	4	2	0	0	12

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الالكترونية للبنوك موضع دراسة الحالة.

- وبالنظر إلى المتغيرات الرئيسية لمخاطر أمن نظم المعلومات المحاسبية المحوسبة، تم تفريغ إجابات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-12) مصفوفة تقييم المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة

م	المتغيرات الرئيسية للمخاطر	البنك (ع)	البنك (خ)	البنك (م)	مجموع نقاط الخطر	نسبة شدة الخطر
1	مخاطر أمن الأفراد العاملين في النظم.	7	3	6	16	53%
2	مخاطر الأمن المادي لنظم المعلومات.	5	3	4	12	40%
3	مخاطر أمن الوصول البرمجي لقاعدة بيانات نظم المعلومات المحاسبية.	6	4	5	15	50%
4	مخاطر أمن النسخ في وسائط غير متصلة بقاعدة البيانات.	4	2	2	8	27%
5	مخاطر تهدد أمن عمليات المدخلات.	7	4	6	17	57%
6	مخاطر أمن عمليات تشغيل نظم المعلومات.	6	3	5	14	47%
7	مخاطر أمن مخرجات نظم المعلومات.	5	4	4	13	43%
8	مخاطر أمن تبادل البيانات عبر شبكات نظم المعلومات.	3	5	3	11	37%
9	مخاطر أمن تعديل وتطوير نظم المعلومات.	6	2	4	12	40%
	مجموع نقاط المخاطر	49	30	39	118	44%
	نسبة شدة المخاطر	54%	33%	43%	44%	

الجدول من إعداد الباحث إستناداً لنتائج الجداول السابقة المتعلقة بمصفوفات تقييم المخاطر المختلفة.

ومن الجدول السابق يتضح ما يلي:

- أن نسب حدوث كل خطر من مخاطر أمن نظم المعلومات المحاسبية المحوسبة على مستوى المتغيرات الرئيسية كانت معظمها أقل من (50%) ويمكن القول بصفة إجمالية بأن إجابات البنوك المشمولة بالدراسة حول مدى حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك

التي يعملون بها، كانت غالبيتها منخفضة بشكل عام وبنسبة (44%)، ولكن لا يعني ذلك عدم وجود مخاطر تهدد أمن نظم المعلومات المحاسبية، فعلى مستوى بعض المخاطر كانت هناك نسبة متوسطة على حدوثها وهنا يجب على هذه البنوك من مواجهة تلك المخاطر بشتى الإجراءات والوسائل.

■ يلاحظ أن البنك (ع) والذي يمثل بنوك القطاع العام يعاني من جود المخاطر أكثر من البنكين الآخرين حيث بلغت نسبة المخاطر فيه (54%) وكان البنك (خ) والذي يمثل بنوك القطاع الخاص أقلها تأثراً بتلك المخاطر وبنسبة (33%) فقط مما يعني وجود فوارق بين القطاعات المختلفة في حدوث تلك المخاطر.

3-2-6: تقييم التهديدات الداخلية التي تسبب مخاطر أمن نظم المعلومات المحاسبية المحوسبة:

■ تم قياس جميع متغيرات التهديدات الداخلية بناءً على عدة مؤشرات لحدوث تلك التهديدات وباستخدام ملاحظات الباحث والسجلات الالكترونية والمقابلات التي أجراها مع مدراء تكنولوجيا المعلومات للبنوك موضع دراسة الحالة العملية وعلى النحو التالي:

3-2-6-1: تقييم التهديدات الداخلية المسببة للمخاطر نتيجة فلسفة الإدارة العليا للبنك: تم التقييم

بناءً على عدة مؤشرات لحدوث تلك التهديدات أهمها:

1. عدم إدراك الإدارة العليا للبنك لأهمية أمن نظم المعلومات المحاسبية.
2. لا يوجد دعم مادي من قبل إدارة المنشأة للجهة المعنية بتطبيق السياسات الأمنية.
3. لا يوجد دعم معنوي من قبل إدارة المنشأة للجهة المعنية بتطبيق السياسات الأمنية.
4. عدم وجود سياسات ومواصفات قياسية واضحة ومعتمدة ومعلنة وموثقة لإدارة مخاطر أمن نظم المعلومات المحاسبية في البنك.
5. عدم وجود خطط إدارية واضحة ومعتمدة ومعلنة وموثقة لإدارة مخاطر أمن نظم المعلومات المحاسبية في البنك.
6. عدم قيام الإدارة بإصدار تشريعات فعالة للحد من مخاطر أمن نظم المعلومات المحاسبية.
7. لا يتم معاقبة الموظفين المخلين بالقرارات والتشريعات الخاصة بأمن نظم المعلومات.
8. شعور إدارة البنك بعدم جدوى تقييم مخاطر أمن نظم المعلومات المحاسبية، لاعتقادها بأن تكلفة تطبيق إجراءات الحماية أكبر من عوائدها المتوقعة.
9. لا تقوم الإدارة بمشاركة الأقسام المختصة بأمن نظم المعلومات للبحث عن أفضل السبل لمواجهة تلك المخاطر.
10. امتناع الإدارة العليا للبنك عن الإفصاح عن تلك المخاطر والخسائر المترتبة عنها، خوفاً من اهتزاز الثقة بسمعة البنك وبمركزه المالي.

■ وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-13) مصفوفة تقييم التهديدات الداخلية المسببة للمخاطر
نتيجة فلسفة الإدارة العليا للبنك

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	1	1	0	1	0	1	1	1	1	0	7
2	البنك (خ)	0	1	0	0	0	0	1	1	1	1	5
3	البنك (م)	1	1	0	1	0	1	1	1	1	0	7
	الإجمالي	2	3	0	2	0	2	3	3	3	1	19

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-2-6-2: قياس التهديدات الداخلية المسببة للمخاطر نتيجة التهديدات التنظيمية للبنك: تم التقييم بناءً

على عدة مؤشرات لحدوث تلك التهديدات أهمها:

1. عدم وجود إدارة أو قسم أو لجنة مستقلة، لها صلاحيات كافية لتقييم ومتابعة مخاطر أمن نظم المعلومات المحاسبية، بهدف حماية تلك النظم.
2. غياب التوصيف الدقيق للوظائف والذي يحدد المسؤوليات والصلاحيات لكل موظف داخل الهيكل التنظيمي للبنك.
3. الفصل غير الواضح بين المهام المتعلقة بنظم المعلومات المحاسبية في البنك.
4. إشراك بعض العاملين باستخدام نفس كلمات السر أو تبادلها بينهم، مما قد يهدر مبدأ تقسيم العمل.
5. النقص الكبير في الموظفين المختصين بأمن نظم المعلومات والذي تتوفر فيهم الخبرة اللازمة.
6. النقص الكبير في الموظفين المختصين بأمن نظم المعلومات والذي يتوفر فيهم التدريب الكافي والخلفية العلمية المطلوبة لذلك.
7. النقص الكبير في الموظفين المختصين بأمن نظم المعلومات والذي تتوفر فيهم المهارات المتعددة المطلوبة لذلك.
8. صعوبة وعدم كفاية تدريب وتأهيل وتوعية الموظفين في مجال تقنيات أمن نظم المعلومات.
9. عدم توافق عمليات التأهيل والتدريب مع التطور المستمر لبرامج أمن نظم المعلومات.
10. الاهتمام غير الكافي بفحص التاريخ الوظيفي والمهني للموظفين الجدد مما قد يؤثر على قاعدة وضع الرجل المناسب في المكان المناسب.

■ وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-14) مصفوفة تقييم التهديدات الداخلية المسببة للمخاطر
نتيجة التهديدات التنظيمية للبنك

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	1	0	0	1	1	0	1	1	1	1	7
2	البنك (خ)	1	0	0	0	0	1	1	1	1	0	5
3	البنك (م)	1	0	1	1	1	1	1	0	0	0	6
	الإجمالي	3	0	1	2	2	2	3	2	2	1	18

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-2-6-3: قياس التهديدات الداخلية المسببة للمخاطر نتيجة إمكانات البنك التكنولوجية: تم التقييم بناءً على عدة مؤشرات لحدوث تلك التهديدات أهمها:

1. تقادم الأجهزة المستخدمة في حفظ وتشغيل البيانات وإنتاج المعلومات وتدقيقها وتخزينها واسترجاعها بسهولة ودقة وسرعة.
2. ضعف فاعلية الأجهزة المستخدمة في حفظ وتشغيل البيانات وإنتاج المعلومات وتدقيقها وتخزينها واسترجاعها بسهولة ودقة وسرعة.
3. تقادم البرامج المستخدمة في حفظ وتشغيل البيانات وإنتاج المعلومات وتدقيقها وتخزينها واسترجاعها بسهولة ودقة وسرعة.
4. ضعف فاعلية البرامج المستخدمة في حفظ وتشغيل البيانات وإنتاج المعلومات وتدقيقها وتخزينها واسترجاعها بسهولة ودقة وسرعة.
5. الصعوبة في إيجاد التوليفة المثلى للأجهزة والبرامج وأجهزة الدعم المساندة لها بعناية، لتحديث وتطوير الأنظمة، بما يؤمن تحقيق أهداف النظام وتأمين عناصر الرقابة.
6. وجود أخطاء في تصميم البرامج والتطبيقات المحاسبية المستخدمة تؤدي إلى إنتاج معلومات خاطئة أو غير دقيقة لفترات طويلة.
7. عدم كفاية عمليات الصيانة الدورية لأجهزة الحاسوب والبرمجيات المستخدمة في تشغيل وحماية نظم المعلومات المحاسبية المحوسبة.
8. اعتماد البنك في الحصول على الأجهزة والبرامج، والدعم الفني لها على مزودين قليلي الخبرة.
9. لا يتم التقييم المستمر لوضع مزودي البنك بالأجهزة والبرامج والدعم الفني في السوق.
10. عدم التوافق ما بين الأنظمة والتطبيقات الموجودة لدى البنك مع الأنظمة والتطبيقات الخاصة بالمنشآت التي قد يتم ربط أنظمة البنك معها.

■ وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتية:

جدول رقم (3-2-15) مصفوفة تقييم التهديدات الداخلية المسببة للمخاطر
نتيجة إمكانات البنك التكنولوجية

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	1	0	0	1	1	0	1	1	1	0	6
2	البنك (خ)	0	0	0	0	1	0	1	0	0	1	3
3	البنك (م)	1	0	0	1	1	0	1	1	0	0	5
	الإجمالي	2	0	0	2	3	0	3	2	1	1	14

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-2-6-4: تقييم التهديدات الداخلية المسببة للمخاطر نتيجة الأفراد العاملين في النظام: تم التقييم بناءً على عدة مؤشرات لحدوث تلك التهديدات أهمها:

1. ضعف إدراك بعض العاملين بالنظام لمهامهم الموكولة لهم (كنسيان كلمة المرور للدخول للنظام، أو السماح لزملاء باستخدامها)، مما يترتب عليها أخطاء فادحة عند التشغيل.
2. سوء استخدام الصلاحيات الواسعة المخولة لبعض الأفراد المسؤولين عن تشغيل النظام ممن لديهم معرفة واسعة بتفاصيل النظام.
3. عدم التزام الأفراد العاملين بالإجراءات المحددة لحماية النظام.
4. إهمال بعض العاملين بنظام المعلومات المحاسبي وعدم بذلهم العناية المهنية الكافية لأداء العمل.
5. نقص التأهيل العلمي والعملية والوعي الرقابي وعدم كفاية التدريب.
6. ارتفاع مستوى خبرة بعض العاملين في مجال التشغيل الإلكتروني، وزيادة معرفتهم أكثر من غيرهم بنقاط الضعف في الضوابط الرقابية المطبقة، مما ينتج عن ذلك مخاطر للنظام.
7. التصرفات الانتقامية للأفراد الغاضبين أثناء عملهم بسبب معاقبتهم وحرمانهم من بعض الحقوق الوظيفية.
8. قيام بعض الأفراد بالكشف عن بعض المعلومات السرية بعد إنهاء خدماتهم بسبب فصلهم من العمل بشكل تعسفي.
9. انخفاض معدل دوران موظفي أنظمة المعلومات لدى البنك.
10. احتفاظ موظفي نظم المعلومات بأسرار الأنظمة ومفاتيح الحل وعدم تعاونهم مع زملائهم في تبادل المعرفة والخبرة.

■ وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-16) مصفوفة تقييم التهديدات الداخلية المسببة للمخاطر نتيجة الأفراد العاملين

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	1	0	1	0	1	1	1	1	1	1	8
2	البنك (خ)	1	0	1	0	1	1	1	0	1	0	6
3	البنك (م)	1	0	1	0	1	1	1	0	1	1	7
	الإجمالي	3	0	3	0	3	3	3	3	3	2	21

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

- 3-2-6-5: تقييم التهديدات الداخلية المسببة للمخاطر نتيجة ضعف نظم الرقابة الداخلية للبنك: تم التقييم بناءً على عدة مؤشرات لحدوث تلك التهديدات أهمها:
1. ضعف كفاية الأدوات والضوابط والإجراءات الرقابية المطبقة في البنك لحماية أمن نظام المعلومات المحاسبي.
 2. عدم فعالية الأدوات والضوابط والإجراءات الرقابية المطبقة في البنك لحماية أمن نظام المعلومات المحاسبي.
 3. عزز التدابير الأمنية لنظم المعلومات.
 4. ضعف كفاءة نظم الرقابة الداخلية للبنك.
 5. عدم فاعلية نظم الرقابة الداخلية للبنك بشكل عام.
 6. عدم إصدار تقارير رقابية دورية حول الأنظمة الآلية، ليتم متابعتها وتقييمها لمواكبة التطورات التي تجري لمواجهة المخاطر.
 7. عدم كفاءة وفعالية إجراءات إدارة المخاطر.
 8. عدم القيام بالتقييم الذاتي لمخاطر أمن نظم المعلومات بحيث يقوم كل موظف بتحديد المخاطر التي يواجهها وتقييم إجراءات مواجهتها.
 9. غياب المسار المرئي للمراجعة فعدم رؤية عمليات إدخال البيانات وتشغيلها سهل من تغيير أو إضافة أو حذف أي بيانات دون ترك أثر يدل على ذلك، وصعوبة اكتشاف ذلك.
 10. لا يوجد تطور مستمر في الممارسات والضوابط الرقابية يواكب المخاطر الأمنية المتطورة.
- وبناءً على ذلك تم تفرغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-17) مصفوفة تقييم التهديدات الداخلية المسببة للمخاطر
نتيجة ضعف نظم الرقابة الداخلية للبنك

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	0	0	1	1	0	1	0	1	1	1	6
2	البنك (خ)	0	0	0	0	0	1	0	1	1	0	4
3	البنك (م)	0	1	1	1	0	1	1	1	1	0	7
	الإجمالي	0	1	2	2	0	3	1	3	3	1	17

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

- 3-2-6-6: تقييم التهديدات الداخلية المسببة للمخاطر نتيجة الكوارث الداخلية للبنك: تم التقييم بناءً على عدة مؤشرات لحدوث تلك التهديدات أهمها:

1. حدوث تخريب داخلي في البنك تسبب في تلف جزئي لموارد النظام.
2. حدوث تخريب داخلي في البنك تسبب في تدمير كلي لموارد النظام.
3. حدوث حرائق داخلية في البنك تسببت في تلف جزئي لموارد النظام.
4. حدوث حرائق داخلية في البنك تسببت في تدمير كلي لموارد النظام.

5. حدوث انقطاع للتيار الكهربائي للبنك، تسبب في تلف جزئي لموارد النظام.
 6. حدوث انقطاع للتيار الكهربائي للبنك، تسبب في تدمير كلي لموارد النظام.
 7. حدوث تسريب للمياه الداخلية في البنك، تسبب في تلف جزئي لموارد النظام.
 8. حدوث تسريب للمياه الداخلية في البنك، تسبب في تدمير كلي لموارد النظام.
 9. حدوث عملية تفجير في البنك تسبب في تلف جزئي لموارد النظام.
 10. حدوث عملية تفجير في البنك تسبب في تدمير كلي لموارد النظام.
- وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-18) مصفوفة تقييم التهديدات الداخلية المسببة للمخاطر
نتيجة الكوارث الداخلية للبنك

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	1	0	1	0	1	0	1	1	1	1	7
2	البنك (خ)	1	0	1	0	1	0	1	0	0	0	4
3	البنك (م)	1	0	0	0	1	0	1	0	1	1	5
	الإجمالي	3	0	2	0	3	0	3	1	2	2	16

■ الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

- بالنظر إلى المتغيرات الرئيسية للتهديدات الداخلية المسببة لمخاطر أمن نظم المعلومات المحاسبية المحوسبة، تم تفريغ إجابات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-19) مصفوفة تقييم التهديدات الداخلية
المسببة لحدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة

م	التهديدات الداخلية لأمن نظم المعلومات المحاسبية	البنك (ع)	البنك (خ)	البنك (م)	مجموع نقاط التهديد	نسبة شدة التهديد
1	فلسفة الإدارة العليا للبنك.	7	5	7	19	63%
2	التهديدات التنظيمية.	7	5	6	18	60%
3	مهددات تتعلق بإمكانات البنك التكنولوجية.	6	3	5	14	47%
4	الأفراد العاملين في نظم المعلومات المحاسبية.	8	6	7	21	70%
5	ضعف الرقابة الداخلية وإدارة المخاطر بالبنك	6	4	7	17	57%
6	حدوث كوارث داخلية في البنك (غير طبيعية).	7	4	5	16	53%
	إجمالي نقاط التهديدات الداخلية	41	27	37	105	58%
	نسبة شدة التهديدات الداخلية	68%	45%	62%	58%	

■ الجدول من إعداد الباحث استناداً لنتائج الجداول السابقة المتعلقة بمصفوفات تقييم التهديدات الداخلية.

ومن الجدول السابق رقم يتضح ما يلي:

- أن نسب حدوث كل تهديد من التهديدات الداخلية المسببة لمخاطر أمن نظم المعلومات المحاسبية المحوسبة على مستوى المتغيرات الرئيسية كانت معظمها أكبر من (50%) ويمكن القول بصفة إجمالية بأن إجابات البنوك المشمولة بالدراسة حول مدى حدوث التهديدات الداخلية المسببة لمخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التي يعملون بها، كانت غالبيتها متوسطة بشكل عام وبنسبة (58%)، مما يعني وجود اتفاق على أن تلك مهددات داخلية تسبب وقوع المخاطر لدى تلك البنوك.
- يلاحظ أن البنك (ع) والذي يمثل بنوك القطاع العام يعاني من جود تلك التهديدات أكثر من البنكين الآخرين حيث بلغت نسبة شدة التهديدات الداخلية فيه (68%) وكان البنك (خ) والذي يمثل بنوك القطاع الخاص أقلها تأثراً بتلك المخاطر وبنسبة (45%) فقط مما يعني وجود فوارق بين القطاعات المختلفة في حدوث تلك التهديدات.

3-2-7: تقييم التهديدات الخارجية التي تسبب مخاطر أمن نظم المعلومات المحاسبية المحوسبة:

- تم تقييم جميع متغيرات التهديدات الخارجية بناء على عدة مؤشرات لحدوث تلك التهديدات وباستخدام ملاحظات الباحث والمقابلات التي أجراها مع مدراء تكنولوجيا المعلومات للبنوك موضع دراسة الحالة العملية وعلى النحو التالي:

3-2-7-1: تقييم التهديدات الخارجية المسببة للمخاطر نتيجة التغير التكنولوجي: تم التقييم بناءً على عدة مؤشرات لحدوث تلك التهديدات أهمها:

1. تقدم التقنية خارجياً أسرع من ممارسة الأمن داخل البنك بسبب التطورات التكنولوجية السريعة والهائلة والمتلاحقة والتي تلي وضع الإجراءات الرقابية في البنك.
2. عدم وجود استقرار نسبي لنظام المعلومات المحاسبية بسبب ارتفاع معدلات التغير في تكنولوجيا المعلومات.
3. عدم وجود استقرار نسبي لنظام المعلومات المحاسبية بسبب ضعف إمكانيات البنك المالية والبشرية لمجاراتها واستيعابها.
4. تصميم أساليب للتلاعب تبنى داخل النظام المحاسبي الإلكتروني يصعب اكتشافها، تؤدي إلى إنتاج معلومات محاسبية خاطئة.
5. عدم توفر بنية تحتية تكنولوجية قوية في الجمهورية اليمنية.

وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-20) مصفوفة تقييم التهديدات الخارجية المسببة للمخاطر نتيجة التغير التكنولوجي

م	إسم البنك	1	2	3	4	5	المجموع
1	البنك (ع)	2	2	0	2	2	8
2	البنك (خ)	2	2	0	2	0	6
3	البنك (م)	2	2	0	2	2	8
	الإجمالي	6	6	0	6	4	22

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

2-7-2-3: تقييم التهديدات الخارجية المسببة للمخاطر نتيجة الكوارث الطبيعية: تم التقييم بناءً على عدة مؤشرات لحدوث تلك التهديدات أهمها:

1. حدوث الزلازل يؤدي إلى حدوث تلف جزئي أو تدمير كلي لموارد النظام
 2. حدوث البراكين، يؤدي إلى حدوث تلف جزئي أو تدمير كلي لموارد النظام
 3. حدوث الفيضانات يؤدي إلى حدوث تلف جزئي أو تدمير كلي لموارد النظام
 4. حدوث السيول يؤدي إلى حدوث تلف جزئي أو تدمير كلي لموارد النظام
 5. حدوث الرياح العاتية والأعاصير، يؤدي إلى حدوث تلف جزئي أو تدمير كلي لموارد النظام
 6. حدوث الصواعق والحرائق الطبيعية يؤدي إلى حدوث تلف جزئي أو تدمير كلي لموارد النظام
 7. حدوث انقطاع التيار الكهربائي لأسباب طبيعية خارجية يؤدي إلى حدوث تلف جزئي أو تدمير كلي لموارد النظام.
 8. حدوث الاضطرابات السياسية المحلية والإقليمية يؤدي إلى حدوث تلف جزئي أو تدمير كلي لموارد النظام
 9. حدوث الحروب الأهلية أو الإقليمية يؤدي إلى حدوث تلف جزئي أو تدمير كلي لموارد النظام.
 10. حدوث التهديدات الإرهابية يؤدي إلى حدوث تلف جزئي أو تدمير كلي لموارد النظام.
- وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-21) مصفوفة تقييم التهديدات الخارجية المسببة للمخاطر نتيجة الكوارث الطبيعية

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	0	0	1	0	1	1	1	1	1	1	7
2	البنك (خ)	0	0	0	1	1	1	1	1	1	1	7
3	البنك (م)	0	0	1	0	1	1	1	1	1	0	6
	الإجمالي	0	0	2	1	3	3	3	3	3	2	20

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-7-2-3: تقييم التهديدات الخارجية المسببة للمخاطر نتيجة المخترقون والقراصنة: تم التقييم بناءً على عدة مؤشرات لحدوث تلك التهديدات أهمها:

1. من أسباب المخاطر التصرفات غير الآمنة من قبل أطراف خارجية كالقراصنة وبشكل دوري ومستمر.
2. حدوث جرائم وقرصنة الحاسوب من قبل المتطفلين الذين يخترقوا نظم الحماية.
3. حدوث مخاطر من قبل أفراد خارجيين رغبة في التحدي.
4. حدوث مخاطر نتيجة أعمال خارجية لنوايا إجرامية وتجسسية.
5. حدوث مخاطر باستغلال نقاط الضعف الموجودة في الصرافات الآلية وبطاقات السحب الالكترونية.

■ وبناءً على ذلك تم تفرغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-22) مصفوفة تقييم التهديدات الخارجية
المسببة للمخاطر نتيجة المخترقون والقراصنة

م	إسم البنك	1	2	3	4	5	المجموع
1	البنك (ع)	2	2	0	2	2	8
2	البنك (خ)	0	0	2	2	2	6
3	البنك (م)	2	0	0	2	2	6
	الإجمالي	4	2	2	6	6	20

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والمسجلات الالكترونية للبنوك موضع دراسة الحالة.

3-7-2-4: تقييم التهديدات الخارجية المسببة للمخاطر نتيجة فيروسات الحاسوب: تم التقييم بناءً على عدة مؤشرات لحدوث تلك التهديدات أهمها:

1. إصابة قواعد بيانات نظم المعلومات بالفيروسات التي قد تتلف البيانات أو تعطل النظام وتؤثر على عملية تشغيل البيانات.
2. الإصابة بالفيروسات أثناء عمليات التشغيل مما يؤثر على عمليات تشغيل نظم المعلومات المحاسبية.
3. وجود الديدان الالكترونية الحاسوبية، التي قد تتلف البيانات أو تعطل النظام وتؤثر على عملية تشغيل البيانات.
4. وجود برامج التجسس المختلفة، التي قد تؤدي إلى تعطل النظام وتؤثر على عملية تشغيل البيانات.
5. وجود برامج الحاسوب الخبيثة التي تعيق سير عمليات النظام بشكل عام.

▪ وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-23) مصفوفة تقييم التهديدات الخارجية المسببة للمخاطر نتيجة فيروسات الحاسوب

م	إسم البنك	1	2	3	4	5	المجموع
1	البنك (ع)	2	2	2	0	2	8
2	البنك (خ)	0	2	2	0	2	6
3	البنك (م)	2	2	0	2	2	8
	الإجمالي	4	6	4	2	6	22

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-2-7-5: تقييم التهديدات الخارجية المسببة للمخاطر نتيجة المنافسة الاقتصادية: تم التقييم بناءً على

عدة مؤشرات لحدوث تلك التهديدات أهمها:

1. رغبة منافسي البنك في الوصول إلى المعلومات السرية الهامة عن عملاء البنك.
2. رغبة منافسي البنك في الوصول إلى المعلومات السرية مثل حجم النشاط وغيرها من المعلومات الهامة.
3. تقديم الخدمات المصرفية الإلكترونية دون مراعاة الآثار التي يمكن أن تحدث عند الاستخدام الفعلي لها.
4. اكتشاف وجود أفراد يعملون لصالح البنوك المنافسة.
5. استقطاب أفراد كانوا يعملوا في البنك من قبل البنوك المنافسة.

▪ وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-24) مصفوفة تقييم التهديدات الخارجية المسببة للمخاطر نتيجة المنافسة الاقتصادية

م	إسم البنك	1	2	3	4	5	المجموع
1	البنك (ع)	2	0	2	0	0	4
2	البنك (خ)	2	2	0	0	2	6
3	البنك (م)	0	2	2	0	2	6
	الإجمالي	4	4	4	0	4	16

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-2-7-6: تقييم التهديدات الخارجية المسببة للمخاطر نتيجة ضعف الرقابة الخارجية: تم التقييم بناءً على عدة مؤشرات لحدوث تلك التهديدات أهمها:

1. عدم إيلاء المراجع الخارجي الأهمية الكافية لمخاطر أمن نظام المعلومات المحاسبي في البنك، عند قيامه بمهامه للتأكد من أن النظام قد تم تصميمه وتشغيله بطريقة ملائمة.
 2. ضعف التأهيل العلمي والعلمي للمراجع الخارجي في موضوع تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة.
 3. الدور غير الفعال للسلطات الرقابية المصرفية الرسمية كالبنك المركزي اليمني بتكثيف حملات تفتيشية مفاجئة لتقييم مخاطر أمن نظم المعلومات المحاسبية لدى البنوك، وإلزامها برفع تقارير بهذا الشأن.
 4. ضعف دور الجهاز المركزي للرقابة والمحاسبة في إلزام البنوك بالاهتمام بأمن نظم المعلومات المحاسبية لدى البنوك، وإلزامها برفع تقارير بهذا الشأن.
 5. عدم قيام الهيئة العامة لمحاربة الفساد المالي والإداري بحملات مفاجئة لتقييم مخاطر أمن نظم المعلومات المحاسبية لدى البنوك، وإلزامها برفع تقارير بهذا الشأن.
- وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-25) مصفوفة تقييم التهديدات الخارجية المسببة للمخاطر
نتيجة ضعف الرقابة الخارجية

م	إسم البنك	1	2	3	4	5	المجموع
1	البنك (ع)	2	0	2	2	2	8
2	البنك (خ)	0	0	2	2	2	6
3	البنك (م)	0	2	2	2	2	8
	الإجمالي	2	2	6	6	6	22

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الالكترونية للبنوك موضع دراسة الحالة.

3-2-7-7: تقييم التهديدات الخارجية المسببة للمخاطر نتيجة ضعف التشريعات والقوانين: تم التقييم بناءً على عدة مؤشرات لحدوث تلك التهديدات أهمها:

1. عدم تحديث القوانين المحلية النافذة التي تهدف إلى حماية أمن نظم المعلومات، سواء كانت قوانين جنائية أو مدنية أو تجارية، فهي تفتقد إلى كثير من النصوص اللازمة.
2. الغموض التشريعي بشأن اختصاص وانطباق القوانين واللوائح المعمول بها لتحديد الحقوق والالتزامات الناتجة عن العمليات المصرفية الالكترونية.
3. اختلاف التشريعات القانونية التي تنظم التعاملات المصرفية الالكترونية بين الدول مما يؤدي إلى تنازع القوانين واختصاصات المحاكم في فض النزاعات التي تنشأ عنها.

4. عدم وجود أطر تشريعية وقانونية متناسقة ومتجانسة على المستوى المحلي والإقليمي لمعاقبة مرتكبي جرائم الحاسوب والانترنت.

5. عدم وجود أطر تشريعية وقانونية متناسقة ومتجانسة على المستوى الدولي لمعاقبة مرتكبي جرائم الحاسوب والانترنت.

■ وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-26) مصفوفة تقييم التهديدات الخارجية المسببة للمخاطر
نتيجة ضعف التشريعات والقوانين

م	إسم البنك	1	2	3	4	5	المجموع
1	البنك (ع)	2	0	2	2	2	8
2	البنك (خ)	2	0	0	2	2	6
3	البنك (م)	2	0	0	2	2	6
	الإجمالي	6	0	2	6	6	20

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الالكترونية للبنوك موضع دراسة الحالة.

3-2-7-8: تقييم التهديدات الخارجية المسببة للمخاطر نتيجة ضعف الوعي الالكتروني للعملاء: تم

التقييم بناءً على عدة مؤشرات لحدوث تلك التهديدات أهمها:

1. نقص الوعي الالكتروني لدى عملاء البنك.
2. عدم التزام العملاء بإجراءات التأمين الوقائية الواجبة لبياناتهم الشخصية.
3. الدور غير الفعّال للبنك في القيام بتوعية عملائه بأمن نظم المعلومات المحاسبية.
4. عدم وجود نشرات وبرامج دورية توعوية من قبل البنك لعملائه.
5. عدم إداك العملاء لأهمية أمن نظم المعلومات المحاسبية.

■ وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-27) مصفوفة تقييم التهديدات الخارجية المسببة للمخاطر
نتيجة ضعف الوعي الالكتروني للعملاء

م	إسم البنك	1	2	3	4	5	المجموع
1	البنك (ع)	2	2	2	0	2	8
2	البنك (خ)	2	2	0	0	2	6
3	البنك (م)	2	2	2	0	2	8
	الإجمالي	6	6	4	0	6	22

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الالكترونية للبنوك موضع دراسة الحالة.

- بالنظر إلى المتغيرات الرئيسية للتهديدات الخارجية المسببة لمخاطر أمن نظم المعلومات المحاسبية المحوسبة، تم تفرغ إجابات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-28) مصفوفة تقييم التهديدات الخارجية

المسببة لحدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة

م	التهديدات الخارجية لأمن نظم المعلومات المحاسبية	البنك (ع)	البنك (خ)	البنك (م)	مجموع نقاط التهديد	نسبة شدة التهديد
1	التغيير التكنولوجي غير المتوازن.	8	6	8	22	73%
2	الكوارث الطبيعية والسياسية.	7	7	6	20	67%
3	المخترقون والقرصنة.	8	6	6	20	67%
4	دخول فيروسات وبرمجيات الحاسوب.	8	6	8	22	73%
5	المنافسة الاقتصادية بين البنوك.	4	6	6	16	53%
6	ضعف الرقابة الخارجية على نظم المعلومات المحاسبية المحوسبة.	8	6	8	22	73%
7	ضعف التشريعات والقوانين المحلية في مجال تكنولوجيا المعلومات.	8	6	6	20	67%
8	نقص الوعي الإلكتروني لدى عملاء البنك.	8	6	8	22	73%
إجمالي نقاط التهديدات الخارجية		59	49	56	164	68%
نسبة شدة التهديدات الخارجية		74%	61%	70%	68%	

الجدول من إعداد الباحث إستناداً لنتائج الجداول السابقة الخاصة بمصفوفات تقييم التهديدات الخارجية.

ومن الجدول السابق يتضح ما يلي:

- أن نسب حدوث كل تهديد من التهديدات الخارجية المسببة لمخاطر أمن نظم المعلومات المحاسبية المحوسبة على مستوى المتغيرات الرئيسية كانت معظمها أكبر من (50%) ويمكن القول بصفة إجمالية بأن إجابات البنوك المشمولة بالدراسة حول مدى حدوث التهديدات الخارجية المسببة لمخاطر أمن نظم المعلومات المحاسبية لدى البنوك التي يعملون بها، كانت غالبيتها مرتفعة بشكل عام وبنسبة (68%)، مما يعني وجود اتفاق على أن تلك مهددات خارجية تسبب وقوع المخاطر لدى تلك البنوك.
- يلاحظ أن البنك (ع) والذي يمثل بنوك القطاع العام يعاني من جود تلك التهديدات أكثر من البنكين الآخرين حيث بلغت نسبة شدة التهديدات الخارجية فيه (74%) وكان البنك (خ) والذي يمثل بنوك القطاع الخاص أقلها تأثراً بتلك المخاطر وبنسبة (61%) فقط مما يعني وجود فوارق بسيطة بين القطاعات المختلفة في حدوث تلك التهديدات.

3-2-8: مدى تأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة:

- تم قياس جميع متغيرات تأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة بناء على عدة مؤشرات لحدوث تلك التأثيرات وباستخدام ملاحظات الباحث والمقابلات التي أجراها مع مدراء تكنولوجيا المعلومات للبنوك موضع الدراسة الاستكشافية وعلى النحو التالي:

3-2-8-1: تقييم تأثير حدوث المخاطر على إتاحة نظم المعلومات المحاسبية: تم التقييم بناءً على عدة

مؤشرات لحدوث تلك التأثيرات أهمها:

1. حدوث حالات التعطيل والتوقف المفاجئ لنظام المعلومات المحاسبي لأوقات معينة.
2. إعاقة وصول المستخدمين والأطراف المستفيدة للبيانات والمعلومات.
3. حدوث خسائر مالية كبيرة بسبب حالات تعطل النظام.
4. اهتزاز المركز التنافسي للبنك مقارنة بالبنوك الأخرى بسبب عدم إتاحة نظم المعلومات المحاسبية في بعض الأوقات.
5. اهتزاز مكانة البنك أمام عملائه وتكبد البنك خسائر تجارية ومالية كبيرة نتيجة تعطل البنك بسبب المخاطر.

- وبناءً على ذلك تم تفرغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-29) مصفوفة تقييم تأثير حدوث المخاطر على إتاحة نظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	المجموع
1	البنك (ع)	2	2	2	2	0	8
2	البنك (خ)	2	0	2	0	0	4
3	البنك (م)	2	2	0	2	0	6
	الإجمالي	6	4	4	4	0	18

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الالكترونية للبنوك موضع دراسة الحالة.

3-2-8-2: تقييم تأثير حدوث المخاطر على سلامة وتكامل نظم المعلومات المحاسبية: تم التقييم بناءً

على عدة مؤشرات لحدوث تلك التأثيرات أهمها:

1. أثر حدوث المخاطر على سلامة عمليات التشغيل بالدقة المطلوبة.
2. أثر حدوث المخاطر على سلامة تجهيز المخرجات، بالدقة والشمولية المطلوبة.
3. أثر حدوث المخاطر على سلامة تجهيز المخرجات في الوقت المناسب (عدم الملائمة).
4. عند حدوث المخاطر يؤدي إلى وقوع سلسلة من الأخطاء نتيجة التحديث الفوري للملفات مما يؤثر على تكامل عملية تجهيز البيانات والمعلومات (ضعف تكامل البيانات).

5. تشغيل النظام بشكل خاطئ وباستخدام برامج غير ملائمة يؤدي إلى حصول البنك لمخرجات مظلة غير صحيحة ينتج عنها قرارات خاطئة.

■ وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-30) مصفوفة تقييم تأثير حدوث المخاطر على سلامة وتكامل نظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	المجموع
1	البنك (ع)	2	2	2	2	0	8
2	البنك (خ)	0	0	2	2	2	6
3	البنك (م)	2	2	0	2	2	8
	الإجمالي	4	4	4	6	4	22

الجدول من إعداد الباحث بناء على الملاحظات والمقابلات والسجلات الالكترونية للبنوك موضع دراسة الحالة.

3-8-2-3: تقييم تأثير حدوث المخاطر على سرية المعلومات المحاسبية: تم التقييم بناءً على عدة مؤشرات لحدوث تلك التأثيرات أهمها:

1. إن حدوث المخاطر أدت إلى سرقة معلومات هامة على درجة عالية من السرية لجهات غير مرغوب فيها.
2. إن حدوث المخاطر أدت إلى تسرب معلومات هامة على درجة عالية من السرية لجهات غير مرغوب فيها.
3. إن حدوث المخاطر يؤدي إلى إطلاع المنافسين على المعلومات المرتبطة بالبنك والتي قد يترتب عليها الإضرار بالموقف التنافسي.
4. إن حدوث المخاطر يؤدي إلى عدم قدرة نظم المعلومات في البنك على التعامل مع الأطراف المستفيدة المختلفة وفقاً لأصول السرية.
5. إن حدوث المخاطر يؤدي إلى عدم قدرة نظم المعلومات في البنك على التعامل مع الأطراف المستفيدة المختلفة وفقاً لأصول الفائدة المرجوة (ضعف الفعالية).

■ وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-31) مصفوفة تقييم تأثير حدوث المخاطر على سرية المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	المجموع
1	البنك (ع)	0	2	2	2	2	8
2	البنك (خ)	0	0	2	0	2	4
3	البنك (م)	0	2	2	0	2	6
	الإجمالي	0	4	6	2	6	18

الجدول من إعداد الباحث بناء على الملاحظات والمقابلات والسجلات الالكترونية للبنوك موضع دراسة الحالة.

3-2-8-4: تقييم تأثير حدوث المخاطر على خصوصية بيانات الأطراف المتعاملة مع البنك: تم التقييم بناءً على عدة مؤشرات لحدوث تلك التأثيرات أهمها:

1. حدوث المخاطر الأمنية لنظم المعلومات المحاسبية يضعف من قدرة البنك في حماية خصوصيات وأسرار عملائه، نتيجة الكشف عن المعلومات الشخصية لهم.
2. حدوث المخاطر يضعف من قدرة البنك في حماية خصوصيات وأسرار عملائه، نتيجة سرقة المعلومات الشخصية لهم.
3. حدوث المخاطر يهدد سمعة البنك نتيجة فقدان الثقة على المدى الطويل.
4. حدوث المخاطر يؤدي إلى فشل البنك في تحقيق متطلبات العملاء بتقديم خدمة مصرفية إلكترونية متطورة وأمنة.
5. حدوث المخاطر الأمنية لنظم المعلومات المحاسبية يؤدي إلى عدم إتاحة الفرصة للعملاء للوصول إلى المعلومات المخزنة الشخصية لتعديلها أو إلغائها.

■ وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-32) مصفوفة تقييم تأثير حدوث المخاطر على خصوصية بيانات الأطراف المتعاملة مع البنك

م	إسم البنك	1	2	3	4	5	المجموع
1	البنك (ع)	2	0	0	2	2	6
2	البنك (خ)	0	2	2	0	2	6
3	البنك (م)	0	2	2	2	2	8
	الإجمالي	2	4	4	4	6	20

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-2-8-5: تقييم تأثير حدوث المخاطر على إثبات تصرفات الأطراف المتعاملة خلال تبادل البيانات إلكترونياً: تم التقييم بناءً على عدة مؤشرات لحدوث تلك التأثيرات أهمها:

1. حدوث المخاطر يؤدي إلى تهرب بعض أطراف المعاملات الإلكترونية من الالتزامات، عن طريق إنكار وقوع أحداث وقعت.
2. حدوث المخاطر يؤدي إلى تهرب بعض أطراف المعاملات الإلكترونية من الالتزامات، عن طريق إدعاء وقوع أحداث لم تقع.
3. حدوث المخاطر تؤثر على إثبات بعض التصرفات مما قد يؤدي ذلك إلى تحمل البنك لخسائر مالية.
4. حدوث المخاطر تؤثر على إثبات بعض التصرفات مما قد يؤدي ذلك إلى فقدان الثقة في مخرجات نظم المعلومات المحاسبية.
5. رفض بعض الجهات الحكومية لحجية مخرجات نظم المعلومات المحاسبية المحوسبة استناداً لنصوص تشريعية، كالقانون التجاري وقانون البنوك.

- وبناءً على ذلك تم تقريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-33) مصفوفة تقييم تأثير حدوث المخاطر على إثبات تصرفات الأطراف المتعاملة خلال تبادل البيانات إلكترونياً

م	إسم البنك	1	2	3	4	5	المجموع
1	البنك (ع)	0	0	2	2	2	6
2	البنك (خ)	0	0	0	2	2	4
3	البنك (م)	0	0	2	2	0	4
	الإجمالي	0	0	4	6	4	14

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع الدراسة الاستكشافية.

- وبالنظر إلى المتغيرات الرئيسية لتأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة، تم تقريغ إجابات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-34) مصفوفة تقييم تأثير حدوث المخاطر

على عناصر أمن نظم المعلومات المحاسبية المحوسبة

م	تأثيرات المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة	البنك (ع)	البنك (خ)	البنك (م)	مجموع نقاط التأثير	نسبة شدة التأثير
1	تأثير المخاطر على إتاحة نظم المعلومات المحاسبية المحوسبة.	8	4	6	18	60%
2	تأثير المخاطر على سلامة وتكامل تجهيز البيانات في نظم المعلومات المحاسبية.	8	6	8	22	73%
3	تأثير المخاطر على سرية المعلومات المحاسبية.	8	4	6	18	60%
4	تأثير المخاطر على خصوصية بيانات الأطراف المتعاملة مع البنك.	6	6	8	20	67%
5	تأثير المخاطر على إثبات تصرفات الأطراف المتعاملة خلال تبادل البيانات إلكترونياً.	6	4	4	14	47%
	إجمالي نقاط تأثيرات المخاطر	36	24	32	92	61%
	نسبة شدة تأثيرات المخاطر	72%	48%	64%	61%	

- الجدول من إعداد الباحث إستناداً لنتائج الجداول السابقة.

ومن الجدول السابق يتضح ما يلي:

- أن نسب التأثيرات المختلفة للمخاطر على أمن نظم المعلومات المحاسبية المحوسبة على مستوى المتغيرات الرئيسية كانت معظمها أكبر من (50%) ويمكن القول بصفة إجمالية بأن إجابات البنوك المشمولة بالدراسة حول مدى تأثير تلك المخاطر على أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التي يعملون بها،

كانت غالبيتها متوسطة بشكل عام وبنسبة (61%)، مما يعني وجود توافق على أن تلك المخاطر تؤثر سلباً على أمن نظم المعلومات المحاسبية لدى تلك البنوك.

- ويلاحظ أن البنك (ع) والذي يمثل بنوك القطاع العام يعاني من جود تأثير المخاطر أكثر من البنكين الآخرين حيث بلغت نسبة شدة تأثير المخاطر فيه (72%) وكان البنك (خ) والذي يمثل بنوك القطاع الخاص أقلها تأثيراً بتلك المخاطر وبنسبة (48%) فقط مما يعني وجود فوارق بين القطاعات المختلفة في تأثيرات تلك المخاطر.

3-2-9: تقييم إجراءات ووسائل حماية أمن نظم المعلومات المحاسبية:

- تم قياس إجراءات الحماية لأمن نظم المعلومات المحاسبية المحوسبة وفق المعايير العالمية المتعارف عليها ومن خلال فحص بعض السجلات الالكترونية لنظم المعلومات المحاسبية والتقارير وبعد إجراء المقابلات تم الوصول للنتائج التالية:

3-2-9-1: تقييم حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية: تم التقييم بناءً على 10 معايير لإجراء تلك الحماية وهي:

1. وجود قسم خاص ومستقل بشكل كافٍ وبإمكانيات مناسبة مسؤول عن تنفيذ أمن نظم المعلومات المحاسبية وحمايتها، ووضع معايير وأسس وضوابط أمنية.
2. وجود دليل عمل مكتوب يتضمن إجراءات أداء العمل لكافة وظائف نظم المعلومات المحاسبية، محدد فيه السلطات والمسؤوليات والكفاءات الملائمة لكل وظيفة داخل النظام.
3. يوجد نظام صلاحية مبرمج بحيث يسمح النظام لكل مستخدم بإدارة نظام المعلومات المحاسبي حسب صلاحياته في التعامل مع ملفات النظام، (مثل قراءة البيانات أو نسخها أو تعديلها...الخ)، من خلال الوصول إلى أجزاء معينة وبيانات محددة.
4. كل مستخدم للنظام له كلمة سر خاصة، فلا يتشارك اثنان بكلمة سر واحدة، ويتم إيقاف صلاحيات المستخدم إذا تم إدخال كلمة المرور خطأ أكثر من العدد المسموح به للمحاولات.
5. هنالك فصل سليم بين الوظائف والمهام المختلفة والمتعارضة لمعالجة البيانات بين المبرمجين والمشغلين والمراقبين والمستخدمين بطريقة تسمح بمراقبة تنفيذ المهام.
6. يعمل البنك على تنفيذ سياسة التدوير الوظيفي للمهام الأساسية لنظم المعلومات المحاسبية، بإجراء تنقلات بين الموظفين من حين لآخر، وإلزامهم بأخذ إجازاتهم السنوية دفعة واحدة.
7. يعقد البنك برامج بواسطة مختصين في أمن نظم المعلومات لتوعية العاملين بالمخاطر التي تهدد أمن نظم المعلومات المحاسبية، وتدريبهم على إتباع الإجراءات الملائمة لمواجهتها.

8. يتم تشجيع الأفراد على اتخاذ مبادرات لحل المشكلات، ومكافأة من يقوم بعمل إيجابي نحو تجسيد نظام الحماية، ومعاقبة من يتعامل سلباً مع المخاطر ويخالفون سياسات الأمن.
9. يعين البنك شخص مسؤول عن حماية النظام يسمى ضابط أمن المعلومات، ويتم تكوين فريق طوارئ، من فنيين وإداريين فاعلين، لمواجهة أي ظرف طارئ يمس بحماية النظام.
10. يتم اختيار موظفي نظم المعلومات المحاسبية بحرص شديد وإجراء تحريات عنهم وعن ماضيهم الوظيفي، والحرص على أن يكونوا ذوي خبرة وثقة وأمانة ويعملون لمصلحة البنك، وعدم إعطاء الموظف حديث التعيين صلاحيات عالية لاستخدام النظام.

■ وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتية:

جدول رقم (3-2-35) مصفوفة تقييم حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	0	0	1	0	1	0	1	0	0	1	4
2	البنك (خ)	1	1	1	1	0	0	1	1	0	1	8
3	البنك (م)	0	0	1	0	1	1	0	1	0	1	5
	الإجمالي	1	1	3	1	3	1	2	2	0	3	17

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

2-9-2-3: تقييم حماية أمن الوصول المادي لنظم المعلومات المحاسبية: تم التقييم بناءً على 10

معايير لإجراء تلك الحماية وهي:

1. وجود خطة طوارئ معلنة وموثقة خاصة لمواجهة الكوارث تتضمن إعداد وحدة متكاملة من تجهيزات الحاسوب والشبكات، ونسخة احتياطية من قاعدة البيانات، في موقع آخر بديل غير الموقع الرئيسي لضمان استمرارية العمل، واستئناف النشاط بصورة سريعة.
2. يتعاقد البنك مع شركات تأمين متخصصة للتأمين على الأجهزة والبرمجيات وشبكات المعلومات والموظفين في نظام المعلومات المحاسبي المحوسب، ضد كافة المخاطر.
3. يتم تصميم مواقع العمل وأماكن الأجهزة والمعدات، بصورة تتلاءم مع التغيرات الطبيعية، ويتم وضع أجهزة النظام في غرف محمية وآمنة، وعدم السماح بالدخول إليها لأي كان.
4. يتم استخدام جميع الوسائل المادية التي تمنع الوصول غير المخول إلى نظم المعلومات المحاسبية وقواعدها كرجال الحراسة، والأقفال والحواجز والغرف المحصنة وغيرها.
5. يستخدم موظفي البنك بطاقات دخول إلكترونية ذكية ممغنطة عليها صورهم الشخصية، للدخول إلى أماكن عملهم عبر البوابات المقفلة المبرمجة وفق الصلاحيات المخولة لهم، ويصدر إنذار مبكر فور الدخول المادي غير المخول.

6. يقوم البنك بتثبيت كاميرات تلفزيونية على خارج مبنى دائرة النظام والممرات الداخلية فيها، وتعمل على مراقبة المستخدمين والأماكن التي توجد تجهيزات النظام، من موقع مركزي.
7. يتم استخدام منظم كهربائي، وبطاريات إضافية، وخزانات طاقة، ومولد كهربائي لتجنب ارتفاع أو انخفاض الطاقة الكهربائية أو انقطاعها، وتعطلها بشكل مفاجئ، والذي يؤدي إلى تلف أجهزة وبرامج الحاسوب أو توقفها عن العمل.
8. يتم تركيب أجهزة كشف الحريق في الأماكن المعرضة للخطر وتجهيزها بالشكل المناسب الذي يساعد على كشف الحريق بأسرع وقت ممكن وسرعة القيام بمقاومة الحريق.
9. يتم استخدام أسقف وحوائط وأرضيات تمنع تسرب المياه، مع استخدام أغطية واقية من الأتربة والماء، وتركيب أجهزة إنذار من المياه والرطوبة.
10. يتم إجراء صيانة دورية ومستمرة لأجهزة النظام ووسائل حمايته بما فيها أجهزة التكييف، لضمان استمرار عملها بفاعلية، ويتم توفير قطع ومعدات بديلة للأجهزة العاملة بشكل سريع فور تعطلها، بما يضمن سلامة الحواسيب وحمايتها.

■ وبناءً على ذلك تم تفرغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-36) مصفوفة تقييم حماية أمن الوصول المادي لنظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	0	0	1	1	0	0	1	1	1	0	5
2	البنك (خ)	0	0	1	1	0	1	1	1	1	1	7
3	البنك (م)	0	1	1	1	0	1	1	1	0	0	6
	الإجمالي	0	1	3	3	0	2	3	3	2	1	18

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-9-2-3: تقييم حماية أمن الوصول البرمجي لنظم المعلومات المحاسبية: تم التقييم بناءً على 10

معايير لإجراء تلك الحماية وهي:

1. يتم التحقق من هوية الشخص أو المعدات التي تحاول الدخول للنظام من خلال خليط من (كلمات مرور/ كروت ذكية/ معرفات بيولوجية/ أجهزة أخرى).
2. يتم استخدام مستويات متتالية من الرقابة على دخول قاعدة البيانات بكلمات مرور متعددة ومختلفة للدخول إلى (الشبكة أو الحاسوب أو سيرفر "خادم" البيانات أو قاعدة البيانات)، ويتم التنبيه للموظفين بعدم إفشاء كلمات المرور السرية، وتكون من الصعب تخمينها.
3. يوجد سجل خاص لجميع الصلاحيات الممنوحة للموظفين المخولين بالدخول للنظام، ويتم برمجة مصفوفة الرقابة على الوصول آلياً، فيتم تحديد كلمة سر خاصة لكل موظف، والملفات أو البرامج التي يصرح له بالوصول إليها.

4. يتم تغيير كلمات السر بشكل دوري ومستمر وخاصة بعد نقل الموظفين ويتم إلغاء كلمة السر الخاصة بالموظف الذي استقال أو أقيل من العمل بشكل فوري.
 5. يتم استخدام برامج الجدران النارية العازلة لمنع الوصول غير المصرح به إلى النظام، ومنع المستخدم من استخدام برامج أو ملفات لا يملك الصلاحية للدخول إليها.
 6. يتم تحديث وتعديل البرامج النارية باستمرار.
 7. يوثق النظام كافة محاولات الوصول غير المصرح بها، ويصدر تقرير حولها يتضمن وقت المحاولة والموقع الذي تمت من خلاله، ويتم معالجة ذلك بإغلاق الفجوات المكتشفة.
 8. يتم إجراء اختبار اختراق النظام بصورة دورية من قبل المراجعين الداخليين أو الخارجيين، أو بواسطة خبرات متخصصة لمعرفة نقاط الضعف في نظم المعلومات المحاسبية.
 9. يحرص البنك على تحميل واستخدام برامج متطورة وأصلية وفعالة مضادة لفيروسات الحاسوب وبرمجياته الخبيثة، ويتم تحديثها بشكل دوري ومستمر.
 10. يتم استخدام وسيلة التشفير لكافة البيانات والمعلومات الهامة المحفوظة في قاعدة البيانات.
- وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (37-2-3) مصفوفة تقييم حماية أمن الوصول البرمجي نظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	1	1	1	1	1	0	0	0	1	0	6
2	البنك (خ)	1	1	1	1	1	0	1	0	1	0	7
3	البنك (م)	1	1	1	1	1	0	0	0	1	0	6
	الإجمالي	3	3	3	3	3	0	1	0	3	0	19

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-2-9-4: قياس حماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية: تم التقييم بناءً على 10 معايير لإجراء تلك الحماية وهي:

1. يقوم البنك بأخذ نسخ احتياطية للبرامج وملفات البيانات الهامة بشكل مستمر ودوري (يومي، أسبوعي، شهري) حسب عدد الحركات اليومية وعمليات النظام.
2. تحفظ النسخ الاحتياطية في خزائن حديدية مقفلة لحمايتها من السرقة أو الحريق.
3. يتم تعيين الأفراد المخولين بالوصول إلى هذه النسخ.
4. توضع نسخة من النسخ الاحتياطية في مكان آمن خارج مقر العمل.
5. تقوم البنك بحفظ النسخ الاحتياطية بالاعتماد على مصدر خارجي مؤتمن يقوم بتخزين البيانات بشكل مستمر.
6. يتم عمل نسخ احتياطية من البيانات على وسائط متحركة باستخدام الخط الساخن في النظام الرئيسي والنظام البديل ويتم أخذها بواسطة وحدات النسخ المخصصة لذلك.

7. يتم تشفير النسخ الاحتياطية من قواعد البيانات لحمايتها من التعديل أو الوصول إليها بطريقة غير مشروعة وذلك لفرض الرقابة عليها.
 8. توجد رقابة كافية على وسائط تخزين البيانات غير المتصلة بالنظام.
 9. يتم فحص تلك الوسائط باستمرار للتأكد من صحتها وسلامتها.
 10. يتم التخلص من وسائط تخزين البيانات والبرامج بطريقة آمنة معينة وعدم رميها في براميل القمامة، حيث توجد إجراءات رقابية كافية لذلك.
- وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-38) مصفوفة تقييم حماية أمن وسائط التخزين
غير المتصلة بنظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	1	1	1	0	0	0	0	1	0	1	5
2	البنك (خ)	1	1	1	1	1	1	0	1	0	1	8
3	البنك (م)	1	1	1	1	0	1	0	1	0	1	7
	الإجمالي	3	3	3	2	1	2	0	3	0	3	20

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-2-9-5: تقييم حماية أمن مدخلات نظم المعلومات المحاسبية: تم التقييم بناءً على 10 معايير لإجراء تلك الحماية وهي:

1. مستندات إدخال البيانات دقيقة وشاملة لمختلف العمليات، وتساعد على تقليل الأخطاء.
2. ويتم إعداد مصدر المدخلات وتعبئتها ومصادقتها من الأشخاص المخولين فقط.
3. وجود برنامج خاص مصمم لمعرفة من قام بإدخال البيانات.
4. يتم تسجيل بيانات المدخلات أولاً بأول وتوجد رقابة كافية لاكتشاف أي نقص فيها.
5. يتم توثيق عمليات إدخال البيانات بما فيها المحاولات، والمخالفات الخاطئة، ومعرفة مصدرها.
6. يتم تحديد أخطاء إدخال البيانات وتتبعها حتى يتم تصحيحها.
7. تتضمن برامج النظام ضوابط تمنع إدخال بيانات خاطئة، حيث تظهر رسالة تحذيرية على الشاشة في حال وجود خطأ.
8. توجد مراجعة تفصيلية للبيانات المدخلة للتأكد من دقتها واكتمالها.
9. ويتم إجراء المراجعة الثنائية لبيانات المستندات المدخلة للتأكد من سلامتها.
10. تتوفر في نظم المعلومات المحاسبية خاصية تصحيح البيانات الخاطئة التي تم إدخالها في الوقت المناسب ضمن حدود الرقابة المسموح بها.

- وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (39-2-3) مصفوفة تقييم حماية أمن مدخلات نظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	0	1	0	1	1	1	0	0	1	0	5
2	البنك (خ)	1	1	1	1	1	1	1	1	1	0	9
3	البنك (م)	1	1	0	1	1	1	0	0	1	0	6
	الإجمالي	2	3	1	3	3	3	1	1	3	0	20

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الالكترونية للبنوك موضع دراسة الحالة.

- 3-2-9-6: تقييم حماية أمن عمليات تشغيل نظم المعلومات المحاسبية: تم التقييم بناءً على 5 معايير لإجراء تلك الحماية وهي:

1. احتواء برنامج التشغيل على وسائل تحدد صلاحية المستخدمين في تشغيل وتحديث البيانات ومنع قراءتها أو نسخها أو تعديلها من غير المخول لهم ذلك.
 2. وجود رقابة آلية مدمجة داخل النظام، من خلا تقارير تحليلية الكترونية لتفاصيل العمليات التشغيلية، تحدد شخص المستخدم ووقت بداية ونهاية الاستخدام، ومكانه وطبيعة الاستخدام، والأخطاء المكتشفة آلياً، ويتم متابعة تلك التقارير بشكل مستمر.
 3. وجود إجراءات كافية تضمن تصحيح الأخطاء، وإعادة تشغيل البيانات التي لم يتم تشغيلها بسبب توقف دورة التشغيل والتأكد من تمام معالجتها، ويتم تمييز العمليات التي تمت معالجتها لتلافي تكرار تشغيلها.
 4. وجود إجراءات للتأكد من أن معالجة البيانات قد تمت بشكل كامل عند حد الانقطاع، من نقطة توقف معينة عند توقف دورة التشغيل لسبب من الأسباب.
 5. عدم السماح بتشغيل النظام خارج فترة الدوام المحددة والمبرمجة آلياً، حيث يتم توقيف عمل التطبيقات المحاسبية إجبارياً نهاية الدوام الرسمي، بحيث يتعذر تشغيله النظام خلاف ذلك.
- وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (40-2-3) مصفوفة تقييم حماية أمن عمليات تشغيل نظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	المجموع
1	البنك (ع)	2	0	2	0	0	4
2	البنك (خ)	2	2	2	2	0	8
3	البنك (م)	2	0	2	2	0	6
	الإجمالي	6	2	6	4	0	18

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الالكترونية للبنوك موضع دراسة الحالة.

3-2-9-7: تقييم حماية أمن مخرجات نظم المعلومات المحاسبية: تم التقييم بناءً على 10 معايير لإجراء تلك الحماية وهي:

1. تحديد صلاحيات الأشخاص المخولين بحفظ مخرجات نظم المعلومات المحاسبية.
 2. يتم حصر أنواع المعلومات وتصنيفها إلى فئات وفقاً لدرجة أهميتها وسريتها.
 3. يتم تحديد مستوى الحماية الواجب توفيره لكل فئة من المعلومات وفقاً لدرجة أهميتها.
 4. وجود إجراءات كافية لعملية توزيع المخرجات، لضمان وصول التقارير والوثائق للجهات المعنية المخولة فقط باستلامها.
 5. وجود الأجهزة والوسائل المناسبة لعملية توزيع المخرجات، لضمان وصول التقارير والوثائق للجهات المعنية المخولة فقط باستلامها.
 6. يتم إجراء صيانة دائمة لوسائل الإخراج (طابعات، فاكسات، شاشات...الخ)، لضمان سلامة عرض المخرجات.
 7. يتم إعداد نسخ مطبوعة لبعض المعلومات المحاسبية الهامة.
 8. يتم تشفير المعلومات الحساسة.
 9. يتيح النظام مسار معين لمراجعة وتتبع سير المعاملات من مرحلة المدخلات إلى مرحلة المخرجات، والعكس.
 10. وجود لجنة متخصصة داخل البنك مخولة بإتلاف المخرجات المهمة والسرية داخل البنك بعد الانتهاء من استخدامها.
- وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-41) مصفوفة تقييم حماية أمن مخرجات نظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	6	7	8	9	10	المجموع
1	البنك (ع)	1	0	0	0	0	1	0	0	1	0	3
2	البنك (خ)	1	1	1	1	1	1	1	0	1	1	9
3	البنك (م)	1	0	0	0	0	1	1	0	1	1	5
	الإجمالي	3	1	1	1	1	3	2	0	3	2	17

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-2-9-8: قياس حماية أمن تبادل البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية: تم التقييم بناءً على 10 معايير لإجراء تلك الحماية وهي:

1. استخدام برامج الجدران النارية لتحديد المعلومات التي يسمح بدخولها أو خروجها من وإلى نظام المعلومات المحاسبي المحوسب للبنك.
2. تشفير البيانات المرسلّة عبر الشبكات للتأكد من أنه لم يتم الكشف عنها أو تعديلها وأنها مرسلّة من الجهة المعنية، وتتوفر وسائل حماية كافية للحفاظ على سرية مفتاح التشفير.

3. استخدام البنك للتوقيع الرقمي الإلكتروني، كوسيلة للتحقق من موثوقية المستخدمين بشكل غير قابل للتزيف، ولضمان عدم إنكار الأطراف المعنية المشاركة في الوثائق الإلكترونية.
 4. استخدام البنك لشهادة رقمية صادرة من جهات فنية معتمدة، عند إرسال أو استلام البيانات عبر الشبكة الخارجية، للتحقق من هوية مرسل الرسائل، وموثوقية المستخدم.
 5. استخدام البنك بروتوكولات أمنية بين البنك والأطراف المتعاملة للحفاظ على سرية المعلومات المحاسبية والتحقق من وصولها للجهة المطلوبة أثناء إجراء المعاملات المالية.
- وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-42) مصفوفة تقييم حماية أمن تبادل البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية

م	إسم البنك	1	2	3	4	5	المجموع
1	البنك (ع)	2	0	0	0	2	4
2	البنك (خ)	2	2	2	0	2	8
3	البنك (م)	2	2	0	0	2	6
	الإجمالي	6	4	2	0	6	18

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-2-9-9: قياس حماية أمن تعديل وتطوير نظم المعلومات المحاسبية: تم التقييم بناءً على 10 معايير لإجراء تلك الحماية وهي:

1. وجود إجراءات كافية وفعالة لرقابة عمليات تطوير البرامج والتطبيقات المحاسبية، وفق إجراءات واضحة ومكتوبة ومحددة.
2. لا تتم أية تعديلات في برمج النظام بدون حصول المبرمجين المختصين على موافقات رسمية من الإدارات المعنية المخولة.
3. وجود فريق متخصص لتعديل وتطوير نظام المعلومات المحاسبي من داخل البنك، وتشرف إدارة البنك على تعديل وتطوير النظام.
4. ضرورة إجراء الاختبار المبدئي بالتشغيل التجريبي للبرامج الجديدة وتعديلاتها قبل اعتمادها بشكل نهائي للتأكد من سلامتها، وقدرتها على تتبع الأخطاء التي قد تحدث أثناء التنفيذ.
5. يتم توثيق كافة التعديلات التي تتم على البرامج والمعدات، وفق الإجراءات المتبعة.

- وبناءً على ذلك تم تفريغ بيانات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-43) مصفوفة تقييم حماية أمن عمليات تعديل وتطوير نظم المعلومات المحاسبية

م	اسم البنك	1	2	3	4	5	المجموع
1	البنك (ع)	0	0	2	2	0	4
2	البنك (خ)	0	2	2	2	2	8
3	البنك (م)	0	2	2	2	2	8
	الإجمالي	0	4	6	6	4	20

الجدول من إعداد الباحث بناءً على الملاحظات والمقابلات والسجلات الالكترونية للبنوك موضع دراسة الحالة.

- وبالنظر إلى المتغيرات الرئيسية لإجراءات ووسائل حماية أمن نظم المعلومات المحاسبية المحوسبة، تم تفريغ إجابات البنوك الثلاثة المشمولة بدراسة الحالة العملية في الجداول الآتي:

جدول رقم (3-2-44) مصفوفة تقييم إجراءات ووسائل حماية أمن نظم المعلومات المحاسبية المحوسبة

م	إجراءات ووسائل حماية أمن نظم المعلومات	البنك (ع)	البنك (خ)	البنك (م)	مجموع نقاط الإجراء	نسبة تطبيق الحماية
1	حماية الأمن التنظيمي للأفراد.	4	8	5	17	57%
2	حماية أمن الوصول المادي.	5	7	6	18	60%
3	حماية أمن الوصول البرمجي.	6	7	6	19	63%
4	حماية أمن وسائط التخزين غير المتصلة بقاعدة البيانات.	5	8	7	20	67%
5	حماية أمن مدخلات النظم.	5	9	6	20	67%
6	حماية أمن عمليات التشغيل.	4	8	6	18	60%
7	حماية أمن المخرجات.	3	9	5	17	57%
8	حماية أمن تبادل البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية.	4	8	6	18	60%
9	حماية أمن التعديل والتطوير	4	8	8	20	67%
	إجمالي نقاط إجراءات الحماية	40	72	55	167	62%
	نسبة تطبيق إجراءات الحماية	44%	80%	61%	62%	

• الجدول من إعداد الباحث إستناداً لنتائج الجداول السابقة.

ومن الجدول السابق يتضح ما يلي:

- أن نسب تطبيق إجراءات ووسائل حماية أمن نظم المعلومات المحاسبية المحوسبة على مستوى المتغيرات الرئيسية كانت معظمها أكبر من (50%) ويمكن القول بصفة إجمالية بأن إجابات البنوك المشمولة بالدراسة حول مدى تطبيق إجراءات ووسائل حماية أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التي يعملون بها، كانت غالبيتها متوسطة بشكل عام وبنسبة (62%)، وهنا يجب على هذه البنوك من زيادة تطبيق تلك الإجراءات والوسائل اللازمة لمواجهة المخاطر الأمنية.
- يلاحظ أن البنك (ع) والذي يمثل بنوك القطاع العام أقل تطبيق لتلك الإجراءات من البنكين الآخرين حيث بلغت نسبة تطبيقه لتلك الإجراءات (44%) وكان البنك (خ) والذي يمثل بنوك القطاع الخاص أكثرها حرصاً على تطبيق وسائل وإجراءات الحماية وبنسبة (80%) فقط مما يعني وجود فوارق كبيرة بين القطاعات المختلفة في تطبيق تلك الإجراءات.

3-2-10: جوانب أخرى متعلقة بإدارة وتقييم مخاطر أمن نظم المعلومات المحاسبية لدى البنوك المتعلقة بدراسة الحالة العملية:

- وبالنظر إلى الجوانب الأخرى المتعلقة بإدارة وتقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة، تم تفرغ إجابات البنوك الثلاثة المشمولة بالدراسة الاستطلاعية من خلال مقياس مكون من 10 درجات كما في الجداول الآتي:

جدول رقم (3-2-45) مصفوفة تقييم الجوانب الأخرى الخاصة المتعلقة بإدارة وتقييم مخاطر أمن نظم المعلومات المحاسبية

م	جوانب أخرى خاصة متعلقة بتقييم المخاطر	البنك (ع)	البنك (خ)	البنك (م)	مجموع نقاط الإجراء	نسبة تطبيق الإجراء
1	وجود إدارة فعالة لتقييم المخاطر في البنك بشكل عام.	5	7	6	18	60%
2	وجود كوادرات متخصصة داخلية لتقييم مخاطر أمن نظم المعلومات المحاسبية.	4	6	5	15	50%
3	يتم تقييم المخاطر الأمنية بواسطة جهات خارجية.	6	7	6	19	63%
4	يتم تقييم المخاطر الأمنية بشكل دوري.	4	7	5	16	53%
5	وجود تقارير موثقة بالتقييم.	5	8	6	19	63%
6	يتم معالجة المخاطر الأمنية لنظم المعلومات بعد التقييم.	4	7	7	18	60%
إجمالي نقاط الإجراءات الخاصة		28	42	35	105	58%
نسبة تطبيق الإجراءات الخاصة		47%	70%	58%	58%	

• الجدول من إعداد الباحث إستناداً لنتائج المقابلات الشخصية، وكسور الأرقام والنسب مقربة للوحدات الصحيح.

ومن الجدول السابق يتضح ما يلي:

- أن نسب تطبيق إجراءات خاصة لتقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة كانت معظمها أكبر من (50%) ويمكن القول بصفة إجمالية بأن إجابات البنوك المشمولة بالدراسة حول مدى تطبيق إجراءات خاصة بتقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التي يعملون بها، كانت غالبيتها متوسطة بشكل عام وبنسبة (58%)، وهنا يجب على هذه البنوك من زيادة تطبيق تلك الإجراءات الخاصة بتقييم المخاطر الأمنية لنظم المعلومات المحاسبية.
- يلاحظ أن البنك (ع) والذي يمثل بنوك القطاع العام كان أقل تطبيق لتلك الإجراءات من البنوك الآخرين حيث بلغت نسبة تطبيقه لتلك الإجراءات (47%) وكان البنك (خ) والذي يمثل بنوك القطاع الخاص أكثرها حرصاً على تطبيق إجراءات تقييم مخاطر أمن نظم المعلومات المحاسبية وبنسبة (70%) مما يعني وجود فوارق بين القطاعات المختلفة في تطبيق تلك الإجراءات.

3-2-11: أهم ملاحظات الباحث من واقع قيامه بدراسة الحالة العملية:

- لاحظ الباحث عند إجراء دراسته للحالة العملية في البنوك الثلاثة المختارة (ع، خ، م) الكثير من الملاحظات على جوانب نقاط الضعف في إجراءات ووسائل الأمن المتبعة لدى تلك البنوك فهي تعتمد حالياً على شركات خارجية لمراقبة أداء الشبكات وأنظمة التشغيل ونورد هنا أهم تلك الملاحظات والمخاطر والتوصيات لعلاجها وحلها كما يتضح بالجدول التالي:

جدول رقم (3-2-46) ملخص لملاحظات وتوصيات الباحث الخاصة بدراسة الحالة العملية:

م	الملاحظات	المخاطر	التوصيات
1	بالنظر لوسائل مراقبة الشبكة وأنظمة تشغيل النظام لوحظ ما يلي: - عدم توفر نظام خاص بمراقبة أداء الشبكة وأنظمة التشغيل. - عدم توفر تقارير تفصيلية دورية عن أداء الشبكة وأنظمة التشغيل، والصيانة الدورية، والتحديثات غير المتوفرة أو التي تم تحميلها. - لا يوجد دليل على القيام بمراقبة حجم وأداء قواعد البيانات لدى البنك.	عدم اكتشاف مشاكل الشبكة وأنظمة التشغيل في وقت مبكر مما قد يؤدي إلى توقف أعمال البنك لفترة مؤقتة.	ضرورة تحميل نظام خاص بمراقبة أداء الشبكة وأنظمة المعلومات، بالإضافة إلى الطلب من الشركة الخارجية توفير تقارير تفصيلية عن أداء الشبكة وأنظمة المعلومات، وإجراء الصيانة الدورية، والتحديثات غير المتوفرة أو التي تم تحميلها. وضرورة المراقبة الدورية لحجم وأداء قواعد البيانات وتوثيق هذه المراقبة.

م	الملاحظات	المخاطر	التوصيات
2	بالنظر لوسائل وإجراءات الحماية المادية لغرفة الأجهزة الرئيسية لوحظ ما يلي: - عدم توفر إجراءات أو وسائل الحماية المادية في المركز الرئيسي. - عدم وجود نظام الدخول بالكرت Access Card. - عدم وجود سجل بالزيارات أو الدخول للبنك ولغرفة الأجهزة الرئيسية. - عدم وجود نظام الإنذار بالحرارة في المركز الرئيسي. - عدم فاعلية نظام التبريد الحالي (المكيفات) في المركز الرئيسي. - عدم وجود وسائل مراقبة درجة الحرارة والرطوبة في المركز الرئيسي. - عدم تزويد غرفة الأجهزة الرئيسية بأرضية خاصة مرتفعة لحماية الكابلات (Raised Floor). - إبقاء غرفة الأجهزة الرئيسية مغلقة دائماً، وفتحها عند الحاجة للدخول فقط. - إخراج أي معدات أو مستلزمات مكتنية غير ضرورية في غرفة الأجهزة الرئيسية.	إن عدم وجود إجراءات الحماية المادية قد ينجم عنه خسائر مالية ومادية. إن الخطر الذي قد ينجم عن الخرق لهذه الأمور يشمل الدخول غير المخول به، أو الضرر والتخريب المتعمد أو السرقة للمعدات أو الوثائق، أو النسخ أو الاطلاع على معلومات حساسة أو حقوق الطبع، أو تغيير في المعدات الحساسة أو المعلومات، أو سوء استخدام البيانات المسترجعة، أو الابتزاز، الاختلاس.	ضرورة تطوير وتطبيق وسائل حماية مادية. وينبغي: - تطبيق نظام الدخول بالكرت Access Card - إنشاء سجل يتم فيه تسجيل أسماء جميع زوار البنك وغرفة الحواسيب الرئيسية. - تطوير إجراءات صيانة وفحص السلامة المادية للأجهزة وأجهزة الإنذار بالحرارة. - تغيير نظام التبريد الحالي (المكيفات) واستبداله بأجهزة جديدة - تركيب وسائل مراقبة درجة الحرارة والرطوبة بغرفة السيرفرات الرئيسية في المركز الرئيسي. - تزويد غرفة الأجهزة الرئيسية بأرضية خاصة مرتفعة لحماية الكابلات (Raised Floor) - إبقاء غرفة الأجهزة الرئيسية مغلقة دائماً، وفتحها عند الحاجة للدخول فقط. - إخراج أي معدات أو مستلزمات مكتنية غير ضرورية في غرفة الأجهزة الرئيسية.
3	من خلال التدقيق في أنظمة حماية شبكة البنك لاحظ الباحث أن البنك لا يمتلك أجهزة وأنظمة حماية من الاختراقات كالجدران النارية (Firewalls)، كما لاحظنا عدم توفر مخطط تفصيلي عن أنظمة وأجهزة شبكة الحاسوب.	إن عدم وجود أنظمة وأجهزة الجدران النارية لحماية شبكة البنك (Firewalls) يسهل عمليات اختراق نظم المعلومات المحاسبية من قبل مخترقين خارجيين. كما أن وجود مخطط تفصيلي لشبكة البنك يوضح ويسهل على إدارة نظم المعلومات المحاسبية من اكتشاف الثغرات والنواقص في الشبكة ويساعد على سرعة حل مشاكلها وصيانتها.	نوصي بضرورة تحميل وتركيب أنظمة وأجهزة حماية للشبكة Firewall، ويجب إنشاء مخطط تفصيلي لشبكة البنك بحيث يتضمن النظم، والسيرفرات (الخوادم)، وعناوين السيرفرات، وأجهزة التغذية الكهربائية (UPS)، وطريقة توصيل الكابلات، ووسائل الحماية، وأجهزة الاتصال بالفروع، وطريقة الاتصال بالإنترنت، وغيرها.

م	الملاحظات	المخاطر	التوصيات
4	<u>من خلال مراجعة إعدادات كلمات المرور لاحظ الباحث أن إعدادات كلمات المرور للأنظمة ضعيفة.</u>	الإعدادات الضعيفة لكلمات المرور تؤدي إلى سهولة اختراق النظام، كلمات المرور العادية والقصيرة غالباً ما تكون سهلة التخمين. إن عدم تعطيل كلمات المرور في حالة إدخالها أكثر من مرة يمكن المخترق من المحاولة في تخمين كلمة المرور حتى يصل إليها.	يوصي الباحث بضرورة إعداد كلمات المرور لتكون كما يلي: - الحد الأدنى لكلمات المرور هو (8) أحرف. - تفعيل خاصية تعقيد كلمات المرور، كأن تكون حروف أبجدية ورموز. - انتهاء صلاحية كلمات المرور كل (30) إلى (45) يوم. - تفعيل خاصية السجل التاريخي لكلمات المرور. - تفعيل خاصية تعطيل كلمات المرور وإعدادها على (3) محاولات خاطئة.
5	<u>عدم وجود آلية لإبلاغ إدارة الحاسب الآلي عن الموظفين المستقلين والمتقاعدين ليتم إلغاء أو إيقاف صلاحياتهم في أنظمة البنك.</u>	إن عدم توفر آلية لإبلاغ إدارة الحاسب الآلي عن الموظفين المستقلين والمتقاعدين، وعدم إلغاء المستخدمين المنتهية خدمتهم ومراجعة صلاحيات المستخدمين بشكل دوري قد يؤدي إلى إمكانية الدخول غير المصرح إلى النظام من قبل أشخاص غير مخولين.	يوصي الباحث بضرورة إيجاد آلية وتوثيقها لإبلاغ إدارة الحاسب الآلي عن الموظفين المستقلين والمتقاعدين، كما يوصي بضرورة مراجعة صلاحيات المستخدمين بشكل دوري وإلغاء صلاحيات المستخدمين المنتهية خدماتهم.
6	<u>من خلال مراجعة سياسة إنشاء أسماء المستخدمين، لوحظ عدم وجود سياسة واضحة وثابتة لإنشاء أسماء المستخدمين بحيث أن بعض الأسماء تكون عبارة عن اختصار لاسم الموظف أو حرف واحد متبوع برقمين</u>	إن توحيد سياسة إنشاء أسماء المستخدمين يمكن من معرفة وتحديد كل مستخدم عن الآخر.	يوصي الباحث بإيجاد سياسة موحدة لإنشاء أسماء المستخدمين، على سبيل المثال أن يكون اختصار لاسم الموظف (الحرف الأول من الاسم الأول، الحرف الثاني من الاسم الثاني، الحرف الثالث من الاسم الثالث). أو أن يكون عبارة عن رقم تعريفي فقط، وما إلى ذلك.
7	<u>من خلال مراجعة سياسات أمن وحماية المعلومات والإجراءات المرتبطة بها المطبقة لدى إدارة تقنية المعلومات، لوحظ ما يلي:</u> * أن هذه السياسات والإجراءات المرتبطة بها والموثقة ليست تفصيلية بشكل كافٍ لتشمل جميع إجراءات أمن وحماية المعلومات، وعلى سبيل	إن عدم وجود سياسة معتمدة رسمياً من قبل إدارة البنك لأمن وحماية المعلومات وكذلك الإجراءات المرتبطة بها قد يؤدي إلى عدم التوافق في تنفيذ مختلف المهام الأمنية لجميع الوظائف والتطبيقات بشكل منفصل وهو ما يتطلب تفسير خاص لمتطلباتها الأمنية.	بغرض التأكد من أن جميع الموظفين يدركون أهمية أمن وحماية المعلومات التي تعكس حجم مخاطر البنك، والغايات والأهداف المتعلقة بأمن وحماية المعلومات، فإننا نوصي بالقيام بتنفيذ مشروع أمني يبدأ بتقييم أمن وحماية المعلومات وذلك لبلورة احتياجات البنك الأمنية، وكذا توثيق أي فجوات بين وضع أمن وحماية معلومات البنك الحالي، ومعايير الأمن والحماية الدولي

م	الملاحظات	المخاطر	التوصيات
	المثال لا تشتمل السياسات الحالية على ما يلي: • توثيق أهداف الإدارة فيما يتعلق بالأصول؛ • تصنيف أصول المعلومات من حيث الأهمية، الحساسية، والسرية. • تحديد مسؤوليات مدراء الأنظمة، المستخدمين، ومدراء قواعد البيانات. • تحديد المسؤوليات عن المراجعة والمتابعة. • تحديد طرق الرقابة والتحقق في الخروقات الأمنية ومحاولات الوصول غير المصرح به. • تحديد مسؤولية المستخدمين لسرية كلمات المرور. • المبادئ الأساسية للمساعدة على ضمان استخدام كلمة المرور وفعالية التطبيق. • أن هذه السياسات والإجراءات المرتبطة بها ليست معتمدة رسمياً من قبل إدارة البنك.		ISO 27001 / BS7799، واستناداً إلى نتائج التقييم يمكن تطوير سياسة لأمن وحماية المعلومات. على الإدارة، عند وضع مثل هذه السياسة الأمنية، الأخذ في عين الاعتبار ما يلي: • توثيق أهداف الإدارة التنفيذية فيما يتعلق بالأصول. • تصنيف أصول المعلومات من حيث الأهمية، الحساسية، والسرية. • تحديد مسؤوليات مدراء الأنظمة، المستخدمين، ومدراء قواعد البيانات. • تحديد المسؤوليات عن المراجعة والمتابعة. • تحديد طرق الرقابة والتحقق في الخروقات الأمنية ومحاولات الوصول غير المصرح به. • تحديد الإجراءات اللازمة لمنح امتيازات صلاحيات الوصول وإدارة وإنهاء أو نقل الموظفين. • تحديد مسؤولية المستخدمين لسرية كلمات المرور. • المبادئ الأساسية للمساعدة على ضمان استخدام كلمة المرور وفعالية التطبيق. • إبلاغ المستخدمين عن مسؤولياتهم في أمن وحماية المعلومات. - كما ينبغي أن تتم الموافقة على هذه السياسات من قبل الإدارة العليا. ويتم تطبيق سياسات أمن وحماية المعلومات والموافقة عليها، ينبغي على البنك وضع برنامج البلاغات الأمنية (<i>Security Awareness Program</i>) وذلك لتعزيز أمن وحماية المعلومات داخل البنك، بحيث يستهدف الإدارة العليا، والفنيين والمستخدمين النهائيين كلاً على حده. - كما أن المفاهيم الأمنية الرئيسية مثل حماية جهاز الحاسوب، وحماية كلمات المرور، وأمن وحماية شبكة

م	الملاحظات	المخاطر	التوصيات
			المعلومات ينبغي إدراجها في خطة تدريبية سنوية، وكذلك إدراج برنامج البلاغات الأمنية في البرنامج التوجيهي عند استخدام موظف جديد من قبل إدارة الموارد البشرية، كما يجب على هذا الموظف التوقيع على وثيقة قبول سياسة الاستخدام.
8	من خلال مراجعة الصلاحيات الممنوحة على النظام، لاحظ الباحث وجود أكثر من اثنين مستخدمين يملكون صلاحيات عليا (Administrator).	إن استخدام مستخدمين ذوي صلاحيات عالية (Superuser access) خطر جداً فقد يؤثر على الحركات المالية، وغير المالية، وتعريف ملفات أمن وحماية الأنظمة، كمنح صلاحيات للدخول لقواعد البيانات، وغيرها، كما أن النشاطات غير المخولة يمكن أن تؤثر على سلامة البيانات ومخرجات النظام. وأن استخدام نفس الصلاحيات من قبل أكثر من شخص واحد يحد من إمكانية المساءلة عن الإجراءات التي يتم تنفيذها، حيث يكون من الصعب تتبع مثل هذه الإجراءات لمستخدم معين.	ينبغي على الإدارة تحديد ومراجعة مستخدمي النظام ذوي الصلاحيات العليا، وينصح بعدم تجاوز عددهم أكثر من 2 مستخدم والقيام بالمراقبة الدورية للملفات الخاصة بالدخول وأنشطة المستخدمين ذوي الصلاحيات العالية على النظام، بالإضافة إلى ذلك يوصي الباحث باستخدام مستخدم مستقل لكل موظف في قسم قواعد البيانات.
9	لاحظ الباحث عدم وجود دليل إجراءات تفصيلي لجميع عمليات النسخ الاحتياطي للبيانات، لوحظ ما يلي: - عدم الاحتفاظ بملفات تسجيل العمليات لعملية النسخ الاحتياطي (Backup Log Files). - عدم القيام بالمراجعة والتوقيع على قائمة متابعة عملية النسخ الاحتياطي من قبل الإدارة بشكل دوري. - عدم القيام بعمليات النسخ الاحتياطي إلى أشرطة التسجيل وكذا أعمال الإقفال اليومي بشكل آلي.	إن القيام بعملية النسخ الاحتياطي والإقفال اليومي بشكل يدوي يزيد من احتمالية عدم إتمام هذه العمليات بسبب أخطاء بشرية كالنسيان أو التعمد أو التأخير في القيام بذلك، كما أن من مسؤوليات إدارة الأنظمة مراجعة ملفات العمليات بشكل دوري للتأكد من إتمام العمليات، وعدم الاحتفاظ بهذه الملفات لا يتيح للإدارة القيام بهذه المسؤوليات. بما أن البنك حالياً يعتمد على أشرطة النسخ الاحتياطي اعتماداً كلياً في حال حصول أضرار للبيئة الحية، فإن عدم تشفير النسخ التي يحتفظ بها خارج البنك قد يؤدي إلى تسرب البيانات في حال	نوصي بضرورة ما يلي: - إعداد وتطوير دليل تفصيلي لإجراءات عملية النسخ الاحتياطي. - استخدام القائمة اليومية لتوثيق عملية النسخ الاحتياطي وذلك لجميع أنواع النسخ الاحتياطي. - المراجعة والتوقيع على قائمة متابعة عملية النسخ الاحتياطي من قبل الإدارة بشكل دوري. - استخدام ومراجعة قائمة متابعة عمليات النسخ الاحتياطي بشكل دائم. - جدولة عمليات النسخ الاحتياطي والإقفال اليومي لتتم بشكل آلي لجميع أنواع النسخ الاحتياطي. - تشفير أشرطة النسخ الاحتياطي التي يتم الاحتفاظ بها خارج موقع البنك.

م	الملاحظات	المخاطر	التوصيات
		وقعت هذه الأشرطة في الأيدي الخاطئة. إن الاحتفاظ بمفتاح الخزينة وعدم تشفير البيانات يجعل من السهل وصول أحد أفراد الحراسة للبيانات وعمل نسخ منها، وبهذه الطريقة لن يتمكن البنك من معرفة ذلك أو تتبعه. علاوة على ذلك، إن عدم قيام إدارة بمراقبة استكمال النسخ الاحتياطي التي تحدث، فإن سلامة عملية النسخ قد تكون عرضة للمخاطر، كما أن سلامة البيانات المرتبطة بها قد تكون على المحك.	
10	يقوم البنك حالياً بإعداد وتطوير خطط لاستمرارية العمل والتغلب على آثار الكوارث (Business Continuity Plan and Disaster Recovery) ، توضح بشكل تفصيلي الخطوات المطلوبة لاسترداد عمليات البنك المهمة في حال تعذر الوصول إلى البيانات أو فشل النظام إلا أنه <u>لوحظ أن هذه الخطط في طور الأعداد ولم تكتمل بعد، وتجرب أو يتم الموافقة عليها.</u> إن خطط استمرارية العمل هي أوسع من خطط التغلب على آثار الكوارث، والتي تميل إلى التركيز على بيئة تكنولوجيا المعلومات. إن الهدف من خطط استمرارية العمل هو استرداد جميع الأعمال الهامة والعمليات بدلاً من مجرد استرداد أنظمة الحاسوب.	إن عدم وجود خطط لاستمرارية العمل (Business Continuity Plan)، وخطط التغلب على آثار الكوارث (Disaster Recovery) تكون محددة، موافق عليها، تم مناقشتها وفحصها، فإن من الصعوبة بمكان على البنك استعادة أعماله اليومية والتي قد تؤدي بشكل مباشر إلى خسائر مالية في حال حدوث كارثة أو أعمال التخريب.	نوصي بضرورة سرعة تطوير خطط لاستمرارية العمل وكذلك خطط التغلب على آثار الكوارث والموافقة عليها رسمياً، بعد القيام بإجراء التجارب اللازمة لضمان نجاحها في حال حدوث أي كارثة. كما يجب أن تتضمن خطط استمرارية العمل ما يلي: - إجراءات النسخ الاحتياطي للبيانات واسترجاعها. - أسماء الأشخاص الذي يتم التواصل معهم عند أي طارئ وأرقام تلفوناتهم. - بيانات تفصيلية عن المورد وأي طرف آخر ذو علاقة. - مسؤوليات المستخدمين والإدارة وفريق أنظمة المعلومات. - الأهمية النسبية للإجراءات التي يجب اتخاذها عند حدوث أي طارئ. - مكان خارجي لحفظ وسائط النسخ الاحتياطي، والمستندات الجوهرية. - دليل إجراءات يتم استخدامه عند حدوث أي عطب على النظام. - تدريب الموظفين المعنيين على تطبيق هذه الخطط للمساعدة في رفع طاقم أنظمة المعلومات والموظفين

م	الملاحظات	المخاطر	التوصيات
			الآخرين بتدريب خاص يساعدهم في حالة حدوث طارئ حقيقي.
11	لاحظ الباحث <u>عدم قيام البنك بإعداد دليل تفصيلي موثق لجميع عمليات نظم المعلومات المحاسبية، وذلك لتنظيم أنشطتها التنفيذية</u> يوماً بعد يوم، بما في ذلك أعمال وخطوات نهاية اليوم أو نهاية الشهر وكذلك إجراءات النسخ الاحتياطية، وغيرها.	إن عدم وجود دليل عمليات شامل ومحدث لإدارة تقنية المعلومات يفصل الأعمال اليومية يوماً بعد يوم، قد يؤدي إلى التعرض لمخاطر تنفيذ المهام بطريقة غير كاملة أو غير متناسقة. وهذا قد يؤدي إلى أخطاء مكلفة في النظام أو قد تؤدي إلى توقف النظام.	يوصي الباحث إدارة تقنية المعلومات بالقيام رسمياً بتطوير وتوثيق دليل عمليات الإدارة لضمان تزويد جميع الأنشطة التنفيذية بالتعليمات المفصلة. ينبغي أن يعالج دليل العمليات ما يلي: - وظائف يتم تشغيلها على أساس يومي. - مسؤوليات تشغيل مختلف الوظائف التشغيلية. - تعليمات حول كيفية تشغيل الوظائف. - تعليمات عن طرق التعامل مع الحالات الاستثنائية. - متطلبات استكمال وتسجيل الأعمال اليومية. - مسؤوليات مراقبة الأنشطة التنفيذية.
12	يعتمد البنك حالياً على إدارة تقنية المعلومات <u>لحل مشاكل المستخدمين لدى البنك، ومن خلال التدقيق لوحظ ما يلي:</u> - عدم وجود أشخاص/قسم محدد للقيام بمعالجة وحل مشاكل المستخدمين، حيث أن معظم موظفي إدارة تقنية المعلومات يقومون بتلك المهمة. - عدم وجود نظام آلي لتوثيق تلك المشاكل وأسبابها ومتابعتها وطريقة حلها. - عدم وجود تحليل	- ما لم يتم تكليف أشخاص محددين للقيام بمهام معالجة وحل مشاكل المستخدمين والإجراءات ذات الصلة وتنفيذها، سيكون من الصعب على الإدارة متابعة ومعالجة طلبات دعم المستخدم النهائي. - وعلاوة على ذلك، سيكون من الصعب ضمان التحكم بشكل مناسب بمثل هذه المشاكل وحلها في الوقت المناسب. - كما إن توفر قاعدة بيانات لمشاكل المستخدمين وأسبابها يساعد على استخراج تقارير	ينبغي على إدارة البنك إنشاء قسم خاص بالدعم الفني وتعيين هذه المسؤولية لموظفين محددين من إدارة تكنولوجيا المعلومات، كما ينبغي أيضاً صياغة الإجراءات ذات الصلة لتسهيل تسجيل وتتبع ومعالجة قضايا المستخدمين. كما يفضل استخدام نظام خاص أو جداول البيانات لتسهيل تسجيل وتتبع مشاكل المستخدمين، بحيث يتم قيد المشكلة وسببها وطريقة حلها.

م	الملاحظات	المخاطر	التوصيات
	إحصائي للمشاكل المرفوعة من قبل المستخدمين إلى إدارة تقنية المعلومات.	تفصيلية وإحصائية تساعد على تجنب تلك المشاكل في المستقبل، أو حلها بشكل أسرع بالرجوع إلى تلك التقارير.	
13	من خلال <u>مراجعة قائمة التغييرات والتعديلات المنفذة على النظام في البنك الرئيسي</u> ، لوحظ عدم وجود خطط تطوير مسبقة، كما أن عدداً كبيراً من المشاكل في النظام تم تسجيلها.	إن إجراء عدد كبير من التعديلات على نظام واحد يعتبر مؤشر كبير على عدم استقرار النظام، مما قد يؤثر على سلامة وصحة التعديلات المطلوبة، وبالتالي عدم ملاءمة النظام لتلبية متطلبات عمل البنك.	نوصي الإدارة بضرورة ما يلي: - التحقق من نوعية التعديلات المطبقة وتحليلها. - إعداد وتطوير خطط دورية لتنفيذ أي تعديلات على النظام. - القيام بدراسة شاملة للنظام والتأكد من ملاءمة النظام لتلبية جميع متطلبات عمل البنك.
14	من خلال مراجعة إجراءات <u>التعديل على نظم المعلومات المحاسبية للبنك</u> ، لاحظ الباحث عدم وجود سياسات وإجراءات تفصيلية توضح وسائل وطرق التعديل والتطوير على قواعد البيانات، والبرمجيات، والنظم والشبكات، والأجهزة. بالإضافة إلى ذلك لاحظ الباحث ما يلي: - طلب تعديل لا يوجد لها طلب رسمي (رسالة أو بريد إلكتروني). - طلب إنزال تعديلات ونموذج إنزال على قواعد البيانات غير متوفرة. - عدم توفر الموافقة المسبقة لجميع طلبات التعديل. - عدم توفر نموذج إجراءات قسم التحليل لجميع طلبات التعديل. - عدم توفر نموذج إجراءات المبرمج لجميع طلبات التعديل. - عدم توفر الوثائق اللازمة لتأكيد إتمام الفحص من قبل قسم التطوير لجميع طلبات التعديل.	إن القصور في توثيق عمليات التعديل على الأنظمة يمكن أن يؤدي إلى تنفيذ تعديلات غير مصرح بها أو لا تتلاءم مع متطلبات المستخدمين أو الإدارة. علاوة على ذلك، قد يؤدي عدم التوثيق الملائم للعمليات، إلى صعوبة الصيانة أو التعديل أو حل مشاكل النظام مستقبلاً.	يوصي الباحث بإعداد دليل وسياسة لتعديل وتطوير نظم المعلومات المحاسبية المحوسبة، بحيث يتضمن على الأقل ما يلي: - <u>منهجية معتمدة</u> : بحيث يتم اعتمادها لجميع التعديلات على الأنظمة. - <u>الموافقة على التعديلات</u> : فصل مهام الطلب والموافقة على التعديلات، وتعيين مسؤولين عن الأنظمة مخولين بالموافقة على التعديلات. - <u>مشاركة المستخدمين</u> : ضرورة مشاركة المستخدمين في فحص التعديلات والتوقيع على قبولها، وهذا يمكن توثيقه من خلال نموذج طلب التعديل. - <u>فحص التعديلات</u> : يجب الفحص والموافقة على التعديلات أو الإضافات على نظم المعلومات قبل تطبيقها على البيئة الحية من قبل المستخدمين، مشرفي أنظمة المعلومات، الدعم الفني للأنظمة ومدير قواعد البيانات. - كما يجب إعداد وتوثيق خطط للفحص ونتائج الفحص، بالإضافة إلى التوثيق الفني للغة البرمجية المستخدمة والكود المستخدم.

م	الملاحظات	المخاطر	التوصيات
	- عدم توفر الوثائق اللازمة لتأكيد إتمام الفحص من قبل قسم مراقبة الجودة لجميع طلبات التعديل.		- إدارة المكتبات: إيجاد إجراءات للتأكد من مراقبة أصول البرامج، وأن التطوير والفحص يتم عملها في بيئة مستقلة عن البيئة الحية مع إجراءات تضمن الوصول إلى مختلف المكتبات والتنقل من مكتبة إلى أخرى، وتضمن أن أصول البرامج هي نفسها البرامج المنفذة في البيئة الحية. - توثيق العمليات: يجب أن يكون دليل المستخدمين ووثائق النظام الفنية متوفرة للنظام الحالي ليتمكن المستخدم من الاطلاع عليها قبل العمل على التعديلات الجديدة. - الجدولة والتطبيق: التأكد من أن التعديلات يجب أن تنظم وتطبق وفقاً لبرنامج زمني متفق عليه بين المستخدمين أو مسؤولي نظم المعلومات المحاسبية وإدارة التعديل والتطوير لتجنب أي تعارض في سير العمل. - التحويل والتحديث: التأكد من وجود خطط للتعديل والتطوير (إن وجد)، ووجود الرقابة للتأكد من أن ذلك قد تم بشكل متقن وكامل. - التدريب: التأكد من أن المستخدمين قد تلقوا التدريب اللازم فيما يتعلق بالتعديلات على الأنظمة. - النماذج المتعلقة بسير العمليات المصرفية: التأكد من أن تلك النماذج محدثة ومتوافقة مع التعديلات المطبقة على النظام. - المراقبة: مراقبة الأنظمة بعد إدخال التعديلات للتأكد من عملها بشكل صحيح. - المراجعة بعد التطبيق: إجراء المراجعة بعد التطبيق لمشاريع التعديلات الكبيرة للتأكد من تحقيق الغرض من مشروع التعديل وأن المشروع يعمل بالشكل المطلوب من قبل الإدارة، وأن إجراءات

م	الملاحظات	المخاطر	التوصيات
			الحماية ومميزات الرقابة تعمل كما هو مخطط لها وأن النظام يعالج البيانات بشكل صحيح. - فصل المهام والواجبات: يجب العمل على فصل المهام والواجبات بين مهام التعديل والتطوير، والفحص والتطبيق على البيئة الحية للنظام.
15	لاحظ الباحث عدم مشاركة المستخدمين أو طالبي التعديل في فحص التعديلات على الأنظمة كما لوحظ عدم قيامهم بالتوقيع بالموافقة على هذه التعديلات قبل تطبيقها في بيئة النظام الحية. كما لا تقوم إدارة تكنولوجيا المعلومات بأخذ الموافقة المسبقة من طالبي التعديل لغرض تطبيق هذه التعديلات في بيئة النظام الحية.	بسبب عدم مشاركة المستخدمين / طالبي التعديل في فحص التعديلات وكذا أخذ الموافقة المسبقة منهم لتطبيق هذه التعديلات في بيئة النظام الحية، فإنه لا يمكن التأكد من: قبول المستخدمين للتعديلات المطلوبة على النظام، ومعرفة كيف ستؤثر تلك التعديلات على طريقة عملهم. - تنفيذ تعديلات غير معتمدة أو معروفة ويحتمل أن تكون بعض التعديلات بغرض الاحتيال.	نوصي بضرورة فحص التعديلات بشكل كامل للتأكد من عملها كما هو متوقع وذلك من قبل موظفي تقنية المعلومات والمستخدمين على حد سواء. وينبغي قيام المستخدمين بالتوقيع على قبول تنفيذ تلك التعديلات قبل تطبيقها في بيئة النظام الحية.
16	لاحظ الباحث عدم القيام بتطبيق التطبيقات الجديدة أو التعديل أو التقارير المنفذة في قسم تطوير الأنظمة في بيئة النظام الحية بطريقة منظمة أو آلية. وكذا عدم استخدام أنظمة إدارة البرامج المصدرية (Source Code) والتي تقوم بترتيب وتطبيق ومراقبة إصدارات الأنظمة.	إن ضمان نقل التعديلات أو التقارير التي تم فحصها والموافق عليها إلى بيئة النظام الحية يعتبر الخطوة الأخيرة وربما كانت أهم خطوة. إن عدم وجود إجراءات للموافقة على تعديل وتطوير نظم المعلومات المحاسبية قد يعرض البنك لمخاطر نقل أو تطبيق تعديلات خاطئة أو غير موافق عليها في بيئة النظام الحية وبالتالي قد تؤثر على سلامة البيانات المالية.	نوصي إدارة البنك بما يلي: - يجب تحديث المكتبات التي تحمل البرامج التنفيذية فقط بعد الحصول على موافقة طالب التعديل. - يجب أن تتضمن بيئة النظام الحية على برامج تنفيذية فقط، والبرامج المصدريّة يجب أن لا تكون متاحة في بيئة النظام الحية. - يجب تنفيذ التعديلات في بيئة النظام الحية فقط بعد أن يتم إجراء الفحص المناسب، وموافقة المستخدمين النهائيين، وكذا تحديث المكتبات التي تحمل البرامج المصدريّة. - يجب تسجيل جميع التعديلات على البرامج المصدريّة. - يجب حفظ جميع إصدارات الأنظمة السابقة التي تم تعديلها لتمكين من استعادة النظام إلى إصدار سابق.

م	الملاحظات	المخاطر	التوصيات
17	لاحظ الباحث <u>عدم وجود آلية لدى البنك لمراجعة تقرير ملف الرسائل اليومي</u> (Message File) والذي يتضمن الرسائل الواردة والصادرة، وذلك بمقارنته مع تقرير تسلسل الرسائل، وتقرير الرسائل غير المُسلّمة.	ما لم يتم مراجعة ومقارنة هذه التقارير بشكل صحيح مع الرسائل، فإن تمرير رسائل غير صحيحة، أو غير مصرح بها وكذلك رسائل احتيالية أمر محتمل.	نوصي البنك بالبدء بتنفيذ آلية رسمية لمراجعة ومقارنة الرسائل الواردة والصادرة عن طريق التحقق من ملف الرسالة مع تقارير الرسائل، ويجب التوقيع على التقرير الناتج وأرشفته ليتم الرجوع له لاحقاً.
18	<u>عدم قيام البنك بوضع إجراءات خاصة لحفظ وأرشفة سجل عمليات نظام سويفت</u> كأرشفة ملفات الرسائل (SAU) وسجل العمليات اليومية. كما لم يحدد آلية للقيام بمراجعة دورية ومنتظمة لسجل العمليات اليومية.	يعتبر تسجيل العمليات وأنشطة المستخدمين خطوة هامة في مراقبة نظام سويفت (SWIFT) المطبق في البنك، ولن يكون البنك قادراً على أداء هذا الدور الرقابي في حال لم يتم مراجعة هذا السجل بشكل دوري، ونتيجة لذلك من المحتمل عدم الانتباه للتجاوزات الأمنية التي قد يتم ارتكابها.	نوصي بوضع آلية رسمية لأرشفة ومراجعة سجل الأحداث اليومية، والذي يعتبر سجل تدقيق يتضمن الأحداث اليومية، وذلك من قبل شخص لا يتحمل أية مسؤوليات تتعلق بنظام سويفت (SWIFT)، وكدليل على وظيفة المراجعة المذكورة، نوصي أيضاً بالتوقيع على سجل الأحداث اليومية وأرشفته وكذلك أرشفة ملف الرسائل ليتم مراجعته لاحقاً.
19	لاحظ الباحث عدم استخدام البنك بشكل دائم لميزات (Possible Duplicate Emission (PDR)) و (Possible Duplicate Reception) التي تساعد في تحديد الرسائل المكررة، بالرغم من عدم وجود إجراء بديل للتعرف على الرسائل المكررة المرسله من قبل البنك.	إن الخطر الرئيسي لعدم استخدام ميزات PDE و PDR هو القيام بنفس العملية مرتين، مما قد يؤدي إلى خسائر مالية للبنك.	نوصي باستخدام ميزات PDE و PDR والتي من شأنها أن تساعد البنك في اكتشاف الرسائل الواردة المكررة والتي استلمت من قبل.

الجدول من إعداد الباحث بناء على الملاحظات والمقابلات والسجلات الإلكترونية للبنوك موضع دراسة الحالة.

3-3: المبحث الثالث:

عرض وتحليل ومناقشة البيانات

مقدمة: يتضمن هذا المبحث عرض وتحليل ومناقشة البيانات الواردة في إجابات أفراد عينة الدراسة على الأسئلة الرئيسية المختلفة سواء فيما يتعلق بالأسئلة العامة التي وردت في الجزئين الأول والثاني، والأسئلة الخاصة بالمحاور الخمسة لهذه الدراسة والتي تناولها الجزء الثالث من الاستقصاء، والتي تعكس آراء أفراد العينة بشأن متغيرات الدراسة والذي تناولها الباحث في الإطار النظري والمتمثلة بكل من: المخاطر التي تهدد أمن نظم المعلومات المحاسبية، وأسبابها المختلفة المتمثلة بمجموعة من التهديدات الداخلية والخارجية والمسببة لحدوث تلك المخاطر، ومدى تأثير حدوث تلك المخاطر على العناصر المكونة لأمن نظم المعلومات المحاسبية المحوسبة، ومن ثم التطرق لمدى كفاية إجراءات وأساليب الحماية المطبقة لدى البنوك التجارية في الجمهورية اليمنية لمواجهة تلك المخاطر، حيث تم تحليل تلك البيانات، تمهيداً لاختبار فرضيات هذه الدراسة، وتبين من التحليل ما يلي:

1-3-3: تحليل البيانات المتعلقة بالخصائص الشخصية والوظيفية لعينة الدراسة

توطئة لتحليل بيانات الدراسة التي تم جمعها بواسطة الاستقصاء، نستعرض بعض الخصائص الشخصية (العلمية والوظيفية) للأفراد المجيبين الممثلين لعينة الدراسة والبالغ عددهم (122) شخص يعملون في دوائر المحاسبة، والرقابة والتدقيق، ودوائر الحاسوب وتكنولوجيا المعلومات، ودوائر المخاطر لدى البنوك التجارية في الجمهورية اليمنية لمعرفة بعض الحقائق المتعلقة بهم كالمؤهل العلمي، والتخصص، والمسمى الوظيفي، والعمر، والخبرة، وعدد الدورات التدريبية، ويمكن تلخيصها بالجدول الآتي:

جدول رقم (1-3-3) الخصائص الشخصية والوظيفية للأفراد الممثلين لعينة الدراسة (ن = 122).

م	الخاصية	تصنيف الفئات	التكرار (Frequency)	النسبة المئوية % (Percent %)
1	المؤهل العلمي	ثانوية عامة	1	0.8
		دبلوم متوسط	4	3.3
		بكالوريوس	98	80.3
		دبلوم عالي	4	3.3
		ماجستير	13	10.7
		دكتوراه	2	1.6
2	التخصص العلمي	محاسبة	72	59.0
		إدارة أعمال	10	8.2
		إدارة عامة	2	1.6
		تمويل ومصارف	9	7.4
		اقتصاد	2	1.6
		علوم حاسوب	21	17.2
		تخصص آخر	6	4.9

م	الخاصية	تصنيف الفئات	التكرار (Frequency)	النسبة المئوية % (Percent %)
3	المسمى الوظيفي.	مدير مالي أو نائبه	6	4.9
		رئيس قسم حسابات	14	11.5
		مدقق داخلي	25	20.5
		مدير إدارة المخاطر	7	5.7
		رئيس قسم الحاسوب	10	8.2
		مبرمج النظام	15	12.3
		مشغل النظام	9	7.4
		مدقق خارجي	29	23.8
		مفتش بنك مركزي أو مراقب عام	7	5.7
4	الفئة العمرية	أقل من 25 سنة	4	3.3
		من 25 إلى أقل من 35 سنة	63	51.6
		من 35 إلى أقل من 45 سنة	40	32.8
		من 45 إلى أقل من 55 سنة	8	6.6
		55 سنة فأكثر	7	5.7
5	عدد سنوات الخبرة في التعامل مع نظم المعلومات لمحاسبيية المحوسبة	أقل من 3 سنوات	7	5.7
		من 3 إلى أقل من 6 سنوات	33	27.0
		من 6 إلى أقل من 10سنوات	38	31.2
		من 10 إلى أقل من 15سنة	32	26.2
		أكثر من 15 سنة	12	9.8
6	عدد الدورات التدريبية في نظم المعلومات المحاسبية	أقل من 3 دورات	39	32.0
		من دورة إلى 3 دورات	49	40.2
		من 4 إلى 6 دورات	16	13.1
		من 7 إلى 10 دورات	9	7.4
		أكثر من 10 دورات	9	7.4
الإجمالي لكل الخصائص		122	% 100	

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS).

يتبين من الجدول السابق رقم (3-3-1) ما يلي:

1. **المؤهل العلمي:** إنَّ حملة شهادة البكالوريوس يمثلون غالبية أفراد العينة الأمر الذي يشير إلى تمتع عينة الدراسة بالتأهيل العلمي المناسب الذي يمكنهم من فهم أسئلة الاستقصاء والإجابة عليها بشكل جيد، إذ بلغ عددهم (98) فرداً بما نسبته (80.3 %) من مجموع الأفراد المشاركين في عينة الدراسة بينما توزعت النسب الباقية على حملة المؤهلات الأخرى، وذلك يعكس واقع هيكل التوصيف الوظيفي في البنوك التجارية في الجمهورية اليمنية، وهذا شيء منطقي إذ يتم في الغالب استقطاب الموارد البشرية التي تحمل الشهادة الجامعية الأولى في الحد الأدنى للقيام بالأعمال المتخصصة، وهذا يدل على أن التأهيل العلمي للمستجيبين كان مناسباً، يوفر درجة مناسبة من المعرفة في مجال الدراسة، ويؤهلهم للإجابة على فقرات أداة الدراسة

(الاستقصاء)، وذلك يعزز من موثوقية التعويل على إجاباتهم عند التحليل، وأن غالبية حملة البكالوريوس تحقق بعض التجانس بنسبة (80.3 %) مما يؤدي لتقارب الآراء.

2. **التخصص العلمي:** نجد أنَّ معظم أفراد عينة الدراسة من تخصص المحاسبة إذ بلغ عددهم (72) فرداً وبنسبة بلغت (59 %)، وهذه النسبة تعطي ثقة ملائمة لأفراد العينة للإجابة على الاستقصاء وفق أسس علمية، بينما بقية التخصصات للمستجيبين لم تتعدى نسبة (41 %) ويعود ذلك لطبيعة الوظائف الإدارية لأفراد العينة والتي تتطلب تخصص المحاسبة أو التخصصات المقاربة منها كإدارة الأعمال والتمويل والاقتصاد، وهذا يوفر اطمئنان لفهمهم واستيعابهم لمحتويات الاستقصاء لصلتهم واطلاعهم على نظم المعلومات المحاسبية المحوسبة، وذلك يعزز من ملائمة المستجيبين وتأهيلهم للإجابة على أسئلة الدراسة بموضوعية وبقدر من المعرفة والدراية، مما يعطي الثقة والدقة في إجاباتهم.

3. **المسمى الوظيفي (الوظيفة الحالية):** إنَّ ما نسبته (23.8 %) من عينة الدراسة هم من المدققين الخارجيين لدى البنوك التجارية في اليمن بواقع (29) فرداً، كما أن ما نسبته (20.5 %) من عينة الدراسة هم من المدققين الداخليين لدى البنوك التجارية في اليمن بواقع (25) فرداً، وتوزعت باقي النسب بين مبرمجي النظم بنسبة (12.3 %)، ورؤساء أقسام الحسابات بنسبة (11.5 %)، ورؤساء أقسام الحاسوب بنسبة (8.2 %)، ومشغلي النظم بنسبة (7.4 %)، ووظائف أخرى بنسبة (16.3 %) تتمثل في مدراء إدارة المخاطر، والمدراء الماليين، ومفتشي البنك المركزي، وهذا يعكس تنوع المسميات الوظيفية بين المستجيبين، ويتضح أن أغلبية الباحثين هم من ذوي العلاقة المباشرة بموضوع الدراسة، لأنها موجهة للفئات ذات العلاقة بتقييم مخاطر أمن نظم المعلومات المحاسبية، وكون أغلبية الأفراد لهم علاقة بالمحاسبة والحاسوب ونظم المعلومات المحاسبية، فإنَّ ذلك يعزز من فهم ووعي المستجيبين لفقرات الاستقصاء، وإعطاء إجابات دقيقة وموضوعية.

4. **الفئة العمرية:** يتضح من الجدول السابق أنَّ الغالبية العظمى من أفراد عينة الدراسة كانت أعمارهم تتراوح بين (25) سنة إلى أقل من (45) سنة أي ما نسبته (84.4 %) من عينة الدراسة هذه النسبة تدل على أن من يشغل المناصب الهامة في نظم المعلومات المحاسبية المحوسبة، هم من فئة الشباب من الكوادر الكفوءة في المحاسبة والحاسوب، وقد يكون تفسير ذلك أن تلك النظم حديثة النشأة نسبياً، بالإضافة إلى أن معظم العاملين فيها من حديثي التخرج، فضلاً عن حاجة مثل هذه النظم لموارد بشرية تتمتع بعقلية شابة تتمكن من إدارة عملياته بكفاءة عالية، ويُعد ذلك مؤشراً على كفاءة وقدرة أفراد العينة في الإجابة على أسئلة الدراسة، بما يعزز الثقة في الإجابة على أسئلة الاستقصاء والوصول إلى حكم معقول على فرضيات الدراسة.

5. **عدد سنوات الخبرة في التعامل مع نظم المعلومات المحاسبية المحوسبة:** إن دقة الإجابة على فقرات الاستقصاء تعتمد بشكل كبير على الخبرة حيث يتضح أن ما نسبته (32.7 %) من أفراد العينة لا تتجاوز خبرتهم (6) سنوات، بينما (9.8 %) من أفراد عينة الدراسة يتمتعون بخبرة كبيرة تتجاوز (15) سنة، والباقي يشكلون (57.5 %) تتراوح خبرتهم بين (3) سنوات و(15) سنة، ويعود انخفاض الخبرات العالية والتي شكلت ما

نسبته (9.8 %)، لحدثة نظم المعلومات المحاسبية المحوسبة خاصة وأن البنوك التجارية التي تنتمي للقطاع الخاص⁽¹⁾ حديثة نسبياً، مما يشير إلى تمتع معظم أفراد عينة الدراسة بخبرات لا بأس بها في معرفة واقع نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية التي يعملون فيها، الأمر الذي يولد الاطمئنان والثقة إلى حد ما لدى الباحث على قدرة عينة الدراسة على استيعاب أسئلة الاستقصاء، والإجابة عليها بصورة مناسبة تعكس واقع خبرتهم في تلك البنوك الأمر الذي يضفي مزيداً من الثقة في دقة إجابات المشاركين، بناءً على تجربة وخبرة عملية، ويعطي لهذه الدراسة بعداً مهنيّاً وأكاديمياً مفيداً في تعزيز نتائجها في الواقع العملي.

6. **عدد الدورات التدريبية في نظم المعلومات المحاسبية المحوسبة:** أن ما نسبته (32 %) من أفراد العينة تلقوا أقل من (3) دورات تدريبية في نظم المعلومات المحاسبية المحوسبة، وقد يعزى ذلك لحدثة بعض البنوك، ولم يمتد على توظيف أفرادها فترة كافية لتلقي دورات تدريبية، وما نسبته (53.3 %) تلقوا دورات تدريبية تتراوح ما بين (1- 6) دورات، وذلك مؤشر على أن أفراد العينة يتمتعون بخبرة متوسطة، وذوي قدرة كافية لفهم كافة متغيرات هذه الدراسة، والإجابة على أسئلة الدراسة بدقة وموضوعية.

وبشكل عام يتضح للباحث مما ورد من تحليل خصائص أفراد عينة الدراسة أنّ غالبية أفراد العينة مؤهلون علمياً وعملياً، وتخصصاتهم لها علاقة مباشرة بنظم المعلومات المحاسبية، ومن ذوي الخبرة والكفاءة نوعاً ما في مجال عملهم، كما أنّ هناك اهتمام إلى حد ما بحضور الدورات التدريبية التأهيلية، ولاشك أنّ هذه المؤشرات المشتركة بين أفراد العينة، إضافة إلى المؤشرات الخاصة بكل فرد تؤهل أفراد العينة في تقديم إجابات مناسبة بما يخص تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة في ضوء إدراكهم ومعرفتهم لواقع نظم المعلومات المحاسبية المحوسبة، وهو ما يعطي إجاباتهم درجة عالية من المصداقية والثقة والموضوعية، يمكن الاعتماد عليها في تحليل البيانات واختبار الفرضيات وتعميم النتائج المبينة عليها.

3-3-2: تحليل البيانات المتعلقة بخصائص البنوك التجارية في الجمهورية اليمنية وطبيعة نظم

المعلومات المحاسبية في تلك البنوك:

ويلخص ذلك الجدول التالي:

جدول رقم (3-3-2) خصائص البنوك التجارية في الجمهورية اليمنية

وطبيعة نظم المعلومات المحاسبية المستخدمة في تلك البنوك حسب آراء أفراد العينة

م	المتغير	الفئة		التكرار (العدد) Frequency	النسبة المئوية % Percent %
1	اسم البنك	البنك	سنة التأسيس	14	11.5
		البنك اليمني للإنشاء والتعمير	1962		

(¹) تمثل البنوك التجارية العاملة في اليمن التابعة للقطاع الخاص، ما نسبته (72 %) تقريباً من مجتمع الدراسة، وعددها (12) بنكاً تجارياً من أصل (16) بنك تجاري .

م	المتغير	الفئة	التكرار (العدد) Frequency	النسبة المئوية % Percent %
		البنك الأهلي اليمني	6	4.9
		يوناييتد بنك ليمنتد	2	1.6
		البنك العربي	5	4.1
		بنك اليمن والكويت	10	8.2
		بنك اليمن الدولي	7	5.7
		مصرف الراجحي	2	1.6
		بنك التسليف التعاوني والزراعي	12	9.8
		البنك التجاري اليمني	6	4.9
		البنك الإسلامي اليمني	5	4.1
		بنك التضامن الإسلامي الدولي	14	11.5
		بنك سبأ الإسلامي	14	11.5
		بنك اليمن والخليج	7	5.7
		مصرف اليمن البحرين الشامل	10	8.2
		بنك قطر الوطني	5	4.1
		مصرف الكريمي للتمويل الأصغر	3	2.5
2	سنة تأسيس البنك	قبل عام 1970 م.	20	16.4
		بين عام 1971 م - وعام 1990 م.	38	31.2
		بعد عام 1990 م.	64	52.4
3	جنسية البنك	بنك يمني.	108	88.5
		بنك عربي غير يمني.	12	9.8
		بنك أجنبي.	2	1.6
4	ملكية البنك	شركة عامة	8	6.6
		خاص	88	72.1
		مختلط	26	21.3
5	الشركة المصممة لنظام المعلومات المستخدم	يمنية	5	4.1
		عربية	79	64.8
		أجنبية	38	31.1
6	نسبة عدد العاملين بنظام المعلومات المحاسبي لإجمالي عدد العاملين	أقل من 10	12	9.8
		من 10 إلى أقل من 20	12	9.8
		من 20 إلى أقل من 30	10	8.2
		من 30 إلى أقل من 40	16	13.1
		من 40 فأكثر	72	59.0

م	المتغير	الفئة	التكرار (العدد) Frequency	النسبة المئوية % Percent %
7	فترة استخدام الحاسوب في نظام المعلومات المحاسبي	أقل من 4 سنوات	15	12.3
		من 4 إلى أقل من 8 سنوات	27	22.1
		من 8 إلى أقل من 12 سنوات	28	23.0
		من 12 إلى أقل من 16 سنة	28	23.0
		أكثر من 16 سنة	24	19.7
8	وجود وتبعية إدارة مخاطر أمن نظم المعلومات المحاسبية	لمجلس الإدارة	20	16.4
		للإدارة التنفيذية	37	30.3
		للتدقيق الداخلي	12	9.8
		لإدارة أخرى	20	16.4
		لا يوجد إدارة لمخاطر أمن نظم المعلومات	33	27.1
9	الخدمة المصرفية الالكترونية الأكثر تعرضاً للخطر	موظفي النظام مباشرة	43	35.2
		الصراف الآلي	25	20.5
		الهاتف الخليوي	5	4.1
		شبكة الانترنت	45	36.9
		نقاط البيع	2	1.6
		خدمات أخرى	2	1.6
10	عدد أجهزة الحاسوب العاملة على شبكة نظام المعلومات المحاسبي	أقل من 20 جهاز	12	9.8
		من 20 إلى أقل من 40 جهاز	5	4.1
		من 40 إلى أقل من 60 جهاز	7	5.7
		من 60 إلى أقل من 80 جهاز	9	7.4
		من 80 حاسوب فأكثر	89	73.0
11	نوعية التشغيل في نظام المعلومات المحاسبي المستخدم	نظام تشغيل على أساس الدفعات	13	10.7
		نظام تشغيل فوري ومباشر	92	75.4
		نظام تشغيل موزع	15	12.3
		نظام آخر	2	1.6
12	مستوى ارتباط نظام المعلومات المحاسبي الخاص في البنك بشبكة الاتصال	شبكة معلومات محلية بين الأقسام (إنترنت)	20	16.4
		شبكة معلومات محلية بين الفروع (إكسترانت)	88	72.1
		شبكة المعلومات العالمية (الإنترنت)	14	11.5
		الإجمالي لكل الخصائص	122	100

• الجداول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS).

يتضح من الجدول السابق رقم (3-3-2) ما يلي:

1. **تسمية البنوك التجارية الذي تنتمي إليه عينة الدراسة:** كما هو واضح من خلال الجدول السابق أن (60.66 %) من عينة الدراسة بواقع (74) فرداً ينتمون إلى ستة بنوك تجارية هي: البنك اليمني للإنشاء والتعمير (14 فرداً)، وبنك التضامن الإسلامي (14 فرداً)، وبنك سبأ الإسلامي (14 فرداً)، وبنك التسليف التعاوني والزراعي (12 فرداً)، وبنك اليمن والكويت (10 أفراد)، ومصرف اليمن البحرين الشامل (10 أفراد)، بينما توزعت باقي أفراد عينة الدراسة على العشرة البنوك الأخرى العاملة في اليمن، وذلك مؤشر على أن البنوك الستة التي تركزت بها عينة الدراسة تملك معظم الإمكانات البشرية المؤهلة العاملة في البنوك التجارية في اليمن، خاصة أن اختيار عينة الدراسة كان وفق حجم متناسب مع الموارد البشرية المتخصصة لدى تلك البنوك، وهذا يعكس على تنوع المشاركين في الاستقصاء من حيث البنوك التي ينتمون إليها، حيث لم تستثني الدراسة أي بنك من البنوك العاملة في الجمهورية اليمنية.
2. **تأسيس البنك:** يلاحظ من الجدول أن (64) فرداً وبما نسبته (52.4 %) من أفراد العينة أفادوا بأن البنوك التجارية في اليمن قد تأسست بعد عام 1990 م، وبالتالي فهي حديثة العهد نسبياً ولا يزيد عمرها عن (23 عاماً)، وقد يكون مرد ذلك التوسع الذي شهدته البنوك التجارية في اليمن بعد تحقيق الوحدة اليمنية المباركة في 22 مايو 1990م، وما اكبتها من تطور في التشريعات والنظم، واهتمام الدولة ببناء اقتصاد جيد، وفتح مجالات مختلفة لتقدمها، وعليه فقد تأسست غالبية البنوك التجارية خلال تلك الفترة، وهذا يعكس حداثة النظم المختلفة المستخدمة، ومدى قدرتها على مواجهة متطلبات الانفتاح العالمي والتطور التقني.
3. **جنسية البنك:** أن ما نسبته (88.5 %) من أفراد العينة وبواقع (108) فرداً، أفادوا بأن البنوك التجارية في اليمن تعتبر بنوك وطنية، مما يعكس سيطرة البنوك التجارية اليمنية على السوق المصرفية في اليمن، وانخفاض حجم الاستثمارات الأجنبية مقارنة بالاستثمارات الوطنية في القطاع المصرفي اليمني.
4. **ملكية البنك:** يتبين من الجدول أعلاه أن عينة الدراسة حسب نوع الملكية تتوزع إلى (88) فرداً وبنسبة (72.1 %) من أفراد العينة ينتموا إلى (12) بنكاً تمثل القطاع الخاص حيث تُعدُّ شركات مُساهمة مغلقة، بينما (26) فرداً وبنسبة (21.3 %) من أفراد العينة ينتموا إلى بنكين هما البنك اليمني للإنشاء والتعمير، وبنك التسليف التعاوني والزراعي، ويُعدان من شركات القطاع المختلط، وقد شارك (8) أفراد وبنسبة (6.6 %) من أفراد العينة ينتموا إلى بنكين هما البنك اليمني الأهلي، وبنك الرافدين، ويُعدان من شركات القطاع العام المملوكة لحكومتَي اليمن والعراق على الترتيب، ويدل هذا التوزيع على تنامي دور القطاع الخاص أو بروز دوره في الاقتصاد الوطني، فضلاً عن دور الدولة في خصخصة كثير من الشركات التابعة للقطاع العام والمختلط، وذلك لما لهذا القطاع من أهمية في النهوض بالاقتصاد، وعليه ونظراً للاهتمام بهذا القطاع فإن الأمر يتطلب أن تكون هناك نظم محاسبية متطورة في تلك البنوك لتحافظ على بقاءها ونموها في سوق المنافسة.

5. الشركة المصممة لنظام المعلومات المستخدم: يلاحظ من الجدول أن (79) فرداً وبما نسبته (64.8 %) من أفراد العينة أفادوا بأن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في اليمن، مصممة من قبل شركات عربية، بينما أفاد (38) فرداً ونسبة (31.1 %) من العينة أن نظم المعلومات لديهم مصممة من قبل شركات أجنبية، وأخيراً أفاد (5) أفراد يمثلوا مصرف الكريمي للتمويل الأصغر، أن نظام المعلومات المحاسبي لديهم مصمم من شركة يمنية، وبالتالي فإن معظم نظم المعلومات المحاسبية لدى تلك البنوك، مصممة من قبل شركات عربية وبشكل خاص أردنية ولبنانية، حسب معرفة الباحث من خلال لقاءاته الشخصية مع مدراء الحاسوب وتكنولوجيا المعلومات في تلك البنوك.

6. نسبة عدد مشغلي نظام المعلومات المحاسبي لإجمالي عدد العاملين في البنك: أن ما نسبته (59 %) من أفراد العينة أفادوا بأن نسبة عدد مشغلي نظام المعلومات المحاسبي إلى عدد العاملين الإجمالي في البنك هي (40%) فأكثر، وذلك مرده لطبيعة الأنشطة المصرفية التي يمارسها البنك والذي يعتبر نظام المعلومات المحاسبي العمود الفقري والأداة الرئيسية لإنجازها، فالمنشآت الكبيرة تحتاج للمزيد من الموارد البشرية والتكنولوجية لتنفيذ نظم أمنية عالية الجودة مقارنة مع المنشآت الصغيرة.

7. فترة استخدام الحاسوب في نظام المعلومات المحاسبي: يلاحظ أن ما نسبته (80.4 %) من أفراد العينة قد أفادوا بأن البنوك التجارية في الجمهورية اليمنية لم يمض على استخدامها لتكنولوجيا الحاسوب في تشغيل نظمها المحاسبية أكثر من (16) سنة، وهذا تأكيد لما سبق القول بحدثة النظم المختلفة لديها في تشغيل نظم المعلومات المحاسبية، ولعل ذلك يشير إلى أن التكنولوجيا تلقى اهتماماً لدى أفراد العينة وحرصهم على إدخال التقنيات الحديثة اللازمة لعمل النظام كالأجهزة والشبكات الحديثة والبرمجيات المتطورة، فطبيعة العمل المصرفي وأنشطته المختلفة تقتضي مواكبة التطورات المتسارعة، فهي العنصر الحاسم لنجاح نظم المعلومات المحاسبية، وتشكل جزءاً هاماً وحيوياً من تركيبة النظام، وأي خلل بها يؤدي إلى خلل في النظام كله.

8. وجود وتبعية إدارة مخاطر أمن نظم المعلومات المحاسبية: أفاد (27.1 %) من أفراد عينة الدراسة بعدم وجود إدارة لمخاطر أمن نظم المعلومات، ومن ضمنها نظم المعلومات المحاسبية، بينما يرى (56.5 %) من أفراد عينة الدراسة أن إدارة مخاطر أمن نظم المعلومات المحاسبية تتبع الإدارة التنفيذية أو التدقيق الداخلي، أو أي إدارة أخرى، ولم يتجاوز تبعية إدارة مخاطر أمن نظم المعلومات لمجلس الإدارة نسبة (16.4 %) حسب رأي أفراد العينة، وذلك مؤشر على عدم إيلاء إدارة البنوك التجارية في اليمن الأهمية اللازمة لإدارة مخاطر أمن نظم المعلومات المحاسبية، وما يترتب على ذلك من حدوث مخاطر كان من الممكن تلافيها.

9. الخدمة المصرفية الالكترونية الأكثر تعرضاً للخطر: يرى (36.9 %) من أفراد عينة الدراسة أن الخدمات المصرفية الأكثر تعرضاً للمخاطر مصدرها شبكة الإنترنت، بينما أفاد (35.2 %) من أفراد عينة الدراسة أن الخدمات المصرفية الأكثر تعرضاً للمخاطر مصدرها الأفراد العاملين في النظام وبشكل مباشر، وقد يُعزى ذلك إلى حداثة ربط نظم المعلومات المحاسبية بشبكات الاتصال، ومعظم العملاء لديهم ثقة منخفضة بإجراء المعاملات

المالية عبر الانترنت بسبب الخوف من اختراق الشبكة وعدم وجود اطار قانوني منظم للعمليات المصرفية عبر الانترنت، ووجود كوادر بشرية غير مؤهلة تأهيل كامل للتعامل مع التطور التقني التي تشهده تلك النظم، كما أنَّ التنوع الكبير للخدمات المصرفية في هذه البنوك يبرر ضرورة تطبيق نظم محاسبية تساعد في إنتاج معلومات دقيقة وفي الوقت المناسب.

10. عدد أجهزة الحاسوب العاملة على شبكة نظام المعلومات المحاسبي: أفاد (73 %) من أفراد عينة الدراسة أن

عدد أجهزة الحاسوب العاملة على شبكة نظام المعلومات المحاسبي أكثر من (80) جهاز، وفي رأي الباحث قد يعود ذلك بصورة أساسية إلى أن أغلب البنوك التجارية اليمنية توجهت إلى استخدام الحاسوب وبرمجياته من أجل تحقيق مستوى عالي من الدقة والسرعة في تنفيذ مختلف العمليات، بالإضافة إلى مزايا التكنولوجيا في تحسين الاتصال بين الوحدات المختلفة داخل دوائر نظم المعلومات المحاسبية لتلك البنوك، بينما يرى (27 %) من أفراد عينة الدراسة أن نظم المعلومات المحاسبية لدى البنوك التي يعملون فيها ترتبط بأجهزة الحاسوب يقل عددها عن (80) حاسوب، وذلك مؤثر إلى أن معظم نظم المعلومات المحاسبية لدى البنوك التجارية في الجمهورية اليمنية لديها بنية تحتية متوسطة إلى حد ما، وتمتلك قدرات لا بأس بها، ولكنها ليست كافية بحيث تؤهلها لأداء نشاطها بالشكل المرغوب.

11. نوعية التشغيل في نظام المعلومات المحاسبي المستخدم: يلاحظ أن معظم أفراد العينة وبنسبة (75.4 %) أفادوا

بأن نظم المعلومات المحاسبية لدى البنوك التجارية التي يعملوا بها يتم تشغيلها على أساس نظام التشغيل الفوري والمباشر، وهذا يدل على أنَّ البنوك التجارية في اليمن تواكب التطورات التكنولوجية فيما يتعلق بنوعية تشغيل نظم المعلومات المحاسبية لديها، وقد يعزى ذلك إلى توجه معظم تلك البنوك للتوسع في بعض الخدمات المصرفية الإلكترونية والتي تتطلب ذلك النوع من نظم التشغيل.

12. مستوى ارتباط نظام المعلومات المحاسبي الخاص في البنك بشبكات الاتصال: وأخيراً فيما يتعلق بمستوى

ارتباط نظم المعلومات بشبكات الاتصال، نلاحظ أن الغالبية من أفراد العينة وبنسبة (72.1 %) أفادوا بأن نظم المعلومات المحاسبية لدى البنوك التجارية العاملة في اليمن ترتبط بشبكة معلومات محلية (إكسترانت) تربط مراكزها الرئيسية بفروعها المختلفة على مستوى الجمهورية، بينما نجد أن (16.4 %) من العينة ترتبط نظم المعلومات المحاسبية من خلال شبكة اتصال محلية تربط بين الأقسام المختلفة داخل البنك فقط (إنترانت)، والملاحظ أنه ولم نجد سوى (11.5 %) من عينة الدراسة ترتبط نظم المعلومات المحاسبية لديهم بشبكة المعلومات العالمية (إنترنت)، وبذلك فإنه يمكن القول أن تلك البنوك تملك بعض الإمكانيات الكافية والقادرة على تطوير نظمها وآليات عملها، حيث أنَّ هناك اهتمام من قبل البنوك التجارية العاملة في اليمن بربط نظم المعلومات المحاسبية بشبكات اتصال محلية، ولكن للأسف لم يجد الباحث نفس الاهتمام فيما يخص ربط نظم المعلومات المحاسبية بشبكة المعلومات العالمية (الإنترنت)، باستثناء البنوك العربية والأجنبية، وهذا يعكس بوضوح حالة متواضعة في استخدام شبكات الاتصال لربط نظم المعلومات المحاسبية، وقد يُعزى ذلك إلى عدم إيلاء البنوك التجارية المحلية في اليمن أهمية للربط بينها وبين البنوك الإقليمية، وهذا ما يجب أخذه في الاعتبار في ظل العولمة وما تفرضه

من ضرورة التكتلات، وبالتالي فإن تلك البنوك بحاجة إلى تطوير نظمها المحاسبية، من خلال ربطها بوسائل اتصال حديثة ومتطورة لكي تحافظ على مستواها التنافسي محلياً وإقليمياً وعالمياً، وهذا يعكس واقع البنوك التجارية في الجمهورية اليمنية التي غالباً ما لا تكون متصلة بمثل هذا النوع من وسائل الاتصال الحديثة، وربما كانت هذه النتيجة عاملاً مهماً في تحديد أنواع المخاطر التي تتعرض لها نظم المعلومات المحوسبة في البنوك المختلفة، حيث أن هناك مخاطر تظهر فقط في البنوك المتصلة بشبكة الإنترنت، لأن مصدرها هو الاتصال بهذه الشبكة.

تحليل بيانات محاور الدراسة الرئيسية

وبهدف تحليل نتائج إجابات عينة الدراسة لأخذ صورة أولية عن تقييمهم لمخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية العاملة في الجمهورية اليمنية، والتي يتم من خلالها الوقوف على أهمية كل من المتغيرات المرشحة للتحليل التي وردت في المحاور التي تناولها الاستقصاء، ومدى توافق الآراء تجاه كل من هذه المتغيرات فقد تم إجراء استعراض عام لنتائج التحليل الوصفي باعتماد المتوسط الحسابي والأهمية النسبية لمتوسط تلك المتغيرات، وكذلك الانحراف المعياري ومعامل الاختلاف لمعرفة درجة توافق أو تباين الآراء بين أفراد عينة الدراسة تجاه كل متغيرات الدراسة وكانت حصيلة التحليل على النحو الآتي:

3-3-3: تحليل البيانات المتعلقة بالمخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة

وفقاً لفرضيات الدراسة ونموذجها يمثل هذا المتغير التابع للدراسة، والهدف من قياسه معرفة مدى حدوث تلك المخاطر لدى البنوك التجارية في الجمهورية اليمنية، وقد تم قياس هذا المتغير من خلال المحاور الأول من محاور الجزء الثالث للاستقصاء والذي تضمن (30) فقره تبرز المخاطر المختلفة التي تهدد أمن نظم المعلومات المحاسبية المحوسبة، حيث قد قام الباحث باستخدام التحليل الوصفي تمهيداً لاختبار الفرضية الأولى، فقد استخرج المتوسطات الحسابية والانحرافات المعيارية ومعاملات الاختلاف والأهمية النسبية ومستوى الخطر ورتبته، وفقاً لآراء أفراد عينة الدراسة حول مضمون كل فقرة من تلك الفقرات التي تقيس تلك المخاطر والجدول التالي يلخص نتائج التحليل الوصفي للفقرات المتعلقة بذلك:

جدول رقم (3-3-3) الإحصاءات الوصفية على مستوى الفقرات والمتغيرات الرئيسية

المتعلقة بحدوث المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة

رقم الفقرة	مخاطر أمن نظم المعلومات المحاسبية	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى الخطر	الترتيب التنازلي
1	قيام بعض موظفي نظم المعلومات باستغلال صلاحياتهم في هذه النظم في خدمة أغراضهم الشخصية بما يتعارض والسياسات الموضوعية من قبل الإدارة والمختصين.	2.229	0.831	37.26	44.6	منخفض	17

رقم الفقرة	مخاطر أمن نظم المعلومات الحاسوبية	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى الخطر	الترتيب التنازلي
2	انتحال صلاحيات شخص مخول بأي طريقة من الطرق نتيجة إهمال المستخدم، والثقة المتبادلة بين الموظفين التي تجعلهم يستخدمون كلمات السر فيما بينهم.	2.754	0.696	25.3	55.0	متوسط	9
2-1	مخاطر أمن الأفراد العاملين في النظم.	2.492	0.671	26.9	49.8	منخفض	الثاني
3	حدوث تلف جزئي أو تدمير كلي لأجهزة ومعدات النظام المادية.	2.000	0.813	40.6	40.0	منخفض	25
4	حدوث أعطال في المكونات المادية والبرمجية للنظام.	2.713	0.732	27.0	54.2	متوسط	11
4-3	مخاطر الأمن المادي لنظم المعلومات.	2.357	0.631	21.7	47.2	منخفض	السادس
5	الوصول البرمجي غير المصرح به إلى برامج النظام والملفات في قاعدة البيانات بواسطة أفراد من داخل البنك بقصد الإضرار والتخريب.	2.024	0.807	40.0	40.4	منخفض	23
6	الوصول البرمجي، غير المصرح به إلى برامج النظام والملفات في قاعدة البيانات بواسطة أفراد أو جهات من خارج البنك، لإنجاز عمليات (تعديل/تدمير/كشف/نسخ وسرقة/استخدام) بطريقة غير مشروعة.	1.827	0.746	40.8	36.6	منخفض	28
7	تلف بعض ملفات البيانات والبرامج ونظم التشغيل نتيجة تعرض قاعدة البيانات لنظام المعلومات الحاسوبي المحسوب للإصابة بالبرامج الخبيثة مثل (الفيروسات، والديدان، وبرامج التجسس).	3.582	0.860	24.0	71.6	مرتفع	1
7-5	مخاطر أمن الوصول البرمجي لقاعدة بيانات نظم المعلومات الحاسوبية.	2.478	0.538	21.7	49.6	منخفض	الثالث
8	ضياع أو سرقة وسائط تخزين البيانات والبرامج الاحتياطية غير المتصلة بقاعدة بيانات نظام المعلومات الحاسوبي المحسوب.	2.205	0.832	37.8	44.0	منخفض	18
9	الوصول غير المصرح به للبيانات والبرامج المخزنة في وسائط غير متصلة بنظام المعلومات الحاسوبي.	2.107	0.713	33.8	42.2	منخفض	21
9-8	مخاطر أمن النسخ في وسائط غير متصلة بقاعدة البيانات.	2.156	0.603	27.9	43.2	منخفض	التاسع
10	الحذف أو التعديل المتعمد لمصادر بيانات مدخلات صحيحة بواسطة الأفراد العاملين في نظام المعلومات الحاسوبي.	2.008	0.886	44.0	40.2	منخفض	24
11	الحذف أو التعديل غير المتعمد لمصادر بيانات مدخلات صحيحة بواسطة الأفراد العاملين في نظام المعلومات الحاسوبي.	3.262	0.811	24.9	65.2	متوسط	4
12	الإدخال المتعمد لبيانات غير سليمة أو مكررة من قبل العاملين في نظام المعلومات الحاسوبي، للقيام بعمليات غير مصرح بها.	2.303	0.726	31.6	46.0	منخفض	15
13	الإدخال غير المتعمد لبيانات غير سليمة أو مكررة من قبل العاملين في نظام المعلومات الحاسوبي، نتيجة السهو وعدم المعرفة.	3.189	0.903	28.3	63.8	متوسط	5

رقم الفقرة	مخاطر أمن نظم المعلومات المحاسبية	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى الخطر	الترتيب التنازلي
14	التأخير المقصود في إدخال بعض البيانات بواسطة العاملين في نظام المعلومات المحاسبي.	2.771	0.831	30.0	55.4	متوسط	7
15	التأخير غير المقصود في إدخال بعض البيانات بواسطة العاملين في نظام المعلومات المحاسبي.	3.443	0.692	20.1	68.8	مرتفع	3
15-10	مخاطر تهدد أمن مدخلات النظم.	2.829	0.462	16.3	56.6	متوسط	الأول
16	إهدار وسرقة وقت تشغيل بعض أجهزة الحاسوب المستخدمة في نظام المعلومات المحاسبي باستغلالها في الأغراض الشخصية.	2.746	0.932	33.9	55.0	متوسط	10
17	تعديل أو حذف البيانات بطريقة مقصودة نتيجة حدوث احتيال وغش من قبل مستخدمي نظام المعلومات المحاسبي أثناء عمليات التشغيل.	2.131	0.760	35.7	42.6	منخفض	20
18	تعديل أو حذف البيانات بطريقة غير مقصودة نتيجة حدوث أخطاء من قبل مستخدمي نظام المعلومات المحاسبي أثناء عمليات التشغيل.	2.836	0.856	30.1	56.8	متوسط	6
19	حدوث عمليات تشغيلية غير مكتملة لبيانات محاسبية تم إدخالها.	2.189	0.672	30.7	43.8	منخفض	19
19-16	مخاطر أمن عمليات تشغيل النظم.	2.475	0.505	20.4	49.6	منخفض	الرابع
20	حذف وإخفاء بنود معينة من مخرجات نظام المعلومات المحاسبي وإنتاج مخرجات مظلة غير سليمة.	1.951	0.870	44.6	39.0	منخفض	27
21	الكشف غير المخول به للمعلومات المحاسبية أثناء عرضها على الشاشات أو طباعتها على الورق أو أثناء التخلص منها بعد استخدامها	3.484	0.794	22.8	69.8	مرتفع	2
22	توجيه وتوزيع وتسليم بعض البيانات والمعلومات المحاسبية لأشخاص غير مخولين باستلام نسخة منها أو لا تتوفر فيهم الأمانة.	2.516	0.784	31.1	50.4	منخفض	14
23	سرقة وسوء استخدام مخرجات نظام (المعلومات المحاسبية) من قبل القائمين على النظام واستغلالها في أغراض شخصية.	1.812	0.795	44.0	36.2	منخفض	30
23-20	مخاطر أمن مخرجات النظم.	2.441	0.538	22.0	48.8	منخفض	الخامس
24	انقطاع وتوقف تدفق البيانات والمعلومات المحولة إلكترونياً عبر شبكات الحاسوب من المركز الرئيسي للبنك إلى الفروع أو العكس.	2.771	0.713	25.7	55.4	متوسط	8
25	اعتراض وصول البيانات المرسلة عبر الشبكات من أجهزة الخوادم لأجهزة المستخدمين، وتعرضها أحياناً للكشف أو التعديل، أو السرقة.	2.303	0.870	37.8	46.0	منخفض	16
26	اختراق مواقع الويب الخاص ببيانات البنك والتجسس على خطوط الاتصالات الخاصة بنقل البيانات.	2.082	0.984	47.3	41.6	منخفض	22
27	إنكار بعض الأطراف المتعاملة مع البنك للبيانات والمعلومات المحاسبية المتبادلة إلكترونياً.	1.828	0.789	43.1	36.6	منخفض	29

رقم الفقرة	مخاطر أمن نظم المعلومات المحاسبية	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى الخطر	الترتيب التنازلي
28	حدوث أخطاء معينة غير مقصودة أثناء نقل البيانات كإرسال بيانات أو معلومات عن طريق الخطأ إلى موقع آخر.	2.623	0.875	33.4	52.4	متوسط	13
28-24	مخاطر أمن تبادل البيانات عبر شبكات النظم.	2.321	0.597	25.7	46.4	منخفض	السابع
29	يتم إجراء تغييرات للنظام وبرامجه بطريقة غير مسموح بها، من قبل أشخاص غير مخولين بذلك، للقيام بعمليات تلاعب واحتيال لاحقة.	1.967	0.978	49.6	39.4	منخفض	26
30	حدوث أخطاء في عدم استكمال التعديلات المطلوبة أثناء عمليات التعديل والتطوير.	2.672	0.866	32.4	53.4	متوسط	12
30-29	مخاطر أمن تعديل وتطوير نظم المعلومات.	2.320	0.784	33.8	46.4	منخفض	الثامن
30-1	المتوسط العام للمخاطر ككل	2.430	0.413	17.0	48.6	منخفض	

• مستوى شدة الخطر حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 ~ 2.59) منخفض، (2.60 ~ 3.39) متوسط، (3.40 ~ 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

تشير النتائج الواردة في الجدول السابق رقم (3-3-3) إلى ما يلي:

■ إن المتوسط الحسابي العام لتقديرات أفراد العينة ككل عن كافة الفقرات والمتغيرات الرئيسية الخاصة بقياس مدى حدوث مخاطر أمن نظم المعلومات المحاسبية المحسوبة لدى البنوك التجارية في الجمهورية اليمنية قد بلغ (2.430) درجة من أصل (5) درجات، وهي قيمة أقل من قيمة المتوسط الحسابي المعياري في هذه الدراسة والبالغة (3) درجات، وبلغت أهمية الموافقة النسبية على حدوث تلك المخاطر (48.6%) والذي تقابل مستوى الخطر المنخفض، وهي أقل من نسبة المتوسط الحسابي المعتمدة في هذه الدراسة والبالغة (60%)، وبلغت قيمة الانحراف المعياري الكلي عن المتوسط الحسابي (0.413) فقط، مما يدل على تقارب الإجابات وأنها تتمحور حول المتوسط الحسابي، ويؤكد ذلك أن معامل الاختلاف للمخاطر ككل لم يتجاوز (17%)، وهي تمثل نسبة ضئيلة وتدل على عدم تشتت واختلاف البيانات عن المتوسط الحسابي، وأن هناك تقارب وانسجام إلى حد كبير بين الأفراد المستجيبين في الإجابة عن فقرات هذا المجال الخاص بقياس مدى حدوث مخاطر أمن نظم المعلومات المحاسبية المحسوبة، وأن حدوث تلك المخاطر بشكل عام منخفضة، أي أن غالبية أفراد عينة الدراسة رأوا بأن المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحسوبة ككل هي منخفضة الحدوث لدى البنوك التجارية العاملة في الجمهورية اليمنية، ويؤكد ذلك قيم المتوسطات الحسابية لمعظم الفقرات والمحاور الخاصة بذلك المحور.

■ إن قيم الانحراف المعياري لجميع الفقرات قد بلغت أقل من الواحد الصحيح، وبلغت لجميعها (0.413) فقط، وهذا يؤكد أن ردود الأفراد المستقصى منهم كانت متفقة مع معظم أفراد العينة، ويدل على أن آراء أفراد العينة بشأن كل فقرة من تلك الفقرات كانت متقاربة إلى حد ما، ويؤكد ذلك أن قيم معامل الاختلاف لتلك الفقرات قد تراوحت بين (20.1% ~ 49.6%)، وهي قيم متوسطة نسبياً تعكس مدى التقارب في وجهات نظر المستجيبين، ومدى تشتت إجاباتهم على كل فقرة منها.

■ إن اتجاهات عينة الدراسة كانت موافقة على حدوث المخاطر الواردة في الفقرات (7، 21، 15، 11، 13) وبشكل جوهري وملحوس وفقاً للترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات التي كانت أكبر من المتوسط الحسابي المعتمد حسب المقياس المستخدم في هذه الدراسة وهو (3) درجات، وقد تراوح المتوسط الحسابي لفقرات محور المخاطر ككل بين (3.189~3.582)، ومعامل الاختلاف لتلك الفقرات لم يتجاوز (28.3%) مما يدل على عدم تشتت الاجابات حول المتوسط الحسابي، وبالتالي فإنَّ المستجيبين يُجمعون بنسبة كبيرة على حدوث تلك المخاطر لدى البنوك التجارية العاملة في الجمهورية اليمنية، ولكن في بقية الفقرات أتت إجابات عينة الدراسة رافضة لحدوث تلك المخاطر بشكل جوهري وملحوس لأن قيم المتوسط الحسابي لتلك الفقرات كانت أقل من المقياس المستخدم في هذه الدراسة والبالغ (3) درجات.

■ كان مستوى حدوث المخاطر مرتفع في ثلاث فقرات فقط هي (7، 21، 15)، من أصل ثلاثين فقرة، والتي يزيد المتوسط الحسابي لكل منها عن (3.4) أي أنه يوجد موافقة على حدوث تلك المخاطر بدرجة مرتفعة، فقد تراوح المتوسط الحسابي لتلك الفقرات بين (3.443~3.582)، ويلاحظ أن الخطر الوارد في الفقرة رقم (7) والذي يتعلق بخطر تلف بعض ملفات البيانات والبرامج ونظم التشغيل نتيجة تعرض قاعدة البيانات لنظام المعلومات المحاسبي المحسوب للإصابة بالبرامج الخبيثة مثل (الفيروسات، والديدان، وبرامج التجسس)، قد احتل المرتبة الأولى حيث نال أعلى متوسط حسابي بلغ (3.582) وبأهمية نسبية بالموافقة على حدوث ذلك الخطر بلغ (71.6%)، وبانحراف معياري (0.860)، ومعامل اختلاف (24%)، وهذا يؤكد أي أن معظم أفراد عينة الدراسة المستقصى منهم كانوا متفقين على أن ذلك الخطر مرتفع ونسبة (71.6%)، وهذا يشير إلى أن أهم المخاطر التي يعاني منها أمن نظم المعلومات المحاسبية لدى البنوك التجارية في الجمهورية اليمنية تتمثل في عدة مخاطر رئيسية منها خطر محو وإتلاف البيانات وملفات البرامج وأنظمة التشغيل الناتجة عن فيروسات الحاسب، يليه خطر الكشف غير المخول به للمعلومات المحاسبية أثناء عرضها على الشاشات أو طباعتها على الورق أو أثناء التخلص منها بعد استخدامها، يليه خطر التأخير غير المقصود في إدخال بعض البيانات بواسطة العاملين في نظام المعلومات المحاسبي، ولعل ذلك يُشير إلى أن ما تعانيه البنوك التجارية في الجمهورية اليمنية من مخاطر قد يرجع إلى المخاطر الناتجة عن فيروسات الحاسب، ومخاطر الكشف غير المخول، والتأخير غير المقصود في إدخال البيانات ولعل ذلك يعود إلى عدم تحديث برامج مكافحة الفيروسات لمواجهة الفيروسات الحديثة بالإضافة إلى ضعف تدريب وتوعية الأفراد العاملين على تلك النظم حول تلك المخاطر، وفي رأي الباحث أن هذا أمر ينبغي تداركه، فتعزيز مهارات هؤلاء الأفراد من خلال التدريب والتأهيل العلمي مطلب رئيس يجب الاعتناء به بدرجة كبيرة ليصبحوا قادرين على التعامل مع المخاطر الجديدة والمتغيرة.

■ كان مستوى المخاطر متوسط في عشر فقرات هي (11، 13، 18، 14، 24، 2، 16، 4، 30، 28)، والذي كان ترتيبها من (4) إلى (13) وفقاً للترتيب التنازلي لقيم المتوسط الحسابي، حيث تراوح المتوسط الحسابي لتلك الفقرات بين (2.623~3.262)، والذي يعكس الأهمية النسبية لحدوث تلك المخاطر حيث تراوح بين (52.4%~65.2%) وبمعامل اختلاف لتلك الفقرات لم يتجاوز (33.9%)، وكان أهم تلك المخاطر هو خطر

الحذف أو التعديل غير المتعمد لمصادر بيانات مدخلات صحيحة بواسطة الأفراد العاملين في نظام المعلومات المحاسبي، والذي جاء في المرتبة الرابعة على مستوى المخاطر ككل، حيث بلغ متوسطه الحسابي (3.262)، ومعامل الاختلاف (24.9%)، وهو ما يدل على انسجام وتقارب كبير بين آراء أفراد العينة على أن ذلك الخطر الذي يهدد أمن نظم المعلومات المحاسبية يحدث بنسبة (65.2%)، وبمستوى متوسط، بينما خطر الإدخال غير المتعمد لبيانات غير سليمة أو مكررة من قبل العاملين في نظام المعلومات المحاسبي، نتيجة السهو وعدم المعرفة جاء في المرتبة الخامسة ومستوى حدوث ذلك الخطر متوسط، وبنسبة موافقة على حدوثه بلغت (63.8%)، وبمتوسط حسابي بلغ (3.189)، ومعامل الاختلاف لا يزيد عن (28.3%)، وهو ما يدل على انسجام وتقارب كبير بين آراء أفراد العينة الذين أفادوا بأن ذلك الخطر الذي يهدد أمن نظم المعلومات المحاسبية يحدث بنسبة (63.8%) وبمستوى متوسط، ويلاحظ الباحث أن حدوث الخطرين السابقين كان مصدره الأفراد العاملين وبطريقة غير متعمدة نتيجة ضعف الخبرة والمهارة وهو ما يستوجب من البنوك الاهتمام بمستوى التدريب والتأهيل والتوعية المستمرة لأولئك الأفراد، بما يؤدي إلى تلاشي نقاط الضعف الموجودة لديهم، وبالتالي التخفيف من تلك المخاطر إلى أدنى درجة ممكنة.

■ كان مستوى المخاطر الواردة في باقي الفقرات منخفضاً، وكان ترتيبها من (14) إلى (30)، حيث تراوح المتوسط الحسابي لتلك المخاطر بين (1.812~2.516)، والذي يقابله الأهمية النسبية لدرجة حدوث تلك المخاطر بين (36.2%~50.3%)، وهذا يعني أن معظم تلك المخاطر كانت منخفضة الحدوث، ويلاحظ أن الخطر الوارد في الفقرة (23) والذي يتعلق بسرقة وسوء استخدام مخرجات النظام (المعلومات المحاسبية) من قبل القائمين على النظام واستغلالها في أغراض شخصية، قد جاء في المرتبة الأخيرة على مستوى المخاطر ككل، وبمتوسط حسابي بلغ (1.812) درجة، وبأهمية نسبية لحدوث ذلك الخطر لم تتجاوز (36.2%)، وانحراف معياري (0.795) فقط، ومعامل اختلاف قدره (44%)، مما يعكس وجود اختلاف إلى حد ما بين آراء المستجيبين حول تلك الفقرة، ونتيجة لذلك خلص الباحث إلى أن سرقة أو سوء استخدام مخرجات النظام من قبل القائمين على النظام واستغلالها في أغراض شخصية نادراً ما تحدث في البنوك التجارية في الجمهورية اليمنية، وأن مستوى حدوث ذلك الخطر في تلك البنوك منخفض جداً، ولعل ذلك يعود إلى مستوى التزام أولئك الأفراد بالأمانة المهنية، كما أن تعيينهم في تلك البنوك غالباً ما يكون مبني على إجراءات صارمة، حيث يتم اختيار موظفي نظم المعلومات المحاسبية بحرص شديد وإجراء تحريات عنهم وعن ماضيهم الوظيفي، والحرص على أن يكونوا من ذوي الثقة والأمانة ويعملون لمصلحة البنك، وعدم إعطاء الموظف حديث التعيين صلاحيات عالية لاستخدام النظام، وبالتالي فإن الموظف لا يقدم على ارتكاب هذا الأمر وخاصة أن هذا الخطر لا يتم إلا بشكل متعمد، كما يعزى انخفاض ذلك الخطر إلى عدم ربط أغلبية نظم المعلومات المحاسبية لدى تلك البنوك بالإنترنت، الأمر الذي يحول دون حدوث خطر سرقة مخرجات تلك النظم عبر شبكة الاتصال العالمية.

■ ويمكن القول بصفة إجمالية بأن إجابات أفراد العينة حول مدى حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التي يعملون بها، كانت غالبيتها ترى بأنها لا تحدث بشكل عام، فقد حصلت (17) فقرة

على درجة موافقة منخفضة، في مقابل حصول (10) فقرات على درجة موافقة متوسطة، وحصول (3) فقرات على درجة موافقة مرتفعة، مما يشير إلى انخفاض تلك المخاطر بشكل عام ولكن لا يعني ذلك عدم وجود مخاطر تهدد أمن نظم المعلومات المحاسبية فعلى مستوى الفقرات الجزئية كانت هناك موافقة لبعض الفقرات على حدوث بعض تلك المخاطر وهنا يجب على هذه البنوك مواجهة تلك المخاطر بشتى الإجراءات والوسائل، وفي هذا الصدد يرى الباحث بأن مخاطر أمن نظم المعلومات المحاسبية تختلف تبعاً لدرجة تطور وتعقيد عمليات البنوك حيث أن معظم البنوك العاملة في الجمهورية اليمنية متقاربة في درجة تطور وتعقيد أنشطتها وانتشارها الجغرافي وبالتالي فإن المخاطر التي تواجه نظمها ليست في نفس مستوى واتساع المخاطر التي تواجه النظم المستخدمة لدى البنوك العالمية ذات الانتشار الدولي الواسع والتي تتميز بدرجة عالية من التطور والتعقيد في أنشطتها وعملياتها.

- وبالنظر إلى المتغيرات الرئيسية لمخاطر أمن نظم المعلومات المحاسبية المحوسبة، وبناءً على المتوسط الحسابي للمخاطر، والأهمية النسبية لها، تم ترتيب المخاطر تنازلياً حسب درجة حدوثها كما بالجدول الآتي:

جدول رقم (3-3-4) الإحصاءات الوصفية للمتغيرات الرئيسية المتعلقة

بحدوث المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة مرتبة تنازلياً حسب الأهمية النسبية⁽¹⁾

رتبة الخطر	المتغيرات الرئيسية للمخاطر	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى شدة الخطر
1	مخاطر تهدد أمن عمليات المدخلات.	2.829	0.462	16.3	56.6	متوسط
2	مخاطر أمن الأفراد العاملين في النظم.	2.492	0.671	26.9	49.8	منخفض
3	مخاطر أمن الوصول البرمجي لقاعدة بيانات نظم المعلومات.	2.478	0.538	21.7	49.6	منخفض
4	مخاطر أمن عمليات تشغيل نظم المعلومات المحاسبية.	2.475	0.505	20.4	49.6	منخفض
5	مخاطر أمن مخرجات نظم المعلومات المحاسبية المحوسبة.	2.441	0.538	22.0	48.8	منخفض
6	مخاطر الأمن المادي لنظم المعلومات.	2.357	0.631	21.7	47.2	منخفض
7	مخاطر أمن تبادل البيانات عبر شبكات نظم المعلومات.	2.321	0.597	25.7	46.4	منخفض
8	مخاطر أمن تعديل وتطوير نظم المعلومات المحاسبية.	2.320	0.784	33.8	46.4	منخفض
9	مخاطر أمن النسخ في وسائط غير متصلة بقاعدة البيانات.	2.156	0.603	27.9	43.2	منخفض
الإجمالي العام		2.430	0.413	17.0	48.6	منخفض

• مستوى شدة الخطر حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 – 2.59) منخفض، (2.60 – 3.39) متوسط، (3.40 – 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

(1) الجدول من إعداد الباحث اعتماداً على مخرجات التحليل الإحصائي SPSS.

ومن الجدول السابق يتضح ما يلي:

- إن قيم المتوسط الحسابي لكل خطر من مخاطر أمن نظم المعلومات المحاسبية المحوسبة على مستوى المتغيرات الرئيسية كانت أقل من المتوسط الحسابي المعياري المعتمد وفق المقياس المستخدم في هذه الدراسة وهو (3) درجات، حيث تراوحت قيمة المتوسط الحسابي لتلك المخاطر بين (2.156) بنسبة (43.2%)، وبمستوى منخفض للمخاطر التي تهدد أمن النسخ في وسائط غير متصلة بقاعدة البيانات، وبين (2.829) بنسبة (56.6%)، وبمستوى متوسط للمخاطر التي تهدد أمن عمليات مدخلات نظم المعلومات المحاسبية وتدل هذه النتيجة على أنَّ المستجيبين يُجمعون بنسبة كبيرة أن حدوث تلك المخاطر لدى البنوك التجارية العاملة في الجمهورية اليمنية كانت منخفضة باستثناء مخاطر المدخلات فكان مستوى حدوثها متوسط.
- بالنظر إلى ترتيب مخاطر أمن نظم المعلومات المحاسبية المحوسبة يلاحظ أن المخاطر التي تهدد أمن عمليات مدخلات نظم المعلومات المحاسبية، قد احتلت المرتبة الأولى وبمستوى متوسط من حيث شدة حدوثها، حيث حصلت على أعلى متوسط حسابي، والذي بلغت قيمته (2.829) درجة، وبمعامل اختلاف لا يتجاوز (16.3%)، ويدل ذلك على انسجام كبير بين آراء أفراد العينة حول أن تلك المخاطر متوسطة الحدوث ولا تتعدى الأهمية النسبية لحدوثها (56.6%)، ولعل ذلك يعود إلى كفاية إجراءات الحماية إلى حدٍ ما والمتبعة لمواجهة مخاطر أمن المدخلات، وأهمها وجود مراجعة تفصيلية للبيانات المدخلة للتأكد من دقتها واكتمالها، كما يتم إجراء المراجعة الثنائية لبيانات المستندات المدخلة للتأكد من سلامتها، كما أن مستندات إدخال البيانات دقيقة وشاملة لمختلف العمليات، وتساعد على تقليل الأخطاء، ويتم إعدادها وتعبئتها ومصادقتها من الأشخاص المخولين فقط، ويوجد برنامج خاص مصمم لمعرفة من قام بإدخال البيانات، وتتضمن برامج النظام ضوابط تمنع إدخال بيانات خاطئة، حيث تظهر رسالة تحذيرية على الشاشة في حال وجود خطأ.
- بينما جاءت مخاطر أمن النسخ في وسائط غير متصلة بقاعدة البيانات في المرتبة التاسعة والأخيرة وبمستوى منخفض من حيث شدة حدوثها، حيث بلغ إجمالي المتوسط الحسابي لها (2.156)، وبمعامل اختلاف لا يتجاوز (27.9%)، ويدل ذلك على تقارب كبير بين آراء أفراد العينة حول أن تلك المخاطر منخفضة ولا تتعدى الأهمية النسبية لحدوثها (43.2%)، ولعل مرد ذلك يعود إلى قيام معظم تلك البنوك بأخذ نسخ احتياطية للبرامج وملفات البيانات الهامة بشكل مستمر ودوري (يومي، أسبوعي، شهري)، وتحفظ في خزائن حديدية مقفلة لحمايتها من السرقة أو الحريق، وتوضع نسخة منها في مكان آمن خارج مقر العمل.
- يستخلص مما سبق، أن مخاطر أمن نظم المعلومات المحاسبية الواردة في الجدولين السابقين كانت منخفضة الحدوث بشكل عام لدى البنوك التجارية في الجمهورية اليمنية، ولكن ذلك لا يعني عدم حدوث بعض تلك المخاطر بشكل جوهري وملحوس، وهو ما يستلزم على إدارات تلك البنوك تداركها أو تخفيضها إلى أدنى حد ممكن.

3-3-4: تحليل البيانات المتعلقة بالتهديدات الداخلية التي تسبب مخاطر أمن نظم المعلومات

المحاسبية المحوسبة:

وفقاً لفرضيات الدراسة ونموذجها تمثل التهديدات الداخلية أحد المتغيرات المستقلة للدراسة، والهدف من قياسها معرفة مدى تسبب تلك التهديدات الداخلية في حدوث المخاطر لدى البنوك التجارية في الجمهورية اليمنية، وقد تم قياس هذا المتغير من خلال المحور الثاني من محاور الجزء الثالث للاستقصاء والذي تضمن (29) فقره تبرز التهديدات الداخلية التي يُعزى اليها حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة، حيث قام الباحث باستخدام التحليل الوصفي تمهيداً لاختبار الفرضية الثانية، فقد استخرج المتوسطات الحسابية والانحرافات المعيارية ومعاملات الاختلاف والأهمية النسبية ومستوى التهديد ورتبته، وفقاً لآراء أفراد عينة الدراسة حول مضمون كل فقرة من تلك الفقرات التي تقيس تلك التهديدات والجدول التالي يلخص نتائج التحليل الوصفي للفقرات المتعلقة بذلك:

جدول رقم (3-3-5) الإحصاءات الوصفية على مستوى الفقرات والمتغيرات الرئيسية

المتعلقة بالتهديدات الداخلية التي تسبب مخاطر أمن نظم المعلومات المحاسبية المحوسبة

رقم الفقرة	التهديدات الداخلية لأمن نظم المعلومات المحاسبية	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى التهديد	رتبة التهديد
31	لا تدرك الإدارة العليا للبنك أهمية أمن نظم المعلومات المحاسبية، فلا تدعم الجهة المعنية بتطبيق السياسات الأمنية مادياً أو معنوياً.	3.320	0.989	29.8	66.4	متوسط	9
32	عدم وجود سياسات وخطط إدارية واضحة ومعتمدة ومعلنة وموثقة لإدارة مخاطر أمن نظم المعلومات المحاسبية في البنك.	3.312	1.099	33.2	66.2	متوسط	11
33	عدم قيام إدارة البنك بإصدار قرارات وتشريعات خاصة فعالة للحد من مخاطر أمن نظم المعلومات المحاسبية، ومعاينة الموظفين المخلين بتلك القواعد.	3.516	1.030	29.2	70.4	مرتفع	7
34	شعور إدارة البنك بعدم جدوى تقييم مخاطر أمن نظم المعلومات المحاسبية، لاعتقادها بأن تكلفة تطبيق إجراءات الحماية أكبر من عوائدها المتوقعة.	2.762	0.987	35.8	55.2	متوسط	21
35	لا تقوم الإدارة بمشاركة الأقسام المختصة لبحث أفضل السبل لمواجهة تلك المخاطر.	3.631	0.873	24.0	72.6	مرتفع	6
36	امتناع الإدارة العليا للبنك عن الإفصاح عن تلك المخاطر والخسائر المترتبة عنها، خوفاً من اهتزاز الثقة بسمعة البنك وبمركزه المالي.	3.713	0.913	24.6	74.2	مرتفع	4
36-31	فلسفة الإدارة العليا للبنك.	3.357	.734	21.8	67.2	متوسط	الثاني
37	عدم وجود إدارة أو قسم أو لجنة مستقلة، لها صلاحيات كافية لتقييم ومتابعة مخاطر أمن نظم المعلومات المحاسبية، بهدف حماية تلك النظم.	3.320	1.108	33.4	66.4	متوسط	10
38	غياب التوصيف الدقيق للوظائف والذي يحدد المسؤوليات والصلاحيات لكل موظف داخل الهيكل التنظيمي للبنك.	3.279	1.207	36.8	65.6	متوسط	15
39	الفصل غير الواضح بين المهام المتعلقة بنظم المعلومات المحاسبية في البنك، كإشراك بعض العاملين باستخدام نفس كلمات السر أو تبادلها بينهم، مما قد يهدر مبدأ تقسيم العمل.	2.713	1.229	45.3	54.2	متوسط	23
40	النقص الكبير للموظفين المختصين بأمن نظم المعلومات	3.303	1.082	32.9	66.0	متوسط	13

رقم الفقرة	التحديات الداخلية لأمن نظم المعلومات المحاسبية	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى التهديد	رتبة التهديد
	الذي تتوفر فيه الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المتعددة والمطلوبة لذلك.						
41	صعوبة وعدم كفاية تدريب وتأهيل وتوعية الموظفين في مجال تقنيات وأسابيل أمن نظم المعلومات، وعدم توافق التدريب مع التطور المستمر لبرامج أمن نظم المعلومات.	3.877	0.905	23.3	77.6	مرتفع	2
42	الاهتمام غير الكافي بفحص التاريخ الوظيفي والمهني للموظفين الجدد مما قد يؤثر على قاعدة وضع الرجل المناسب في المكان المناسب.	3.344	1.104	33.1	66.8	متوسط	8
42-37	التهديدات التنظيمية.	3.306	0.853	25.8	66.2	متوسط	الثالث
43	تقلد الأجهزة والبرامج المستخدمة وضعف فاعليتها في حفظ وتشغيل البيانات وإنتاج المعلومات وتدقيقها وتخزينها واسترجاعها بسهولة ودقة وسرعة.	2.699	0.908	33.6	54.0	متوسط	25
44	الصعوبة في إيجاد التوليفة المثلى للأجهزة والبرامج وأجهزة الدعم المساندة لها بعناية، لتحديث وتطوير الأنظمة، بما يؤمن تحقيق أهداف النظام وتأمين عناصر الرقابة.	2.541	0.892	35.1	50.8	منخفض	27
45	وجود أخطاء في تصميم البرامج والتطبيقات المحاسبية المستخدمة تؤدي إلى إنتاج معلومات خاطئة أو غير دقيقة لفترات طويلة.	2.713	0.999	36.9	54.2	متوسط	24
46	عدم كفاية عمليات الصيانة الدورية لأجهزة الحاسوب والبرمجيات المستخدمة في تشغيل وحماية نظم المعلومات المحاسبية المحوسبة.	2.754	0.696	25.3	55.0	متوسط	22
47	اعتماد البنك في الحصول على الأجهزة والبرامج، والدعم الفني لها على مزودين قليلي الخبرة، ولا يتم التقييم المستمر لوضعهم في السوق.	2.828	0.799	28.3	57.6	متوسط	20
48	عدم التوافق والتوافق ما بين الأنظمة والتطبيقات الموجودة لدى البنك مع الأنظمة والتطبيقات الخاصة بالمنشآت التي قد يتم ربط أنظمة البنك معها.	2.393	1.008	42.8	47.8	منخفض	29
48-43	التهديدات المتعلقة بإمكانيات البنك التكنولوجية.	2.654	0.606	22.9	53.0	متوسط	السادس
49	سوء استخدام الصلاحيات الواسعة المخولة لبعض الأفراد المسؤولين عن تشغيل النظام ممن لديهم معرفة واسعة بتفاصيل النظام، وعدم التزامهم بالإجراءات المحددة لحمايته.	3.156	1.128	35.7	63.12	متوسط	18
50	ضعف إدراك بعض العاملين بالنظام لمهامهم الموكولة لهم (كسيان كلمة المرور للدخول للنظام، أو السماح لزملاء باستخدامها)، مما يترتب عليها أخطاء فادحة عند التشغيل.	3.746	0.895	23.9	75.0	مرتفع	3
51	إهمال بعض العاملين بنظام المعلومات المحاسبي وعدم بذلهم العناية المهنية الكافية لأداء العمل، لنقص التأهيل والخبرة والوعي الرقابي.	4.066	0.800	19.7	81.4	مرتفع	1
52	ارتفاع مستوى خبرة بعض العاملين في مجال التشغيل الإلكتروني، وزيادة معرفتهم أكثر من غيرهم بنقاط الضعف في الضوابط الرقابية المطبقة، مما ينتج عن ذلك مخاطر للنظام.	3.312	0.927	28.0	66.2	متوسط	12
53	التصرفات الانتقامية للأفراد الغاضبين سواء أثناء عملهم بسبب معاقبتهم أو بعد إنهاء خدماتهم بسبب فصلهم من العمل، حيث يقوموا بالكشف عن بعض المعلومات السرية.	3.205	1.003	31.3	64.0	متوسط	16
54	انخفاض معدل دوران موظفي أنظمة المعلومات لدى البنك، واحتفاظهم بأسرار الأنظمة ومفاتيح الحل وعدم تعاونهم مع زملائهم في تبادل المعرفة والخبرة.	3.639	0.900	24.7	72.8	مرتفع	5

رقم الفقرة	التهديدات الداخلية لأمن نظم المعلومات المحاسبية	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى التهديد	رتبة التهديد
54-49	التهديدات المتعلقة بالأفراد العاملين في النظم.	3.521	0.708	20.1	70.4	مرتفع	الأول
55	عجز التدابير الأمنية لتنظيم المعلومات، وعدم كفاية وفعالية الأدوات والضوابط والإجراءات الرقابية المطبقة في البنك لحماية أمن نظم المعلومات المحاسبية.	2.459	0.762	31.0	49.2	منخفض	28
56	ضعف كفاءة وفعالية نظم الرقابة الداخلية للبنك وعدم إصدار تقارير رقابية دورية حول الأنظمة الآلية، ليتم متابعتها وتقييمها لمواكبة التطورات التي تجري لمواجهة المخاطر.	2.680	0.718	26.8	53.6	متوسط	26
57	عدم كفاءة وفعالية إجراءات إدارة المخاطر، وعدم القيام بالتقييم الذاتي لمخاطر أمن نظم المعلومات بحيث يقوم كل موظف بتحديد المخاطر التي يواجهها وتقييم إجراءات مواجهتها	3.295	0.768	23.2	66.0	متوسط	14
58	غياب المسار المرني للمراجعة فعدم رؤية عمليات إدخال البيانات وتشغيلها سهل من تغيير أو إضافة أو حذف أي بيانات دون ترك أثر يدل على ذلك، وصعوبة اكتشاف ذلك	3.049	0.7255	23.8	61.0	متوسط	19
58-55	ضعف الرقابة الداخلية وإدارة المخاطر في البنك.	2.871	0.508	17.7	57.4	متوسط	الخامس
59	حدوث كوارث غير طبيعية من البيئة الداخلية للبنك (كالتخريب، والحريق، وانقطاع الكهرباء، وتسريب المياه)، تسبب تلك الكوارث تلف جزئي أو تدمير كلي لموارد النظام.	3.172	1.237	39.0	63.4	متوسط	17
59	حدوث كوارث داخلية في البنك (غير طبيعية).	3.172	1.237	39.0	63.4	متوسط	الرابع
59-31	المتوسط العام للتهديدات الداخلية ككل	3.147	0.591	18.8	63.0	متوسط	

- مستوى التهديد حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 – 2.59) منخفض، (2.60 – 3.39) متوسط، (3.40 – 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

تشير النتائج الواردة في الجدول السابق إلى ما يلي:

- إن المتوسط الحسابي الإجمالي لتقديرات أفراد العينة عن كافة الفقرات والمتغيرات الرئيسية التي تقيس التهديدات الداخلية التي تسبب حدوث مخاطر أمن نظم المعلومات المحاسبية المحسوبة لدى البنوك التجارية في الجمهورية اليمنية قد بلغ (3.147) درجة من أصل (5) درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي المعياري في هذه الدراسة والبالغة (3) درجات، والأهمية النسبية لتلك التهديدات قدرها (63.0%)، والذي يقابل مستوى التهديد المتوسط، وهي أكبر من نسبة المتوسط الحسابي المعتمدة في هذه الدراسة والبالغة (60%)، وبلغت قيمة الانحراف المعياري عن المتوسط الحسابي (0.591) فقط، مما يدل على تقارب الإجابات وأنها تتمحور حول المتوسط الحسابي، ويؤكد ذلك أن معامل الاختلاف لم يتجاوز (18.8%)، وهي تمثل نسبة ضئيلة وتدل على عدم تشتت واختلاف البيانات عن المتوسط الحسابي، وأن هناك تقارب وانسجام إلى حد كبير بين معظم أفراد عينة الدراسة في الإجابة عن فقرات هذا المحور الخاص بقياس التهديدات الداخلية المسببة لمخاطر أمن نظم المعلومات المحاسبية المحسوبة، وأن مستوى تلك التهديدات الداخلية والتي تسبب مخاطر أمن

نظم المعلومات المحاسبية المحوسبة كان بشكل عام متوسط لدى البنوك التجارية العاملة في الجمهورية اليمنية، ويؤكد ذلك قيم المتوسطات الحسابية لمعظم المتغيرات الفرعية والرئيسية الخاصة بذلك المحور.

■ إن قيم الانحراف المعياري لمعظم الفقرات قد بلغت أقل من الواحد الصحيح، وبلغت لجميعها (0.591) فقط، مما يدل على أن آراء أفراد العينة لمعظم تلك الفقرات كانت متقاربة إلى حد ما، ويؤكد ذلك أن قيم معامل الاختلاف لتلك الفقرات قد تراوحت بين (19.7%~45.3%)، وهي قيم متوسطة نسبياً تعكس مدى التقارب في وجهات نظر المستجيبين، ومدى تشتت إجاباتهم على كل فقرة منها.

■ إن اتجاهات عينة الدراسة كانت إيجابية في (19) فقرة كان ترتيبها من (1) إلى (19) حسب الترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات حيث كانت أكبر من المتوسط الحسابي المعتمد وفق المقياس المستخدم في هذه الدراسة وهو (3) درجات، ولكن بقية الفقرات العشر التي حملت الرتب من (20) إلى (29) كانت إجابات أفراد العينة عليها سلبية وغير مؤيدة لها لأن قيم المتوسط الحسابي لتلك الفقرات كانت أقل من (3) درجات، وقد تراوح المتوسط الحسابي لجميع الفقرات بين (2.393~4.066)، ومعامل الاختلاف لتلك الفقرات لم يتجاوز (39%) مما يدل على تقارب الاجابات حول المتوسط الحسابي، وتدل هذه النتيجة على أنَّ المستجيبين يجمعون بنسبة متوسطة إلى حدٍ ما على أن حدوث تلك المخاطر لدى البنوك التجارية العاملة في الجمهورية اليمنية يُعزى إلى تلك التهديدات الداخلية.

■ وكان مستوى التهديدات الداخلية مرتفع في سبع فقرات فقط، ترتيبها يقع بين (1~7) والتي يزيد المتوسط الحسابي لكل منها عن (3.4) درجة، أي أنه يوجد موافقة على أن تلك التهديدات الداخلية تتسبب في حدوث المخاطر بدرجة مرتفعة، فقد تراوح المتوسط الحسابي لتلك الفقرات بين (3.516~4.066)، ويلاحظ أن التهديد الوارد في الفقرة رقم (51) والذي يتعلق بإهمال بعض العاملين بنظام المعلومات المحاسبي وعدم بذلهم العناية المهنية الكافية لأداء العمل، لنقص التأهيل والخبرة والوعي الرقابي قد احتل المرتبة الأولى بأعلى متوسط حسابي بلغ (4.066) وبأهمية نسبية بلغت (81.4%)، وبانحراف معياري (0.800)، ومعامل اختلاف لم يتجاوز (19.7%)، وهذا يؤكد أن معظم أفراد عينة الدراسة المستقصى منهم كانوا متفقين على أن ذلك التهديد مرتفع ونسبة (81.4%)، وهذا يشير إلى أن أهم التهديدات الداخلية التي يُعزى إليها حدوث مخاطر أمن نظم المعلومات المحاسبية لدى البنوك التجارية في الجمهورية اليمنية، هي تلك التهديدات المتعلقة بإهمال بعض العاملين بنظم المعلومات المحاسبية وعدم بذلهم العناية المهنية الكافية لأداء العمل، لنقص التأهيل والخبرة والوعي الرقابي، وأيضاً صعوبة وعدم كفاية تدريب وتأهيل وتوعية الموظفين في مجال تقنيات وأساليب أمن نظم المعلومات، وكذلك عدم توافق التدريب مع التطور المستمر لبرامج أمن نظم المعلومات، بالإضافة إلى ذلك ضعف إدراك بعض العاملين بالنظام لمهامهم الموكلة لهم (كنسيان كلمة المرور للدخول للنظام، أو السماح لزملاء باستخدامها)، مما يترتب عليها أخطاء فادحة عند التشغيل، وتلك التهديدات، نالت

موافقة غالبية أفراد عينة الدراسة على أنها تهديدات داخلية تؤدي إلى حدوث المخاطر وبمستوى مرتفع وبأهمية نسبية تراوحت بين (75.0%~81.4%)، وفي رأي الباحث أن هذه النتيجة تتسجم وتتفق مع نوعية المخاطر التي ظهرت عند مناقشة المحور الأول وكان حدوثها يُعزى لضعف تأهيل وتدريب العاملين وهذا أمر يستوجب من البنوك التجارية العاملة في اليمن تداركه، فإن فعالية وكفاءة أمن نظم المعلومات المحاسبية يعتمد على مدى كفاءة الأفراد القائمين على تشغيل تلك النظم، فالتكنولوجيا يمكن تقليدها لكن معرفة الأفراد تبقى هي المتميزة.

■ وكان مستوى التهديدات الداخلية متوسط الأهمية في (19) فقرة والتي كان ترتيبها بين (8~26) وفقاً للترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات، حيث تراوح المتوسط الحسابي لها بين (2.680~3.344) والذي يعكس مدى الأهمية النسبية لتلك التهديدات الواقع بين (53.6%~66.8%)، وبمعامل اختلاف لتلك الفقرات لم يتجاوز (45.3%)، وكان أهم التهديدات الداخلية المسببة لمخاطر أمن نظم المعلومات المحاسبية وبمستوى متوسط هو التهديد المتعلق بالاهتمام غير الكافي بفحص التاريخ الوظيفي والمهني للموظفين الجدد مما قد يؤثر على قاعدة وضع الرجل المناسب في المكان المناسب، والذي جاء في المرتبة (8) على مستوى التهديدات الداخلية ككل، حيث بلغ متوسطه الحسابي (3.344)، وبمعامل الاختلاف (33.1%)، وهو ما يدل على انسجام وتقارب كبير بين آراء أفراد العينة على أن ذلك التهديد يسبب مخاطر لأمن نظم المعلومات المحاسبية بنسبة (66.8%)، بينما التهديد الداخلي المتعلق بضعف كفاءة وفعالية نظم الرقابة الداخلية للبنك وعدم إصدار تقارير رقابية دورية حول الأنظمة الآلية، لئتم متابعتها وتقييمها لمواكبة التطورات التي تجري لمواجهة المخاطر، جاء في المرتبة (26) وبمتوسط حسابي بلغ (2.680)، ومعامل الاختلاف لا يزيد عن (26.8%)، وهو ما يدل على انسجام وتقارب كبير إلى حد ما بين آراء أفراد العينة الذين أفادوا بأن ذلك التهديد يسبب مخاطر لأمن نظم المعلومات المحاسبية وبمستوى متوسط الأهمية بنسبة (53.6%)، وهو ما يستوجب من البنوك الاهتمام برفع فعالية وكفاءة نظم الرقابة الداخلية وخصوصاً فيما يتعلق بالرقابة على نظم المعلومات المحاسبية المحوسبة، بما يؤدي إلى تلاشي نقاط الضعف الموجودة لديهم، وبالتالي التخفيف من تلك التهديدات المسببة للمخاطر إلى أدنى حد ممكن.

■ بينما كان مستوى التهديدات الواردة في ثلاث فقرات رقمها (44، 55، 48) منخفضاً، والتي كان ترتيبها من (27) إلى (29) وفقاً للترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات، وقد تراوح المتوسط الحسابي لتلك التهديدات بين (2.393~2.541)، والذي يعكس مدى الأهمية النسبية لتلك التهديدات والذي تراوح بين (47.8%~50.8%)، وهذا يعني أن تلك التهديدات كانت منخفضة، ويلاحظ أن التهديد الوارد في الفقرة (48) والمتعلق بعدم التوائم والتوافق ما بين الأنظمة والتطبيقات الموجودة لدى البنك مع الأنظمة والتطبيقات الخاصة بالمنشآت التي قد يتم ربط أنظمة البنك معها قد جاء في المرتبة الأخيرة على مستوى التهديدات الداخلية ككل، وبمتوسط حسابي (2.393)، وبأهمية نسبية لذلك التهديد لا تتجاوز (47.8%)، وانحراف معياري (1.008)،

ومعامل اختلاف قدره (47.8%)، مما يعكس وجود اختلاف إلى حد ما بين آراء المستجيبين حول ذلك التهديد، ونتيجة لذلك يرى الباحث أن حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، لا يُعزى إلى التهديد المتعلق بعدم التوافق ما بين الأنظمة والتطبيقات الموجودة لدى البنك مع الأنظمة والتطبيقات الخاصة بالمنشآت التي قد يتم ربط أنظمة البنك معها، وقد يرجع ذلك إلى ندرة أو قلة عدد البنوك التجارية في اليمن المرتبط نظمها مع نظم منشآت أخرى عبر شبكات الاتصال، وعدم قيامها بأنشطة تتعلق بالتجارة الالكترونية بشكل واسع.

- ويمكن القول بصفة إجمالية بأن إجابات أفراد العينة حول التهديدات الداخلية التي تسبب مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التي يعملون بها، كانت غالبيتها ترى بأن هناك تهديدات داخلية تسبب المخاطر فقد حصلت (7) فقرة على درجة موافقة مرتفعة، في مقابل حصول (19) فقرات على درجة موافقة متوسطة، وحصول (3) فقرات فقط على درجة موافقة منخفضة، مما يشير إلى أن التهديدات الداخلية تسبب المخاطر وبمستوى أهمية متوسط لا يقل عن (63%) وهنا يجب على هذه البنوك مواجهة تلك التهديدات المسببة لمخاطر أمن نظم المعلومات المحاسبية المحوسبة بشتى الإجراءات والوسائل.
- وبالنظر إلى المتغيرات الرئيسية للتهديدات الداخلية المسببة لمخاطر أمن نظم المعلومات المحاسبية المحوسبة، وبناءً على المتوسط الحسابي لتلك التهديدات، والأهمية النسبية لها، تم ترتيب محاور التهديدات الداخلية تنازلياً، كما هو مبين في الجدول الآتي:

جدول رقم (3-3-6) الإحصاءات الوصفية للمتغيرات الرئيسية المتعلقة بالتهديدات الداخلية

المسببة لحدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة مرتبة تنازلياً حسب الأهمية النسبية⁽¹⁾

رتبة التهديد	التهديدات الداخلية المسببة لمخاطر أمن نظم المعلومات المحاسبية	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى التهديد
1	الأفراد العاملين في نظم المعلومات المحاسبية.	3.521	0.708	20.1	70.4	مرتفع
2	فلسفة الإدارة العليا للبنك.	3.357	.734	21.8	67.2	متوسط
3	التهديدات التنظيمية.	3.306	0.853	25.8	66.2	متوسط
4	حدوث كوارث داخلية في البنك (غير طبيعية).	3.172	1.237	39.0	63.4	متوسط
5	ضعف الرقابة الداخلية وإدارة المخاطر بالبنك	2.871	0.508	17.7	57.4	متوسط
6	مهددات تتعلق بإمكانات البنك التكنولوجية.	2.654	0.606	22.9	53.0	متوسط
الإجمالي العام		3.147	0.591	18.8	63.0	متوسط

• مستوى التهديد حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 – 2.59) منخفض، (2.60 – 3.39) متوسط، (3.40 – 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

(1) الجدول من إعداد الباحث اعتماداً على مخرجات التحليل الإحصائي SPSS.

ومن الجدول السابق يتضح ما يلي:

- إن أهم التهديدات الداخلية التي تؤدي إلى حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة هي التهديدات التي تتعلق بالأفراد العاملين في نظم المعلومات المحاسبية المحوسبة بالمرتبة الأولى ثم يليها التهديدات المتعلقة بفلسفة الإدارة العليا للبنك بالمرتبة الثانية، يليها التهديدات التنظيمية، ثم تهديدات الكوارث الداخلية، ثم ضعف الرقابة الداخلية وإدارة المخاطر في البنك، وكان أقلها أهمية هي التهديدات المتعلقة بإمكانات البنك التكنولوجية.
- إن قيم المتوسط الحسابي لكل تهديد من التهديدات الداخلية المسببة لمخاطر أمن نظم المعلومات المحاسبية على مستوى المتغيرات الرئيسية كانت أكبر من المتوسط الحسابي المعتمد وفق المقياس المستخدم في هذه الدراسة وهو (3) درجات، ماعدا التهديد المتعلق بضعف الرقابة الداخلية وإدارة المخاطر بالبنك والتهديد المتعلق بإمكانات البنك التكنولوجية، وقد تراوحت قيمة المتوسط الحسابي لتلك التهديدات بين (2.654) بنسبة (53%)، وبمستوى منخفض للتهديد الداخلي المتعلق بإمكانات البنك التكنولوجية، وبين (3.521) بنسبة (70.4%)، وبمستوى مرتفع للتهديد الداخلي المتعلق بالأفراد العاملين في نظم المعلومات المحاسبية المحوسبة، وبمعامل اختلاف لم يتجاوز (39%) وتدل هذه النتيجة على أنَّ المستجيبين يجمعون بنسبة كبيرة إلى حد ما أن التهديدات الداخلية تسبب مخاطر أمن نظم المعلومات المحاسبية لدى البنوك التجارية العاملة في الجمهورية اليمنية، وبمستوى متوسط.
- بالنظر إلى ترتيب التهديدات الداخلية المسببة لمخاطر أمن نظم المعلومات المحاسبية المحوسبة في الجدول السابق أعلاه رقم (3-3-6) يلاحظ أن التهديدات المتعلقة بالأفراد العاملين في نظم المعلومات المحاسبية المحوسبة، قد احتلت المرتبة الأولى وبمستوى مرتفع، حيث حصلت على أعلى متوسط حسابي، والذي بلغت قيمته (3.521) درجة، وبمعامل اختلاف لا يتجاوز (20.1%)، ويدل ذلك على انسجام كبير بين آراء أفراد العينة حول أن تلك التهديدات مرتفعة وتتسبب في حدوث المخاطر وبأهمية نسبية مرتفعة للموافقة بلغت (70.4%)، ولعل ذلك يعود إلى عدم كفاية أو تطبيق السياسات المتعلقة بحماية أمن الأفراد التنظيمي لدى البنوك الخاضعة للدراسة.
- بينما جاءت التهديدات الأخرى بمستوى متوسط الأهمية، وقد كانت التهديدات المتعلقة بإمكانات البنك التكنولوجية في المرتبة السادسة والأخيرة وبمستوى متوسط، حيث بلغ إجمالي المتوسط الحسابي لها (2.654)، وبمعامل اختلاف لا يتجاوز (22.9%)، ويدل ذلك على تقارب بين آراء أفراد العينة حول أن تلك التهديدات متوسطة وتتسبب في حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة، وبأهمية نسبية لا تتجاوز (53%)، ولعل مرد ذلك يعود إلى أن كل البنوك التجارية في اليمن سعت لامتلاك أحدث وسائل الاتصالات وتكنولوجيا المعلومات في ظل المنافسة الاقتصادية في الصناعة المصرفية.

- يستخلص الباحث مما سبق، أن التهديدات الداخلية الواردة في الجدولين السابقين كانت متوسطة بشكل عام وتتنسب في حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية وبأهمية نسبية بلغت (63 %) حسب آراء عينة الدراسة.

3-3-5: تحليل البيانات المتعلقة بالتهديدات الخارجية التي تسبب مخاطر أمن نظم المعلومات المحاسبية المحوسبة:

وفقاً لفرضيات الدراسة ونموذجها تمثل التهديدات الخارجية أحد المتغيرات المستقلة للدراسة، والهدف من قياسها معرفة مدى تسبب تلك التهديدات الخارجية في حدوث المخاطر لدى البنوك التجارية في الجمهورية اليمنية، وقد تم قياس هذا المتغير من خلال المحور الثالث من محاور الجزء الثالث للاستقصاء والذي تضمن (17) فقره تبرز التهديدات الخارجية التي يُعزّي إليها حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة، حيث قام الباحث باستخدام التحليل الوصفي تمهيداً لاختبار الفرضية الثالثة، فقد استخرج المتوسطات الحسابية والانحرافات المعيارية ومعاملات الاختلاف والأهمية النسبية ومستوى التهديد ورتبته، وفقاً لآراء أفراد عينة الدراسة حول مضمون كل فقرة من تلك الفقرات التي تقيس تلك التهديدات والجدول التالي يلخص نتائج التحليل الوصفي للفقرات المتعلقة بذلك:

جدول رقم (3-3-7) الإحصاءات الوصفية على مستوى الفقرات والمتغيرات الرئيسية المتعلقة بالتهديدات الخارجية التي تسبب مخاطر أمن نظم المعلومات المحاسبية المحوسبة

رقم الفقرة	التهديدات الخارجية لأمن نظم المعلومات المحاسبية	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى التهديد	رتبة التهديد
60	التطورات التكنولوجية السريعة والهائلة والمتلاحقة والتي تلي وضع الإجراءات الرقابية في البنك، فتقدم التقنية خارجياً أسرع من ممارسة الأمن داخل البنك.	4.033	0.781	19.4	80.6	مرتفع	5
61	عدم وجود استقرار نسبي لنظام المعلومات، بسبب ارتفاع معدلات التغير في تكنولوجيا المعلومات، مقابل ضعف إمكانيات البنك المالية والبشرية لمجاراتها واستيعابها.	3.639	0.936	25.7	72.8	مرتفع	12
62	تصميم أساليب للتلاعب تبنى داخل النظام المحاسبي الإلكتروني يصعب اكتشافها، تؤدي إلى إنتاج معلومات محاسبية خاطئة.	2.738	0.821	30.0	54.8	متوسط	16
63	عدم توفر بنية تحتية تكنولوجية قوية في الجمهورية اليمنية.	3.754	1.006	26.8	75.0	مرتفع	9
63-60	التغير التكنولوجي غير المتوازن	3.541	0.632	17.9	70.8	مرتفع	الخامس
64	حدوث الكوارث الطبيعية والبيئية كالزلازل، والبراكين، والفيضانات والسيول، والرياح العاتية والأعاصير، والصواعق، والحرائق الطبيعية وانقطاع التيار الكهربائي لأسباب طبيعية خارجية، يؤدي إلى حدوث تلف جزئي أو تدمير كلي لموارد النظام (أجهزة، وبرامج، وملفات بيانات، وأفراد).	3.221	0.857	26.6	64.4	متوسط	14
65	حدوث كوارث غير طبيعية (بشرية)، كالاضطرابات السياسية المحلية والإقليمية، والحروب، والتهديدات الإرهابية.	3.738	0.968	25.9	74.8	مرتفع	10
65-64	الكوارث الطبيعية والسياسية	3.480	0.803	23.0	69.6	مرتفع	السادس

رقم الفقرة	التهديدات الخارجية لأمن نظم المعلومات المحاسبية	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى التهديد	رتبة التهديد
66	جرائم وقرصنة الحاسوب نتيجة تصرفات غير أمينة من قبل أطراف خارجية كالقرصنة والمتطفلين الذين يخترقوا نظم الحماية، رغبة في التحدي، أو لنوايا إجرامية وتجسسية.	3.303	0.770	23.3	66.0	متوسط	13
66	المخترقون والقرصنة	3.303	0.770	23.3	66.0	متوسط	السابع
67	الإصابة بالبرامج الخبيثة (الفيروسات والديدان، وبرامج التجسس)، التي قد تتلف البيانات أو تعطل النظام وتؤثر على عملية تشغيل البيانات.	4.066	0.746	18.3	81.4	مرتفع	3
67	دخول فيروسات وبرمجيات الحاسوب الخبيثة للنظام	4.066	0.746	18.3	81.4	مرتفع	الثاني
68	رغبة منافسي البنك في الوصول إلى المعلومات السرية كعملاء البنك، وحجم النشاط وغيرها من المعلومات الهامة.	2.607	0.787	30.1	52.2	متوسط	17 (الأخير)
69	زيادة المنافسة بين البنوك والذي جعلتها تقوم بتقديم الخدمات المصرفية الإلكترونية دون مراعاة الآثار التي يمكن أن تحدث عند الاستخدام الفعلي.	3.107	0.677	21.8	62.2	متوسط	15
69-68	المنافسة الاقتصادية بين البنوك	2.857	0.583	20.4	57.2	متوسط	الثامن
70	عدم إبلء المراجع الخارجي الأهمية الكافية لمخاطر أمن نظام المعلومات المحاسبي في البنك، عند قيامه بمهامه للتأكد من أن النظام قد تم تصميمه وتشغيله بطريقة ملائمة.	3.738	0.769	20.6	74.8	مرتفع	11
71	عدم قيام البنك المركزي والسلطات الرقابية الرسمية بتكثيف حملات تفتيشية مفاجئة لتقييم مخاطر أمن نظم المعلومات المحاسبية لدى البنوك، وإلزامها برفع تقارير بهذا الشأن.	3.844	0.953	24.8	76.8	مرتفع	7
71-70	ضعف الرقابة الخارجية على نظم المعلومات المحاسبية المحوسبة	3.791	0.721	19.0	75.8	مرتفع	الرابع
72	عدم تحديث القوانين المحلية النافذة التي تهدف إلى حماية أمن نظم المعلومات، سواء كانت قوانين جنائية أو مدنية أو تجارية، فهي تفتقد إلى كثير من النصوص اللازمة.	4.049	0.790	19.5	81.0	مرتفع	4
73	الغموض التشريعي بشأن اختصاص وانطباق القوانين واللوائح المعمول بها لتحديد الحقوق والالتزامات الناتجة عن العمليات المصرفية الإلكترونية.	4.139	0.633	15.2	82.8	مرتفع	1
74	اختلاف التشريعات القانونية التي تنظم التعاملات المصرفية الإلكترونية بين الدول مما يؤدي إلى تنازع القوانين واختصاصات المحاكم في فض النزاعات التي تنشأ عنها.	3.820	0.909	23.8	76.4	مرتفع	8
75	عدم وجود أطر تشريعية وقانونية متناسقة ومتجانسة على المستوى المحلي والإقليمي والدولي لمعاقبة مرتكبي جرائم الحاسوب والانترنت.	3.902	0.856	21.9	78.0	مرتفع	6
75-72	ضعف التشريعات والقوانين المحلية في مجال تكنولوجيا المعلومات.	3.978	0.611	15.3	79.6	مرتفع	الثالث
76	نقص الوعي الإلكتروني لدى عملاء البنك وعدم إتباعهم إجراءات التأمين الوقائية الواجبة لبياناتهم الشخصية، وضعف دور البنك في القيام بتوعيتهم.	4.123	0.744	18.0	82.4	مرتفع	2
76	نقص الوعي الإلكتروني لعملاء البنك	4.123	0.744	18.0	82.4	مرتفع	الأول
76-60	المتوسط العام لمجال التهديدات الخارجية ككل	3.642	0.412	11.3	72.8	مرتفع	

• مستوى التهديد حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 – 2.59) منخفض، (2.60 – 3.39) متوسط، (3.40 – 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

تشير النتائج الواردة في الجدول السابق إلى ما يلي:

- إن المتوسط الحسابي الإجمالي لتقديرات أفراد العينة عن كافة الفقرات والمتغيرات الرئيسية التي تقيس التهديدات الخارجية التي تسبب حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية قد بلغ (3.642) درجة من أصل (5) درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي المعياري في هذه الدراسة والبالغة (3) درجات، والأهمية النسبية لتلك التهديدات قدرها (72.8%)، والذي يقابل مستوى التهديد المرتفع، وهي أكبر من نسبة المتوسط الحسابي المعتمدة في هذه الدراسة والبالغة (60%)، وبلغت قيمة الانحراف المعياري عن المتوسط الحسابي (0.412) فقط، مما يدل على تقارب الإجابات وأنها تتمحور حول المتوسط الحسابي، ويؤكد ذلك أن معامل الاختلاف لم يتجاوز (11.3%)، وهي تمثل نسبة ضئيلة وتدل على عدم تشتت واختلاف البيانات عن المتوسط الحسابي، وأن هناك تقارب وانسجام إلى حد كبير بين معظم أفراد عينة الدراسة في الإجابة عن فقرات هذا المحور الخاص بقياس التهديدات الخارجية المسببة لمخاطر أمن نظم المعلومات المحاسبية المحوسبة، وأن مستوى تلك التهديدات الخارجية والتي تسبب مخاطر أمن نظم المعلومات المحاسبية المحوسبة كان بشكل عام مرتفع لدى البنوك التجارية العاملة في الجمهورية اليمنية، ويؤكد ذلك قيم المتوسطات الحسابية لمعظم المتغيرات الفرعية والرئيسية الخاصة بذلك المحور.
- إن قيم الانحراف المعياري لجميع الفقرات قد بلغت أقل من الواحد الصحيح، عدا الفقرة رقم (63)، وبلغ الانحراف المعياري للمجال ككل (0.412) فقط، مما يدل على أن آراء أفراد العينة لمعظم تلك الفقرات كانت متقاربة إلى حد ما، ويؤكد ذلك أن قيم معامل الاختلاف لتلك الفقرات قد تراوحت بين (15.2%~30.1%)، وهي قيم منخفضة نسبياً تعكس مدى التقارب في وجهات نظر المستجيبين.
- إن اتجاهات عينة الدراسة كانت إيجابية في (15) فقرة كان ترتيبها من (1) إلى (15) حسب الترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات حيث كانت أكبر من المتوسط الحسابي المعتمد وفق المقياس المستخدم في هذه الدراسة وهو (3) درجات، ولكن الفقرتان (62)، و(68) وللتين حملتا الرتبتيين (16) و(17) كانت إجابات أفراد العينة عليهما سلبية وغير مؤيدة لهما لأن قيم المتوسط الحسابي لكليهما كانت أقل من (3) درجات، وقد تراوح المتوسط الحسابي لجميع الفقرات بين (2.607~4.139)، ومعامل الاختلاف لتلك الفقرات لم يتجاوز (30.1%) مما يدل على تقارب الاجابات حول المتوسط الحسابي، وتدل هذه النتيجة على أن المستجيبين يجمعون بنسبة متوسطة إلى حد ما على أن حدوث تلك المخاطر لدى البنوك التجارية العاملة في الجمهورية اليمنية يُعزى إلى تلك التهديدات الخارجية.
- وكان مستوى التهديدات الخارجية مرتفع في (12) فقرة، ترتيبها يقع بين (1~12) والتي يزيد المتوسط الحسابي لكل منها عن (3.4) درجة، أي أنه يوجد موافقة على أن تلك التهديدات الخارجية تتسبب في حدوث المخاطر بدرجة مرتفعة، فقد تراوح المتوسط الحسابي لتلك الفقرات بين (3.639~4.139)، **ويلاحظ أن**

التهديد الوارد في الفقرة رقم (73) والذي يتعلق بالغموض التشريعي بشأن اختصاص وانطباق القوانين واللوائح المعمول بها لتحديد الحقوق والالتزامات الناتجة عن العمليات المصرفية الالكترونية، قد احتل المرتبة الأولى بأعلى متوسط حسابي بلغ (4.139) وبأهمية نسبية بلغت (82.8%)، وبانحراف معياري (0.633)، ومعامل اختلاف لم يتجاوز (15.2%)، وهذا يؤكد أن معظم أفراد عينة الدراسة المستقصى منهم كانوا متفقين على أن ذلك التهديد مرتفع ونسبة (82.8%)، وهذا يشير إلى أن حدوث مخاطر أمن نظم المعلومات المحاسبية لدى البنوك التجارية في الجمهورية اليمنية قد يُعزى إلى الغموض التشريعي بشأن اختصاص وانطباق القوانين واللوائح المعمول بها لتحديد الحقوق والالتزامات الناتجة عن العمليات المصرفية الالكترونية، وأيضاً نقص الوعي الالكتروني لدى عملاء البنك وعدم إتباعهم إجراءات التأمين الوقائية الواجبة لبياناتهم الشخصية، وضعف دور البنك في القيام بتوعيتهم، وكذلك الإصابة بالبرامج الخبيثة (الفيروسات والديدان، وبرامج التجسس)، التي قد تتلف البيانات أو تعطل النظام وتؤثر على عملية تشغيل البيانات، بالإضافة إلى ذلك عدم تحديث القوانين المحلية النافذة التي تهدف إلى حماية أمن نظم المعلومات، سواء كانت قوانين جنائية أو مدنية أو تجارية، فهي تفتقد إلى كثير من النصوص اللازمة، وتلك التهديدات نالت موافقة غالبية أفراد عينة الدراسة على أنها تهديدات خارجية تؤدي إلى حدوث المخاطر وبمستوى مرتفع وبأهمية نسبية تراوحت بين (81.0%~82.8%)، وفي رأي الباحث أن هذه النتيجة تنسجم وتتفق مع نوعية المخاطر التي ظهرت عند مناقشة المحور الأول وكان أهمها المخاطر الناتجة عن الفيروسات، أو تلك المخاطر الناتجة عن الأفراد بشكل غير متعمد، وهذا أمر يستوجب من البنوك التجارية العاملة في اليمن تداركه.

■ وكان مستوى التهديدات الخارجية متوسط الأهمية في (5) فقرات والتي كان ترتيبها بين (13~17) وفقاً للترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات، حيث تراوح المتوسط الحسابي لها بين (2.607~3.303) والذي يعكس مدى الأهمية النسبية لتلك التهديدات الواقع بين (52.2%~66.0%)، وبمعامل اختلاف لتلك الفقرات لم يتجاوز (30.1%)، وكان أهم التهديدات الخارجية المسببة لمخاطر أمن نظم المعلومات المحاسبية وبمستوى متوسط هو التهديد المتعلق بجرائم وقرصنة الحاسوب نتيجة تصرفات غير أمينة من قبل أطراف خارجية كالقرصنة والمتطفلين الذين يخترقوا نظم الحماية، رغبةً في التحدي، أو لنوايا إجرامية وتجسسية، والذي جاء في المرتبة (13) على مستوى التهديدات الخارجية ككل، والسابع على مستوى المتغيرات الرئيسية، حيث بلغ متوسطه الحسابي (3.303)، ومعامل الاختلاف (23.3%)، وهو ما يدل على انسجام وتقارب كبير بين آراء أفراد العينة على أن ذلك التهديد يسبب مخاطر لأمن نظم المعلومات المحاسبية بنسبة (66.0%)، **بينما التهديد الخارجي المتعلق برغبة منافسي البنك في الوصول إلى المعلومات السرية كعملاء البنك، وحجم النشاط وغيرها من المعلومات الهامة، جاء في المرتبة (17) والأخير، وبمتوسط حسابي بلغ (2.607)، ومعامل الاختلاف لا يزيد عن (30.1%)، وهو ما يدل على انسجام وتقارب إلى حد ما بين آراء أفراد العينة الذين أفادوا بأن ذلك التهديد يسبب مخاطر لأمن نظم المعلومات المحاسبية وبمستوى متوسط الأهمية بنسبة**

(52.2%)، وهو ما يستوجب من البنوك الاهتمام بمواجهة خطر القرصنة والمتطفلين، خصوصاً في ظل اعتماد تلك البنوك على شبكات الاتصال المختلفة بما فيها الانترنت لتداول بياناتها، وبما يؤدي إلى التخفيف من تهديدات القرصنة المسببة للمخاطر إلى أدنى حد ممكن.

- ويمكن القول بصفة إجمالية بأن إجابات أفراد العينة حول التهديدات الخارجية التي تسبب مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التي يعملون بها، كانت غالبيتها ترى بأن هناك تهديدات خارجية تسبب المخاطر فقد حصل (12) تهديد على درجة موافقة مرتفعة، في مقابل حصول (5) تهديدات على درجة موافقة متوسطة، ولا يوجد تهديد حصل على درجة موافقة منخفضة، مما يشير إلى أن التهديدات الخارجية تسبب المخاطر وبمستوى أهمية مرتفع لا يقل عن (72.8%) وهنا يجب على هذه البنوك مواجهة تلك التهديدات المسببة لمخاطر أمن نظم المعلومات المحاسبية المحوسبة بشتى الإجراءات والوسائل.
- **بالنظر إلى المتغيرات الرئيسية للتهديدات الخارجية التي تسبب مخاطر أمن نظم المعلومات المحاسبية المحوسبة، وبناءً على المتوسط الحسابي لتلك التهديدات، والأهمية النسبية لها، تم ترتيب محاور التهديدات الخارجية تنازلياً، كما هو مبين في الجدول الآتي:**

جدول رقم (3-3-8) الإحصاءات الوصفية للمتغيرات الرئيسية المتعلقة بالتهديدات الخارجية

التي قد تسبب حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة مرتبة تنازلياً حسب الأهمية النسبية⁽¹⁾

رتبة التهديد	التهديدات الخارجية المسببة لمخاطر أمن نظم المعلومات المحاسبية	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى التهديد
1	نقص الوعي الإلكتروني لدى عملاء البنك.	4.123	0.744	18.0	82.4	مرتفع
2	دخول فيروسات وبرمجيات الحاسوب.	4.066	0.746	18.3	81.4	مرتفع
3	ضعف التشريعات والقوانين المحلية في مجال تكنولوجيا المعلومات.	3.978	0.611	15.3	79.6	مرتفع
4	ضعف الرقابة الخارجية على نظم المعلومات المحاسبية المحوسبة للبنوك.	3.791	0.721	19.0	75.8	مرتفع
5	التغيير التكنولوجي غير المتوازن.	3.541	0.632	17.9	70.8	مرتفع
6	الكوارث الطبيعية والسياسية.	3.480	0.803	23.0	69.6	مرتفع
7	المخترقون والقرصنة.	3.303	0.770	23.3	66.0	متوسط
8	المنافسة الاقتصادية بين البنوك.	2.857	0.583	20.4	57.2	متوسط
	المتوسط العام	3.642	0.412	11.3	72.8	مرتفع

• مستوى التهديد الخارجي حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 – 2.59) منخفض، (2.60 – 3.39) متوسط، (3.40 – 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

(1) الجدول من إعداد الباحث اعتماداً على مخرجات التحليل الإحصائي SPSS.

ومن الجدول السابق يتضح ما يلي:

■ إن أهم التهديدات الخارجية التي تؤدي إلى حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة هي التهديدات التي تتعلق بنقص الوعي الإلكتروني لدى عملاء البنك بالمرتبة الأولى ثم يليها التهديدات المتعلقة بدخول فيروسات وبرمجيات الحاسوب بالمرتبة الثانية، يليها ضعف التشريعات والقوانين المحلية في مجال تكنولوجيا المعلومات، ثم ضعف الرقابة الخارجية على نظم المعلومات المحاسبية المحوسبة للبنوك، ثم التغيير التكنولوجي غير المتوازن، والكوارث الطبيعية والسياسية، ثم المخترقون والقراصنة، وكان أقلها أهمية هي التهديدات المتعلقة بالمنافسة الاقتصادية بين البنوك.

■ إن قيم المتوسط الحسابي لكل تهديد من التهديدات الخارجية المسببة لمخاطر أمن نظم المعلومات المحاسبية على مستوى المتغيرات الرئيسية كانت أكبر من المتوسط الحسابي المعتمد وفق المقياس المستخدم في هذه الدراسة وهو (3) درجات، ماعدا التهديدات المتعلقة بالمخترقين والقراصنة والمنافسة الاقتصادية بين البنوك، وقد تراوحت قيمة المتوسط الحسابي لتلك التهديدات بين (4.123) بنسبة (82.4%)، وبمستوى مرتفع للتهديد الخارجي المتعلق بنقص الوعي الإلكتروني لدى عملاء البنوك، وبين (2.857) بنسبة (57.2%)، وبمستوى متوسط للتهديد الخارجي المتعلق بالمنافسة الاقتصادية بين البنوك، وبمعامل اختلاف لم يتجاوز (23.3%) وتدل هذه النتيجة على أنَّ المستجيبين يجمعون بنسبة كبيرة إلى حد ما أن التهديدات الخارجية تسبب مخاطر أمن نظم المعلومات المحاسبية لدى البنوك التجارية العاملة في الجمهورية اليمنية، وبمستوى مرتفع.

بالنظر إلى ترتيب التهديدات الخارجية المسببة لمخاطر أمن نظم المعلومات المحاسبية المحوسبة في الجدول السابق أعلاه رقم (4-3-6) يلاحظ أن التهديدات المتعلقة بنقص الوعي الإلكتروني لدى عملاء البنك، قد احتلت المرتبة الأولى وبمستوى مرتفع، حيث حصلت على أعلى متوسط حسابي، والذي بلغت قيمته (4.123) درجة، وبمعامل اختلاف لا يتجاوز (18%)، ويدل ذلك على انسجام كبير بين آراء أفراد العينة حول أن تلك التهديدات مرتفعة وتسبب في حدوث المخاطر بنسبة (70.4%)، ولعل ذلك يعود إلى انخفاض وعي العملاء وعدم إلمامهم الكافي بكيفية استخدام نظام الانترنت المصرفي وعدم إحاطتهم بإجراءات التأمين والوقاية، وعدم قيام البنوك بتوعية العملاء وتعريفهم بالاحتياطات الأمنية الواجب اتخاذها وحدود مسؤوليتهم، حيث أن جزء لا يستهان به ليسوا على دراية كافية بهذا المجال، فالتكنولوجيا قد تكون بلا فائدة لمن لا يملك القدرة والمعرفة على التعامل معها.

■ بينما جاءت التهديدات المتعلقة بالمنافسة الاقتصادية بين البنوك في المرتبة السادسة والأخيرة وبمستوى متوسط، حيث بلغ إجمالي المتوسط الحسابي لها (2.857)، وبمعامل اختلاف لا يتجاوز (20.4%)، ويدل ذلك على تقارب بين آراء أفراد العينة حول أن تلك التهديدات متوسطة وتسبب في حدوث مخاطر أمن نظم المعلومات

المحاسبية المحوسبة وبأهمية نسبية لا تتجاوز (57.2%)، ولعل مرد ذلك يعود إلى عدم اكتشاف أي حالة تجسس أو اختراق بين تلك البنوك.

- يستخلص الباحث مما سبق، أن التهديدات الخارجية الواردة في الجدولين السابقين كانت مرتفعة بشكل عام وتتسبب في حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية وبأهمية نسبية بلغت (63 %) حسب آراء عينة الدراسة.

3-3-6: تحليل البيانات المتعلقة بمدى تأثير حدوث المخاطر على عناصر أمن نظم المعلومات

المحاسبية المحوسبة:

وفقاً لفرضيات الدراسة ونموذجها يمثل تأثير المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة أحد المتغيرات المستقلة للدراسة، والهدف من قياسها معرفة مدى تأثير حدوث تلك المخاطر على عناصر أمن تلك النظم، وقد تم قياس هذا المتغير من خلال المحور الرابع من محاور الجزء الثالث للاستقصاء والذي تضمن (14) فقره تبرز مدى تأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة، حيث قام الباحث باستخدام التحليل الوصفي تمهيداً لاختبار الفرضية الرابعة، فقد استخرج المتوسطات الحسابية والانحرافات المعيارية ومعاملات الاختلاف والأهمية النسبية ومستوى التهديد ورتبته، وفقاً لآراء أفراد عينة الدراسة حول مضمون كل فقرة من تلك الفقرات التي تقيس تلك التأثيرات والجدول التالي يلخص نتائج التحليل الوصفي للفقرات المتعلقة بذلك:

جدول رقم (3-3-9) الإحصاءات الوصفية على مستوى الفقرات والمتغيرات الرئيسية

المتعلقة بمدى تأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة

الترتيب	مستوى تأثير الخطر	الأهمية النسبية 100 %	معامل الاختلاف 100 %	الانحراف المعياري	المتوسط الحسابي	مدى تأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة	رقم الفقرة
14	متوسط	55.2	35.8	0.987	2.762	تعرض نظام المعلومات المحاسبي بالبنك للتعطيل بسبب المخاطر يؤثر على استرجاع البيانات والمعلومات ويترتب على ذلك خسائر مالية كبيرة، وقد يؤدي ذلك إلى خروج البنك من السوق وإفلاسه.	77
10	متوسط	65.4	31.4	1.028	3.271	تدمير البنية التحتية لنظم المعلومات المحاسبية وتوقفها لفترات طويلة يؤدي إلى إعاقة وصول المستخدمين والأطراف المستفيدة، مما يفقد البنك فرص نشاط حقيقية.	78
7	مرتفع	69.4	28.2	0.980	3.467	حالات التعطيل والتوقف المفاجئ لنظام المعلومات المحاسبي للبنك لبعض الوقت يؤدي إلى اهتزاز مكانة البنك أمام عملائه وتكبده خسائر تجارية ومالية كبيرة.	79
الرابع	متوسط	63.2	26.6	0.840	3.167	تأثير المخاطر على إتاحة نظم المعلومات المحاسبية المحوسبة.	79-77
9	متوسط	67.8	27.0	0.913	3.385	حدوث مخاطر أمن نظم المعلومات المحاسبية يؤثر على سلامة تجهيز البيانات وعمليات التشغيل والمخرجات، بالدقة والشمولية المطلوبة وفي الوقت المناسب.	80
1	مرتفع	77.8	23.4	0.910	3.885	تشغيل النظام بشكل خاطئ وباستخدام برامج غير ملائمة يؤدي إلى حصول البنك لمخرجات غير دقيقة وغير سليمة، يؤثر على صحتها ومصداقيتها.	81

الترتيب	مستوى تأثير الخطر	الأهمية النسبية 100 %	معامل الاختلاف %100	الانحراف المعياري	المتوسط الحسابي	مدى تأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة	رقم الفقرة
5	مرتفع	70.8	24.1	0.854	3.541	تعرض نظم المعلومات المحاسبية المحوسبة بالبنك إلى أي خطر يخفض من تكامل تلك النظم مع بعضها البعض على مستوى الأقسام والفروع، فوقع خطأ ما يؤدي إلى وقوع سلسلة من الأخطاء نتيجة التحديث الفوري للملفات.	82
الأول	مرتفع	72	21.2	0.764	3.604	تأثير المخاطر على سلامة وتكامل تجهيز البيانات في نظم المعلومات المحاسبية.	82-80
3	مرتفع	73.2	31.3	1.147	3.664	إن اقتحام نظام المعلومات المحاسبية من أطراف غير مخولة بالدخول، يؤدي إلى إمكانية سرقة أو تسرب معلومات هامة على درجة عالية من السرية لجهات غير مرغوب فيها.	83
12	متوسط	56.6	23.5	0.664	2.828	إن حدوث مخاطر أمن نظم المعلومات المحاسبية يؤدي إلى إطلاع المنافسين على المعلومات المرتبطة بالبنك والتي قد يترتب عليها الإضرار بالموقف التنافسي.	84
6	مرتفع	70.6	28.5	1.005	3.539	إن حدوث المخاطر يؤدي إلى عدم قدرة نظام المعلومات المحاسبية بالبنك على التعامل مع الأطراف المستفيدة المختلفة وفقاً لأصول السرية والفائدة المرجوة.	85
الثالث	متوسط	66.8	24.0	0.801	3.342	تأثير المخاطر على سرية المعلومات المحاسبية.	85-83
2	مرتفع	73.8	24.0	0.882	3.689	إن حدوث مخاطر أمن نظم المعلومات المحاسبية يؤدي إلى ضعف قدرة البنك في حماية خصوصيات وأسرار عملائه، نتيجة سرقة أو كشف المعلومات الشخصية لهم والتي يتم جمعها واستخدامها والاحتفاظ بها من قبل نظام المعلومات المحاسبية للبنك.	86
4	مرتفع	72.0	25.7	0.924	3.598	إن تعرض البنك لمخاطر أمن نظم المعلومات المحاسبية يهدد سمعته نتيجة فقدان الثقة وفشل البنك في تحقيق متطلبات العملاء بتقديم خدمة مصرفية إلكترونية متطورة وأمنة.	87
8	مرتفع	68.4	25.7	0.879	3.418	إن حدوث مخاطر أمن نظم المعلومات المحاسبية يؤدي إلى عدم إتاحة الفرصة للعملاء للوصول إلى المعلومات المخزنة الشخصية لتعديلها أو إلغائها.	88
الثاني	مرتفع	71.4	19.7	0.703	3.568	تأثير المخاطر على خصوصية بيانات الأطراف المتعاملة مع البنك.	88-86
11	متوسط	57.6	26.6	0.766	2.877	حدوث المخاطر يؤدي إلى تهريب بعض أطراف المعاملات الإلكترونية من الالتزامات، عن طريق إنكار وقوع أحداث وقعت أو ادعاء وقوع أحداث لم تقع، وقد يؤدي ذلك إلى تحمل البنك لخسائر مالية وفقدان الثقة في مخرجات نظم المعلومات المحاسبية.	89
13	متوسط	55.8	29.2	0.815	2.787	رفض بعض الجهات الحكومية لحجية مخرجات نظم المعلومات المحاسبية المحوسبة استناداً لنصوص تشريعية، كالقانون التجاري وقانون البنوك.	90
الخامس	متوسط	56.6	21.8	0.618	2.832	تأثير المخاطر على إثبات تصرفات الأطراف المتعاملة خلال تبادل البيانات إلكترونياً.	90-89
	متوسط	66.0	17.8	0.586	3.303	المتوسط العام لتأثير المخاطر ككل.	90-77

مستوى التهديد حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 – 2.59) منخفض، (2.60 – 3.39) متوسط، (3.40 – 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

تشير النتائج الواردة في الجدول السابق إلى ما يلي:

- إن المتوسط الحسابي الإجمالي لتقديرات أفراد العينة عن كافة الفقرات والمتغيرات الرئيسية التي تقيس مدى تأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية قد بلغ (3.303) درجة من أصل (5) درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي المعياري في هذه الدراسة والبالغة (3) درجات، والأهمية النسبية لتلك التهديدات قدرها (66%)، والذي يقابل مستوى التهديد المتوسط، وهي أكبر من نسبة المتوسط الحسابي المعتمدة في هذه الدراسة والبالغة (60%)، وبلغت قيمة الانحراف المعياري عن المتوسط الحسابي (0.586) فقط، مما يدل على تقارب الإجابات وأنها تتمحور حول المتوسط الحسابي، ويؤكد ذلك أن معامل الاختلاف لم يتجاوز (17.8%)، وهي تمثل نسبة ضئيلة وتدل على عدم تشتت واختلاف البيانات عن المتوسط الحسابي، وأن هناك تقارب وانسجام إلى حد كبير بين معظم أفراد عينة الدراسة في الإجابة عن فقرات هذا المحور الخاص بقياس مدى تأثير المخاطر على عناصر أمن نظم المعلومات المحاسبية، وأن مستوى تلك التأثيرات كان بشكل عام متوسط لدى البنوك التجارية العاملة في الجمهورية اليمنية، ويؤكد ذلك قيم المتوسطات الحسابية لمعظم المتغيرات الفرعية والرئيسية الخاصة بذلك المحور.
- إن قيم الانحراف المعياري لمعظم الفقرات قد بلغت أقل من الواحد الصحيح، وبلغ الانحراف المعياري للمجال ككل (0.586) فقط، مما يدل على أن آراء أفراد العينة لمعظم تلك الفقرات كانت متقاربة إلى حد ما، ويؤكد ذلك أن قيم معامل الاختلاف لتلك الفقرات قد تراوحت بين (23.4%~35.8%)، وهي قيم منخفضة نسبياً تعكس مدى التقارب في وجهات نظر المستجيبين.
- إن اتجاهات عينة الدراسة كانت إيجابية في (10) فقرات كان ترتيبها من (1) إلى (10) حسب الترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات حيث كانت أكبر من المتوسط الحسابي المعتمد وفق المقياس المستخدم في هذه الدراسة وهو (3) درجات، ولكن أربع فقرات ترتيبها من (11) إلى (14) حسب الترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات كانت إجابات أفراد العينة عليها سلبية وغير مؤيدة لها لأن قيم المتوسط الحسابي لكلا منها كانت أقل من (3) درجات، وقد تراوح المتوسط الحسابي لجميع الفقرات بين (2.762~3.885)، ومعامل الاختلاف لتلك الفقرات لم يتجاوز (35.8%) مما يدل على تقارب الإجابات حول المتوسط الحسابي، وتدل هذه النتيجة على أن المستجيبين يجمعون بنسبة متوسطة إلى حد ما على أن حدوث تلك المخاطر لدى البنوك التجارية العاملة في الجمهورية اليمنية تؤثر على عناصر أمن نظم المعلومات المحاسبية المحوسبة لدى تلك البنوك.
- وكان مستوى تأثيرات حدوث المخاطر مرتفع في (8) فقرات ترتيبها يقع بين (1~8) والتي يزيد المتوسط الحسابي لكل منها عن (3.4) درجة، أي أنه يوجد موافقة على أن حدوث تلك المخاطر يؤثر على عناصر أمن نظم المعلومات بدرجة مرتفعة، فقد تراوح المتوسط الحسابي لتلك الفقرات بين (3.418~3.885)، ويلاحظ أن التأثير الوارد في الفقرة رقم (81) والذي يتعلق بتشغيل النظام بشكل خاطئ وباستخدام برامج غير ملائمة

يؤدي إلى حصول البنك لمخرجات غير دقيقة وغير سليمة، يؤثر على صحتها ومصداقيتها، قد احتل المرتبة الأولى بأعلى متوسط حسابي بلغ (3.885) بأهمية نسبية بلغت (77.8%)، وبانحراف معياري (0.910)، ومعامل اختلاف لم يتجاوز (23.4%)، وهذا يؤكد أن معظم أفراد عينة الدراسة المستقصى منهم كانوا متفقين على أن ذلك التأثير مرتفع ونسبة (77.8%)، وهذا يشير إلى أن حدوث مخاطر أمن نظم المعلومات المحاسبية لدى البنوك التجارية في الجمهورية اليمنية قد يتسبب في حصول البنك لمخرجات غير دقيقة وغير سليمة، يؤثر على صحتها ومصداقيتها، وضعف قدرة البنك في حماية خصوصيات وأسرار عملائه، نتيجة سرقة أو كشف المعلومات الشخصية لهم والتي يتم جمعها واستخدامها والاحتفاظ بها من قبل نظام المعلومات المحاسبي للبنك، وإمكانية سرقة أو تسرب معلومات هامة على درجة عالية من السرية لجهات غير مرغوب فيها، وتلك التأثيرات نالت موافقة غالبية أفراد عينة الدراسة على أن حدوث المخاطر يؤدي إلى حدوث تلك التأثيرات السلبية على أمن نظم المعلومات المحاسبية وبمستوى مرتفع بأهمية نسبية تراوحت بين (68.4%~77.8%)، وفي رأي الباحث أن هذا أمر يستوجب من البنوك التجارية العاملة في اليمن تداركه بشتى وسائل الحماية.

■ وكان مستوى تأثيرات حدوث المخاطر متوسط في (6) فقرات والتي كان ترتيبها بين (9~14) وفقاً للترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات، حيث تراوح المتوسط الحسابي لها بين (2.762~3.385) والذي يعكس مدى الأهمية النسبية لتلك التهديدات الواقع بين (55.2%~67.8%)، وبمعامل اختلاف لتلك الفقرات لم يتجاوز (30.1%)، وكان أهم تأثيرات حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية وبمستوى متوسط هو التأثير المتعلق بسلامة تجهيز البيانات وعمليات التشغيل والمخرجات، بالدقة والشمولية المطلوبة وفي الوقت المناسب، والذي جاء في المرتبة (9) على مستوى تأثيرات المخاطر ككل، حيث بلغ متوسطه الحسابي (3.385)، ومعامل الاختلاف (27%)، وهو ما يدل على انسجام وتقارب كبير بين آراء أفراد العينة على أن حدوث المخاطر يؤثر على عناصر أمن نظم المعلومات المحاسبية بنسبة (67.8%)، بينما التأثير المتعلق بتعرض نظام المعلومات المحاسبي بالبنك للتعطيل بسبب المخاطر يؤثر على استرجاع البيانات والمعلومات ويترتب على ذلك خسائر مالية كبيرة، وقد يؤدي ذلك إلى خروج البنك من السوق وإفلاسه، جاء في المرتبة (14) والأخير، وبمتوسط حسابي بلغ (2.762)، ومعامل الاختلاف لا يزيد عن (35.8%)، وهو ما يدل على انسجام وتقارب إلى حد ما بين آراء أفراد العينة الذين أفادوا بأن حدوث المخاطر يؤثر على عناصر أمن نظم المعلومات المحاسبية بنسبة وبمستوى متوسط الأهمية بنسبة (55.2%)، وهو ما يستوجب من البنوك الاهتمام وبما يؤدي إلى التخفيف من تأثيرات تلك المخاطر إلى أدنى حد ممكن.

■ ويمكن القول بصفة إجمالية بأن إجابات أفراد العينة حول تأثيرات حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التي يعملون بها، كانت غالبيتها ترى بأن هناك تأثيرات لتلك المخاطر فقد حصل (8) من التأثيرات على درجة موافقة مرتفعة، في مقابل حصول (6) تأثيرات على درجة موافقة متوسطة، ولا يوجد تأثير حصل على درجة موافقة منخفضة، مما يشير إلى أن المخاطر تؤثر على

عناصر أمن نظم المعلومات المحاسبية وبمستوى أهمية متوسط ولا يقل عن (66%) وهنا يجب على هذه البنوك مواجهة تلك المخاطر المؤثرة على أمن نظم المعلومات المحاسبية المحوسبة بشتى الإجراءات والوسائل.

- بالنظر إلى المتغيرات الرئيسية لمدى تأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة، وبناءً على المتوسط الحسابي لتلك التأثيرات، والأهمية النسبية لها، تم ترتيب متغيرات تلك التأثيرات تنازلياً، كما هو مبين في الجدول (10-3-3):

جدول رقم (10-3-3) الإحصاءات الوصفية للمتغيرات الرئيسية المتعلقة بتأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة مرتبة تنازلياً حسب الأهمية النسبية⁽¹⁾

رتبة التأثير	تأثيرات المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى التهديد
1	تأثير المخاطر على سلامة وتكامل تجهيز البيانات في نظم المعلومات المحاسبية.	3.604	0.764	21.2	72.0	مرتفع
2	تأثير المخاطر على خصوصية بيانات الأطراف المتعاملة مع البنك.	3.568	0.703	19.7	71.4	مرتفع
3	تأثير المخاطر على سرية المعلومات المحاسبية.	3.342	0.801	24.0	66.8	متوسط
4	تأثير المخاطر على إتاحة نظم المعلومات المحاسبية المحوسبة.	3.167	0.840	26.6	63.2	متوسط
5	تأثير المخاطر على إثبات تصرفات الأطراف المتعاملة خلال تبادل البيانات إلكترونياً.	2.832	0.618	21.8	56.6	متوسط
	المتوسط العام	3.303	0.586	17.8	66.0	متوسط

مستوى تأثير المخاطر حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 – 2.59) منخفض، (2.60 – 3.39) متوسط، (3.40 – 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

ومن الجدول السابق يتضح ما يلي:

- أن أهم التأثيرات لحدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة هو تأثير المخاطر على سلامة وتكامل تجهيز البيانات في نظم المعلومات المحاسبية، والذي جاء في المرتبة الأولى ثم يليها تأثير المخاطر على خصوصية بيانات الأطراف المتعاملة مع البنك بالمرتبة الثانية، يليها تأثير المخاطر على سرية المعلومات المحاسبية، ثم تأثير المخاطر على إتاحة نظم المعلومات المحاسبية المحوسبة، وكان أقلها أهمية هي تأثير المخاطر على إثبات تصرفات الأطراف المتعاملة خلال تبادل البيانات إلكترونياً.
- إن قيم المتوسط الحسابي لكل تهديد من التهديدات الخارجية المسببة لمخاطر أمن نظم المعلومات المحاسبية على مستوى المتغيرات الرئيسية كانت أكبر من المتوسط الحسابي المعتمد وفق المقياس المستخدم في هذه الدراسة وهو (3) درجات، ماعدا تأثير المخاطر على إثبات تصرفات الأطراف المتعاملة خلال تبادل البيانات

(1) الجدول من إعداد الباحث اعتماداً على مخرجات التحليل الإحصائي SPSS.

الالكترونيًا، وقد تراوحت قيمة المتوسط الحسابي لتلك التأثيرات بين (2.832) بنسبة (56.6%)، وبمستوى متوسط لتأثير حدوث المخاطر على إثبات تصرفات الأطراف المتعاملة خلال تبادل البيانات الكترونياً، وبين (3.604) بنسبة (72%)، وبمستوى مرتفع لتأثير المخاطر على سلامة وتكامل تجهيز البيانات في نظم المعلومات المحاسبية، وبمعامل اختلاف لم يتجاوز (26.6%) للمتغيرات ككل، وتدل هذه النتيجة على أنَّ المستجيبين يجمعون بنسبة كبيرة إلى حدٍ ما أن حدوث المخاطر يؤثر على عناصر أمن نظم المعلومات المحاسبية لدى البنوك التجارية العاملة في الجمهورية اليمنية، وبمستوى متوسط، وبأهمية نسبية للموافقة لا تقل عن (66%).

■ بالنظر إلى ترتيب المتغيرات الرئيسية لتأثيرات حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة في الجدول السابق أعلاه رقم (3-3-10) يلاحظ أن تأثير المخاطر على سلامة وتكامل تجهيز البيانات في نظم المعلومات المحاسبية، قد احتل المرتبة الأولى وبمستوى مرتفع، حيث حصلت على أعلى متوسط حسابي، والذي بلغت قيمته (3.604) درجة، وبمعامل اختلاف لا يتجاوز (21.2%)، ويدل ذلك على انسجام كبير بين آراء أفراد العينة حول أن حدوث المخاطر يؤثر على سلامة وتكامل تجهيز البيانات في نظم المعلومات المحاسبية بنسبة (72%)، ولعل ذلك قد يعود إلى وجود برامج في نظم المعلومات المحاسبية المحوسبة لا تعمل بشكل جيد ومتربط فيما بينها، فتحتوى على أخطاء ، ولا يتم الحصول على النتائج المطلوبة بشكل دقيق، في الوقت المناسب.

■ بينما جاء تأثير المخاطر على إثبات تصرفات الأطراف المتعاملة خلال تبادل البيانات الكترونياً في المرتبة الخامسة والأخيرة وبمستوى متوسط، حيث بلغ إجمالي المتوسط الحسابي لها (2.832)، وبمعامل اختلاف لا يتجاوز (21.8%)، ويدل ذلك على تقارب بين آراء أفراد العينة حول أن حدوث المخاطر يؤثر على إثبات تصرفات الأطراف المتعاملة خلال تبادل البيانات الكترونياً وبأهمية نسبية لا تتجاوز (56.6%)، ولعل مرد ذلك يعود إلى استخدام البنوك الخاضعة للدراسة الوسائل المختلفة للتحقق من صحة التعاملات التي تعزز عدم الإنكار وتحدد المسؤوليات في التعاملات المصرفية الإلكترونية.

■ **يستخلص الباحث مما سبق،** إن تأثيرات حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة في الجدولين السابقين كانت مرتفعة بشكل عام وتتسبب في تأثيرات سلبية على أمن تلك النظم لدى البنوك التجارية في الجمهورية اليمنية وبأهمية نسبية بلغت (66%) حسب آراء عينة الدراسة.

3-3-7: تحليل البيانات المتعلقة بحماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات

المحاسبية المحوسبة

وفقاً لفرضيات الدراسة ونموذجها تمثل حماية الأمن التنظيمي للأفراد أحد المتغيرات الفرعية المستقلة للدراسة، والهدف من قياسها معرفة مدى تطبيق إجراءات ووسائل حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، وقد تم قياس هذا المتغير من خلال أحد المتغيرات الرئيسية للمحور الخامس من محاور الجزء الثالث للاستقصاء والذي تضمن (10) فقرات تبرز مدى تطبيق البنوك لإجراءات ووسائل حماية الأمن التنظيمي، حيث قام الباحث باستخدام التحليل الوصفي تمهيداً لاختبار الفرضية الخامسة، فقد استخرج المتوسطات الحسابية والانحرافات المعيارية ومعاملات الاختلاف والأهمية النسبية ومستوى الحماية ورتبته، وفقاً لآراء أفراد عينة الدراسة حول مضمون كل فقرة من تلك الفقرات التي تقيس مدى تطبيق تلك الإجراءات والجدول التالي يلخص نتائج التحليل الوصفي للفقرات المتعلقة بذلك:

جدول رقم (3-3-11) الإحصاءات الوصفية على مستوى الفقرات المتعلقة بمدى تطبيق

إجراءات ووسائل حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية المحوسبة

رقم الفقرة	حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية المحوسبة	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى تطبيق الحماية	الترتيب التنازلي
91	يوجد في البنك قسم خاص ومستقل بشكل كافي وبإمكانات مناسبة مسؤول عن تنفيذ أمن نظم المعلومات المحاسبية وحمايتها، ووضع معايير وأسس وضوابط أمنية.	2.639	0.739	28.0	52.8	متوسط	(8)
92	يوجد دليل عمل مكتوب يتضمن إجراءات أداء العمل لكافة وظائف نظم المعلومات المحاسبية، محدد فيه السلطات والمسئوليات والكفاءات الملزمة لكل وظيفة داخل النظام.	3.492	0.893	25.5	69.8	مرتفع	(4)
93	يوجد نظام صلاحية مبرمج بحيث يسمح للنظام لكل مستخدم بإدارة نظم المعلومات المحاسبية حسب صلاحياته في التعامل مع ملفات النظام، (مثل قراءة البيانات أو نسخها أو تعديلها...الخ)، من خلال الوصول إلى أجزاء معينة وبيانات محددة.	3.787	0.845	23.0	75.8	مرتفع	(2)
94	كل مستخدم للنظام له كلمة سر خاصة، فلا يتشارك اثنان بكلمة سر واحدة، ويتم إيقاف صلاحيات المستخدم إذا تم إدخال كلمة المرور خطأ أكثر من العدد المسموح به للمحاولات.	4.148	0.849	20.5	83.6	مرتفع	(1)
95	هناك فصل سليم بين الوظائف والمهام المختلفة والمتعارضة لمعالجة البيانات بين المبرمجين والمشغلين والمراقبين والمستخدمين بطريقة تسمح بمراقبة تنفيذ المهام.	3.771	0.831	22.0	75.4	مرتفع	(3)
96	يعمل البنك على تنفيذ سياسة التدوير الوظيفي للمهام الأساسية لنظم المعلومات المحاسبية، بإجراء تنقلات بين الموظفين من حين لآخر، والزامهم بأخذ إجازاتهم السنوية دفعة واحدة.	2.426	0.667	27.4	48.6	منخفض	(10)

رقم الفقرة	حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية المحوسبة	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى تطبيق الحماية	الترتيب التنازلي
97	يعقد البنك برامج بواسطة مختصين في أمن نظم المعلومات لتوعية العاملين بالمخاطر التي تهدد أمن نظم المعلومات المحاسبية، وتدريبهم على إتباع الإجراءات الملائمة لمواجهتها.	2.443	0.862	35.3	48.8	منخفض	(9)
98	يتم تشجيع الأفراد على اتخاذ مبادرات لحل المشكلات، ومكافأة من يقوم بعمل إيجابي نحو تجسيد نظام الحماية، ومراقبة من يتعامل سلباً مع المخاطر ويخالفون سياسات الأمن.	2.779	0.766	27.6	55.6	متوسط	(6)
99	يعين البنك شخص مسؤول عن حماية النظام يسمى ضابط أمن المعلومات، ويتم تكوين فريق طوارئ، من فنيين وإداريين فاعلين، لمواجهة أي ظرف طارئ يمس بحماية النظام.	2.762	0.680	24.6	55.2	متوسط	(7)
100	يتم اختيار موظفي نظم المعلومات المحاسبية بحرص شديد وإجراء تحريات عنهم وعن ماضيهم الوظيفي، والحرص على أن يكونوا ذوي خبرة وثقة وأمانة ويعملون لمصلحة البنك، وعدم إعطاء الموظف حديث التعيين صلاحيات عالية لاستخدام النظام.	3.295	0.984	29.8	66.0	متوسط	(5)
	المتوسط العام	3.154	0.517	16.4	63.0	متوسط	

• مستوى تطبيق إجراءات الحماية حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 ~ 2.59) منخفض، (2.60 ~ 3.39) متوسط، (3.40 ~ 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

تشير النتائج الواردة في الجدول رقم (3-3) أعلاه إلى ما يلي:

- إن المتوسط الحسابي الإجمالي لتقديرات أفراد العينة عن كافة الفقرات التي تقيس مدى تطبيق إجراءات ووسائل حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية قد بلغ (3.154) درجة من أصل (5) درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي المعياري في هذه الدراسة والبالغة (3) درجات، وبأهمية نسبية بالموافقة على أن البنوك التجارية في اليمن تطبق تلك الإجراءات قدرها (63%)، والذي يعكس مستوى الحماية المتوسط، وهي أكبر من نسبة المتوسط الحسابي المعتمدة في هذه الدراسة والبالغة (60%)، وبلغت قيمة الانحراف المعياري عن المتوسط الحسابي (0.517) فقط، مما يدل على تقارب الإجابات وأنها تتمحور حول المتوسط الحسابي، ويؤكد ذلك أن معامل الاختلاف لم يتجاوز (16.4%) للمتغير ككل، وهي تمثل نسبة ضئيلة وتدل على عدم تشتت واختلاف البيانات عن المتوسط الحسابي، وأن هناك تقارب وانسجام إلى حد كبير بين معظم أفراد عينة الدراسة في الإجابة عن فقرات هذا المتغير وأن مستوى تطبيق إجراءات ووسائل حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية المحوسبة كان بشكل عام متوسطاً لدى البنوك التجارية العاملة في الجمهورية اليمنية، ويؤكد ذلك قيم المتوسطات الحسابية لمعظم الفقرات.
- إن قيم الانحراف المعياري لجميع الفقرات كانت أقل من الواحد الصحيح، وبلغ الانحراف المعياري للمجال ككل (0.517) فقط، مما يدل على أن آراء أفراد العينة لمعظم تلك الفقرات كانت متقاربة إلى حد ما، ويؤكد

ذلك أن قيم معامل الاختلاف لتلك الفقرات قد تراوحت بين (20.5%~35.3%)، وهي قيم منخفضة نسبياً تعكس مدى التقارب في وجهات نظر المستجيبين.

■ إن اتجاهات عينة الدراسة كانت إيجابية في (5) فقرات كان ترتيبها من (1) إلى (5) حسب الترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات حيث كانت أكبر من المتوسط الحسابي المعتمد وفق المقياس المستخدم في هذه الدراسة وهو (3) درجات، بينما (5) فقرات والتي ترتيبها من (6) إلى (10) كانت إجابات أفراد العينة عليها سلبية وغير مؤيدة لهما لأن قيم المتوسط الحسابي لكلا منها كانت أقل من (3) درجات، وقد تراوح المتوسط الحسابي لجميع الفقرات بين (2.426~4.148) درجة، وبمعامل اختلاف لتلك الفقرات لم يتجاوز (35.3%)، وتدل هذه النتيجة على أن المستجيبين يجمعون بنسبة متوسطة إلى حد ما على أن مستوى تطبيق إجراءات ووسائل حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية لدى البنوك التجارية العاملة في الجمهورية اليمنية كان متوسطاً.

■ كان مستوى تطبيق إجراءات ووسائل الحماية مرتفعاً في (4) فقرات، ترتيبها يقع بين (1~4) والتي يزيد المتوسط الحسابي لكل منها عن (3.4) درجة، أي أنه يوجد موافقة على أن تلك الإجراءات والوسائل تطبق لدى البنوك التجارية في الجمهورية اليمنية بدرجة مرتفعة، فقد تراوح المتوسط الحسابي لتلك الفقرات بين (3.492~4.148) درجة، ويلاحظ أن إجراء الحماية الوارد في الفقرة رقم (94) والذي يتعلق بأن كل مستخدم للنظام له كلمة سر خاصة، فلا يتشارك اثنان بكلمة سر واحدة، ويتم إيقاف صلاحيات المستخدم إذا تم إدخال كلمة المرور خطأ أكثر من العدد المسموح به للمحاولات، قد نال المرتبة الأولى بأعلى متوسط حسابي بلغ (4.148) درجة، وبأهمية نسبية بلغت (83.6%)، وبانحراف معياري (0.849)، ومعامل اختلاف لم يتجاوز (20.5%)، وهذا يؤكد أن معظم أفراد عينة الدراسة المستقصى منهم كانوا متفقين على أن تطبيق ذلك الإجراء مرتفع وبنسبة (83.6%)، وهذا يشير إلى أن أهم إجراءات حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية لدى البنوك التجارية في الجمهورية اليمنية تتمثل في الإجراء السابق ذكره والذي نال المرتبة الأولى، بالإضافة للإجراءات المتعلقة بوجود نظم صلاحية مبرمجة تسمح لكل مستخدم بإدارة نظام المعلومات المحاسبي حسب صلاحياته في التعامل مع ملفات النظام، (مثل قراءة البيانات أو نسخها أو تعديلها...الخ)، من خلال الوصول إلى أجزاء معينة وبيانات محددة، وهناك فصل سليم بين الوظائف والمهام المختلفة والمتعارضة لمعالجة البيانات بين المبرمجين والمشغلين والمراقبين والمستخدمين بطريقة تسمح بمراقبة تنفيذ المهام، كما يوجد دليل عمل مكتوب يتضمن إجراءات أداء العمل لكافة وظائف نظم المعلومات المحاسبية، محدد فيه السلطات والمسؤوليات والكفاءات الملائمة لكل وظيفة داخل النظام، وتلك نقاط قوة في نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية تعمل على تخفيض مخاطر أمن الأفراد إلى أدنى حد ممكن، وتلك الإجراءات نالت موافقة غالبية أفراد عينة الدراسة على أنها مطبقة وبمستوى مرتفع وبأهمية نسبية تراوحت بين (69.8%~83.6%)، وفي رأي الباحث أن هذه النتيجة تنسجم

وتتفق مع مستوى حدوث مخاطر أمن الأفراد العاملين والتي ظهرت عند مناقشة المحور الأول، وهذا أمر يستوجب من البنوك التجارية العاملة في اليمن المحافظة على مستوى تطبيق تلك الإجراءات وتعزيز تطبيقها بما يؤدي إلى رفع فعالية وكفاءة تلك الإجراءات لمواجهة تلك المخاطر.

■ كان مستوى تطبيق إجراءات الحماية متوسطاً في (4) فقرات والتي كان ترتيبها بين (5~8) وفقاً للترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات، حيث تراوح المتوسط الحسابي لها بين (2.639~3.295) درجة، وذلك يعكس مدى الأهمية النسبية لتطبيق تلك الإجراءات الواقع بين (52.8%~66.0%)، وبمعامل اختلاف لتلك الفقرات لم يتجاوز (29.8%)، وكان أهم إجراء مطبق لحماية الأمن التنظيمي للأفراد بمستوى متوسط هو الإجراء المتعلق باختيار موظفي نظم المعلومات المحاسبية بحرص شديد وإجراء تحريات عنهم وعن ماضيهم الوظيفي، والحرص على أن يكونوا ذوي خبرة وثقة وأمانة ويعملون لمصلحة البنك، وعدم إعطاء الموظف حديث التعيين صلاحيات عالية لاستخدام النظام، والذي جاء في المرتبة (5)، حيث بلغ متوسط الحسابي (3.295) درجة، وبمعامل اختلاف (29.8%)، وهو ما يدل على انسجام وتقارب كبير بين آراء أفراد العينة على أن ذلك الإجراء يطبق لدى البنوك التجارية بأهمية نسبية للموافقة بلغت (66%)، وهو ما يستوجب من البنوك تعزيز ذلك الإجراء.

■ كان مستوى تطبيق إجراءات الحماية منخفضاً في الفقرتين (97، 96) والتي كان ترتيبها (9 و10) وفقاً للترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرتين، حيث تراوح المتوسط الحسابي لها بين (2.426~2.443) درجة وذلك يعكس مدى الأهمية النسبية لتطبيق تلك الإجراءات الواقع بين (48.6%~48.8%)، وبمعامل اختلاف لتلك الفقرتين لم يتجاوز (35.3%)، وتتمثل تلك الإجراءات التي نالت مستوى تطبيق منخفض في: الإجراء المتعلق بأن البنك يعمل على تنفيذ سياسة التدوير الوظيفي للمهام الأساسية لنظم المعلومات المحاسبية، بإجراء تنقلات بين الموظفين من حين لآخر، وإلزامهم بأخذ إجازاتهم السنوية دفعة واحدة، والإجراء المتعلق بأن البنك يعقد برامج بواسطة مختصين في أمن نظم المعلومات لتوعية العاملين بالمخاطر التي تهدد أمن نظم المعلومات المحاسبية، وتدريبهم على إتباع الإجراءات الملائمة لمواجهة تلك المخاطر، وانخفاض تطبيق تلك الإجراءات يعد من نقاط الضعف في تلك النظم وهو ما يستدعي من البنوك التجارية في الجمهورية اليمنية العمل على تطبيق تلك الإجراءات بكفاءة وفعالية حتى يمكن تلافي المخاطر التي قد تحدث نتيجة ضعف مستوى تطبيقها.

■ ويمكن للباحث القول بصفة إجمالية بأن إجابات أفراد العينة حول مستوى تطبيق إجراءات ووسائل حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية المحسوبة لدى البنوك التي يعملون بها، كانت غالبيتها ترى بأن هناك تطبيق لتلك الإجراءات فقد حصل (4) إجراءات على درجة موافقة مرتفعة، في مقابل حصول (4) إجراءات على درجة موافقة متوسطة، وحصل إجراءين على درجة موافقة منخفضة، مما يشير إلى أن إجراءات حماية الأمن التنظيمي للأفراد مطبقة ولكن بشكل غير كافي، حيث بلغت الأهمية النسبية للموافقة على تطبيق تلك الإجراءات (63%) وبمستوى متوسط، وهنا يجب على البنوك التجارية في الجمهورية اليمنية

العمل على رفع كفاءة وفعالية تطبيق تلك الإجراءات لمواجهة مخاطر أمن نظم المعلومات المحاسبية بشكل عام، ومخاطر أمن الأفراد العاملين في تلك النظم على وجه الخصوص.

3-3-8: تحليل البيانات المتعلقة بحماية الأمن المادي لنظم المعلومات المحاسبية

وفقاً لفرضيات الدراسة ونموذجها تمثل حماية الأمن المادي للنظم أحد المتغيرات الفرعية المستقلة للدراسة، والهدف من قياسها معرفة مدى تطبيق إجراءات ووسائل حماية الأمن المادي لنظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، وقد تم قياس هذا المتغير من خلال أحد المتغيرات الرئيسية للمحور الخامس من محاور الجزء الثالث للاستقصاء والذي تضمن (11) فقرة تبرز مدى تطبيق البنوك لإجراءات ووسائل حماية الأمن المادي، حيث قام الباحث باستخدام التحليل الوصفي تمهيداً لاختبار الفرضية الخامسة، فقد استخرج المتوسطات الحسابية والانحرافات المعيارية ومعاملات الاختلاف والأهمية النسبية ومستوى الحماية ورتبته، وفقاً لآراء أفراد عينة الدراسة حول مضمون كل فقرة من تلك الفقرات التي تقيس مدى تطبيق تلك الإجراءات والجدول التالي يلخص نتائج التحليل الوصفي للفقرات المتعلقة بذلك:

جدول رقم (3-3-12) الإحصاءات الوصفية على مستوى الفقرات المتعلقة بمدى تطبيق

إجراءات ووسائل حماية الأمن المادي لنظم المعلومات المحاسبية

رقم الفقرة	حماية الأمن المادي لنظم المعلومات المحاسبية	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى تطبيق الحماية	الترتيب التنازلي
101	توجد خطة طوارئ معلنة وموثقة خاصة لمواجهة الكوارث تتضمن إعداد وحدة متكاملة من تجهيزات الحاسوب والشبكات، ونسخة احتياطية من قاعدة البيانات، في موقع آخر بديل غير الموقع الرئيسي لضمان استمرارية العمل، واستئناف النشاط بصورة سريعة.	2.664	0.745	28.0	53.2	متوسط	9
102	تتضمن خطة الطوارئ مصفوفة مخاطر أمن نظم المعلومات المحاسبية المتوقعة، والأثر الناتج، والجهة المتأثرة، والتصرف اللازم لمواجهتها.	2.508	0.695	27.7	50.2	منخفض	10
103	يتعاقد البنك مع شركات تأمين متخصصة للتأمين على الأجهزة والبرمجيات وشبكات المعلومات والموظفين في نظام المعلومات المحاسبي المحوسب، ضد كافة المخاطر.	3.402	1.041	30.6	68.0	مرتفع	7
104	يتم تصميم مواقع العمل وأماكن الأجهزة والمعدات، بصورة تتلاءم مع التغيرات الطبيعية، ويتم وضع أجهزة النظام في غرف محمية وأمنة، وعدم السماح بالدخول إليها لأي كان.	3.164	0.816	25.8	63.2	متوسط	8
105	يتم استخدام جميع الوسائل المادية التي تمنع الوصول غير المخول إلى نظم المعلومات	3.689	0.988	26.8	73.8	مرتفع	5

رقم الفقرة	حماية الأمن المادي لنظم المعلومات المحاسبية	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى تطبيق الحماية	الترتيب التنازلي
	المحاسبية وقواعدها كرجال الحراسة، والأقفال والحواجز والغرف المحصنة وغيرها.						
106	يستخدم موظفي البنك بطاقات دخول الكترونية ذكية ممغنطة عليها صورهم الشخصية، للدخول إلى أماكن عملهم عبر البوابات المقفلة المبرمجة وفق الصلاحيات المخولة لهم، ويصدر إنذار مبكر فور الدخول المادي غير المخول.	2.107	0.800	37.9	42.2	منخفض	11
107	يقوم البنك بتثبيت كاميرات تلفزيونية على خارج مبنى دائرة النظام والممرات الداخلية فيها، وتعمل على مراقبة المستخدمين والأماكن التي توجد تجهيزات النظام، من موقع مركزي.	3.762	0.872	23.1	75.2	مرتفع	3
108	يتم استخدام منظم كهربائي، وبطاريات إضافية، وخزانات طاقة، ومولد كهربائي لتجنب ارتفاع أو انخفاض الطاقة الكهربائية أو انقطاعها، وتعطلها بشكل مفاجئ، والذي يؤدي إلى تلف أجهزة وبرامج الحاسوب أو توقفها عن العمل.	4.123	0.744	18.1	82.4	مرتفع	2
109	يتم تركيب أجهزة كشف الحريق في الأماكن المعرضة للخطر وتجهيزها بالشكل المناسب الذي يساعد على كشف الحريق بأسرع وقت ممكن وسرعة القيام بمقاومة الحريق.	4.164	0.753	18.1	83.2	مرتفع	1
110	يتم استخدام أسقف وحوائط وأرضيات تمنع تسرب المياه، مع استخدام أغطية واقية من الأتربة والماء، وتركيب أجهزة إنذار من المياه والرطوبة.	3.525	1.107	31.4	70.4	مرتفع	6
111	يتم إجراء صيانة دورية ومستمرة لأجهزة النظام ووسائل حمايته بما فيها أجهزة التكييف، لضمان استمرار عملها بفاعلية، ويتم توفير قطع ومعدات بديلة للأجهزة العاملة بشكل سريع فور تعطلها، بما يضمن سلامة الحواسيب وحمايتها.	3.656	0.951	26.1	73.0	مرتفع	4
111-101	المتوسط العام	3.342	0.571	17.1	66.8	متوسط	

• مستوى تطبيق إجراءات الحماية حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 ~ 2.59) منخفض، (2.60 ~ 3.39) متوسط، (3.40 ~ 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

تشير النتائج الواردة في الجدول السابق رقم (3-3-12) إلى ما يلي:

- إن المتوسط الحسابي الإجمالي لتقديرات أفراد العينة عن كافة الفقرات التي تقيس مدى تطبيق إجراءات ووسائل حماية الأمن المادي لنظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية قد بلغ (3.342) درجة من أصل (5) درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي المعياري في هذه الدراسة والبالغة (3) درجات، وبأهمية نسبية بالموافقة على أن البنوك التجارية في اليمن تطبق تلك

الإجراءات قدرها (66.8%) والذي يعكس مستوى الحماية المتوسط، وهي أكبر من نسبة المتوسط الحسابي المعتمدة في هذه الدراسة والبالغة (60%)، وبلغت قيمة الانحراف المعياري عن المتوسط الحسابي (0.571) فقط، مما يدل على تقارب الإجابات وأنها تتمحور حول المتوسط الحسابي، ويؤكد ذلك أن معامل الاختلاف لم يتجاوز (17.1%) للمتغير ككل، وهي تمثل نسبة ضئيلة وتدل على عدم تشتت واختلاف البيانات عن المتوسط الحسابي، وأن هناك تقارب وانسجام إلى حد كبير بين معظم أفراد عينة الدراسة في الإجابة عن فقرات هذا المتغير وأن مستوى تطبيق إجراءات ووسائل حماية الأمن المادي لنظم المعلومات المحاسبية المحوسبة كان بشكل عام متوسطاً لدى البنوك التجارية العاملة في الجمهورية اليمنية، ويؤكد ذلك قيم المتوسطات الحسابية لمعظم الفقرات.

- إن قيم الانحراف المعياري لمعظم الفقرات كانت أقل من الواحد الصحيح، وبلغ الانحراف المعياري للمجال ككل (0.571) فقط، مما يدل على أن آراء أفراد العينة لمعظم تلك الفقرات كانت متقاربة إلى حد ما، ويؤكد ذلك أن قيم معامل الاختلاف لتلك الفقرات قد تراوحت بين (18.1%~37.9%)، وهي قيم منخفضة ومتوسطة نسبياً تعكس مدى التقارب في وجهات نظر المستجيبين.
- إن اتجاهات عينة الدراسة كانت إيجابية في (8) فقرات كان ترتيبها من (1) إلى (8) حسب الترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات حيث كانت أكبر من المتوسط الحسابي المعتمد وفق المقياس المستخدم في هذه الدراسة وهو (3) درجات، بينما (3) فقرات والتي ترتيبها من (9) إلى (11) كانت إجابات أفراد العينة عليها سلبية وغير مؤيدة لها لأن قيم المتوسط الحسابي لكلا منها كانت أقل من (3) درجات، وقد تراوح المتوسط الحسابي لجميع الفقرات بين (2.107~4.164) درجة، وبمعامل اختلاف لتلك الفقرات لم يتجاوز (37.9%)، وتدل هذه النتيجة على أن المستجيبين يجمعون بنسبة متوسطة إلى حد ما على أن مستوى تطبيق إجراءات ووسائل حماية الأمن المادي لنظم المعلومات المحاسبية لدى البنوك التجارية العاملة في الجمهورية اليمنية كان متوسطاً.
- كان مستوى تطبيق إجراءات ووسائل حماية الأمن المادي مرتفعاً في (7) فقرات، ترتيبها يقع بين (1~7) والتي يزيد المتوسط الحسابي لكل منها عن (3.4) درجة، أي أنه يوجد موافقة على أن تلك الإجراءات والوسائل تطبق لدى البنوك التجارية في الجمهورية اليمنية بدرجة مرتفعة، فقد تراوح المتوسط الحسابي لتلك الفقرات بين (3.402~4.164) درجة، ويلاحظ أن إجراء الحماية الوارد في الفقرة رقم (109) والذي يتعلق بأنه يتم تركيب أجهزة كشف الحريق في الأماكن المعرضة للخطر وتجهيزها بالشكل المناسب الذي يساعد على كشف الحريق بأسرع وقت ممكن وسرعة القيام بمقاومة الحريق، قد احتل المرتبة الأولى بأعلى متوسط حسابي بلغ (4.164) وبأهمية نسبية بلغت (83.2%)، وبانحراف معياري (0.753)، ومعامل اختلاف لم يتجاوز (18.1%)، وهذا يؤكد أن معظم أفراد عينة الدراسة المستقصى منهم كانوا متفقين على أن تطبيق ذلك الإجراء مرتفع وبنسبة (83.2%)، وهذا يشير إلى أن أهم إجراءات حماية الأمن المادي لنظم المعلومات المحاسبية لدى البنوك التجارية في الجمهورية اليمنية تتمثل في الإجراء السابق ذكره والذي نال المرتبة

الأولى، بالإضافة للإجراءات المتعلقة باستخدام منظم كهربائي، وبطاريات إضافية، وخزانات طاقة، ومولد كهربائي لتجنب ارتفاع أو انخفاض الطاقة الكهربائية أو انقطاعها، وتعطلها بشكل مفاجئ، والذي يؤدي إلى تلف أجهزة وبرامج الحاسوب أو توقفها عن العمل، وقيام البنك بتنشيط كاميرات تلفزيونية على خارج مبنى دائرة النظام والممرات الداخلية فيها، وتعمل على مراقبة المستخدمين والأماكن التي توجد تجهيزات النظام، من موقع مركزي، وتلك نقاط قوة في نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في اليمن تعمل على تخفيض مخاطر الأمن المادي لتلك النظم إلى أدنى حد ممكن، وتلك الإجراءات نالت موافقة غالبية أفراد عينة الدراسة على أنها مطبقة وبمستوى مرتفع وبأهمية نسبية تراوحت بين (68%~83.2%)، وفي رأي الباحث أن هذه النتيجة تتسجم وتتفق مع مستوى حدوث مخاطر الأمن المادي التي ظهرت عند مناقشة المحور الأول، وهذا أمر يستوجب من البنوك التجارية العاملة في اليمن المحافظة على مستوى تطبيق تلك الإجراءات وتعزيز تطبيقها بما يؤدي إلى رفع فعالية وكفاءة تلك الإجراءات لمواجهة تلك المخاطر.

■ كان مستوى تطبيق إجراءات الحماية متوسطاً في الفقرتين (104، 101) والتي كان ترتيبها (8) و(9) وفقاً للترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات، حيث تراوح المتوسط الحسابي لها بين (2.664~3.164) درجة وذلك يعكس مدى الأهمية النسبية لتطبيق تلك الإجراءات الواقع بين (53.2%~63.2%)، وبمعامل اختلاف لتلك الفقرتين لم يتجاوز (28%)، وكان أهم إجراء مطبق لحماية الأمن المادي بمستوى متوسط هو الإجراء المتعلق بتصميم مواقع العمل وأماكن الأجهزة والمعدات بصورة تتلاءم مع التغيرات الطبيعية، ويتم وضع أجهزة النظام في غرف محمية وأمنة، وعدم السماح بالدخول إليها لأي كان، والذي جاء في المرتبة (8)، حيث بلغ متوسطه الحسابي (3.164)، ومعامل الاختلاف (25.8%)، وهو ما يدل على انسجام وتقارب كبير بين آراء أفراد العينة على أن ذلك الإجراء يطبق لدى البنوك التجارية بأهمية نسبية للموافقة بلغت (63.2%)، وهو ما يستوجب من البنوك تعزيز ذلك الإجراء.

■ كان مستوى تطبيق إجراءات الحماية منخفضاً في الفقرتين (102، 106) والتي كان ترتيبها (10) و(11) وفقاً للترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرتين، حيث تراوح المتوسط الحسابي لها بين (2.107~2.508) درجة وذلك يعكس مدى الأهمية النسبية لتطبيق تلك الإجراءات الواقع بين (42.2%~50.2%)، وبمعامل اختلاف لتلك الفقرتين بلغ (27.7%)، و(37.9%)، وتتمثل الإجراءات التي نالت مستوى تطبيق منخفض في الإجراءات التي تتعلق بتضمين خطة الطوارئ مصفوفة مخاطر أمن نظم المعلومات المحاسبية المتوقعة، والأثر الناتج، والجهة المتأثرة، والتصرف اللازم لمواجهة، واستخدام موظفي البنك بطاقات دخول الكترونية ذكية ممغنطة عليها صورهم الشخصية، للدخول إلى أماكن عملهم عبر البوابات المقفلة المبرمجة وفق الصلاحيات المخولة لهم، ويصدر إنذار مبكر فور الدخول المادي غير المخول، وانخفاض تطبيق تلك الإجراءات يعد من نقاط الضعف في تلك النظم، وهو ما يستدعي من البنوك التجارية في

الجمهورية اليمنية العمل على تطبيق تلك الإجراءات بكفاءة وفاعلية حتى يمكن تلافي المخاطر التي قد تحدث نتيجة ضعف مستوى تطبيقها.

■ ويمكن للباحث القول بصفة إجمالية بأن إجابات أفراد العينة حول مستوى تطبيق إجراءات ووسائل حماية الأمن المادي لنظم المعلومات المحاسبية المحوسبة لدى البنوك التي يعملون بها، كانت غالبيتها ترى بأن هناك تطبيق لتلك الإجراءات فقد حصل (7) إجراءات على درجة موافقة مرتفعة، في مقابل حصول إجراءات على درجة موافقة متوسطة، كما حصل إجراءات على درجة موافقة منخفضة، مما يشير إلى أن إجراءات حماية الأمن المادي مطبقة ولكن بشكل غير كافٍ، حيث بلغت الأهمية النسبية للموافقة على تطبيق تلك الإجراءات (66.8%) وبمستوى متوسط ، وهنا يجب على البنوك التجارية في الجمهورية اليمنية العمل على رفع كفاءة وفاعلية تطبيق تلك الإجراءات لمواجهة مخاطر أمن نظم المعلومات المحاسبية بشكل عام، ومخاطر الأمن المادي في تلك النظم على وجه الخصوص.

3-3-9: تحليل البيانات المتعلقة بحماية أمن الوصول البرمجي لقاعدة البيانات المتصلة بنظم المعلومات المحاسبية المحوسبة

وفقاً لفرضيات الدراسة ونموذجها تمثل حماية أمن الوصول البرمجي لقاعدة البيانات أحد المتغيرات الفرعية المستقلة للدراسة، والهدف من قياسها معرفة مدى تطبيق إجراءات ووسائل حماية أمن الوصول البرمجي لقاعدة البيانات المتصلة بنظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، وقد تم قياس هذا المتغير من خلال أحد المتغيرات الرئيسية للمحور الخامس من محاور الجزء الثالث للاستقصاء والذي تضمن (9) فقرات تبرز مدى تطبيق البنوك لإجراءات ووسائل حماية أمن الوصول البرمجي، حيث قام الباحث باستخدام التحليل الوصفي تمهيداً لاختبار الفرضية الخامسة، فقد استخرج المتوسطات الحسابية والانحرافات المعيارية ومعاملات الاختلاف والأهمية النسبية ومستوى الحماية ورتبته، وفقاً لآراء أفراد عينة الدراسة حول مضمون كل فقرة من تلك الفقرات التي تقيس مدى تطبيق تلك الإجراءات والجدول التالي يلخص نتائج التحليل الوصفي للفقرات المتعلقة بذلك:

جدول رقم (3-3-13) الإحصاءات الوصفية على مستوى الفقرات المتعلقة بمدى تطبيق إجراءات ووسائل حماية أمن الوصول البرمجي لقاعدة البيانات المتصلة بنظم المعلومات المحاسبية المحوسبة

رقم الفقرة	حماية أمن الوصول البرمجي لقاعدة البيانات المتصلة بنظم المعلومات	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى الحماية	الترتيب
112	يتم التحقق من هوية الشخص أو المعدات التي تحاول الدخول للنظام من خلال خليط من (كلمات مرور/ كروت ذكية/ معرفات بيولوجية/ أجهزة أخرى).	3.730	0.872	23.4	74.6	مرتفع	(3)
113	يتم استخدام مستويات متتالية من الرقابة على دخول قاعدة البيانات بكلمات مرور متعددة ومختلفة للدخول إلى	3.689	1.012	27.4	73.8	مرتفع	(4)

رقم الفقرة	حماية أمن الوصول البرمجي لقاعدة البيانات المتصلة بنظم المعلومات	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى الحماية	الترتيب
	(الشبكة أو الحاسوب أو سيرفر البيانات أو قاعدة البيانات)، ويتم التنبيه للموظفين بعدم إفشاء كلمات المرور لسرية، وتكون من الصعب تخمينها.						
114	يوجد سجل خاص لجميع الصلاحيات الممنوحة للموظفين المخولين بالدخول للنظام، ويتم برمجة مصفوفة الرقابة على الوصول آلياً، فيتم تحديد كلمة سر خاصة لكل موظف، والملفات والبرامج التي يصرح له بالوصول إليها	3.762	0.909	24.2	75.2	مرتفع	(2)
115	يتم تغيير كلمات السر بشكل دوري ومستمر وخاصة بعد نقل الموظفين ويتم إلغاء كلمة السر الخاصة بالموظف الذي استقال أو أقيل من العمل بشكل فوري.	3.869	0.926	24.0	77.4	مرتفع	(1)
116	يتم استخدام برامج الجدران النارية العازلة لمنع الوصول غير المصرح به إلى النظام، ومنع المستخدم من استخدام برامج أو ملفات لا يملك الصلاحية للدخول إليها، ويتم تحديث تلك البرامج وتعديلها باستمرار.	3.451	1.004	29.1	69.0	مرتفع	(5)
117	يوثق النظام كافة محاولات الوصول غير المصرح بها، ويصدر تقرير حولها يتضمن وقت المحاولة والموقع الذي تمت من خلاله، ويتم معالجة ذلك بإغلاق الفجوات المكتشفة.	3.452	1.053	30.6	69.0	مرتفع	(6)
118	يتم إجراء اختبار اختراق النظام بصورة دورية من قبل المراجعين الداخليين أو الخارجيين، أو بواسطة خبرات متخصصة لمعرفة نقاط الضعف في نظم المعلومات الحاسوبية.	2.303	0.726	31.6	46.0	منخفض	(9)
119	يحرص البنك على تحميل واستخدام برامج متطورة وأصلية وفعالة مضادة لفيروسات الحاسوب وبرمجياته الخبيثة، ويتم تحديثها بشكل دوري ومستمر.	3.189	0.865	27.1	63.8	متوسط	(7)
120	يتم استخدام وسيلة التشفير لكافة البيانات والمعلومات الهامة المحفوظة في قاعدة البيانات.	2.787	0.864	31.0	55.8	متوسط	(8)
	المتوسط العام	3.359	0.689	21.0	67.0	متوسط	

- مستوى تطبيق إجراءات الحماية حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 ~ 2.59) منخفض، (2.60 ~ 3.39) متوسط، (3.40 ~ 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

تشير النتائج الواردة في الجدول السابق رقم (3-3-13) إلى ما يلي:

- إن المتوسط الحسابي الإجمالي لتقديرات أفراد العينة عن كافة الفقرات التي تقيس مدى تطبيق إجراءات ووسائل حماية أمن الوصول البرمجي لقاعدة بيانات نظم المعلومات الحاسوبية المحسوبة لدى البنوك التجارية في الجمهورية اليمنية قد بلغ (3.359) درجة من أصل (5) درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي المعياري في هذه الدراسة والبالغة (3) درجات، وبأهمية نسبية بالموافقة على أن البنوك التجارية في اليمن تطبق تلك الإجراءات قدرها (67%)، والذي يعكس مستوى الحماية المتوسط، وهي أكبر من نسبة المتوسط الحسابي المعتمدة في هذه الدراسة والبالغة (60%)، وبلغت قيمة الانحراف المعياري عن المتوسط

الحسابي (0.689) فقط، مما يدل على تقارب الإجابات وأنها تتمحور حول المتوسط الحسابي، ويؤكد ذلك أن معامل الاختلاف لم يتجاوز (21%) للمتغير ككل، وهي تمثل نسبة منخفضة تدل على عدم تشتت واختلاف البيانات عن المتوسط الحسابي، وأن هناك تقارب وانسجام إلى حد كبير بين معظم أفراد عينة الدراسة في الإجابة عن فقرات هذا المتغير وأن مستوى تطبيق إجراءات ووسائل حماية أمن الوصول البرمجي لقاعدة بيانات نظم المعلومات المحاسبية المحوسبة كان بشكل عام متوسطاً لدى البنوك التجارية العاملة في الجمهورية اليمنية، ويؤكد ذلك قيم المتوسطات الحسابية لمعظم الفقرات.

■ إن قيم الانحراف المعياري لمعظم الفقرات كانت أقل من الواحد الصحيح، وبلغ الانحراف المعياري للمجال ككل (0.689) فقط، مما يدل على أن آراء أفراد العينة لمعظم تلك الفقرات كانت متقاربة إلى حد ما، ويؤكد ذلك أن قيم معامل الاختلاف لتلك الفقرات قد تراوحت بين (24%~31.6%)، وهي قيم منخفضة ومتوسطة نسبياً تعكس مدى التقارب في وجهات نظر المستجيبين.

■ إن اتجاهات عينة الدراسة كانت إيجابية في (7) فقرات كان ترتيبها من (1) إلى (7) حسب الترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات حيث كانت أكبر من المتوسط الحسابي المعتمد وفق المقياس المستخدم في هذه الدراسة وهو (3) درجات، بينما الفقرتين (120، 118) والتي ترتيبها (9، 8) على التوالي، كانت إجابات أفراد العينة عليهما سلبية وغير مؤيدة لهما لأن قيم المتوسط الحسابي لكلا منهما كانت أقل من (3) درجات، وقد تراوح المتوسط الحسابي لجميع الفقرات بين (2.303~3.869) درجة، وبمعامل اختلاف لتلك الفقرات لم يتجاوز (31.6%)، وتدلل هذه النتيجة على أن المستجيبين يجمعون بنسبة متوسطة إلى حد ما على أن مستوى تطبيق إجراءات ووسائل حماية الأمن البرمجي لقاعدة البيانات المتصلة بنظم المعلومات المحاسبية لدى البنوك التجارية العاملة في الجمهورية اليمنية كان متوسطاً.

■ كان مستوى تطبيق إجراءات ووسائل حماية الأمن البرمجي مرتفعاً في (6) فقرات، ترتيبها يقع بين (1~6) والتي يزيد المتوسط الحسابي لكل منها عن (3.4) درجة، أي أنه يوجد موافقة على أن تلك الإجراءات والوسائل تطبق لدى البنوك التجارية في الجمهورية اليمنية بدرجة مرتفعة، فقد تراوح المتوسط الحسابي لتلك الفقرات بين (3.452~3.869) درجة، ويلاحظ أن إجراء الحماية الوارد في الفقرة رقم (115) والذي يتعلق بأنه يتم تغيير كلمات السر بشكل دوري ومستمر وخاصة بعد نقل الموظفين ويتم إلغاء كلمة السر الخاصة بالموظف الذي استقال أو أقيّل من العمل بشكل فوري، قد احتل المرتبة الأولى بأعلى متوسط حسابي بلغ (3.869) درجة، وبأهمية نسبية بلغت (77.4%)، وبانحراف معياري (0.926)، ومعامل اختلاف لم يتجاوز (24%)، وهذا يؤكد أن معظم أفراد عينة الدراسة المستقصى منهم كانوا متفقين على أن تطبيق ذلك الإجراء مرتفع وبنسبة (77.4%)، وهذا يشير إلى أن أهم إجراءات حماية الأمن البرمجي لنظم المعلومات المحاسبية لدى البنوك التجارية في الجمهورية اليمنية تتمثل في الإجراء السابق ذكره والذي نال المرتبة الأولى بالإضافة للإجراءات المتعلقة بوجود سجل خاص لجميع الصلاحيات الممنوحة للموظفين المخولين بالدخول للنظام، ويتم برمجة مصفوفة الرقابة على الوصول آلياً، فيتم تحديد كلمة سر خاصة لكل موظف، والملفات أو البرامج التي

يصرح له بالوصول إليها، والتحقق من هوية الشخص أو المعدات التي تحاول الدخول للنظام من خلال خليط من (كلمات مرور/ كروت ذكية/ معرفات بيولوجية/ أجهزة أخرى)، وتلك نقاط قوة في نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في اليمن تعمل على تخفيض مخاطر الأمن البرمجي لتلك النظم إلى أدنى حد ممكن، وتلك الإجراءات نالت موافقة غالبية أفراد عينة الدراسة على أنها مطبقة وبمستوى مرتفع وبأهمية نسبية تراوحت بين (69%~77.4%)، وفي رأي الباحث أن هذه النتيجة تتسجم وتتفق مع مستوى حدوث مخاطر الأمن البرمجي للنظم التي ظهرت عند مناقشة المحور الأول، وهذا أمر يستوجب من البنوك التجارية العاملة في اليمن المحافظة على مستوى تطبيق تلك الإجراءات وتعزيز تطبيقها بما يؤدي إلى رفع فعالية وكفاءة تلك الإجراءات لمواجهة تلك المخاطر.

■ كان مستوى تطبيق إجراءات الحماية متوسطاً في الفقرتين (119، 120) والتي كان ترتيبها (7) و(8) وفقاً للترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات، حيث تراوح المتوسط الحسابي لها بين (2.787~3.189) درجة، والذي يعكس مدى الأهمية النسبية لتطبيق تلك الإجراءات الواقع بين (55.8%~63.8%)، وبمعامل اختلاف لتلك الفقرتين لم يتجاوز (31%)، وكان أهم إجراء مطبق لحماية الأمن البرمجي بمستوى متوسط هو الإجراء المتعلق بتحميل واستخدام برامج متطورة وأصلية وفعالة مضادة لفيروسات الحاسوب وبرمجياته الخبيثة، ويتم تحديثها بشكل دوري ومستمر، والذي جاء في المرتبة (7)، حيث بلغ متوسطه الحسابي (3.189)، ومعامل الاختلاف (27.1%)، وهو ما يدل على انسجام وتقارب كبير بين آراء أفراد العينة على أن ذلك الإجراء يطبق لدى البنوك التجارية بأهمية نسبية للموافقة بلغت (63.8%)، وهو ما يستوجب من البنوك تعزيز ذلك الإجراء.

■ كان مستوى تطبيق إجراءات الحماية منخفضاً في الفقرة (118) والمتعلقة بإجراء اختبار اختراق النظام بصورة دورية من قبل المراجعين الداخليين أو الخارجيين، أو بواسطة خبرات متخصصة لمعرفة نقاط الضعف في نظم المعلومات المحاسبية، وكان ترتيبها (9) وفقاً للترتيب التنازلي لقيمة المتوسط الحسابي لتلك الفقرة، والتي بلغت (2.303) درجة والذي يعكس مدى الأهمية النسبية لتطبيق ذلك الإجراءات والتي بلغت (46%)، وبمعامل اختلاف لتلك الفقرة بلغ (31.6%)، وانخفاض تطبيق ذلك الإجراءات يعد من نقاط الضعف في تلك النظم، وهو ما يستدعي من البنوك التجارية في الجمهورية اليمنية العمل على تطبيق ذلك الإجراء بكفاءة وفعالية حتى يمكن تلافي المخاطر التي قد تحدث نتيجة ضعف مستوى تطبيقه.

■ ويمكن للباحث القول بصفة إجمالية بأن إجابات أفراد العينة حول مستوى تطبيق إجراءات ووسائل حماية أمن الوصول البرمجي لقاعدة البيانات المتصلة بنظم المعلومات المحاسبية المحوسبة لدى البنوك التي يعملون بها، كانت غالبيتها ترى بأن هناك تطبيق لتلك الإجراءات فقد حصل (6) إجراءات على درجة موافقة مرتفعة، في مقابل حصول إجراءين على درجة موافقة متوسطة، كما حصل إجراء واحد على درجة موافقة منخفضة، مما يشير إلى أن إجراءات حماية الأمن البرمجي مطبقة ولكن بشكل غير كافٍ، حيث بلغت الأهمية النسبية للموافقة على تطبيق تلك الإجراءات (67%) وبمستوى متوسط، وهنا يجب على البنوك التجارية في الجمهورية اليمنية

العمل على رفع كفاءة وفعالية تطبيق تلك الإجراءات لمواجهة مخاطر أمن نظم المعلومات المحاسبية بشكل عام، ومخاطر الأمن البرمجي في تلك النظم على وجه الخصوص.

3-3-10: تحليل البيانات المتعلقة بحماية أمن وسائط التخزين غير المتصلة بنظم المعلومات

المحاسبية المحوسبة

وفقاً لفرضيات الدراسة ونموذجها تمثل حماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية أحد المتغيرات الفرعية المستقلة للدراسة، والهدف من قياسها معرفة مدى تطبيق إجراءات ووسائل حماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، وقد تم قياس هذا المتغير من خلال أحد المتغيرات الرئيسية للمحور الخامس من محاور الجزء الثالث للاستقصاء والذي تضمن (4) فقرات تبرز مدى تطبيق البنوك لإجراءات ووسائل حماية أمن وسائط التخزين، حيث قام الباحث باستخدام التحليل الوصفي تمهيداً لاختبار الفرضية الخامسة، فقد استخرج المتوسطات الحسابية والانحرافات المعيارية ومعاملات الاختلاف والأهمية النسبية ومستوى الحماية ورتبته، وفقاً لآراء أفراد عينة الدراسة حول مضمون كل فقرة من تلك الفقرات التي تقيس مدى تطبيق تلك الإجراءات والجدول التالي يلخص نتائج التحليل الوصفي للفقرات المتعلقة بذلك:

جدول رقم (3-3-14) الإحصاءات الوصفية على مستوى الفقرات المتعلقة بمدى تطبيق إجراءات ووسائل حماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية المحوسبة

رقم الفقرة	حماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى تطبيق الحماية	الترتيب التنازلي
121	يقوم البنك بأخذ نسخ احتياطية للبرامج وملفات البيانات الهامة بشكل مستمر ودوري (يومي، أسبوعي، شهري)، وتحفظ في خزائن حديدية مقللة لحمايتها من السرقة أو الحريق، وتوضع نسخة منها في مكان آمن خارج مقر العمل.	4.344	0.689	15.9	86.8	مرتفع جداً	(1)
122	يتم تشفير النسخ الاحتياطية من قواعد البيانات لحمايتها من التعديل أو الوصول إليها بطريقة غير مشروعة وذلك لفرض الرقابة عليها.	2.459	0.728	29.6	49.2	متوسط	(4) والآخر
123	توجد رقابة كافية على وسائط تخزين البيانات غير المتصلة بالنظام، ويتم فحص تلك الوسائط باستمرار للتأكد من صحتها وسلامتها.	3.238	0.881	27.2	64.8	متوسط	(3)
124	يتم التخلص من وسائط تخزين البيانات والبرامج بطريقة آمنة معينة وعدم رميها في براميل القمامة، حيث توجد إجراءات رقابية كافية لذلك.	3.607	1.064	29.5	72.2	مرتفع	(2)
124-121	المتوسط العام	3.412	0.627	18.4	68.2	مرتفع	

- مستوى تطبيق إجراءات الحماية حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 ~ 2.59) منخفض، (2.60 ~ 3.39) متوسط، (3.40 ~ 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

تشير النتائج الواردة في الجدول رقم (3-3-14) أعلاه إلى ما يلي:

- إن المتوسط الحسابي الإجمالي لتقديرات أفراد العينة عن كافة الفقرات التي تقيس مدى تطبيق إجراءات ووسائل حماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية قد بلغ (3.412) درجة من أصل (5) درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي المعياري في هذه الدراسة والبالغة (3) درجات، وبأهمية نسبية بالموافقة على أن البنوك التجارية في اليمن تطبيق تلك الإجراءات قدرها (68.2%) والذي يعكس مستوى الحماية المرتفع، وهي أكبر من نسبة المتوسط الحسابي المعتمدة في هذه الدراسة والبالغة (60%)، وبلغت قيمة الانحراف المعياري عن المتوسط الحسابي (0.627) فقط، مما يدل على تقارب الإجابات وأنها تتمحور حول المتوسط الحسابي، ويؤكد ذلك أن معامل الاختلاف لم يتجاوز (18.4%) للمتغير ككل، وهي تمثل نسبة ضئيلة وتدل على عدم تشتت واختلاف البيانات عن المتوسط الحسابي، وأن هناك تقارب وانسجام إلى حد كبير بين معظم أفراد عينة الدراسة في الإجابة عن فقرات هذا المتغير وأن مستوى تطبيق إجراءات ووسائل حماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية المحوسبة كان بشكل عام مرتفعاً لدى البنوك التجارية العاملة في الجمهورية اليمنية، ويؤكد ذلك قيم المتوسطات الحسابية لتلك الفقرات.
- إن قيم الانحراف المعياري لمعظم الفقرات كانت أقل من الواحد الصحيح، وبلغ الانحراف المعياري للمجال ككل (0.627) فقط، مما يدل على أن آراء أفراد العينة لمعظم تلك الفقرات كانت متقاربة إلى حد ما، ويؤكد ذلك أن قيم معامل الاختلاف لتلك الفقرات قد تراوحت بين (15.9%~29.6%)، وهي قيم منخفضة نسبياً تعكس مدى التقارب في وجهات نظر المستجيبين.
- إن اتجاهات عينة الدراسة كانت إيجابية في جميع تلك الفقرات حيث كانت أكبر من المتوسط الحسابي المعتمد وفق المقياس المستخدم في هذه الدراسة وهو (3) درجات، باستثناء الفقرة (122) كانت إجابات أفراد العينة عليها سلبية وغير مؤيدة لها لأن قيمة المتوسط الحسابي لها كانت أقل من (3) درجات، وقد تراوح المتوسط الحسابي لجميع الفقرات بين (2.459~4.344) درجة، وبمعامل اختلاف لتلك الفقرات لم يتجاوز (29.6%)، وتدل هذه النتيجة على أن المستجيبين يجمعون بنسبة متوسطة إلى حد ما على أن مستوى تطبيق إجراءات ووسائل أمن حماية وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية لدى البنوك التجارية العاملة في الجمهورية اليمنية كان مرتفعاً.
- كان مستوى تطبيق إجراءات ووسائل حماية أمن وسائط التخزين مرتفع جداً، ومرتفع في الفقرتين (121)، (124)، والتي يزيد المتوسط الحسابي لكل منها عن (3.4) درجة، أي أنه يوجد موافقة على أن تلك الإجراءات والوسائل تطبق لدى البنوك التجارية في الجمهورية اليمنية بدرجة مرتفعة جداً أو مرتفعة، فقد بلغ المتوسط الحسابي للفقرتين بين (3.607، 4.344) درجة، ويلاحظ أن إجراء الحماية الوارد في الفقرة رقم (121) والذي يتعلق بأخذ نسخ احتياطية للبرامج وملفات البيانات الهامة بشكل مستمر ودوري (يومي، أسبوعي، شهري)، وتحفظ في خزائن حديدية مقفلة لحمايتها من السرقة أو الحريق، وتوضع نسخة منها في مكان آمن خارج مقر العمل، قد احتل المرتبة الأولى بأعلى متوسط حسابي بلغ (4.344) وبأهمية نسبية بلغت (86.8%)، وبانحراف معياري (0.689)، ومعامل اختلاف لم يتجاوز (15.9%)، وهذا يؤكد أن معظم أفراد عينة الدراسة المستقصى منهم كانوا متفقين على أن تطبيق ذلك الإجراء مرتفع وبنسبة (86.8%)، وهذا يشير إلى أن أهم إجراءات حماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية لدى البنوك التجارية في

الجمهورية اليمنية تتمثل في الإجراء السابق ذكره والذي نال المرتبة الأولى، بالإضافة للإجراءات المتعلقة بالتخلص من وسائط تخزين البيانات والبرامج بطريقة آمنة معينة وعدم رميها في براميل القمامة، حيث توجد إجراءات رقابية كافية لذلك، وتلك نقاط قوة في نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في اليمن تعمل على تخفيض مخاطر أمن وسائط التخزين لتلك النظم إلى أدنى حد ممكن، وتلك الإجراءات نالت موافقة غالبية أفراد عينة الدراسة على أنها مطبقة وبمستوى مرتفع وبأهمية نسبية تراوحت بين (72.2%~86.8%)، وفي رأي الباحث أن هذه النتيجة تتسجم وتتفق مع مستوى حدوث مخاطر أمن وسائط التخزين غير المتصلة بالنظم والتي ظهرت عند مناقشة المحور الأول، وهذا أمر يستوجب من البنوك التجارية العاملة في اليمن المحافظة على مستوى تطبيق تلك الإجراءات وتعزيز تطبيقها بما يؤدي إلى رفع فعالية وكفاءة تلك الإجراءات لمواجهة تلك المخاطر.

■ كان مستوى تطبيق إجراءات الحماية متوسطاً في الفقرتين (122، 123) والتي كان ترتيبها (3) و(4) وفقاً للترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات، فقد نال الإجراء المتعلق بتشفير النسخ الاحتياطية من قواعد البيانات لحمايتها من التعديل أو الوصول إليها بطريقة غير مشروعة وذلك لفرض الرقابة عليها، المرتبة الرابعة والأخيرة بمتوسط حسابي بلغ (2.459) وبأهمية نسبية للموافقة بلغت (49.2%)، وبمعامل اختلاف بلغ (29.6)، وهو ما يدل على تقارب كبير بين آراء أفراد العينة على أن ذلك الإجراء يطبق لدى البنوك التجارية بأهمية نسبية للموافقة لا تتجاوز (49.2%)، وانخفاض تطبيق ذلك الإجراء يعد من نقاط الضعف في تلك النظم، وهو ما يستدعي من البنوك التجارية في الجمهورية اليمنية العمل على تطبيق ذلك الإجراء بكفاءة وفعالية حتى يمكن تلافي المخاطر التي قد تحدث نتيجة ضعف مستوى تطبيقه.

■ ويمكن للباحث القول بصفة إجمالية بأن إجابات أفراد العينة حول مستوى تطبيق إجراءات ووسائل حماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية المحوسبة لدى البنوك التي يعملون بها، كانت غالبيتها ترى بأن هناك تطبيق لتلك الإجراءات فقد حصل إجراء على درجة موافقة مرتفعة جداً، وحصل إجراء على درجة موافقة مرتفعة، بينما حصل إجراءين على درجة موافقة متوسطة، مما يشير إلى أن إجراءات حماية الأمن المادي مطبقة وبدرجة مرتفعة ولكن بشكل غير كافٍ، حيث بلغت الأهمية النسبية للموافقة على تطبيق تلك الإجراءات (68.2%) بمستوى مرتفع، وهنا يجب على البنوك التجارية في الجمهورية اليمنية العمل على رفع كفاءة وفعالية تطبيق تلك الإجراءات لمواجهة مخاطر أمن نظم المعلومات المحاسبية بشكل عام، ومخاطر أمن وسائط التخزين غير المتصلة بتلك النظم على وجه الخصوص.

4-3-11: تحليل البيانات المتعلقة بحماية أمن مدخلات نظم المعلومات المحاسبية المحوسبة

وفقاً لفرضيات الدراسة ونموذجها تمثل حماية أمن مدخلات نظم المعلومات المحاسبية أحد المتغيرات الفرعية المستقلة للدراسة، والهدف من قياسها معرفة مدى تطبيق إجراءات ووسائل حماية أمن مدخلات نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، وقد تم قياس هذا المتغير من خلال أحد المتغيرات الرئيسية للمحور الخامس من محاور الجزء الثالث للاستقصاء والذي تضمن (5) فقرات تبرز مدى تطبيق البنوك لإجراءات ووسائل حماية أمن المدخلات، حيث قام الباحث باستخدام التحليل الوصفي تمهيداً لاختبار الفرضية الخامسة، فقد استخرج المتوسطات الحسابية والانحرافات المعيارية ومعاملات الاختلاف والأهمية

النسبية ومستوى الحماية ورتبته، وفقاً لآراء أفراد عينة الدراسة حول مضمون كل فقرة من تلك الفقرات التي تقيس مدى تطبيق تلك الإجراءات والجدول التالي يلخص نتائج التحليل الوصفي للفقرات المتعلقة بذلك:

جدول رقم (3-3-15) الإحصاءات الوصفية على مستوى الفقرات المتعلقة

بمدى تطبيق إجراءات ووسائل حماية أمن مدخلات نظم المعلومات المحاسبية المحوسبة

رقم الفقرة	حماية أمن مدخلات نظم المعلومات المحاسبية المحوسبة	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى تطبيق الحماية	الترتيب التنازلي
125	مستندات إدخال البيانات دقيقة وشاملة لمختلف العمليات، وتساعد على تقليل الأخطاء، ويتم إعدادها وتعبئتها ومصادقتها من الأشخاص المخولين فقط، ويوجد برنامج خاص مصمم لمعرفة من قام بإدخال البيانات.	3.566	0.890	24.9	71.4	مرتفع	(2)
126	يتم تسجيل بيانات المدخلات أولاً بأول وتوجد رقابة كافية لاكتشاف أي نقص فيها، ويتم توثيق عمليات إدخال البيانات بما فيها المحاولات، والمخالفات الخاطئة، ومعرفة مصدرها.	3.369	0.706	20.9	67.4	متوسط	(4)
127	يتم تحديد أخطاء إدخال البيانات وتتبعها حتى يتم تصحيحها وتتضمن برامج النظام ضوابط تمنع إدخال بيانات خاطئة، حيث تظهر رسالة تحذيرية على الشاشة في حال وجود خطأ.	3.434	0.792	23.1	68.6	مرتفع	(3)
128	توجد مراجعة تفصيلية للبيانات المدخلة للتأكد من دقتها واكتمالها، ويتم إجراء المراجعة الثانية لبيانات المستندات المدخلة للتأكد من سلامتها.	3.721	0.730	19.6	74.4	مرتفع	(1)
129	تتوفر في نظم المعلومات المحاسبية خاصية تصحيح البيانات الخاطئة التي تم إدخالها في الوقت المناسب ضمن حدود الرقابة المسموح بها.	3.205	0.861	26.9	64.0	متوسط	(5)
	المتوسط العام	3.459	0.585	16.9	69.2	مرتفع	

• مستوى تطبيق إجراءات الحماية حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 ~ 2.59) منخفض، (2.60 ~ 3.39) متوسط، (3.40 ~ 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

تشير النتائج الواردة في الجدول السابق رقم (3-3-15) إلى ما يلي:

- إن المتوسط الحسابي الإجمالي لتقديرات أفراد العينة عن كافة الفقرات التي تقيس مدى تطبيق إجراءات ووسائل حماية أمن مدخلات نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية قد بلغ (3.459) درجة من أصل (5) درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي المعياري في هذه الدراسة والبالغة (3) درجات، وبأهمية نسبية بالموافقة على أن البنوك التجارية في اليمن تطبيق تلك

الإجراءات قدرها (69.2%) والذي يعكس مستوى الحماية المرتفع، وهي أكبر من نسبة المتوسط الحسابي المعتمدة في هذه الدراسة والبالغة (60%)، وبلغت قيمة الانحراف المعياري عن المتوسط الحسابي (0.585) فقط، مما يدل على تقارب الإجابات وأنها تتمحور حول المتوسط الحسابي، ويؤكد ذلك أن معامل الاختلاف لم يتجاوز (16.9%) للمتغير ككل، وهي تمثل نسبة ضئيلة وتدل على عدم تشتت واختلاف البيانات عن المتوسط الحسابي، وأن هناك تقارب وانسجام إلى حد كبير بين معظم أفراد عينة الدراسة في الإجابة عن فقرات هذا المتغير وأن مستوى تطبيق إجراءات ووسائل حماية أمن مدخلات نظم المعلومات المحاسبية المحوسبة كان بشكل عام مرتفعاً لدى البنوك التجارية العاملة في الجمهورية اليمنية، ويؤكد ذلك قيم المتوسطات الحسابية لتلك الفقرات.

■ إن قيم الانحراف المعياري لجميع الفقرات كانت أقل من الواحد الصحيح، وبلغ الانحراف المعياري للمجال ككل (0.585) فقط، مما يدل على أن آراء أفراد العينة لمعظم تلك الفقرات كانت متقاربة إلى حد ما، ويؤكد ذلك أن قيم معامل الاختلاف لتلك الفقرات قد تراوحت بين (19.6%~26.9%)، وهي قيم منخفضة نسبياً تعكس مدى التقارب في وجهات نظر المستجيبين.

■ إن اتجاهات عينة الدراسة كانت إيجابية في جميع تلك الفقرات حيث كانت أكبر من المتوسط الحسابي المعتمد وفق المقياس المستخدم في هذه الدراسة وهو (3) درجات، وقد تراوح المتوسط الحسابي لجميع الفقرات بين (3.205~3.721) درجة، وبمعامل اختلاف لتلك الفقرات لم يتجاوز (26.9%)، وتدل هذه النتيجة على أن المستجيبين يجمعون بنسبة متوسطة إلى حد ما على أن مستوى تطبيق إجراءات ووسائل أمن مدخلات نظم المعلومات المحاسبية لدى البنوك التجارية العاملة في الجمهورية اليمنية كان مرتفعاً.

■ كان مستوى تطبيق إجراءات ووسائل حماية أمن المدخلات مرتفعاً في ثلاث فقرات كان ترتيبها بين (1~3)، والتي يزيد المتوسط الحسابي لكل منها عن (3.4) درجة، أي أنه يوجد موافقة على أن تلك الإجراءات والوسائل تطبق لدى البنوك التجارية في الجمهورية اليمنية بدرجة مرتفعة، فقد تراوح المتوسط الحسابي لها بين (3.434~3.721) درجة، ويلاحظ أن إجراء الحماية الوارد في الفقرة رقم (128) والذي يتعلق بوجود مراجعة تفصيلية للبيانات المدخلة للتأكد من دقتها واكتمالها، ويتم إجراء المراجعة الثنائية لبيانات المستندات المدخلة للتأكد من سلامتها، قد احتل المرتبة الأولى بأعلى متوسط حسابي بلغ (3.721) وبأهمية نسبية بلغت (74.4%)، وبانحراف معياري (0.730)، ومعامل اختلاف لم يتجاوز (19.6%)، وهذا يؤكد أن معظم أفراد عينة الدراسة المستقصى منهم كانوا متفقين على أن تطبيق ذلك الإجراء مرتفع ونسبة (74.4%)، وهذا يشير إلى أن أهم إجراءات حماية أمن مدخلات نظم المعلومات المحاسبية لدى البنوك التجارية في الجمهورية اليمنية تتمثل في الإجراء السابق ذكره والذي نال المرتبة الأولى، بالإضافة للإجراءات المتعلقة بمستندات إدخال البيانات والتي تتميز بأنها دقيقة وشاملة لمختلف العمليات، وتساعد على تقليل الأخطاء، ويتم إعدادها وتعبئتها ومصادقتها من الأشخاص المخولين فقط، ويوجد برنامج خاص مصمم لمعرفة من قام بإدخال البيانات، كما يتم تحديد أخطاء إدخال البيانات وتتبعها حتى يتم تصحيحها وتتضمن برامج النظام ضوابط تمنع إدخال بيانات

خاطئة، حيث تظهر رسالة تحذيرية على الشاشة في حال وجود خطأ، وتلك الإجراءات نالت موافقة غالبية أفراد عينة الدراسة على أنها مطبقة وبمستوى مرتفع وبأهمية نسبية تراوحت بين (68.6%~74.4%)، وفي رأي الباحث أن هذه النتيجة تنسجم وتتفق مع مستوى حدوث مخاطر أمن المدخلات التي ظهرت عند مناقشة المحور الأول، وهذا أمر يستوجب من البنوك التجارية العاملة في اليمن المحافظة على مستوى تطبيق تلك الإجراءات وتعزيز تطبيقها بما يؤدي إلى رفع فعالية وكفاءة تلك الإجراءات لمواجهة تلك المخاطر.

■ كان مستوى تطبيق إجراءات الحماية متوسطاً في الفقرتين (129، 126) والتي كان ترتيبها (4) و(5) وفقاً للترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات، فقد نال الإجراءات المتعلقة بتوافر خاصية تصحيح البيانات الخاطئة التي تم إدخالها في الوقت المناسب ضمن حدود الرقابة المسموح بها، المرتبة الخامسة والأخيرة بمتوسط حسابي بلغ (3.205) وبأهمية نسبية للموافقة بلغت (64%)، وبمعامل اختلاف بلغ (26.9)، وهو ما يدل على تقارب كبير بين آراء أفراد العينة على أن ذلك الإجراء يطبق لدى البنوك التجارية بأهمية نسبية للموافقة لا تتجاوز (64%)، وانخفاض تطبيق ذلك الإجراء يعد من نقاط الضعف في تلك النظم، وهو ما يستدعي من البنوك التجارية في الجمهورية اليمنية العمل على تطبيق ذلك الإجراء بكفاءة وفاعلية حتى يمكن تلافي المخاطر التي قد تحدث نتيجة ضعف مستوى تطبيقه.

■ ويمكن للباحث القول بصفة إجمالية بأن إجابات أفراد العينة حول مستوى تطبيق إجراءات ووسائل حماية أمن مدخلات نظم المعلومات المحاسبية المحوسبة لدى البنوك التي يعملون بها، كانت غالبيتها ترى بأن هناك تطبيق لتلك الإجراءات فقد حصل ثلاثة إجراءات على درجة موافقة مرتفعة، بينما حصل إجراءان على درجة موافقة متوسطة، مما يشير إلى أن إجراءات حماية أمن المخرجات مطبقة وبدرجة مرتفعة ولكن بشكل غير كافٍ، حيث بلغت الأهمية النسبية للموافقة على تطبيق تلك الإجراءات (69.2%) بمستوى مرتفع، وهنا يجب على البنوك التجارية في الجمهورية اليمنية العمل على رفع كفاءة وفاعلية تطبيق تلك الإجراءات لمواجهة مخاطر أمن نظم المعلومات المحاسبية بشكل عام، ومخاطر أمن مدخلات تلك النظم على وجه الخصوص.

3-3-12: تحليل البيانات المتعلقة بحماية أمن عمليات التشغيل البرمجي لنظم المعلومات

المحاسبية المحوسبة

وفقاً لفرضيات الدراسة ونموذجها تمثل حماية أمن التشغيل البرمجي للنظم أحد المتغيرات الفرعية المستقلة للدراسة، والهدف من قياسها معرفة مدى تطبيق إجراءات ووسائل حماية أمن عمليات التشغيل البرمجي لنظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، وقد تم قياس هذا المتغير من خلال أحد المتغيرات الرئيسية للمحور الخامس من محاور الجزء الثالث للاستقصاء والذي تضمن (5) فقرات تبرز مدى تطبيق البنوك لإجراءات ووسائل حماية أمن التشغيل البرمجي، حيث قام الباحث باستخدام التحليل الوصفي تمهيداً لاختبار الفرضية الخامسة، فقد استخرج المتوسطات الحسابية والانحرافات المعيارية ومعاملات الاختلاف

والأهمية النسبية ومستوى الحماية ورتبته، وفقاً لآراء أفراد عينة الدراسة حول مضمون كل فقرة من تلك الفقرات التي تقيس مدى تطبيق تلك الإجراءات والجدول التالي يلخص نتائج التحليل الوصفي للفقرات المتعلقة بذلك:

جدول رقم (3-3-16) الإحصاءات الوصفية على مستوى الفقرات المتعلقة بمدى تطبيق إجراءات ووسائل حماية أمن عمليات التشغيل البرمجي لنظم المعلومات المحاسبية المحوسبة

رقم الفقرة	حماية أمن عمليات التشغيل البرمجي لنظم المعلومات المحاسبية المحوسبة	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى الحماية	الترتيب التنازلي
130	يحتوي برنامج التشغيل على وسائل تحدد صلاحية المستخدمين في تشغيل وتحديث البيانات ومنع قراءتها أو نسخها أو تعديلها من غير المخول لهم ذلك.	3.812	0.806	21.1	76.2	مرتفع	(1)
131	توجد رقابة آلية مدمجة داخل النظام، من خلا تقارير تحليلية الكترونية لتفاصيل العمليات التشغيلية، تحدد شخص المستخدم ووقت بداية ونهاية الاستخدام، ومكانه وطبيعته، والأخطاء المكتشفة آلياً، ويتم المتابعة المستمرة تلك التقارير.	3.369	0.694	20.6	67.4	متوسط	(4)
132	توجد إجراءات كافية تضمن تصحيح الأخطاء، وإعادة تشغيل البيانات التي لم يتم تشغيلها بسبب توقف دورة التشغيل والتأكد من تمام معالجتها، ويتم تمييز العمليات التي تمت معالجتها لتلافي تكرار تشغيلها.	3.418	0.713	20.9	68.2	مرتفع	(3)
133	توجد إجراءات للتأكد من أن معالجة البيانات قد تمت بشكل كامل عند حد الانقطاع، من نقطة توقف معينة عند توقف دورة التشغيل لسبب من الأسباب.	3.451	0.863	25.0	69.0	مرتفع	(2)
134	يتم توقيف عمل التطبيقات المحاسبية إجبارياً نهاية الدوام الرسمي، فلا يسمح بتشغيل النظام خارج فترة الدوام المحددة والمبرمجة آلياً، بحيث يتعذر تشغيله النظام خلاف ذلك.	2.393	0.733	30.7	47.8	منخفض	(5)
	المتوسط العام	3.284	0.539	16.4	65.6	متوسط	

• مستوى تطبيق إجراءات الحماية حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 ~ 2.59) منخفض، (2.60 ~ 3.39) متوسط، (3.40 ~ 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

تشير النتائج الواردة في الجدول السابق رقم (3-3-16) إلى ما يلي:

- إن المتوسط الحسابي الإجمالي لتقديرات أفراد العينة عن كافة الفقرات التي تقيس مدى تطبيق إجراءات ووسائل حماية أمن عمليات التشغيل البرمجي لنظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية قد بلغ (3.284) درجة من أصل (5) درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي المعياري في هذه الدراسة والبالغة (3) درجات، وبأهمية نسبية بالموافقة على أن البنوك التجارية في اليمن تطبيق تلك الإجراءات قدرها (65.6%)، والذي يعكس مستوى الحماية المتوسط، وهي أكبر من نسبة المتوسط الحسابي المعتمدة في هذه الدراسة

والبالغة (60%)، وبلغت قيمة الانحراف المعياري عن المتوسط الحسابي (0.539) فقط، مما يدل على تقارب الإجابات وأنها تتمحور حول المتوسط الحسابي، ويؤكد ذلك أن معامل الاختلاف لم يتجاوز (16.4%) للمتغير ككل، وهي تمثل نسبة منخفضة تدل على عدم تشتت واختلاف البيانات عن المتوسط الحسابي، وأن هناك تقارب وانسجام إلى حد كبير بين معظم أفراد عينة الدراسة في الإجابة عن فقرات هذا المتغير وأن مستوى تطبيق إجراءات ووسائل حماية أمن عمليات التشغيل البرمجي لنظم المعلومات المحاسبية المحوسبة كان بشكل عام متوسطاً لدى البنوك التجارية العاملة في الجمهورية اليمنية، ويؤكد ذلك قيم المتوسطات الحسابية لمعظم الفقرات.

■ إن قيم الانحراف المعياري لجميع الفقرات كانت أقل من الواحد الصحيح، وبلغ الانحراف المعياري للمجال ككل (0.539) فقط، مما يدل على أن آراء أفراد العينة لمعظم تلك الفقرات كانت متقاربة إلى حد ما، ويؤكد ذلك أن قيم معامل الاختلاف لتلك الفقرات قد تراوحت بين (20.6%~30.7%)، وهي قيم منخفضة ومتوسطة نسبياً تعكس مدى التقارب في وجهات نظر المستجيبين.

■ إن اتجاهات عينة الدراسة كانت إيجابية في (4) فقرات كان ترتيبها من (1) إلى (4) حسب الترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات حيث كانت أكبر من المتوسط الحسابي المعتمد وفق المقياس المستخدم في هذه الدراسة وهو (3) درجات، بينما الفقرة (134) والتي كان ترتيبها (5)، أتت إجابات أفراد العينة عليها سلبية وغير مؤيدة لها لأن قيمة المتوسط الحسابي لها كانت أقل من (3) درجات، وقد تراوح المتوسط الحسابي لجميع الفقرات بين (2.393~3.812) درجة، وبمعامل اختلاف لتلك الفقرات لم يتجاوز (30.7%)، وتدلل هذه النتيجة على أن المستجيبين يجمعون بنسبة متوسطة إلى حد ما على أن مستوى تطبيق إجراءات ووسائل حماية أمن تشغيل نظم المعلومات المحاسبية لدى البنوك التجارية العاملة في الجمهورية اليمنية كان متوسطاً.

■ كان مستوى تطبيق إجراءات ووسائل حماية أمن التشغيل مرتفعاً في (3) فقرات، ترتيبها يقع بين (1~3) والتي يزيد المتوسط الحسابي لكل منها عن (3.4) درجة، أي أنه يوجد موافقة على أن تلك الإجراءات والوسائل تطبق لدى البنوك التجارية في الجمهورية اليمنية بدرجة مرتفعة، فقد تراوح المتوسط الحسابي لتلك الفقرات بين (3.812~3.418) درجة، ويلاحظ أن إجراء الحماية الوارد في الفقرة رقم (130) والذي يتعلق باحتواء برامج التشغيل على وسائل تحدد صلاحية المستخدمين في تشغيل وتحديث البيانات ومنع قراءتها أو نسخها أو تعديلها من غير المخول لهم ذلك، قد احتل المرتبة الأولى بأعلى متوسط حسابي بلغ (3.812) درجة، وبأهمية نسبية بلغت (76.2%)، وبانحراف معياري (0.806)، ومعامل اختلاف لم يتجاوز (21.1%)، وهذا يؤكد أن معظم أفراد عينة الدراسة المستقصى منهم كانوا متفقين على أن تطبيق ذلك الإجراء مرتفع وبنسبة (76.2%)، وهذا يشير إلى أن أهم إجراءات حماية أمن تشغيل نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية تتمثل في الإجراء السابق ذكره والذي نال المرتبة الأولى بالإضافة للإجراءات المتعلقة بوجود إجراءات للتأكد من أن معالجة البيانات قد تمت بشكل كامل عند حد الانقطاع، من نقطة توقف معينة عند توقف دورة التشغيل لسبب من الأسباب، ووجود إجراءات كافية تضمن تصحيح الأخطاء، وإعادة تشغيل البيانات التي لم يتم تشغيلها بسبب توقف دورة

التشغيل والتأكد من تمام معالجتها، ويتم تمييز العمليات التي تمت معالجتها لتلافي تكرار تشغيلها، وتلك نقاط قوة في نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في اليمن تعمل على تخفيض مخاطر أمن تشغيل تلك النظم إلى أدنى حد ممكن، وتلك الإجراءات نالت موافقة غالبية أفراد عينة الدراسة على أنها مطبقة وبمستوى مرتفع بأهمية نسبية تراوحت بين (68.2%~76.2%)، وفي رأي الباحث أن هذه النتيجة تنسجم وتتفق مع مستوى حدوث مخاطر أمن التشغيل التي ظهرت عند مناقشة المحور الأول، وهذا أمر يستوجب من البنوك التجارية العاملة في اليمن المحافظة على مستوى تطبيق تلك الإجراءات وتعزيز تطبيقها بما يؤدي إلى رفع فعالية وكفاءة تلك الإجراءات لمواجهة تلك المخاطر.

■ كان مستوى تطبيق إجراءات حماية أمن التشغيل متوسطاً في الفقرة (131)، وتتعلق بوجود رقابة آلية مدمجة داخل النظام، من خلا تقارير تحليلية إلكترونية لتفاصيل العمليات التشغيلية، تحدد شخص المستخدم ووقت بداية ونهاية الاستخدام، ومكانه وطبيعته، والأخطاء المكتشفة آلياً، ويتم المتابعة المستمرة تلك التقارير، ونال ذلك الإجراء المرتبة (4)، حيث بلغ متوسطه الحسابي (3.369)، ومعامل الاختلاف (20.6%)، وهو ما يدل على انسجام وتقارب كبير بين آراء أفراد العينة على أن ذلك الإجراء يطبق لدى البنوك التجارية بأهمية نسبية للموافقة بلغت (67.4%)، وهو ما يستوجب من البنوك تعزيز ذلك الإجراء.

■ كان مستوى تطبيق إجراءات حماية أمن التشغيل منخفضاً في الفقرة (134) والمتعلقة بتوقيف عمل التطبيقات المحاسبية إجبارياً نهاية الدوام الرسمي، فلا يسمح بتشغيل النظام خارج فترة الدوام المحددة والمبرمجة آلياً، بحيث يتعذر تشغيله النظام خلاف ذلك، وكان ترتيبها (5) وفقاً للترتيب التنازلي لقيمة المتوسط الحسابي لتلك الفقرة، والتي بلغت (2.393) درجة والذي يعكس مدى الأهمية النسبية لتطبيق ذلك الإجراءات والتي لم تتجاوز (47.8%)، وبمعامل اختلاف لتلك الفقرة بلغ (30.7)، وانخفاض تطبيق ذلك الإجراءات يعد من نقاط الضعف في تلك النظم، وهو ما يستدعي من البنوك التجارية في الجمهورية اليمنية العمل على تطبيق ذلك الإجراء بكفاءة وفاعلية حتى يمكن تلافي المخاطر التي قد تحدث نتيجة ضعف مستوى تطبيقه.

■ ويمكن للباحث القول بصفة إجمالية بأن إجابات أفراد العينة حول مستوى تطبيق إجراءات ووسائل حماية أمن عمليات التشغيل البرمجي لنظم المعلومات المحاسبية المحوسبة لدى البنوك التي يعملون بها، كانت غالبيتها ترى بأن هناك تطبيق لتلك الإجراءات فقد حصل (4) إجراءات على درجة موافقة مرتفعة، في مقابل حصول إجراء على درجة موافقة متوسطة، كما حصل إجراء واحد على درجة موافقة منخفضة، مما يشير إلى أن إجراءات حماية أمن عمليات التشغيل مطبقة ولكن بشكل غير كافٍ، حيث بلغت الأهمية النسبية للموافقة على تطبيق تلك الإجراءات (65.6%) وبمستوى متوسط، وهنا يجب على البنوك التجارية في الجمهورية اليمنية العمل على رفع كفاءة وفاعلية تطبيق تلك الإجراءات لمواجهة مخاطر أمن نظم المعلومات المحاسبية بشكل عام، ومخاطر أمن عمليات التشغيل لتلك النظم على وجه الخصوص.

3-3-13: تحليل البيانات المتعلقة بحماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة

وفقاً لفرضيات الدراسة ونموذجها تمثل حماية أمن مخرجات نظم المعلومات أحد المتغيرات الفرعية المستقلة للدراسة، والهدف من قياسها معرفة مدى تطبيق إجراءات ووسائل حماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، وقد تم قياس هذا المتغير من خلال أحد المتغيرات الرئيسية للمحور الخامس من محاور الجزء الثالث للاستقصاء والذي تضمن (6) فقرات تبرز مدى تطبيق البنوك لإجراءات ووسائل حماية أمن المخرجات، حيث قام الباحث باستخدام التحليل الوصفي تمهيداً لاختبار الفرضية الخامسة، فقد استخرج المتوسطات الحسابية والانحرافات المعيارية ومعاملات الاختلاف والأهمية النسبية ومستوى الحماية ورتبته، وفقاً لآراء أفراد عينة الدراسة حول مضمون كل فقرة من تلك الفقرات التي تقيس مدى تطبيق تلك الإجراءات والجدول التالي يلخص نتائج التحليل الوصفي للفقرات المتعلقة بذلك:

جدول رقم (3-3-17) الإحصاءات الوصفية على مستوى الفقرات المتعلقة

بمدى تطبيق إجراءات ووسائل حماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة

رقم الفقر	حماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى الحماية	الترتيب
135	يتم حصر أنواع المعلومات وتصنيفها إلى فئات وفقاً لدرجة أهميتها وسريتها، وتحديد مستوى الحماية الواجب توفيره لكل فئة منها.	2.836	0.708	24.9	56.8	متوسط	(5)
136	توجد وسائل وإجراءات كافية لعملية توزيع المخرجات، لضمان وصول التقارير والوثائق للجهات المعنية المخولة فقط باستلامها.	2.779	0.686	24.7	55.6	متوسط	(6)
137	يتم إجراء صيانة دائمة لوسائط الإخراج (طابعات، فاكسات، شاشات...الخ)، لضمان سلامة عرض المخرجات.	3.566	0.823	23.0	71.4	مرتفع	(1)
138	يتم إعداد نسخ مطبوعة لبعض المعلومات المحاسبية الهامة، وتشفير المعلومات الحساسة.	3.393	0.940	27.7	67.8	متوسط	(2)
139	يتيح النظام مسار معين لمراجعة وتتبع سير المعاملات من مرحلة المدخلات إلى مرحلة المخرجات، والعكس.	3.230	0.831	25.7	64.6	متوسط	(4)
140	يقوم البنك بإتلاف المخرجات المهمة والسرية بعد الانتهاء من استخدامها بواسطة لجنة متخصصة ومخولة بذلك، ويتم إتلاف داخل البنك.	3.303	0.889	26.9	66.0	متوسط	(3)
	المتوسط العام	3.184	0.590	18.6	63.6	متوسط	

- مستوى تطبيق إجراءات الحماية حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 ~ 2.59) منخفض، (2.60 ~ 3.39) متوسط، (3.40 ~ 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

تشير النتائج الواردة في الجدول السابق رقم (3-3-17) إلى ما يلي:

- إن المتوسط الحسابي الإجمالي لتقديرات أفراد العينة عن كافة الفقرات التي تقيس مدى تطبيق إجراءات ووسائل حماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية قد بلغ (3.184) درجة من أصل (5) درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي المعياري في هذه الدراسة والبالغة (3) درجات، وبأهمية نسبية بالموافقة على أن البنوك التجارية في اليمن تطبق تلك الإجراءات قدرها (63.6%)، والذي يعكس مستوى الحماية المتوسط، وهي أكبر من نسبة المتوسط الحسابي المعتمدة في هذه الدراسة والبالغة (60%)، وبلغت قيمة الانحراف المعياري عن المتوسط الحسابي (0.590) فقط، مما يدل على تقارب الإجابات وأنها تتمحور حول المتوسط الحسابي، ويؤكد ذلك أن معامل الاختلاف لم يتجاوز (18.6%) للمتغير ككل، وهي تمثل نسبة منخفضة تدل على عدم تشتت واختلاف البيانات عن المتوسط الحسابي، وأن هناك تقارب وانسجام إلى حد كبير بين معظم أفراد عينة الدراسة في الإجابة عن فقرات هذا المتغير وأن مستوى تطبيق إجراءات ووسائل حماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة كان بشكل عام متوسطاً لدى البنوك التجارية العاملة في الجمهورية اليمنية، ويؤكد ذلك قيم المتوسطات الحسابية لمعظم الفقرات.
- إن قيم الانحراف المعياري لجميع الفقرات كانت أقل من الواحد الصحيح، وبلغ الانحراف المعياري للمجال ككل (0.590) فقط، مما يدل على أن آراء أفراد العينة لمعظم تلك الفقرات كانت متقاربة إلى حد ما، ويؤكد ذلك أن قيم معامل الاختلاف لتلك الفقرات قد تراوحت بين (23%~27.7%)، وهي قيم منخفضة نسبياً تعكس مدى التقارب في وجهات نظر المستجيبين.
- إن اتجاهات عينة الدراسة كانت إيجابية في (4) فقرات كان ترتيبها من (1) إلى (4) حسب الترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات حيث كانت أكبر من المتوسط الحسابي المعتمد وفق المقياس المستخدم في هذه الدراسة وهو (3) درجات، بينما الفقرتين (135،136) والتي كان ترتيبها (5~6)، أتت إجابات أفراد العينة عليهما سلبية وغير مؤيدة لهما لأن قيمة المتوسط الحسابي لكليهما كانت أقل من (3) درجات، وقد تراوح المتوسط الحسابي لجميع الفقرات بين (2.779~3.566) درجة، وبمعامل اختلاف لتلك الفقرات لم يتجاوز (27.7%)، وتدلل هذه النتيجة على أن المستجيبين يجمعون بنسبة متوسطة إلى حد ما على أن مستوى تطبيق إجراءات ووسائل حماية أمن مخرجات نظم المعلومات المحاسبية لدى البنوك التجارية العاملة في الجمهورية اليمنية كان متوسطاً.
- كان مستوى تطبيق إجراءات ووسائل حماية أمن المخرجات مرتفعاً في فقرة واحدة رقم (137)، والذي يتعلق باحتواء برامج التشغيل على وسائل تحدد صلاحية المستخدمين في تشغيل وتحديث البيانات ومنع قراءتها أو نسخها أو تعديلها من غير المخول لهم ذلك، حيث يزيد المتوسط الحسابي لها عن (3.4) درجة وقد احتل المرتبة الأولى بأعلى متوسط حسابي بلغ (3.566) درجة، وبأهمية نسبية بلغت (71.4%)، وبانحراف معياري (0.823)، ومعامل اختلاف لم يتجاوز (23%)، وهذا يؤكد أن معظم أفراد عينة الدراسة المستقصى

منهم كانوا متفقين على أن تطبيق ذلك الإجراء مرتفع وبنسبة (71.4%)، وهذا يشير إلى أن أهم إجراء مطبق لحماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية يتمثل في الإجراء السابق ذكره، ويعتبر من نقاط القوة لتلك النظم ويجب على تلك البنوك المحافظة على مستوى تطبيق ذلك الإجراء.

■ كان مستوى تطبيق إجراءات حماية أمن المخرجات متوسطاً في باقي الفقرات وكان أهمها الفقرة (131)، وتتعلق بإعداد نسخ مطبوعة لبعض المعلومات المحاسبية الهامة، وتشفير المعلومات الحساسة، ونال ذلك الإجراء المرتبة (2)، حيث بلغ متوسطه الحسابي (3.393)، وبمعامل اختلاف (27.7%)، وهو ما يدل على انسجام وتقارب كبير بين آراء أفراد العينة على أن ذلك الإجراء يطبق لدى البنوك التجارية بأهمية نسبية للموافقة بلغت (67.8%)، وفي رأي الباحث أن هذه النتيجة تتسجم وتتفق مع مستوى حدوث مخاطر أمن المخرجات التي ظهرت عند مناقشة المحور الأول، وهذا أمر يستوجب من البنوك التجارية العاملة في اليمن العمل على رفع مستوى تطبيق تلك الإجراءات وتعزيز تطبيقها بما يؤدي إلى رفع فعالية وكفاءة تلك الإجراءات لمواجهة تلك المخاطر.

■ ويمكن للباحث القول بصفة إجمالية بأن إجابات أفراد العينة حول مستوى تطبيق إجراءات ووسائل حماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة لدى البنوك التي يعملون بها، كانت غالبيتها ترى بأن تطبيق تلك الإجراءات متوسطة نسبياً فقد حصل إجراء واحد فقط على درجة موافقة مرتفعة، في مقابل حصول (5) إجراءات على درجة موافقة متوسطة، ولم يكن هناك أي إجراء حصل على درجة موافقة منخفضة، مما يشير إلى أن إجراءات حماية أمن عمليات التشغيل مطبقة ولكن بشكل غير كافٍ، حيث بلغت الأهمية النسبية للموافقة على تطبيق تلك الإجراءات (63.6%) وبمستوى متوسط، وهنا يجب على البنوك التجارية في الجمهورية اليمنية العمل على رفع كفاءة وفعالية تطبيق تلك الإجراءات لمواجهة مخاطر أمن نظم المعلومات المحاسبية بشكل عام، ومخاطر أمن مخرجات تلك النظم على وجه الخصوص.

3-14: تحليل البيانات المتعلقة بحماية أمن البيانات المنقولة عبر شبكات نظم المعلومات

المحاسبية المحوسبة:

وفقاً لفرضيات الدراسة ونموذجها تمثل حماية أمن البيانات المنقولة عبر الشبكات أحد المتغيرات الفرعية المستقلة للدراسة، والهدف من قياسها معرفة مدى تطبيق إجراءات ووسائل حماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، وقد تم قياس هذا المتغير من خلال أحد المتغيرات الرئيسية للمحور الخامس من محاور الجزء الثالث للاستقصاء والذي تضمن (5) فقرات تبرز مدى تطبيق البنوك لإجراءات ووسائل حماية أمن البيانات المنقولة عبر الشبكات، حيث قام الباحث باستخدام التحليل الوصفي تمهيداً لاختبار الفرضية الخامسة، فقد استخرج المتوسطات الحسابية والانحرافات المعيارية ومعاملات الاختلاف والأهمية النسبية ومستوى الحماية ورتبته، وفقاً لآراء أفراد عينة الدراسة حول

مضمون كل فقرة من تلك الفقرات التي تقيس مدى تطبيق تلك الإجراءات والجدول التالي يلخص نتائج التحليل الوصفي للفقرات المتعلقة بذلك:

جدول رقم (3-3-18) الإحصاءات الوصفية على مستوى الفقرات المتعلقة بمدى تطبيق

إجراءات ووسائل حماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية المحوسبة

رقم الفقرة	حماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى الحماية	الترتيب التنازلي
141	تستخدم برامج الجدران النارية لتحديد المعلومات التي يسمح بدخولها أو خروجها من وإلى نظام المعلومات المحاسبي المحوسب للبنك.	3.557	0.891	25.0	71.2	مرتفع	(1)
142	يتم تشفير البيانات المرسلة عبر الشبكات للتأكد من أنه لم يتم الكشف عنها أو تعديلها وأنها مرسلة من الجهة المعنية، وتتوفر وسائل حماية كافية للحفاظ على سرية مفتاح التشفير.	3.196	0.663	20.7	64.0	متوسط	(3)
143	يستخدم البنك التوقيع الرقمي الإلكتروني، كوسيلة للتحقق من موثوقية المستخدمين بشكل غير قابل للتزيف، ولضمان عدم إنكار الأطراف المعنية المشاركة في الوثائق الإلكترونية.	2.680	0.805	30.0	53.6	متوسط	(4)
144	يتم استخدام شهادة رقمية صادرة من جهات فنية معتمدة، عند إرسال أو استلام البيانات عبر الشبكة الخارجية، للتحقق من هوية مرسل الرسائل، وموثوقية المستخدم.	2.459	0.532	21.6	49.2	منخفض	(5) الأخيرة
145	يتم استخدام بروتوكولات أمنية بين البنك والأطراف المتعاملة للحفاظ على سرية المعلومات المحاسبية والتحقق من وصولها للجهة المطلوبة أثناء إجراء المعاملات المالية.	3.279	0.718	21.9	65.6	متوسط	(2)
-141 145	المتوسط العام	3.034	0.506	16.7	60.6	متوسط	

• مستوى تطبيق إجراءات الحماية حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 ~ 2.59) منخفض، (2.60 ~ 3.39) متوسط، (3.40 ~ 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

تشير النتائج الواردة في الجدول السابق رقم (3-3-18) إلى ما يلي:

- إن المتوسط الحسابي الإجمالي لتقديرات أفراد العينة عن كافة الفقرات التي تقيس مدى تطبيق إجراءات ووسائل حماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية قد بلغ (3.034) درجة من أصل (5) درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي المعياري في هذه الدراسة والبالغة (3) درجات، وبأهمية نسبية بالموافقة على أن البنوك التجارية في اليمن

تطبيق تلك الإجراءات قدرها (60.6%)، والذي يعكس مستوى الحماية المتوسط، وهي أكبر من نسبة المتوسط الحسابي المعتمدة في هذه الدراسة والبالغة (60%)، وبلغت قيمة الانحراف المعياري عن المتوسط الحسابي (0.506) فقط، مما يدل على تقارب الإجابات وأنها تتمحور حول المتوسط الحسابي، ويؤكد ذلك أن معامل الاختلاف لم يتجاوز (16.7%) للمتغير ككل، وهي تمثل نسبة منخفضة تدل على عدم تشتت واختلاف البيانات عن المتوسط الحسابي، وأن هناك تقارب وانسجام إلى حد كبير بين معظم أفراد عينة الدراسة في الإجابة عن فقرات هذا المتغير وأن مستوى تطبيق إجراءات ووسائل حماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية المحوسبة كان بشكل عام متوسطاً لدى البنوك التجارية العاملة في الجمهورية اليمنية، ويؤكد ذلك قيم المتوسطات الحسابية لمعظم الفقرات.

- إن قيم الانحراف المعياري لجميع الفقرات كانت أقل من الواحد الصحيح، وبلغ الانحراف المعياري للمجال ككل (0.506) فقط، مما يدل على أن آراء أفراد العينة لمعظم تلك الفقرات كانت متقاربة إلى حد ما، ويؤكد ذلك أن قيم معامل الاختلاف لتلك الفقرات قد تراوحت بين (20.7%~30%)، وهي قيم منخفضة نسبياً تعكس مدى التقارب في وجهات نظر المستجيبين.
- إن اتجاهات عينة الدراسة كانت إيجابية في (3) فقرات كان ترتيبها من (1) إلى (3) حسب الترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات حيث كانت أكبر من المتوسط الحسابي المعتمد وفق المقياس المستخدم في هذه الدراسة وهو (3) درجات، بينما الفقرتين (143،144) والتي كان ترتيبهما (5~6)، أتت إجابات أفراد العينة عليهما سلبية وغير مؤيدة لهما لأن قيمة المتوسط الحسابي لكليهما كانت أقل من (3) درجات، وقد تراوح المتوسط الحسابي لجميع الفقرات بين (2.459~3.557) درجة، وبمعامل اختلاف لتلك الفقرات لم يتجاوز (30%)، وتدلل هذه النتيجة على أن المستجيبين يجمعون بنسبة متوسطة إلى حد ما على أن مستوى تطبيق إجراءات ووسائل حماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية لدى البنوك التجارية العاملة في الجمهورية اليمنية كان متوسطاً.
- كان مستوى تطبيق إجراءات ووسائل حماية أمن البيانات المنقولة عبر الشبكات مرتفعاً في فقرة واحدة رقم (141)، والتي تتعلق باستخدام برامج الجدران النارية لتحديد المعلومات التي يسمح بدخولها أو خروجها من وإلى نظام المعلومات المحاسبي المحوسب للبنك، حيث يزيد المتوسط الحسابي لها عن (3.4) درجة وقد نالت المرتبة الأولى بأعلى متوسط حسابي بلغ (3.557) درجة، وبأهمية نسبية بلغت (71.2%)، وبانحراف معياري (0.891)، ومعامل اختلاف لم يتجاوز (25%)، وهذا يؤكد أن معظم أفراد عينة الدراسة المستقصى منهم كانوا متفقين على أن تطبيق ذلك الإجراء مرتفع وبنسبة (71.2%)، وهذا يشير إلى أن أهم إجراء مطبق لحماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية يتمثل في الإجراء السابق ذكره، ويعتبر من نقاط القوة لتلك النظم ويجب على تلك البنوك المحافظة على مستوى تطبيق ذلك الإجراء.

- كان مستوى تطبيق إجراءات حماية أمن البيانات المنقولة عبر الشبكات متوسطاً في (3) فقرات وكان أهمها الفقرة (145)، والتي تتعلق باستخدام بروتوكولات أمنية بين البنك والأطراف المتعاملة للحفاظ على سرية المعلومات المحاسبية والتحقق من وصولها للجهة المطلوبة أثناء إجراء المعاملات المالية، ونال ذلك الإجراء المرتبة (2)، حيث بلغ متوسطه الحسابي (3.279)، وبمعامل اختلاف (21.9%)، وبأهمية نسبية للموافقة بلغت (65.6%)، والفقرة رقم (142) التي تتعلق بتشفير البيانات المرسلة عبر الشبكات للتأكد من أنه لم يتم الكشف عنها أو تعديلها وأنها مرسلة من الجهة المعنية، وتتوفر وسائل حماية كافية للحفاظ على سرية مفتاح التشفير، ونال ذلك الإجراء المرتبة (3)، حيث بلغ متوسطه الحسابي (3.196)، وبمعامل اختلاف (20.7%)، وبأهمية نسبية للموافقة بلغت (64%)، وهو ما يدل على انسجام وتقارب كبير بين آراء أفراد العينة على أن تلك الإجراءات تطبق لدى البنوك التجارية، وفي رأي الباحث أن هذه النتيجة تتسجم وتتفق مع مستوى حدوث مخاطر أمن البيانات المنقولة عبر شبكات نظم المعلومات التي ظهرت عند مناقشة المحور الأول، وهذا أمر يستوجب من البنوك التجارية العاملة في اليمن العمل على رفع مستوى تطبيق تلك الإجراءات وتعزيز تطبيقها بما يؤدي إلى رفع فعالية وكفاءة تلك الإجراءات لمواجهة تلك المخاطر.
- كان مستوى تطبيق إجراءات حماية أمن البيانات المنقولة عبر الشبكات منخفضاً في الفقرة (144) والمتعلقة باستخدام شهادة رقمية صادرة من جهات فنية معتمدة، عند إرسال أو استلام البيانات عبر الشبكة الخارجية، للتحقق من هوية مرسل الرسائل، وموثوقية المستخدم، وقد جاءت في المرتبة الخامسة والأخيرة وفقاً للترتيب التنازلي لقيمة المتوسط الحسابي لتلك الفقرة، والتي بلغت (2.459) درجة والذي يعكس مدى الأهمية النسبية لتطبيق ذلك الإجراءات والتي لم تتجاوز (49.2%)، وبمعامل اختلاف لتلك الفقرة بلغ (21.6%)، وانخفاض تطبيق ذلك الإجراءات يعد من نقاط الضعف في تلك النظم، وهو ما يستدعي من البنوك التجارية في الجمهورية اليمنية العمل على تطبيق ذلك الإجراء بكفاءة وفاعلية حتى يمكن تلافي المخاطر التي قد تحدث نتيجة ضعف مستوى تطبيقه.
- ويمكن للباحث القول بصفة إجمالية بأن إجابات أفراد العينة حول مستوى تطبيق إجراءات ووسائل حماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية المحوسبة لدى البنوك التي يعملون بها، كانت غالبيتها ترى بأن مستوى تطبيق تلك الإجراءات متوسط، فقد حصل إجراء واحد فقط على درجة موافقة مرتفعة، في مقابل حصول (3) إجراءات على درجة موافقة متوسطة، كما حصل إجراء واحد فقط على درجة موافقة منخفضة، مما يشير إلى أن إجراءات حماية أمن البيانات المنقولة عبر الشبكات مطبقة ولكن بشكل غير كافٍ، حيث بلغت الأهمية النسبية للموافقة على تطبيق تلك الإجراءات (60.6%) وبمستوى متوسط، وهنا يجب على البنوك التجارية في الجمهورية اليمنية العمل على رفع كفاءة وفاعلية تطبيق تلك الإجراءات لمواجهة مخاطر أمن نظم المعلومات المحاسبية بشكل عام، ومخاطر أمن البيانات المنقولة عبر شبكات تلك النظم على وجه الخصوص.

3-3-15: تحليل البيانات المتعلقة بحماية أمن تعديل تطوير نظم المعلومات المحاسبية المحوسبة:

وفقاً لفرضيات الدراسة ونموذجها تمثل حماية أمن تعديل وتطوير نظم أحد المتغيرات الفرعية المستقلة للدراسة، والهدف من قياسها معرفة مدى تطبيق إجراءات ووسائل حماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، وقد تم قياس هذا المتغير من خلال أحد المتغيرات الرئيسية للمحور الخامس من محاور الجزء الثالث للاستقصاء والذي تضمن (5) فقرات تبرز مدى تطبيق البنوك لإجراءات ووسائل حماية أمن التعديل والتطوير، حيث قام الباحث باستخدام التحليل الوصفي تمهيداً لاختبار الفرضية الخامسة، فقد استخرج المتوسطات الحسابية والانحرافات المعيارية ومعاملات الاختلاف والأهمية النسبية ومستوى الحماية ورتبته، وفقاً لآراء أفراد عينة الدراسة حول مضمون كل فقرة من تلك الفقرات التي تقيس مدى تطبيق تلك الإجراءات والجدول التالي يلخص نتائج التحليل الوصفي للفقرات المتعلقة بذلك:

جدول رقم (3-3-19) الإحصاءات الوصفية على مستوى الفقرات المتعلقة بمدى

تطبيق إجراءات ووسائل حماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة

الترتيب	مستوى الحماية	الأهمية النسبية % 100	معامل الاختلاف %100	الانحراف المعياري	المتوسط الحسابي	حماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة	رقم الفقرة
(5) والأخيرة	متوسط	65.0	29.4	0.956	3.246	توجد إجراءات كافية وفعالة لرقابة عمليات تطوير البرامج والتطبيقات المحاسبية، وفق معايير وإجراءات واضحة ومكتوبة ومحددة.	146
(3)	مرتفع	70.6	31.6	1.114	3.533	لا تتم أية تعديلات في برمج النظام بدون حصول المبرمجين المختصين على موافقات رسمية من الإدارات المعنية المخولة.	147
(1)	مرتفع	76.0	21.1	0.802	3.795	هناك فريق متخصص لتعديل وتطوير نظم المعلومات المحاسبية من داخل البنك، وتشرف إدارة البنك على تعديل وتطوير النظام.	148
(2)	مرتفع	72.2	27.3	0.982	3.615	يتم إجراء الاختبار المبدئي بالتنسيق مع فريق المبرمجين الجديده وتعديلاتها قبل اعتمادها بشكل نهائي للتأكد من سلامتها، وقدرتها على تتبع الأخطاء التي قد تحدث أثناء التنفيذ.	149
(4)	مرتفع	70.4	29.9	1.038	3.525	يتم توثيق كافة التعديلات التي تتم على البرامج والمعدات، وفق الإجراءات المتبعة.	150
	مرتفع	70.8	23.1	0.819	3.543	المتوسط العام	

• مستوى تطبيق إجراءات الحماية حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 ~ 2.59) منخفض، (2.60 ~ 3.39) متوسط، (3.40 ~ 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

تشير النتائج الواردة في الجدول رقم (3-3-19) أعلاه إلى ما يلي:

- إن المتوسط الحسابي الإجمالي لتقديرات أفراد العينة عن كافة الفقرات التي تقيس مدى تطبيق إجراءات ووسائل حماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية قد بلغ (3.543) درجة من أصل (5) درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي المعياري في هذه الدراسة والبالغة (3) درجات، وبأهمية نسبية بالموافقة على أن البنوك التجارية في اليمن تطبيق تلك الإجراءات قدرها (70.8%) والذي يعكس مستوى الحماية المتوسط، وهي أكبر من نسبة المتوسط الحسابي المعتمدة في هذه الدراسة والبالغة (60%)، وبلغت قيمة الانحراف المعياري عن المتوسط الحسابي (0.819) فقط، مما يدل على تقارب الإجابات وأنها تتمحور حول المتوسط الحسابي، ويؤكد ذلك أن معامل الاختلاف لم يتجاوز (31.6%) للمتغير ككل، وهي تمثل نسبة ضئيلة وتدل على عدم تشتت واختلاف البيانات عن المتوسط الحسابي، وأن هناك تقارب وانسجام إلى حد كبير بين معظم أفراد عينة الدراسة في الإجابة عن فقرات هذا المتغير وأن مستوى تطبيق إجراءات ووسائل حماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة كان بشكل عام مرتفعاً لدى البنوك التجارية العاملة في الجمهورية اليمنية، ويؤكد ذلك قيم المتوسطات الحسابية لمعظم الفقرات.
- إن قيم الانحراف المعياري لمعظم الفقرات كانت أقل من الواحد الصحيح، وبلغ الانحراف المعياري للمجال ككل (0.819) فقط، مما يدل على أن آراء أفراد العينة لمعظم تلك الفقرات كانت متقاربة إلى حد ما، ويؤكد ذلك أن قيم معامل الاختلاف لتلك الفقرات قد تراوحت بين (21.1%~31.6%)، وهي قيم متوسطة نسبياً تعكس مدى التقارب في وجهات نظر المستجيبين.
- إن اتجاهات عينة الدراسة كانت إيجابية في جميع الفقرات حيث كانت أكبر من المتوسط الحسابي المعتمد وفق المقياس المستخدم في هذه الدراسة وهو (3) درجات، وقد تراوح المتوسط الحسابي لجميع الفقرات بين (3.246~3.795) درجة، وبمعامل اختلاف لتلك الفقرات لم يتجاوز (31.6%)، وتدل هذه النتيجة على أن المستجيبين يجمعون بنسبة مرتفعة إلى حد ما على أن مستوى تطبيق إجراءات ووسائل حماية أمن تعديل وتطوير نظم المعلومات المحاسبية لدى البنوك التجارية العاملة في الجمهورية اليمنية كان مرتفعاً.
- كان مستوى تطبيق إجراءات ووسائل حماية التعديل والتطوير مرتفعاً في (4) فقرات، ترتيبها يقع بين (1~4) والتي يزيد المتوسط الحسابي لكل منها عن (3.4) درجة، أي أنه يوجد موافقة على أن تلك الإجراءات والوسائل تطبق لدى البنوك التجارية في الجمهورية اليمنية بدرجة مرتفعة، فقد تراوح المتوسط الحسابي لتلك الفقرات بين (3.525~3.795) درجة، ويلاحظ أن إجراء الحماية الوارد في الفقرة رقم (148) والذي يتعلق بوجود فريق متخصص لتعديل وتطوير نظام المعلومات المحاسبي من داخل البنك، وتشرف إدارة البنك على تعديل وتطوير النظام، قد احتل المرتبة الأولى بأعلى متوسط حسابي بلغ (3.795) وبأهمية

نسبية بلغت (76%)، وبانحراف معياري (0.802)، ومعامل اختلاف لم يتجاوز (21.1%)، وهذا يؤكد أن معظم أفراد عينة الدراسة المستقصى منهم كانوا متفقين على أن تطبيق ذلك الإجراء مرتفع ونسبة (76%)، وهذا يشير إلى أن أهم إجراءات حماية أمن تعديل وتطوير نظم المعلومات المحاسبية لدى البنوك التجارية في الجمهورية اليمنية تتمثل في الإجراء السابق ذكره والذي نال المرتبة الأولى، بالإضافة للإجراءات المتعلقة بالاختبار المبدئي بالتشغيل التجريبي للبرامج الجديدة وتعديلاتها قبل اعتمادها بشكل نهائي للتأكد من سلامتها، وقدرتها على تتبع الأخطاء التي قد تحدث أثناء التنفيذ، لا تتم أية تعديلات في برمج النظام بدون حصول المبرمجين المختصين على موافقات رسمية من الإدارات المعنية المخولة، كما يتم توثيق كافة التعديلات التي تتم على البرامج والمعدات، وفق الإجراءات المتبعة، وتلك الإجراءات نالت موافقة غالبية أفراد عينة الدراسة على أنها مطابقة وبمستوى مرتفع وبأهمية نسبية تراوحت بين (70.4%~76%)، وفي رأي الباحث أن هذه النتيجة تنسجم وتتفق مع مستوى حدوث مخاطر أمن التعديل والتطوير التي ظهرت عند مناقشة المحور الأول، وهذا أمر يستوجب من البنوك التجارية العاملة في اليمن المحافظة على مستوى تطبيق تلك الإجراءات وتعزيز تطبيقها بما يؤدي الى رفع فعالية وكفاءة تلك الإجراءات لمواجهة تلك المخاطر.

■ كان مستوى تطبيق إجراءات الحماية متوسطاً في الفقرة (146) المتعلقة بوجود إجراءات كافية وفعالة لرقابة عمليات تطوير البرامج والتطبيقات المحاسبية، وفق معايير وإجراءات واضحة ومكتوبة، وكان ترتيبها (5) فقد جاءت في المرتبة الأخيرة وفقاً للترتيب التنازلي لقيم المتوسط الحسابي لتلك الفقرات، بلغ المتوسط الحسابي لها بين (3.246) درجة، بأهمية نسبية للموافقة على تطبيق ذلك الإجراءات لم يتجاوز (65%)، وبمعامل اختلاف للفقرتين لا يزيد عن (29.4%)، وهو ما يستوجب من البنوك تعزيز ذلك الإجراء.

■ ويمكن للباحث القول بصفة إجمالية بأن إجابات أفراد العينة حول مستوى تطبيق إجراءات ووسائل حماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة لدى البنوك التي يعملون بها، كانت غالبيتها ترى بأن هناك تطبيق لتلك الإجراءات فقد حصل (5) إجراءات على درجة موافقة مرتفعة، في مقابل حصول إجراء واحد على درجة موافقة متوسطة، ولم يكن هناك إجراء حصل على درجة موافقة منخفضة، مما يشير إلى أن إجراءات حماية أمن التعديل والتطوير مطبقة ولكن بشكل غير كافٍ نسبياً، حيث بلغت الأهمية النسبية للموافقة على تطبيق تلك الإجراءات (70.8%) وبمستوى مرتفع، وهنا يجب على البنوك التجارية في الجمهورية اليمنية العمل على رفع كفاءة وفعالية تطبيق تلك الإجراءات لمواجهة مخاطر أمن نظم المعلومات المحاسبية بشكل عام، ومخاطر أمن التعديل والتطوير في تلك النظم على وجه الخصوص.

3-4-16: تحليل البيانات المتعلقة بإجراءات ووسائل حماية أمن نظم المعلومات المحاسبية المحوسبة ككل:

بالنظر إلى المتغيرات الرئيسية لإجراءات ووسائل حماية أمن نظم المعلومات المحاسبية المحوسبة، وبناءً على المتوسط الحسابي لتلك المتغيرات، والأهمية النسبية لها، تم ترتيب تلك المتغيرات الرئيسية تنازلياً، كما هو مبين في الجدول الآتي:

جدول رقم (3-3-20) الإحصاءات الوصفية للمتغيرات الرئيسية المتعلقة بإجراءات ووسائل حماية أمن نظم المعلومات المحاسبية المحوسبة مرتبة تنازلياً حسب الأهمية النسبية (1)

الرتبة (الترتيب التنازلي)	إجراءات ووسائل حماية أمن نظم المعلومات	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %100	الأهمية النسبية % 100	مستوى تطبيق الحماية
1	حماية أمن التعديل والتطوير.	3.543	0.819	23.1	70.8	مرتفع
2	حماية أمن مدخلات النظم.	3.459	0.585	16.9	69.2	مرتفع
3	حماية أمن وسائط التخزين غير المتصلة بقاعدة البيانات.	3.412	0.627	18.4	68.2	مرتفع
4	حماية أمن الوصول البرمجي.	3.359	0.689	21.0	67.0	متوسط
5	حماية أمن الوصول المادي.	3.342	0.571	17.1	66.8	متوسط
6	حماية أمن عمليات التشغيل.	3.284	0.539	16.4	65.6	متوسط
7	حماية أمن المخرجات	3.184	0.590	18.6	63.6	متوسط
8	حماية الأمن التنظيمي للأفراد.	3.154	0.517	16.4	63.0	متوسط
9	حماية أمن تبادل البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية.	3.034	0.506	16.7	60.6	متوسط
150-91	المتوسط العام	3.349	0.553	16.5	67.0	متوسط

• مستوى تطبيق إجراءات الحماية حسب المتوسط الحسابي: أقل من (1.80) منخفض جداً، (1.80 ~ 2.59) منخفض، (2.60 ~ 3.39) متوسط، (3.40 ~ 4.19) مرتفع، أكثر من (4.20) مرتفع جداً.

(1) الجدول من إعداد الباحث اعتماداً على مخرجات التحليل الإحصائي SPSS.

ومن الجدول السابق رقم (3-3-20) يتضح ما يلي:

■ إن أهم إجراءات ووسائل حماية أمن نظم المعلومات المحاسبية المحوسبة هي الإجراءات والوسائل التي تتعلق بحماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة بالمرتبة الأولى ثم يليها إجراءات حماية أمن مدخلات النظم بالمرتبة الثانية، يليها إجراءات حماية أمن وسائط التخزين غير المتصلة بقاعدة البيانات، وكان أقلها أهمية هي الإجراءات المتعلقة بحماية أمن تبادل البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية.

■ أن قيم المتوسط الحسابي لكل إجراء من إجراءات حماية أمن نظم المعلومات المحاسبية على مستوى المتغيرات الرئيسية كانت أكبر من المتوسط الحسابي المعتمد وفق المقياس المستخدم في هذه الدراسة وهو (3) درجات، وقد تراوحت قيمة المتوسط الحسابي لتلك الإجراءات بين (3.034) بنسبة (60.6%)، وبمستوى متوسط لإجراءات حماية أمن تبادل البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية، وبين (3.543) بنسبة (70.8%)، وبمستوى مرتفع بإجراءات حماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة، وبمعامل اختلاف لم يتجاوز (23.1%) وتدل هذه النتيجة على أن المستجيبين يجمعون بنسبة كبيرة إلى حد ما أن إجراءات ووسائل حماية أمن نظم المعلومات المحاسبية لدى البنوك التجارية العاملة في الجمهورية اليمنية، مطابقة وبمستوى متوسط.

■ بالنظر إلى ترتيب إجراءات ووسائل حماية أمن نظم المعلومات المحاسبية المحوسبة في الجدول السابق أعلاه رقم (4-3-20) يلاحظ أن الإجراءات والوسائل المتعلقة بحماية أمن التعديل والتطوير قد نالت المرتبة الأولى وبمستوى مرتفع، حيث حصلت على أعلى متوسط حسابي، والذي بلغت قيمته (3.543) درجة، وبمعامل اختلاف لا يتجاوز (23.1%)، ويدل ذلك على انسجام كبير بين آراء أفراد العينة حول أن تطبيق تلك الإجراءات كانت مرتفعة وبأهمية نسبية للموافقة مرتفعة حيث بلغت (70.8%)، ولعل ذلك يعود إلى تطبيق البنوك للعديد من الإجراءات الرقابية على التكنولوجيا المستخدمة في العمل من أجل ضمان استمرارية عملها على الشكل الأمثل لتقليل احتمالية فشلها أو قصورها وذلك بإجراء عمليات الصيانة الوقائية المستمرة.

■ وقد جاءت الإجراءات الأخرى بمستوى تطبيق متوسط ومرتفع الأهمية، حيث احتلت إجراءات حماية أمن تبادل البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية في المرتبة التاسعة والأخيرة وبمستوى متوسط، حيث بلغ إجمالي المتوسط الحسابي لها (3.034)، وبمعامل اختلاف لا يتجاوز (16.7%)، ويدل ذلك على تقارب بين آراء أفراد العينة حول أن تطبيق تلك الإجراءات متوسطة وبأهمية نسبية لا تتجاوز

(60.6%)، ولعل مرد ذلك يعود إلى أن استخدام كلاً من التوقيع الإلكتروني والشهادات الرقمية عند إرسال واستلام البيانات يشوبه الضعف والقصور فإجراءات الحماية غير كافية في ذلك الجانب لدى البنوك التجارية في الجمهورية اليمنية.

يستخلص الباحث مما سبق، أن إجراءات ووسائل الحماية الواردة في الجدولين السابقين كان مستوى تطبيقها متوسطاً بشكل عام لحماية أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية وبأهمية نسبية بلغت (67%) حسب آراء عينة الدراسة، وبالتالي، فإننا يمكن القول إن آليات إجراءات الحماية مقبولة إلى حد ما، ولكنها ليست الأمثل، وينبغي رصدها ومتابعتها وإجراء اختبارات دورية لتقليل تأثير المخاطر التي يمكن أن تؤثر بشكل كبير على أمن نظم المعلومات المحاسبية.

3-4: المبحث الرابع

التحليل الاستدلالي للبيانات لاختبار فرضيات الدراسة وتفسير نتائجها

مقدمة:

بعد أن تم عرض وتحليل ومناقشة بيانات الدراسة في المبحث السابق يتم في هذا المبحث اختبار فرضيات الدراسة بحسب ترتيبها، عند مستوى الثقة (95%) ومستوى الدلالة (5%) والتي نقبل عندها وجود علاقات بين متغيرات الدراسة من عدمها، وقد تم استخدام البرنامج الإحصائي (SPSS) لإيجاد القيم المحسوبة لمعاملات كلاً من الفروق، والارتباط، والانحدار، ومستوى التباين للقيمة (T) أو (F)، ومقارنتها بقيمة الدلالة الإحصائية (0.05) المعتمدة لقبول أو رفض الفرضيات، فمثلاً يتم اختبار الفرضيات الخمس الأولى من خلال التحقق من أن المتوسط الحسابي لإجابات أفراد العينة أقل أو أكبر بدرجة معنوية من المتوسط الحسابي المعتمد في هذه الدراسة والبالغ (3) درجات والمقابل للأهمية النسبية (60%)، ويكون معيار القبول أو الرفض للفرضيات هو مستوى الدلالة الإحصائية (0.05)، وستكون قاعدة القرار رفض الفرضية العدمية إذا كانت قيمة الوسط الحسابي أكبر وذات دلالة إحصائية من قيمة أداه القياس البالغة (3) درجات، وقبول الفرضية العدمية إذا كانت قيمة الوسط الحسابي أقل وذات دلالة إحصائية من أداه القياس البالغة (3) درجات، ويتم بيان ذلك على النحو الآتي:

3-4-1: نتيجة اختبار الفرضية الأولى:

تنص الفرضية العدمية الأولى (H^0-1) على أنه: "لا تحدث مخاطر جوهرية وملموسة تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية"، وتنص الفرضية البديلة لها (H^1-1) على أنه: "تحدث مخاطر جوهرية وملموسة تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية"، وتهدف هذه الفرضية إلى معرفة مدى حدوث مخاطر جوهرية وملموسة تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، وللتحقق من أن متوسط كل فقرة من الفقرات المتعلقة بحدوث تلك المخاطر أقل أو أكبر من المتوسط الفرضي المعياري لأداة القياس (3)، بدرجة جوهرية معنوية إحصائية وليست ناتجة عن الصدفة وفق آراء عينة الدراسة على أسئلة الاستقصاء، لجأ الباحث إلى استخدام اختبار (T) للعينة الواحدة (One Sample T-test) لدراسة دلالة الفروق، حيث تم الاعتماد على مستوى الدلالة الإحصائية المعنوية ($\alpha=0.05$) كأساس لقبول الفرضية العدمية أو رفضها، وقد قام الباحث بإجراء الاختبار الإحصائي لكل نوع على حده من أنواع المخاطر التي وردت في الاستقصاء، وكانت النتائج كما في الجدول الآتي:

جدول رقم (3-4-1) نتيجة اختبار (T) لعينة الدراسة بشأن الفقرات الرئيسية والفرعية
للفرضية الأولى المتعلقة بحدوث المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة⁽¹⁾

رقم الفقرة	مخاطر أمن نظم المعلومات المحاسبية	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة الفرضية العدمية
1	قيام بعض موظفي نظم المعلومات باستغلال صلاحياتهم في هذه النظم في خدمة أغراضهم الشخصية بما يتعارض والسياسات الموضوعة من قبل الإدارة والمختصين.	2.229	-10.240	0.000	معنوية	قبول
2	انتحال صلاحيات شخص مخول بأي طريقة من الطرق نتيجة إهمال المستخدم، والثقة المتبادلة بين الموظفين التي تجعلهم يستخدمون كلمات السر فيما بينهم.	2.754	-3.902	0.000	معنوية	قبول
2-1	مخاطر أمن الأفراد العاملين في النظم.	2.492	-8.364	0.000	معنوية	قبول
3	حدوث تلف جزئي أو تدمير كلي لأجهزة ومعدات النظام المادية.	2.000	-13.584	0.000	معنوية	قبول
4	حدوث أعطال في المكونات المادية والبرمجية للنظام.	2.713	-4.325	0.000	معنوية	قبول
4-3	مخاطر الأمن المادي لنظم المعلومات.	2.357	-11.256	0.000	معنوية	قبول
5	الوصول البرمجي غير المصرح به إلى برامج النظام والملفات في قاعدة البيانات بواسطة أفراد من داخل البنك بقصد الإضرار والتخريب.	2.024	-13.340	0.000	معنوية	قبول
6	الوصول البرمجي، غير المصرح به إلى برامج النظام والملفات في قاعدة البيانات بواسطة أفراد أو جهات من خارج البنك، لإنجاز عمليات (تعديل/تدمير/كشف/نسخ وسرقة/استخدام) بطريقة غير مشروعة.	1.827	-17.349	0.000	معنوية	قبول
7	تلف بعض ملفات البيانات والبرامج ونظم التشغيل نتيجة تعرض قاعدة البيانات لنظام المعلومات المحاسبي المحسوب للإصابة بالبرامج الخبيثة مثل (الفيروسات، والديدان، وبرامج التجسس).	3.582	7.467	0.000	معنوية	رفض
7-5	مخاطر أمن الوصول البرمجي لقاعدة بيانات نظم المعلومات المحاسبية.	2.478	-10.701	0.000	معنوية	قبول
8	ضياح أو سرقة وسائط تخزين البيانات والبرامج الاحتياطية غير المتصلة بقاعدة بيانات نظام المعلومات المحاسبي المحسوب.	2.205	-10.548	0.000	معنوية	قبول
9	الوصول غير المصرح به للبيانات والبرامج المخزنة في وسائط غير متصلة بنظام المعلومات المحاسبي المحسوب.	2.107	-13.829	0.000	معنوية	قبول
9-8	مخاطر أمن النسخ في وسائط غير متصلة بقاعدة البيانات.	2.156	-15.457	0.000	معنوية	قبول
10	الحذف أو التعديل المتعمد لمصادر بيانات مدخلات صحيحة بواسطة الأفراد العاملين في نظام المعلومات المحاسبي.	2.008	-12.364	0.000	معنوية	قبول

(¹) الجدول من إعداد الباحث اعتماداً على مخرجات برنامج SPSS.

رقم الفقرة	مخاطر أمن نظم المعلومات المحاسبية	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفرق	نتيجة الفرضية العدمية
11	الحذف أو التعديل غير المتعمد لمصادر بيانات مدخلات صحيحة بواسطة الأفراد العاملين في نظام المعلومات المحاسبي.	3.262	3.572	0.001	معنوية	رفض
12	الإدخال المتعمد لبيانات غير سليمة أو مكررة من قبل العاملين في نظام المعلومات المحاسبي، للقيام بعمليات غير مصرح بها.	2.303	-10.600	0.000	معنوية	قبول
13	الإدخال غير المتعمد لبيانات غير سليمة أو مكررة من قبل العاملين في نظام المعلومات المحاسبي، نتيجة السهو وعدم المعرفة.	3.189	2.306	0.023	معنوية	رفض
14	التأخير المقصود في إدخال بعض البيانات بواسطة العاملين في نظام المعلومات المحاسبي.	2.771	- 3.050	0.003	معنوية	قبول
15	التأخير غير المقصود في إدخال بعض البيانات بواسطة العاملين في نظام المعلومات المحاسبي.	3.443	7.055	0.000	معنوية	رفض
15-10	مخاطر تهدد أمن مدخلات النظم.	2.829	- 4.076	0.000	معنوية	قبول
16	إهدار وسرقة وقت تشغيل بعض أجهزة الحاسوب المستخدمة في نظام المعلومات المحاسبي باستغلالها في الأغراض الشخصية.	2.746	-3.011	0.003	معنوية	قبول
17	تعديل أو حذف البيانات بطريقة مقصودة نتيجة حدوث احتيال وغش من قبل مستخدمي نظام المعلومات المحاسبي أثناء عمليات التشغيل.	2.131	-12.626	0.000	معنوية	قبول
18	تعديل أو حذف البيانات بطريقة غير مقصودة نتيجة حدوث أخطاء من قبل مستخدمي نظام المعلومات المحاسبي أثناء عمليات التشغيل.	2.836	-2.115	0.037	معنوية	قبول
19	حدوث عمليات تشغيلية غير مكتملة لبيانات محاسبية تم إدخالها.	2.189	-13.335	0.000	معنوية	قبول
19-16	مخاطر أمن عمليات تشغيل النظم.	2.475	-11.461	0.000	معنوية	قبول
20	حذف وإخفاء بنود معينة من مخرجات نظام المعلومات المحاسبي وإنتاج مخرجات مظلة غير سليمة.	1.951	-13.311	0.000	معنوية	قبول
21	الكشف غير المخول به للمعلومات المحاسبية أثناء عرضها على الشاشات أو طباعتها على الورق أو أثناء التخلص منها بعد استخدامها	3.484	6.719	0.000	معنوية	رفض
22	توجيه وتوزيع وتسليم بعض البيانات والمعلومات المحاسبية لأشخاص غير مخولين باستلام نسخة منها أو لا تتوفر فيهم الأمانة.	2.516	-6.809	0.000	معنوية	قبول
23	سرقة وسوء استخدام مخرجات النظام (المعلومات المحاسبية) من قبل القائمين على النظام واستغلالها في أغراض شخصية.	1.812	-16.492	0.000	معنوية	قبول
23-20	مخاطر أمن مخرجات النظم.	2.441	-11.467	0.000	معنوية	قبول
24	انقطاع وتوقف تدفق البيانات والمعلومات المحولة	2.771	-3.554	0.001	معنوية	قبول

رقم الفقرة	مخاطر أمن نظم المعلومات المحاسبية	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة الفرضية العدمية
	الالكترونياً عبر شبكات الحاسوب من المركز الرئيسي للبنك إلى الفروع أو العكس.					
25	اعتراض وصول البيانات المرسلّة عبر الشبكات من أجهزة الخوادم لأجهزة المستخدمين، وتعرضها أحياناً للكشف أو التعديل، أو السرقة.	2.303	-8.836	0.000	معنوية	قبول
26	اختراق مواقع الويب الخاص ببيانات البنك والتجسس على خطوط الاتصالات الخاصة بنقل البيانات.	2.082	-10.304	0.000	معنوية	قبول
27	إنكار بعض الأطراف المتعاملة مع البنك للبيانات والمعلومات المحاسبية المتبادلة الكترونياً.	1.828	-16.402	0.000	معنوية	قبول
28	حدوث أخطاء معينة غير مقصودة أثناء نقل البيانات كإرسال بيانات أو معلومات عن طريق الخطأ إلى موقع آخر.	2.623	-4.759	0.000	معنوية	قبول
28-24	مخاطر أمن تبادل البيانات عبر شبكات النظم.	2.321	-12.539	0.000	معنوية	قبول
29	يتم إجراء تغييرات للنظام وبرامجه بطريقة غير مسموح بها، من قبل أشخاص غير مخولين بذلك، للقيام بعمليات تلاعب واحتيال لاحقة.	1.967	-11.657	0.000	معنوية	قبول
30	حدوث أخطاء في عدم استكمال التعديلات المطلوبة أثناء عمليات التعديل والتطوير.	2.672	-4.179	0.000	معنوية	قبول
30-29	مخاطر أمن تعديل وتطوير نظم المعلومات.	2.320	-9.575	0.000	معنوية	قبول
30-1	المؤشرات العامة للمخاطر ككل	2.430	-15.215	0.000	معنوية	قبول

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS).

• مستوى الدلالة الإحصائية المعنوية المعيارية ($\alpha \leq 0.05$)، عند مستوى الثقة 95 %، ومتوسط أداة القياس الافتراضي = (3)، ودرجة الحرية (df=121).

يتبين من الجدول السابق رقم (3-4-1) ما يلي:

- بلغت قيمة المتوسط الحسابي الإجمالي على مستوى محور المخاطر ككل لجميع الفقرات (2.430) درجة من أصل خمس درجات، وهي قيمة أقل من قيمة المتوسط الحسابي الفرضي المعياري لأداة القياس في هذه الدراسة وهي (3) درجات وفقاً لمقياس ليكرت الخماسي، وبدلالة معنوية حيث كانت قيمة مستوى الدلالة المحسوبة ($P=0.000$)، وهي أقل من قيمة مستوى الدلالة المعنوية الإحصائية المعتمد لهذه الدراسة والبالغة ($\alpha=0.05$)، وذلك يعني بشكل عام عدم حدوث مخاطر جوهرية تهدد أمن نظم المعلومات المحاسبية المحسوبة لدى البنوك التجارية في الجمهورية اليمنية وبدلالة معنوية إحصائية، ويمكن تعميم هذه النتيجة على المجتمع الكلي للدراسة.
- إنَّ قيم مستوى المعنوية المحسوبة لمعاملات (T) لجميع الفقرات تقل عن قيمة مستوى الدلالة المعنوية المعتمد لهذه الدراسة والبالغة ($\alpha=0.05$)، مما يدل على أن هناك فروقاً معنوية إحصائية بين المتوسط الحسابي لإجابات أفراد العينة عن تلك الفقرات الخاصة بمخاطر أمن نظم المعلومات المحاسبية المحسوبة، والمتوسط

الفرضي المعياري لأداة القياس البالغ (3)، وبالتالي نستنتج أنَّ أفراد العينة كانوا موافقين أو رافضين لمضمون كل فقرة من تلك الفقرات المتعلقة بحدوث المخاطر المدروسة بشكل معنوي عند مستوى ثقة (95%)، وليس نتيجة الحظ والصدفة، وعليه يمكن تعميم النتيجة على مجتمع الدراسة الكلي على مستوى جميع فقرات محور المخاطر ككل.

■ تم قبول وتعميم الفرضية العدمية الأولى على مستوى الفقرات التي كانت قيم المتوسط الحسابي لها أصغر من (3)، والفرق معنوي وله دلالة إحصائية، وذلك يعني أنه لا تحدث مخاطر جوهرية وملموسة تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، من وجهة نظر أفراد عينة الدراسة وبما يخص تلك الفقرات في ذلك المحور.

■ تم رفض الفرضية العدمية الأولى وقبول وتعميم الفرضية البديلة لها على مستوى الفقرات التي كانت قيم المتوسط الحسابي لها أكبر من (3)، والفرق معنوي وله دلالة إحصائية، وذلك يعني حدوث مخاطر جوهرية وملموسة تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية، من وجهة نظر أفراد عينة الدراسة وبما يخص الفقرات (7، 11، 13، 15، 21)، وبدرجات متفاوتة، حيث يتضح أن خطر تلف بعض ملفات البيانات والبرامج ونظم التشغيل نتيجة تعرض قاعدة البيانات لنظام المعلومات المحاسبي المحسوب للإصابة بالبرامج الخبيثة مثل (الفيروسات، والديدان، وبرامج التجسس)، وخطر الحذف أو التعديل غير المتعمد لمصادر بيانات مدخلات صحيحة بواسطة الأفراد العاملين في نظام المعلومات المحاسبي، وخطر الإدخال غير المتعمد لبيانات غير سليمة أو مكررة من قبل العاملين في نظام المعلومات المحاسبي، نتيجة السهو وعدم المعرفة، هي أهم تلك المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية.

■ وبشكل عام ومن خلال ما سبق من تحليل ودلائل إحصائية فقد تمَّ قبول الفرضية العدمية الأولى التي تنص على أنه: “لا تحدث مخاطر جوهرية وملموسة تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية”، حيث كان الوزن النسبي لتلك المخاطر (48.6%)، وهي أقل من (60 %) بدلالة إحصائية أقل من (5%)، وقد يعود ذلك إلى أن البنوك التجارية في الجمهورية اليمنية تمتلك وسائل وتستخدم مجموعة من الإجراءات الإدارية والتنظيمية والرقابية والتقنية بشكل أو بآخر للسيطرة على تلك المخاطر، والتي سيتم التطرق لها أثناء تحليل الفرضية الخامسة، ولكن عدم حدوث تلك المخاطر بشكل عام لا يعني عدم حدوثها بشكل مطلق وإنما درجة حدوثها دون متوسط أداة القياس، فقد اتضح من خلال التحليل الإحصائي بأن مستوى حدوث تلك المخاطر متوسط لأن مخاطر أمن نظم المعلومات المحاسبية المحوسبة قائمة بحكم طبيعة العمل في البنوك التجارية العاملة في الجمهورية اليمنية والتي يعتمد نشاطها بالدرجة الأولى على تقديم الخدمات المصرفية الإلكترونية، وما ينتج عنها من مخاطر تحدث بدرجات متفاوتة تتوقف على كفاءة وفعالية وسائل وإجراءات الحماية والسيطرة المطبقة لدى تلك البنوك، ومستوى التهديدات الداخلية والخارجية الموجودة.

3-4-2: نتيجة اختبار الفرضية الثانية:

تنص الفرضية العدمية الثانية (H^0-2) على أنه: "لا يُعزى حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية إلى مجموعة من التهديدات الداخلية"، وتنص الفرضية البديلة لها (H^1-2) على أنه: "يُعزى حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية إلى مجموعة من التهديدات الداخلية"، وتهدف هذه الفرضية إلى معرفة مدى وجود تهديدات داخلية تسبب حدوث مخاطر لأمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، وللتحقق من أن متوسط كل فقرة من الفقرات المتعلقة بتلك التهديدات أقل أو أكبر من المتوسط الفرضي المعياري لأداة القياس (3)، بدرجة جوهرية معنوية إحصائياً وليست ناتجة عن الصدفة وفق آراء عينة الدراسة، لجأ الباحث إلى استخدام اختبار (T) للعينة الواحدة (*One Sample T-test*) لدراسة دلالة تلك الفروق، حيث تم الاعتماد على مستوى الدلالة الإحصائية المعنوية ($\alpha=0.05$) كأساس لقبول الفرضية العدمية أو رفضها (وفق قاعدة القرار المبينة سابقاً)،⁽¹⁾ وقد قام الباحث بإجراء الاختبار الإحصائي لكل نوع على حده من أنواع التهديدات الداخلية التي وردت في الاستقصاء، وقد كانت النتائج كما في الجدول الآتي:

جدول رقم (3-4-2) نتيجة اختبار (T) لعينة الدراسة بشأن الفقرات الرئيسية والفرعية

للفرضية الثانية والمتعلقة بالتهديدات الداخلية المسببة لحدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة⁽²⁾

رقم الفقرة	التهديدات الداخلية لأمن نظم المعلومات المحاسبية	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة الفرضية العدمية
31	لا تترك الإدارة العليا للبنك أهمية أمن نظم المعلومات المحاسبية، فلا تدعم الجهة المعنية بتطبيق السياسات الأمنية مادياً أو معنوياً.	3.320	3.567	0.001	معنوية	رفض
32	عدم وجود سياسات وخطط إدارية واضحة ومعتمدة ومعلنة وموثقة لإدارة مخاطر أمن نظم المعلومات المحاسبية في البنك.	3.312	3.130	0.002	معنوية	رفض
33	عدم قيام إدارة البنك بإصدار قرارات وتشريعات خاصة فعالة للحد من مخاطر أمن نظم المعلومات المحاسبية، ومعاينة الموظفين المخليين بتلك القواعد.	3.516	5.536	0.000	معنوية	رفض
34	شعور إدارة البنك بعدم جدوى تقييم مخاطر أمن نظم المعلومات المحاسبية، لاعتقادها بأن تكلفة تطبيق إجراءات الحماية أكبر من عوائدها المتوقعة.	2.762	-2.658	0.009	معنوية	قبول
35	لا تقوم الإدارة بمشاركة الأقسام المختصة لبحث أفضل السبل لمواجهة تلك المخاطر.	3.631	7.977	0.000	معنوية	رفض
36	امتناع الإدارة العليا للبنك عن الإفصاح عن تلك المخاطر والخسائر المترتبة عنها، خوفاً من اهتزاز الثقة بسمعة البنك وبمركزه المالي.	3.713	8.623	0.000	معنوية	رفض
36-31	فلسفة الإدارة العليا للبنك.	3.357	5.363	0.000	معنوية	رفض

(¹) بالعودة إلى آلية وإجراءات تحليل ومعالجة البيانات في المبحث الأول من هذا الفصل.

(²) الجدول من إعداد الباحث اعتماداً على مخرجات برنامج SPSS.

رقم الفقرة	التهديدات الداخلية لأمن نظم المعلومات المحاسبية	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفرق	نتيجة الفرضية العدمية
37	عدم وجود إدارة أو قسم أو لجنة مستقلة، لها صلاحيات كافية لتقييم ومتابعة مخاطر أمن نظم المعلومات المحاسبية، بهدف حماية تلك النظم.	3.320	3.187	0.002	معنوية	رفض
38	غياب التوصيف الدقيق للوظائف والذي يحدد المسؤوليات والصلاحيات لكل موظف داخل الهيكل التنظيمي للبنك.	3.279	2.549	0.012	معنوية	رفض
39	الفصل غير الواضح بين المهام المتعلقة بنظم المعلومات المحاسبية في البنك، كإشراك بعض العاملين باستخدام نفس كلمات السر أو تبادلها بينهم، مما قد يهدد مبدأ تقسيم العمل.	2.713	-2.577	0.011	معنوية	قبول
40	النقص الكبير في الموظفين المختصين بأمن نظم المعلومات والذي تتوفر فيهم الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المتعددة المطلوبة لذلك.	3.303	3.095	0.002	معنوية	رفض
41	صعوبة وعدم كفاية تدريب وتأهيل وتوعية الموظفين في مجال تقنيات وأسابيل أمن نظم المعلومات، وعدم توافق التدريب مع التطور المستمر لبرامج أمن نظم المعلومات.	3.877	10.701	0.000	معنوية	رفض
42	الاهتمام غير الكافي بفحص التاريخ الوظيفي والمهني للموظفين الجدد مما قد يؤثر على قاعدة وضع الرجل المناسب في المكان المناسب.	3.344	3.444	0.001	معنوية	رفض
42-37	تهديدات تنظيمية.	3.306	3.962	0.000	معنوية	رفض
43	تقادم الأجهزة والبرامج المستخدمة وضعف فاعليتها في حفظ وتشغيل البيانات وإنتاج المعلومات وتدقيقها وتخزينها واسترجاعها بسهولة ودقة وسرعة.	2.699	-3.689	0.000	معنوية	قبول
44	الصعوبة في إيجاد التوليفة المثلى للأجهزة والبرامج وأجهزة الدعم المساندة لها بعناية، لتحديث وتطوير الأنظمة، بما يؤمن تحقيق أهداف النظام وتأمين عناصر الرقابة.	2.541	-5.683	0.000	معنوية	قبول
45	وجود أخطاء في تصميم البرامج والتطبيقات المحاسبية المستخدمة تؤدي إلى إنتاج معلومات خاطئة أو غير دقيقة لفترات طويلة.	2.713	-3.169	0.002	معنوية	قبول
46	عدم كفاية عمليات الصيانة الدورية لأجهزة الحاسوب والبرمجيات المستخدمة في تشغيل وحماية نظم المعلومات المحاسبية المحوسبة.	2.754	-3.902	0.000	معنوية	قبول
47	اعتماد البنك في الحصول على الأجهزة والبرامج، والدعم الفني لها على مزودين قليلي الخبرة، ولا يتم التقييم المستمر لوضعهم في السوق.	2.828	-2.377	0.019	معنوية	قبول
48	عدم التوائم والتوافق ما بين الأنظمة والتطبيقات الموجودة لدى البنك مع الأنظمة والتطبيقات الخاصة بالمنشآت التي قد يتم ربط أنظمة البنك معها.	2.393	-6.642	0.000	معنوية	قبول
48-43	تهديدات متعلقة بإمكانات البنك التكنولوجية.	2.654	-6.298	0.000	معنوية	قبول
49	سوء استخدام الصلاحيات الواسعة المخولة لبعض الأفراد المسؤولين عن تشغيل النظام ممن لديهم معرفة واسعة بنفاصيل النظام، وعدم التزامهم بالإجراءات المحددة لحمايته.	3.156	1.525	0.130	غير معنوية	رفض ولا يمكن تعميمها
50	ضعف إدراك بعض العاملين بالنظام لمهامهم الموكولة لهم (كنسيان كلمة المرور للدخول للنظام، أو السماح لزملاء باستخدامها)، مما يترتب عليها أخطاء فادحة عند التشغيل.	3.746	9.196	0.000	معنوية	رفض
51	إهمال بعض العاملين بنظام المعلومات المحاسبي وعدم بذلهم العناية المهنية الكافية لأداء العمل، لنقص التأهيل	4.066	14.709	0.000	معنوية	رفض

رقم الفقرة	التهديدات الداخلية لأمن نظم المعلومات المحاسبية	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة الفرضية العدمية
	والخبرة والوعي الرقابي.					
52	ارتفاع مستوى خبرة بعض العاملين في مجال التشغيل الإلكتروني، وزيادة معرفتهم أكثر من غيرهم بنقاط الضعف في الضوابط الرقابية المطبقة، مما ينتج عن ذلك مخاطر للنظام.	3.312	3.708	0.000	معنوية	رفض
53	التصرفات الانتقامية للأفراد الغاضبين سواء أثناء عملهم بسبب معاقبتهم أو بعد إنهاء خدماتهم بسبب فصلهم من العمل، حيث يقوموا بالكشف عن بعض المعلومات السرية.	3.205	2.255	0.026	معنوية	رفض
54	انخفاض معدل دوران موظفي أنظمة المعلومات لدى البنك، واحتفاظهم بأسرار الأنظمة ومفاتيح الحل وعدم تعاونهم مع زملائهم في تبادل المعرفة والخبرة.	3.639	7.842	0.000	معنوية	رفض
54-49	تهديدات متعلقة بالأفراد العاملين في النظم.	3.521	8.117	0.000	معنوية	رفض
55	عجز التدابير الأمنية لنظم المعلومات، وعدم كفاية وفعالية الأدوات والضوابط والإجراءات الرقابية المطبقة في البنك لحماية أمن نظام المعلومات المحاسبي.	2.459	-7.840	0.000	معنوية	قبول
56	ضعف كفاءة وفعالية نظم الرقابة الداخلية للبنك وعدم إصدار تقارير رقابية دورية حول الأنظمة الآلية، لئتم متابعتها وتقييمها لمواكبة التطورات التي تجري لمواجهة المخاطر.	2.680	-4.912	0.000	معنوية	قبول
57	عدم كفاءة وفعالية إجراءات إدارة المخاطر، وعدم القيام بالتقييم الذاتي لمخاطر أمن نظم المعلومات بحيث يقوم كل موظف بتحديد المخاطر التي يواجهها وتقييم إجراءات مواجهتها	3.295	4.244	0.000	معنوية	رفض
58	غياب المسار المرني للمراجعة فعدم رؤية عمليات إدخال البيانات وتشغيلها سهل من تغيير أو إضافة أو حذف أي بيانات دون ترك أثر يدل على ذلك، وصعوبة اكتشاف ذلك.	3.049	0.749	0.456	غير معنوية	رفض ولا يمكن تعميمها
58-55	ضعف الرقابة الداخلية وإدارة المخاطر بالبنك.	2.871	-2.805	0.006	معنوية	قبول
59	حدوث كوارث غير طبيعية من البيئة الداخلية للبنك (كالتخريب، والحريق، وانقطاع الكهرباء، وتسريب المياه)، تسبب تلك الكوارث تلف جزئي أو تدمير كلي لموارد النظام.	3.172	1.536	0.127	غير معنوية	رفض ولا يمكن تعميمها
59	حدوث كوارث داخلية في البنك (غير طبيعية).	3.172	1.536	0.127	غير معنوية	رفض ولا يمكن تعميمها
59-31	المؤشرات العامة للتهديدات الداخلية ككل	3.147	2.740	0.007	معنوية	رفض

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS).
• مستوى الدلالة الإحصائية المعنوية المعيارية ($\alpha=0.05$)، عند مستوى الثقة 95 %، ومتوسط أداة القياس الإحصائي = (3)، ودرجة الحرية (df=121).

يتبين من الجدول السابق رقم (3-4-2) ما يلي:

- إن قيم مستوى المعنوية المحسوبة لمعاملات (T) لمعظم الفقرات تقل عن مستوى الدلالة المعنوية المعتمد في هذه الدراسة والبالغة ($\alpha=0.05$)، مما يدل على أن هناك فروقاً معنوية إحصائية بين المتوسط الحسابي لتلك الفقرات الخاصة بالتهديدات الداخلية المسببة لحدوث مخاطر أمن نظم المعلومات المحاسبية، والمتوسط الفرضي المعياري لأداة القياس (3)، وبالتالي نستنتج أن أفراد العينة كانوا موافقين أو رافضين لمضمون تلك الفقرات بشكل معنوي،

عند مستوى ثقة (95%)، وعليه يمكن تعميم النتيجة على مجتمع الدراسة الكلي على مستوى جميع فقرات محور التهديدات الداخلية ماعدا الفقرات (49، 58، 59) فلا يمكن تعميم نتائجها، حيث كانت الفروق غير معنوية بل كانت ناتجة عن الحظ والصدفة.

■ تم قبول وتعميم الفرضية العدمية الثانية على مستوى الفقرات الفرعية والرئيسية التي كانت قيم المتوسط الحسابي لها أصغر من (3)، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية لا يُعزى للتهديدات الداخلية في تلك البنوك، وبما يخص تلك الفقرات في ذلك المحور.

■ تم رفض الفرضية العدمية الثانية وقبول وتعميم الفرضية البديلة لها على مستوى الفقرات الفرعية والرئيسية التي كانت قيم المتوسط الحسابي لها أكبر من (3)، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية يُعزى للتهديدات الداخلية في تلك البنوك، بما يخص تلك الفقرات في ذلك المحور.

■ بلغت قيمة المتوسط الحسابي الإجمالي على مستوى محور التهديدات الداخلية لجميع الفقرات (3.147) درجة من أصل خمس درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي الفرضي المعياري لأداة القياس في هذه الدراسة وهي (3) درجات وفقاً لمقياس ليكرت الخماسي، وبدلالة معنوية حيث بلغت قيمة مستوى الدلالة المحسوبة ($P=0.007$)، وهي أقل من مستوى قيمة الدلالة المعنوية المعتمد لهذه الدراسة ($\alpha=0.05$)، ويعني ذلك بشكل عام وجود تهديدات داخلية تسبب حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة وبدلالة معنوية إحصائية، ويمكن تعميم هذه النتيجة على المجتمع الكلي للدراسة.

■ ومن خلال ما سبق من تحليل ودلائل إحصائية فقد تمّ رفض الفرضية العدمية الثانية التي تنص على أنه: "لا يُعزى حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية إلى مجموعة من التهديدات الداخلية لدى تلك البنوك"، وتم قبول الفرضية البديلة القائلة: "يُعزى حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية إلى مجموعة من التهديدات الداخلية لدى تلك البنوك".

3-5-3: نتيجة اختبار الفرضية الثالثة:

تنص الفرضية العدمية الثالثة (H^0-3) على أنه: "لا يُعزى حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية إلى مجموعة من التهديدات الخارجية"، وتنص الفرضية البديلة لها (H^1-3) على أنه: "يُعزى حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية إلى مجموعة من التهديدات الخارجية"، وتهدف هذه الفرضية إلى معرفة مدى وجود تهديدات خارجية تسبب حدوث مخاطر لأمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، وللتحقق من أنّ متوسط كل فقرة من الفقرات المتعلقة بتلك التهديدات أقل أو أكبر من المتوسط الفرضي المعياري لأداة القياس (3)، بدرجة جوهريّة معنوية إحصائية وليست ناتجة عن الصدفة وفق

أراء عينة الدراسة، لجأ الباحث إلى استخدام اختبار (T) للعينة الواحدة (One Sample T-test) لدراسة دلالة تلك الفروق، حيث تم الاعتماد على مستوى الدلالة الإحصائية المعنوية ($\alpha=0.05$) كأساس لقبول الفرضية العدمية أو رفضها (وفق قاعدة القرار المبينة سابقاً)⁽¹⁾، وقد قام الباحث بإجراء الاختبار الإحصائي لكل نوع على حده من أنواع التهديدات الخارجية التي وردت في الاستقصاء وقد كانت النتائج كما في الجدول الآتي:

جدول رقم (3-4-3) نتيجة اختبار (T) لعينة الدراسة بشأن الفقرات الرئيسية والفرعية للمحور الثالث والمتعلقة بالتهديدات الخارجية المسببة لحدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة⁽²⁾

رقم الفقرة	التهديدات الخارجية لأمن نظم المعلومات المحاسبية	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة الفرضية العدمية
60	التطورات التكنولوجية السريعة والهائلة والمتلاحقة والتي تلي وضع الإجراءات الرقابية في البنك، فتقدم التقنية خارجياً أسرع من ممارسة الأمن داخل البنك.	4.033	14.600	0.000	معنوية	رفض
61	عدم وجود استقرار نسبي لنظام المعلومات، بسبب ارتفاع معدلات التغير في تكنولوجيا المعلومات، مقابل ضعف إمكانيات البنك المالية والبشرية لمجاراتها واستيعابها.	3.639	7.540	0.000	معنوية	رفض
62	تصميم أساليب للتلاعب تبنى داخل النظام المحاسبي الإلكتروني يصعب اكتشافها، تؤدي إلى إنتاج معلومات محاسبية خاطئة.	2.738	-3.528	0.001	معنوية	قبول
63	عدم توفر بنية تحتية تكنولوجية قوية في الجمهورية اليمنية.	3.754	8.274	0.000	معنوية	رفض
63-60	التغيير التكنولوجي غير المتوازن	3.541	9.446	0.000	معنوية	رفض
64	حدوث الكوارث الطبيعية والبيئية كالزلازل، والبراكين، والفيضانات والسيول، والرياح العاتية والأعاصير، والصواعق، والحرائق الطبيعية وانقطاع التيار الكهربائي لأسباب طبيعية خارجية، يؤدي إلى حدوث تلف جزئي أو تدمير كلي لموارد النظام (أجهزة، وبرامج، وملفات بيانات، وأفراد).	3.221	2.850	0.005	معنوية	رفض
65	حدوث كوارث غير طبيعية (بشرية)، كالاضطرابات السياسية المحلية والإقليمية، والحروب، والتهديدات الإرهابية.	3.738	8.409	0.000	معنوية	رفض
65-64	الكوارث الطبيعية والسياسية	3.480	6.588	0.000	معنوية	رفض
66	جرائم وقرصنة الحاسوب نتيجة تصرفات غير أمينة من قبل أطراف خارجية كالقرصنة والمتطفلين الذين يخترقوا نظم الحماية، رغبة في التحدي، أو لنوايا إجرامية وتجسسية.	3.303	4.349	0.000	معنوية	رفض
66	المخترقون والقرصنة	3.303	4.349	0.000	معنوية	رفض
67	الإصابة بالبرامج الخبيثة (الفيروسات والديدان، وبرامج التجسس)، التي قد تتلف البيانات أو تعطل النظام وتؤثر على عملية تشغيل البيانات.	4.066	15.761	0.000	معنوية	رفض
67	دخول فيروسات وبرمجيات الحاسوب الخبيثة للنظام	4.066	15.761	0.000	معنوية	رفض

(¹) بالعودة إلى آلية وإجراءات تحليل ومعالجة البيانات في المبحث الأول من هذا الفصل.

(²) الجدول من إعداد الباحث اعتماداً على مخرجات برنامج SPSS.

رقم الفقرة	التهديدات الخارجية لأمن نظم المعلومات المحاسبية	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفرق	نتيجة الفرضية العدمية
68	رغبة منافسي البنك في الوصول إلى المعلومات السرية كعملاء البنك، وحجم النشاط وغيرها من المعلومات الهامة.	2.607	-5.516	0.000	معنوية	قبول
69	زيادة المنافسة بين البنوك والذي جعلتها تقوم بتقديم الخدمات المصرفية الإلكترونية دون مراعاة الآثار التي يمكن أن تحدث عند الاستخدام الفعلي.	3.107	1.736	0.085	غير معنوية	رفض ولا يمكن تعميمها
69-68	المنافسة الاقتصادية بين البنوك	2.857	-2.714	0.008	معنوية	قبول
70	عدم إيلاء المراجع الخارجي الأهمية الكافية لمخاطر أمن نظام المعلومات المحاسبي في البنك، عند قيامه بمهامه للتأكد من أن النظام قد تم تصميمه وتشغيله بطريقة ملائمة.	3.738	10.592	0.000	معنوية	رفض
71	عدم قيام البنك المركزي والسلطات الرقابية الرسمية بتكثيف حملات تفتيشية مفاجئة لتقييم مخاطر أمن نظم المعلومات المحاسبية لدى البنوك، وإلزامها برفع تقارير بهذا الشأن.	3.844	9.779	0.000	معنوية	رفض
71-70	ضعف الرقابة الخارجية على نظم المعلومات.	3.791	12.116	0.000	معنوية	رفض
72	عدم تحديث القوانين المحلية النافذة التي تهدف إلى حماية أمن نظم المعلومات، سواء كانت قوانين جنائية أو مدنية أو تجارية، فهي تفتقد إلى كثير من النصوص اللازمة.	4.049	14.651	0.000	معنوية	رفض
73	الغموض التشريعي بشأن اختصاص وانطباق القوانين واللوائح المعمول بها لتحديد الحقوق والالتزامات الناتجة عن العمليات المصرفية الإلكترونية.	4.139	19.850	0.000	معنوية	رفض
74	اختلاف التشريعات القانونية التي تنظم التعاملات المصرفية الإلكترونية بين الدول مما يؤدي إلى تنازع القوانين واختصاصات المحاكم في فض النزاعات التي تنشأ عنها.	3.820	9.957	0.000	معنوية	رفض
75	عدم وجود أطر تشريعية وقانونية متناسقة ومتجانسة على المستوى المحلي والإقليمي والدولي لمعاقبة مرتكبي جرائم الحاسوب والانترنت.	3.902	11.624	0.000	معنوية	رفض
75-72	ضعف التشريعات والقوانين المحلية في مجال تكنولوجيا المعلومات.	3.978	17.655	0.000	معنوية	رفض
76	نقص الوعي الإلكتروني لدى عملاء البنك وعدم إتباعهم إجراءات التأمين الوقائية الواجبة لبياناتهم الشخصية، وضعف دور البنك في القيام بتوعيتهم.	4.123	16.649	0.000	معنوية	رفض
76	نقص الوعي الإلكتروني لعملاء البنك	4.123	16.649	0.000	معنوية	رفض
76-60	المؤشرات العامة للتهديدات الخارجية ككل	3.642	17.210	0.000	معنوية	رفض

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS).
• مستوى الدلالة الإحصائية المعنوية المعيارية ($\alpha=0.05$)، عند مستوى الثقة 95 %، ومتوسط أداة القياس الإحصائي = (3)، ودرجة الحرية (df=121).

يتبين من الجدول السابق رقم (3-4-3) ما يلي:

- بلغت قيمة المتوسط الحسابي الإجمالي على مستوى محور التهديدات الخارجية لجميع الفقرات (3.642) درجة من أصل خمس درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي الفرضي المعياري لأداة القياس في هذه الدراسة وهي (3) درجات وفقاً لمقياس ليكرت الخماسي، وبدلالة معنوية حيث بلغت قيمة مستوى الدلالة

المحسوبة ($P=0.000$)، وهي أقل من مستوى قيمة الدلالة المعنوية المعتمد لهذه الدراسة ($\alpha=0.05$)، ويعني ذلك بشكل عام وجود تهديدات خارجية تسبب حدوث مخاطر أمن نظم المعلومات المحاسبية المحسوبة وبدلالة معنوية إحصائية، ويمكن تعميم هذه النتيجة على المجتمع الكلي للدراسة.

■ إنَّ قيم مستوى المعنوية المحسوبة لمعاملات (T) لمعظم الفقرات تقل عن مستوى الدلالة المعنوية المعتمد في هذه الدراسة والبالغة ($\alpha=0.05$)، مما يدل على أن هناك فروقاً معنوية إحصائية بين المتوسط الحسابي لتلك الفقرات الخاصة بالتهديدات الخارجية المسببة لحدوث مخاطر أمن نظم المعلومات المحاسبية، والمتوسط الفرضي المعياري لأداة القياس (3)، وبالتالي نستنتج أنَّ أفراد العينة كانوا موافقين أو رافضين لمضمون تلك الفقرات بشكل معنوي، عند مستوى ثقة (95%)، وعليه يمكن تعميم النتيجة على مجتمع الدراسة الكلي على مستوى جميع فقرات محور التهديدات الخارجية ماعدا التهديد الوارد في الفقرة رقم (69) المتعلقة بزيادة المنافسة بين البنوك والذي جعلتها تقوم بتقديم الخدمات المصرفية الإلكترونية دون مراعاة الآثار التي يمكن أن تحدث عند الاستخدام الفعلي، فلا يمكن تعميم نتائج تلك الفقرة، حيث كانت الفروق غير معنوية بل كانت ناتجة عن الحظ والصدفة.

■ تم قبول وتعميم الفرضية العدمية الثالثة على مستوى الفقرات الفرعية والرئيسية التي كانت قيم المتوسط الحسابي لها أصغر من (3)، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن حدوث مخاطر أمن نظم المعلومات المحاسبية المحسوبة لدى البنوك التجارية في الجمهورية اليمنية لا يُعزى للتهديدات الخارجية في تلك البنوك من وجهة نظر أفراد عينة الدراسة وبما يخص تلك الفقرات في ذلك المحور.

■ تم رفض الفرضية العدمية الثالثة وقبول وتعميم الفرضية البديلة لها على مستوى الفقرات الفرعية والرئيسية التي كانت قيم المتوسط الحسابي لها أكبر من (3)، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن حدوث مخاطر أمن نظم المعلومات المحاسبية المحسوبة لدى البنوك التجارية في الجمهورية اليمنية يُعزى للتهديدات الخارجية في تلك البنوك من وجهة نظر عينة الدراسة وبما يخص تلك الفقرات في ذلك المحور.

■ وبشكل عام ومن خلال ما سبق من تحليل ودلائل إحصائية فقد تمَّ رفض الفرضية العدمية الثالثة التي تنص على أنه: "لا يُعزى حدوث مخاطر أمن نظم المعلومات المحاسبية المحسوبة لدى البنوك التجارية في الجمهورية اليمنية إلى مجموعة من التهديدات الخارجية لدى تلك البنوك"، وتم قبول الفرضية البديلة القائلة: "يُعزى حدوث مخاطر أمن نظم المعلومات المحاسبية المحسوبة لدى البنوك التجارية في الجمهورية اليمنية إلى مجموعة من التهديدات الخارجية لدى تلك البنوك".

3-4-4: نتيجة اختبار الفرضية الرابعة:

تنص الفرضية العدمية الرابعة (H^0-4) على أنه: "لا يؤثر حدوث مخاطر أمن نظم المعلومات المحاسبية المحسوبة لدى البنوك التجارية في الجمهورية اليمنية على العناصر المكونة لأمن تلك النظم المتمثلة ب(إتاحة النظم، وصحة وسلامة وتكامل التشغيل، وسرية وخصوصية المخرجات، وعدم إنكار العمليات) لدى تلك البنوك"، وتنص الفرضية البديلة لها (H^1-4) على أنه: "يؤثر حدوث مخاطر أمن نظم المعلومات المحاسبية

المحوسبة لدى البنوك التجارية في الجمهورية اليمنية على العناصر المكونة لأمن تلك النظم المتمثلة ب(إتاحة النظم، وصحة وسلامة وتكامل التشغيل، وسرية وخصوصية المخرجات، وعدم إنكار العمليات) لدى تلك البنوك"، وللتحقق من أن متوسط كل فقرة من الفقرات المتعلقة بتلك التأثيرات أقل أو أكبر من المتوسط الفرضي المعياري لأداة القياس (3)، بدرجة جوهرية معنوية إحصائياً وليست ناتجة عن الصدفة وفق آراء عينة الدراسة، لجأ الباحث إلى استخدام اختبار (T) للعينة الواحدة (One Sample T-test) لدراسة دلالة تلك الفروق، حيث تم الاعتماد على مستوى الدلالة الإحصائية المعنوية ($\alpha=0.05$) كأساس لقبول الفرضية العدمية أو رفضها (وفق قاعدة القرار المبينة سابقاً)⁽¹⁾، وقد قام الباحث بإجراء الاختبار الإحصائي لكل تأثير على حده من التأثيرات التي وردت في الاستقصاء وقد كانت النتائج كما في الجدول الآتي:

جدول رقم (3-4) نتيجة اختبار (T) لعينة الدراسة بشأن الفقرات الرئيسية والفرعية للفرضية الرابعة والمتعلقة بتأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة⁽²⁾

رقم الفقرة	تأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة الفرضية العدمية
77	تعرض نظام المعلومات المحاسبي بالبنك للتعطيل بسبب المخاطر يؤثر على استرجاع البيانات والمعلومات ويترتب على ذلك خسائر مالية كبيرة، وقد يؤدي ذلك إلى خروج البنك من السوق وإفلاسه.	2.762	-2.658	0.009	معنوية	قبول
78	تدمير البنية التحتية لنظم المعلومات المحاسبية وتوقفها لفترات طويلة يؤدي إلى إعاقه وصول المستخدمين والأطراف المستفيدة، مما يفقد البنك فرص نشاط حقيقية.	3.271	2.904	0.004	معنوية	رفض
79	حالات التعطيل والتوقف المفاجئ لنظام المعلومات المحاسبي للبنك لبعض الوقت يؤدي إلى اهتزاز مكانة البنك أمام عملائه وتكبّد البنك خسائر تجارية ومالية كبيرة.	3.467	5.262	0.000	معنوية	رفض
79-77	تأثير المخاطر على إتاحة نظم المعلومات المحاسبية.	3.167	2.191	0.030	معنوية	رفض
80	حدوث مخاطر أمن نظم المعلومات المحاسبية يؤثر على سلامة تجهيز البيانات وعمليات التشغيل والمخرجات، بالدقة والشمولية المطلوبة وفي الوقت المناسب.	3.385	4.660	0.000	معنوية	رفض
81	تشغيل النظام بشكل خاطئ وباستخدام برامج غير ملائمة يؤدي إلى حصول البنك لمخرجات غير دقيقة وغير سليمة، يؤثر على صحتها ومصداقيتها.	3.885	10.735	0.000	معنوية	رفض
82	تعرض نظم المعلومات المحاسبية المحوسبة بالبنك إلى أي خطر يخفف من تكامل تلك النظم مع بعضها البعض على مستوى الأقسام والفروع، فوقع خطأ ما يؤدي إلى وقوع سلسلة من الأخطاء نتيجة التحديث الفوري للملفات.	3.541	6.995	0.000	معنوية	رفض
82-80	تأثير المخاطر على سلامة وتكامل تجهيز البيانات في نظم المعلومات المحاسبية.	3.604	8.723	0.000	معنوية	رفض
83	إن اقتحام نظام المعلومات المحاسبي من أطراف غير مخولة بالدخول، يؤدي إلى إمكانية سرقة أو تسرب معلومات هامة على درجة عالية من السرية لجهات غير مرغوب فيها.	3.664	6.393	0.000	معنوية	رفض
84	إن حدوث مخاطر أمن نظم المعلومات المحاسبية يؤدي إلى إطلاع المنافسين على المعلومات المرتبطة بالبنك والتي قد يترتب عليها الإضرار بالموقف التنافسي.	2.828	-2.862	0.005	معنوية	قبول

(1) بالعودة إلى آلية وإجراءات تحليل ومعالجة البيانات في المبحث الأول من هذا الفصل.

(2) الجدول من إعداد الباحث اعتماداً على مخرجات برنامج SPSS.

رقم الفقرة	تأثير حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة الفرضية العدمية
85	إن حدوث المخاطر يؤدي إلى عدم قدرة نظم المعلومات المحاسبية في البنك على التعامل مع الأطراف المستفيدة المختلفة وفقاً لأصول السرية والفائدة المرجوة.	3.539	5.852	0.000	معنوية	رفض
85-83	تأثير المخاطر على سرية المعلومات المحاسبية.	3.342	4.709	0.000	معنوية	رفض
86	إن حدوث مخاطر أمن نظم المعلومات المحاسبية يؤدي إلى ضعف قدرة البنك في حماية خصوصيات وأسرار عملائه، نتيجة سرقة أو كشف المعلومات الشخصية لهم والتي يتم جمعها واستخدامها والاحتفاظ بها من قبل نظام المعلومات المحاسبية للبنك.	3.689	8.621	0.000	معنوية	رفض
87	إن تعرض البنك لمخاطر أمن نظم المعلومات المحاسبية يهدد سمعته نتيجة فقدان الثقة وفشل البنك في تحقيق متطلبات العملاء بتقديم خدمة مصرفية إلكترونية متطورة وأمنة.	3.598	7.152	0.000	معنوية	رفض
88	إن حدوث مخاطر أمن نظم المعلومات المحاسبية يؤدي إلى عدم إتاحة الفرصة للعملاء للوصول لمعلوماتهم المخزنة الشخصية لتعديلها أو إلغائها.	3.418	5.248	0.000	معنوية	رفض
88-86	تأثير المخاطر على خصوصية بيانات الأطراف المتعاملة مع البنك.	3.568	8.919	0.000	معنوية	رفض
89	حدوث المخاطر يؤدي إلى تهرب بعض أطراف المعاملات الإلكترونية من الالتزامات، عن طريق إنكار وقوع أحداث وقعت أو ادعاء وقوع أحداث لم تقع، وقد يؤدي ذلك إلى تحمل البنك لخسائر مالية وفقدان الثقة في مخرجات نظم المعلومات المحاسبية.	2.877	-1.771	0.079	غير معنوية	قبول ولا يمكن تعميمها
90	رفض بعض الجهات الحكومية لحجية مخرجات نظم المعلومات المحاسبية المحوسبة استناداً لنصوص تشريعية، كالقانون التجاري وقانون البنوك.	2.787	-2.887	0.005	معنوية	قبول
90-89	تأثير المخاطر على إثبات تصرفات الأطراف المتعاملة خلال تبادل البيانات إلكترونياً.	2.832	-3.000	0.003	معنوية	قبول
90-77	المؤشرات العامة لتأثيرات المخاطر ككل	3.303	5.700	0.000	معنوية	رفض

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS).
• مستوى الدلالة الإحصائية المعنوية المعيارية ($\alpha=0.05$)، عند مستوى الثقة 95 %، ومتوسط أداة القياس الإقراضي ($\alpha=0.05$)، ودرجة الحرية ($df=121$).

يتبين من الجدول السابق رقم (3-4-4) ما يلي:

■ بلغت قيمة المتوسط الحسابي الإجمالي على مستوى محور التأثيرات ككل ولجميع الفقرات (3.303) درجة من أصل خمس درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي الفرضي المعياري لأداة القياس في هذه الدراسة وهي (3) درجات وفقاً لمقياس ليكرت الخماسي، وبدلالة معنوية حيث بلغت قيمة مستوى الدلالة المحسوبة ($P=0.000$)، وهي أقل من مستوى قيمة الدلالة المعنوية المعتمد لهذه الدراسة ($\alpha=0.05$)، ويعني ذلك بشكل عام وجود تأثيرات لحدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة وبدلالة معنوية إحصائياً، ويمكن تعميم هذه النتيجة على المجتمع الكلي للدراسة.

■ إن قيم مستوى المعنوية المحسوبة لمعاملات (T) لمعظم الفقرات تقل عن مستوى الدلالة المعنوية المعتمد في هذه الدراسة والبالغة ($\alpha=0.05$)، مما يدل على أن هناك فروقاً معنوية إحصائية بين المتوسط الحسابي لتلك الفقرات الخاصة بتأثيرات حدوث المخاطر على عناصر أمن نظم المعلومات المحاسبية المحوسبة، والمتوسط الفرضي المعياري لأداة القياس (3)، وبالتالي نستنتج أن أفراد العينة كانوا موافقين أو رافضين لمضمون تلك الفقرات بشكل معنوي، عند مستوى ثقة (95%)، وعليه يمكن تعميم النتيجة على مجتمع الدراسة الكلي على مستوى جميع فقرات محور التأثيرات

ماعدًا التأثير الوارد في الفقرة رقم (89) المتعلق بتهرب بعض أطراف المعاملات الالكترونية من الالتزامات، عن طريق إنكار وقوع أحداث وقعت أو ادعاء وقوع أحداث لم تقع، وقد يؤدي ذلك إلى تحمل البنك لخسائر مالية وفقدان الثقة في مخرجات نظم المعلومات المحاسبية، فلا يمكن تعميم نتائج تلك الفقرة، فقد كانت الفروق غير معنوية بل كانت ناتجة عن الحظ والصدفة.

■ تم قبول وتعميم الفرضية العدمية الرابعة على مستوى الفقرات الفرعية والرئيسية التي كانت قيم المتوسط الحسابي لها أصغر من (3)، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن حدوث مخاطر لا يؤثر على عناصر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، من وجهة نظر أفراد عينة الدراسة وبما يخص تلك الفقرات في ذلك المحور.

■ تم رفض الفرضية العدمية الرابعة وقبول وتعميم الفرضية البديلة لها على مستوى الفقرات الفرعية والرئيسية التي كانت قيم المتوسط الحسابي لها أكبر من (3)، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن حدوث المخاطر يؤثر على عناصر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية من وجهة نظر عينة الدراسة وبما يخص تلك الفقرات في ذلك المحور.

■ وبشكل عام ومن خلال ما سبق من تحليل ودلائل إحصائية فقد تمّ رفض الفرضية العدمية الرابعة التي تنص على أنه: "لا يؤثر حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية على العناصر المكونة لأمن تلك النظم المتمثلة ب(إتاحة النظم، وصحة وسلامة وتكامل التشغيل، وسرية وخصوصية المخرجات، وعدم إنكار العمليات) لدى تلك البنوك"، وتم قبول الفرضية البديلة القائلة: "يؤثر حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية على العناصر المكونة لأمن تلك النظم المتمثلة ب(إتاحة النظم، وصحة وسلامة وتكامل التشغيل، وسرية وخصوصية المخرجات، وعدم إنكار العمليات) لدى تلك البنوك".

3-4-5: نتيجة اختبار الفرضية الخامسة:

تنص الفرضية العدمية الخامسة (H^0-5) على أنه: "لا تطبق البنوك التجارية في الجمهورية اليمنية أساليب وإجراءات كافية وفعّالة لحماية أمن نظم المعلومات المحاسبية المحوسبة من المخاطر التي تتهددها وفق القواعد المحلية والأسس والمعايير الدولية"، وتنص الفرضية البديلة لها (H^1-5) على أنه: "تطبق البنوك التجارية في الجمهورية اليمنية أساليب وإجراءات كافية وفعّالة لحماية أمن نظم المعلومات المحاسبية المحوسبة من المخاطر التي تتهددها وفق القواعد المحلية والأسس والمعايير الدولية"، وتهدف هذه الفرضية إلى معرفة مدى تطبيق أساليب وإجراءات كافية وفعّالة لحماية أمن نظم المعلومات المحاسبية المحوسبة من قبل البنوك التجارية في الجمهورية اليمنية، وللتحقق من أنّ متوسط كل فقرة من الفقرات المتعلقة بتطبيق تلك الأساليب والإجراءات أقل أو أكبر من المتوسط الفرضي المعياري لأداة القياس (3)، بدرجة جوهريّة معنوية إحصائية وليست ناتجة عن الصدفة وفق آراء عينة الدراسة، لجأ الباحث إلى استخدام اختبار (T) للعينة الواحدة (One Sample T-test) لدراسة دلالة تلك الفروق، حيث تم الاعتماد على مستوى الدلالة الإحصائية المعنوية ($\alpha=0.05$) كأساس لقبول

الفرضية العدمية أو رفضها (وفق قاعدة القرار المبينة سابقاً) ⁽¹⁾، وقد قام الباحث بإجراء الاختبار الإحصائي لكل نوع على حده من أنواع الأساليب وإجراءات الحماية الواردة في الاستقصاء وقد كانت النتائج على النحو الآتي:

3-4-5-1: اختبار مدى تطبيق أساليب وإجراءات حماية الأمن التنظيمي للأفراد: تمهيداً لاختبار

الفرضية الخامسة التي تهدف إلى معرفة مدى تطبيق أساليب وإجراءات حماية أمن نظم المعلومات المحاسبية المحوسبة من قبل البنوك التجارية في الجمهورية اليمنية تم التحقق من مدى تطبيق البُعد الأول من الأبعاد الخاصة بتلك الأساليب والإجراءات وهو ما يتعلق بحماية الأمن التنظيمي للأفراد العاملين في تلك النظم وقد تم إجراء الاختبار الإحصائي لكل فقرة على حده من فقرات بُعد أساليب وإجراءات حماية الأمن التنظيمي للأفراد والواردة في قائمة الاستقصاء حيث كانت النتائج على النحو الآتي:

جدول رقم (3-4-5) نتيجة اختبار (T) لعينة الدراسة على مستوى الفقرات المتعلقة

بحماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية المحوسبة ⁽²⁾

رقم الفقرة	حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة اختبار الفرضية
91	يوجد في البنك قسم خاص ومستقل بشكل كافي وبإمكانيات مناسبة مسؤول عن تنفيذ أمن نظم المعلومات المحاسبية وحمايتها، ووضع معايير وأسس وضوابط أمنية.	2.639	-5.388	0.000	معنوية	قبول
92	يوجد دليل عمل مكتوب يتضمن إجراءات أداء العمل لكافة وظائف نظم المعلومات المحاسبية، محدد فيه السلطات والمسئوليات والكفاءات اللازمة لكل وظيفة داخل النظام.	3.492	6.083	0.000	معنوية	رفض
93	يوجد نظام صلاحية مبرمج بحيث يسمح النظام لكل مستخدم بإدارة نظام المعلومات المحاسبي حسب صلاحياته في التعامل مع ملفات النظام، (مثل قراءة البيانات أو نسخها أو تعديلها...الخ)، من خلال الوصول إلى أجزاء معينة وبيانات محددة.	3.787	10.282	0.000	معنوية	رفض
94	كل مستخدم للنظام له كلمة سر خاصة، فلا يتشارك اثنان بكلمة سر واحدة، ويتم إيقاف صلاحيات المستخدم إذا تم إدخال كلمة المرور خطأ أكثر من العدد المسموح به للمحاولات.	4.148	14.918	0.000	معنوية	رفض
95	هناك فصل سليم بين الوظائف والمهام المختلفة والمتعارضة لمعالجة البيانات بين المبرمجين والمشغلين والمراقبين والمستخدمين بطريقة تسمح بمراقبة تنفيذ المهام.	3.771	10.240	0.000	معنوية	رفض
96	يعمل البنك على تنفيذ سياسة التدوير الوظيفي للمهام الأساسية لنظم المعلومات المحاسبية، بإجراء تنقلات بين الموظفين من حين لآخر، وإلزامهم بأخذ إجازاتهم السنوية دفعة واحدة.	2.426	-9.501	0.000	معنوية	قبول

⁽¹⁾ بالعودة إلى آلية وإجراءات تحليل ومعالجة البيانات في المبحث الأول من هذا الفصل.

⁽²⁾ الجدول من إعداد الباحث اعتماداً على مخرجات برنامج SPSS.

رقم الفقرة	حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة اختبار الفرضية
97	يعقد البنك برامج بواسطة مختصين في أمن نظم المعلومات لتوعية العاملين بالمخاطر التي تهدد أمن نظم المعلومات المحاسبية، وتدريبهم على إتباع الإجراءات الملائمة لمواجهتها.	2.443	-7.134	0.000	معنوية	قبول
98	يتم تشجيع الأفراد على اتخاذ مبادرات لحل المشكلات، ومكافأة من يقوم بعمل إيجابي نحو تجسيد نظام الحماية، ومعاقبة من يتعامل سلباً مع المخاطر ويخالفون سياسات الأمن.	2.779	-3.191	0.002	معنوية	قبول
99	يعين البنك شخص مسؤول عن حماية النظام يسمى ضابط أمن المعلومات، ويتم تكوين فريق طوارئ، من فنيين وإداريين فاعلين، لمواجهة أي ظرف طارئ يمس بحماية النظام.	2.762	-3.856	0.000	معنوية	قبول
100	يتم اختيار موظفي نظم المعلومات المحاسبية بحرص شديد وإجراء تحريات عنهم وعن ماضيهم الوظيفي، والحرص على أن يكونوا ذوي خبرة وثقة وأمانة ويعملون لمصلحة البنك، وعدم إعطاء الموظف حديث التعيين صلاحيات عالية لاستخدام النظام.	3.295	3.309	0.001	معنوية	رفض
-91 100	المؤشرات العامة لتطبيق حماية أمن الأفراد	3.154	3.290	0.001	معنوية	رفض

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS).
• مستوى الدلالة الإحصائية المعنوية المعيارية ($\alpha=0.05$)، عند مستوى الثقة 95 %، ومتوسط أداة القياس الافتراضي = (3)، ودرجة الحرية (df=121).

يتبين من الجدول السابق رقم (3-4-5) ما يلي:

- إنَّ قيم مستوى المعنوية المحسوبة لمعاملات (T) لجميع الفقرات تقل عن مستوى الدلالة المعنوية المعتمد في هذه الدراسة وبالبالغة ($\alpha=0.05$)، مما يدل على أن هناك فروقاً معنوية إحصائية بين المتوسط الحسابي لتلك الفقرات المتعلقة بحماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية، والمتوسط الفرضي المعياري لأداة القياس (3)، وبالتالي نستنتج أنَّ أفراد العينة كانوا موافقين أو رافضين لمضمون تلك الفقرات بشكل معنوي، عند مستوى ثقة (95%)، وعليه يمكن تعميم نتيجة تلك الفقرات على مجتمع الدراسة الكلي.
- تم رفض الفرضية العدمية الخامسة وقبول وتعميم الفرضية البديلة لها على مستوى (5) فقرات في ذلك البُعد والتي كانت قيم المتوسط الحسابي لها أكبر من (3) درجات، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن البنوك التجارية في الجمهورية اليمنية تطبق وسائل وإجراءات حماية الأمن التنظيمي للأفراد المتعلقة بتلك الفقرات، بينما تم قبول وتعميم الفرضية العدمية الخامسة على مستوى (5) فقرات في ذلك البُعد والتي كانت قيم المتوسط الحسابي لها أصغر من (3) درجات، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن البنوك التجارية في الجمهورية اليمنية لا تطبق وسائل وإجراءات حماية الأمن التنظيمي للأفراد المتعلقة بتلك الفقرات.
- وبشكل عام فقد بلغت قيمة المتوسط الحسابي الإجمالي على مستوى البُعد المتعلق بحماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية لجميع الفقرات (3.154) درجة من أصل خمس درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي الفرضي المعياري لأداة القياس في هذه الدراسة وهي (3) درجات وفقاً لمقياس ليكرت

الخماسي، وبدلالة معنوية حيث بلغت قيمة مستوى الدلالة المحسوبة ($P=0.001$)، وهي أقل من مستوى قيمة الدلالة المعنوية المعتمد لهذه الدراسة ($\alpha=0.05$)، ويعني ذلك بشكل عام أن البنوك التجارية العاملة في الجمهورية اليمنية تطبق أساليب وإجراءات لحماية أمن الأفراد العاملين في نظم المعلومات المحاسبية المحسوبة وبدلالة معنوية إحصائياً، ويمكن تعميم هذه النتيجة على المجتمع الكلي للدراسة.

3-4-5-2: اختبار مدى تطبيق أساليب وإجراءات حماية الأمن المادي: كجزء من اختبار

الفرضية الخامسة التي تهدف إلى معرفة مدى تطبيق أساليب وإجراءات حماية أمن نظم المعلومات المحاسبية المحسوبة من قبل البنوك التجارية في الجمهورية اليمنية تم التحقق من مدى تطبيق البُعد الثاني من الأبعاد الخاصة بتلك الأساليب والإجراءات وهو ما يتعلق بحماية الأمن المادي لتلك النظم، وقد تم إجراء الاختبار الإحصائي لكل فقرة على حده من فقرات بُعد أساليب وإجراءات حماية الأمن المادي والواردة في قائمة الاستقصاء حيث كانت النتائج على النحو الآتي:

جدول رقم (3-4-6) نتيجة اختبار (T) لعينة الدراسة على مستوى الفقرات

المتعلقة بحماية الأمن المادي لنظم المعلومات المحاسبية المحسوبة (1)

رقم الفقرة	حماية الأمن المادي لنظم المعلومات المحاسبية	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفرق	نتيجة اختبار الفرضية
101	توجد خطة طوارئ معلنة وموثقة خاصة لمواجهة الكوارث تتضمن إعداد وحدة متكاملة من تجهيزات الحاسوب والشبكات، ونسخة احتياطية من قاعدة البيانات، في موقع آخر بديل غير الموقع الرئيسي لضمان استمرارية العمل، واستئناف النشاط بصورة سريعة.	2.664	- 4.980	0.000	معنوية	قبول
102	تتضمن خطة الطوارئ مصفوفة مخاطر أمن نظم المعلومات المحاسبية المتوقعة، والأثر الناتج، والجهة المتأثرة، والتصرف اللازم لمواجهتها.	2.508	-7.813	0.000	معنوية	قبول
103	يتعاقد البنك مع شركات تأمين متخصصة للتأمين على الأجهزة والبرمجيات وشبكات المعلومات والموظفين في نظام المعلومات المحاسبي المحسوب، ضد كافة المخاطر.	3.402	4.258	0.000	معنوية	رفض
104	يتم تصميم مواقع العمل وأماكن الأجهزة والمعدات، بصورة تتلاءم مع التغيرات الطبيعية، ويتم وضع أجهزة النظام في غرف محمية وآمنة، وعدم السماح بالدخول إليها لأي كان.	3.16	2.217	0.028	معنوية	رفض
105	يتم استخدام جميع الوسائل المادية التي تمنع الوصول غير المخول إلى نظم المعلومات المحاسبية وقواعد كرجال الحراسة، والأقفال والحواجز والغرف المحصنة وغيرها.	3.689	7.696	0.000	معنوية	رفض
106	يستخدم موظفي البنك بطاقات دخول إلكترونية ذكية مغلقة عليها صورهم الشخصية، للدخول إلى أماكن	2.107	-12.322	0.000	معنوية	قبول

(1) الجدول من إعداد الباحث اعتماداً على مخرجات برنامج SPSS.

رقم الفقرة	حماية الأمن المادي لتنظم المعلومات المحاسبية	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفرق	نتيجة اختبار الفرضية
	عملهم عبر البوابات المقفلة المبرمجة وفق الصلاحيات المخولة لهم، ويصدر إنذار مبكر فور الدخول المادي غير المخول.					
107	يقوم البنك بتثبيت كاميرات تلفزيونية على خارج مبنى دائرة النظام والممرات الداخلية فيها، وتعمل على مراقبة المستخدمين والأماكن التي توجد تجهيزات النظام، من موقع مركزي.	3.762	9.651	0.000	معنوية	رفض
108	يتم استخدام منظم كهربائي، وبطاريات إضافية، وخزانات طاقة، ومولد كهربائي لتجنب ارتفاع أو انخفاض الطاقة الكهربائية أو انقطاعها، وتعطلها بشكل مفاجئ، والذي يؤدي إلى تلف أجهزة وبرامج الحاسوب أو توقفها عن العمل.	4.123	16.649	0.000	معنوية	رفض
109	يتم تركيب أجهزة كشف الحريق في الأماكن المعرضة للخطر وتجهيزها بالشكل المناسب الذي يساعد على كشف الحريق بأسرع وقت ممكن وسرعة القيام بمقاومة الحريق.	4.164	17.059	0.000	معنوية	رفض
110	يتم استخدام أسقف وحوائط وأرضيات تمنع تسرب المياه، مع استخدام أغشية واقية من التربة والماء، وتركيب أجهزة إنذار من المياه والرطوبة.	3.525	5.232	0.000	معنوية	رفض
111	يتم إجراء صيانة دورية ومستمرة لأجهزة النظام ووسائل حمايته بما فيها أجهزة التكييف، لضمان استمرار عملها بفاعلية، ويتم توفير قطع ومعدات بديلة للأجهزة العاملة بشكل سريع فور تعطلها، بما يضمن سلامة الحواسيب وحمايتها.	3.656	7.612	0.000	معنوية	رفض
-101 111	المؤشرات العامة لتطبيق حماية الأمن المادي	3.342	6.607	0.000	معنوية	رفض

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS).
• مستوى الدلالة الإحصائية المعنوية المعيارية ($\alpha=0.05$)، عند مستوى الثقة 95 %، ومتوسط أداة القياس الافتراضي = (3)، ودرجة الحرية (df=121).

يتبين من الجدول السابق رقم (3-4-6) ما يلي:

- إنَّ قيم مستوى المعنوية المحسوبة لمعاملات (T) لجميع الفقرات تقل عن مستوى الدلالة المعنوية المعتمد في هذه الدراسة والبالغة ($\alpha=0.05$)، مما يدل على أن هناك فروقاً معنوية إحصائية بين المتوسط الحسابي لتلك الفقرات المتعلقة بحماية الأمن المادي لتنظم المعلومات المحاسبية، والمتوسط الفرضي المعياري لأداة القياس (3)، وبالتالي نستنتج أنَّ أفراد العينة كانوا موافقين أو رافضين لمضمون تلك الفقرات بشكل معنوي، عند مستوى ثقة (95%)، وعليه يمكن تعميم نتيجة تلك الفقرات على مجتمع الدراسة الكلي.
- تم رفض الفرضية العدمية الخامسة وقبول وتعميم الفرضية البديلة لها على مستوى (8) فقرات في ذلك البُعد والتي كانت قيم المتوسط الحسابي لها أصغر من (3) درجات، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن البنوك التجارية في الجمهورية اليمنية تطبق وسائل وإجراءات حماية الأمن المادي المتعلقة

بتلك الفقرات، بينما تم قبول وتعميم الفرضية العدمية الخامسة على مستوى (3) فقرات في ذلك البُعد والتي كانت قيم المتوسط الحسابي لها أصغر من (3) درجات، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن البنوك التجارية في الجمهورية اليمنية لا تطبق وسائل وإجراءات حماية الأمن المادي المتعلقة بتلك الفقرات.

وبشكل عام فقد بلغت قيمة المتوسط الحسابي الإجمالي على مستوى البُعد المتعلق بحماية الأمن المادي لنظم المعلومات المحاسبية المحوسبة لجميع الفقرات (3.342) درجة من أصل خمس درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي الفرضي المعياري لأداة القياس في هذه الدراسة وهي (3) درجات وفقاً لمقياس ليكرت الخماسي، وبدلالة معنوية حيث بلغت قيمة مستوى الدلالة المحسوبة ($P=0.000$)، وهي أقل من مستوى قيمة الدلالة المعنوية المعتمد لهذه الدراسة ($\alpha=0.05$)، ويعني ذلك بشكل عام أن البنوك التجارية العاملة في الجمهورية اليمنية تطبق أساليب وإجراءات لحماية الأمن المادي لنظم المعلومات المحاسبية المحوسبة وبدلالة معنوية إحصائية، ويمكن تعميم هذه النتيجة على المجتمع الكلي للدراسة.

3-5-4-3: اختبار مدى تطبيق أساليب وإجراءات حماية أمن الوصول البرمجي: كجزء

من اختبار الفرضية الخامسة التي تهدف إلى معرفة مدى تطبيق أساليب وإجراءات حماية أمن نظم المعلومات المحاسبية المحوسبة من قبل البنوك التجارية في الجمهورية اليمنية تم التحقق من مدى تطبيق البُعد الثالث من الأبعاد الخاصة بتلك الأساليب والإجراءات وهو ما يتعلق بحماية أمن الوصول البرمجي لقواعد بيانات تلك النظم، وقد تم إجراء الاختبار الإحصائي لكل فقرة على حدة من فقرات بُعد أساليب وإجراءات حماية أمن الوصول البرمجي والواردة في قائمة الاستقصاء حيث كانت النتائج على النحو الآتي:

جدول رقم (3-4-7) نتيجة اختبار (T) لعينة الدراسة على مستوى الفقرات

المتعلقة بحماية أمن الوصول البرمجي لقواعد بيانات نظم المعلومات المحاسبية المحوسبة⁽¹⁾

رقم الفقرة	حماية أمن الوصول البرمجي	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة الفرضية العدمية
112	يتم التحقق من هوية الشخص أو المعدات التي تحاول الدخول للنظام من خلال خليط من (كلمات مرور/ كروت ذكية/ معرفات بيولوجية/ أجهزة أخرى).	3.730	9.237	0.000	معنوية	رفض
113	يتم استخدام مستويات متتالية من الرقابة على دخول قاعدة البيانات بكلمات مرور متعددة ومختلفة للدخول إلى (الشبكة أو الحاسوب أو سيرفر "خادم" البيانات أو قاعدة البيانات)، ويتم التنبيه للموظفين بعدم إفشاء كلمات المرور لسرية، وتكون من الصعب تخمينها.	3.689	7.507	0.000	معنوية	رفض
114	يوجد سجل خاص لجميع الصلاحيات الممنوحة للموظفين المخولين بالدخول للنظام، ويتم برمجة مصفوفة الرقابة على الوصول آلياً، فيتم تحديد كلمة سر خاصة لكل موظف، والملفات أو البرامج التي يصرح له بالوصول إليها.	3.762	9.257	0.000	معنوية	رفض

(¹) الجدول من إعداد الباحث اعتماداً على مخرجات برنامج SPSS.

رقم الفقرة	حماية أمن الوصول البرمجي	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة الفرضية العدمية
115	يتم تغيير كلمات السر بشكل دوري ومستمر وخاصة بعد نقل الموظفين ويتم إلغاء كلمة السر الخاصة بالموظف الذي استقال أو أقيل من العمل بشكل فوري.	3.869	10.356	0.000	معنوية	رفض
116	يتم استخدام برامج الجدران النارية العازلة لمنع الوصول غير المصرح به إلى النظام، ومنع المستخدم من استخدام برامج أو ملفات لا يملك الصلاحية للدخول إليها، ويتم تحديث تلك البرامج وتعديلها باستمرار.	3.451	4.955	0.000	معنوية	رفض
117	يوثق النظام كافة محاولات الوصول غير المصرح بها، ويصدر تقرير حولها يتضمن وقت المحاولة والموقع الذي تمت من خلاله، ويتم معالجة ذلك بإغلاق الفجوات المكتشفة.	3.452	4.728	0.000	معنوية	رفض
118	يتم إجراء اختبار اختراق النظام بصورة دورية من قبل المراجعين الداخليين أو الخارجيين، أو بواسطة خبرات متخصصة لمعرفة نقاط الضعف في نظم المعلومات المحاسبية.	2.303	-10.600	0.000	معنوية	قبول
119	يحرص البنك على تحميل واستخدام برامج متطورة وأصلية وفعالة مضادة لفيروسات الحاسوب وبرمجياته الخبيثة، ويتم تحديثها بشكل دوري ومستمر.	3.189	2.406	0.018	معنوية	رفض
120	يتم استخدام وسيلة التشفير لكافة البيانات والمعلومات الهامة المحفوظة في قاعدة البيانات.	2.787	-2.722	0.007	معنوية	قبول
-112 120	المؤشرات العامة لتطبيق حماية أمن الوصول البرمجي	3.359	5.752	0.000	معنوية	رفض

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS).
• مستوى الدلالة الإحصائية المعنوية المعيارية ($\alpha=0.05$)، عند مستوى ثقة 95 %، ومتوسط أداة القياس الافتراضي = (3)، ودرجة الحرية (df=121).

يتبين من الجدول السابق رقم (3-4-7) ما يلي:

- إن قيم مستوى المعنوية المحسوبة لمعاملات (T) لجميع الفقرات تقل عن مستوى الدلالة المعنوية المعتمد في هذه الدراسة والبالغة ($\alpha=0.05$)، مما يدل على أن هناك فروقاً معنوية إحصائية بين المتوسط الحسابي لتلك الفقرات المتعلقة بحماية أمن الوصول البرمجي لقواعد بيانات نظم المعلومات المحاسبية، والمتوسط الفرضي المعياري لأداة القياس (3)، وبالتالي نستنتج أن أفراد العينة كانوا موافقين أو رافضين لمضمون تلك الفقرات بشكل معنوي، عند مستوى ثقة (95%)، وعليه يمكن تعميم نتيجة تلك الفقرات على مجتمع الدراسة.
- تم رفض الفرضية العدمية الخامسة وقبول وتعميم الفرضية البديلة لها على مستوى (7) فقرات في ذلك البُعد والتي كانت قيم المتوسط الحسابي لها أكبر من (3) درجات، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن البنوك التجارية في الجمهورية اليمنية تطبق وسائل وإجراءات حماية أمن الوصول البرمجي المتعلقة بتلك الفقرات، بينما تم قبول وتعميم الفرضية العدمية الخامسة لفقرتين في ذلك البُعد والتي كانت قيم المتوسط الحسابي لهما أصغر من (3) درجات، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن البنوك التجارية في الجمهورية اليمنية لا تطبق وسائل وإجراءات حماية أمن الوصول البرمجي المتعلقة بتلك الفقرتين.
- وبشكل عام فقد بلغت قيمة المتوسط الحسابي الإجمالي على مستوى البُعد المتعلق بحماية الأمن المادي لنظم المعلومات المحاسبية المحسوبة لجميع الفقرات (3.359) درجة من أصل خمس درجات، وهي قيمة أكبر من

قيمة المتوسط الحسابي الفرضي المعياري لأداة القياس في هذه الدراسة وهي (3) درجات وفقاً لمقياس ليكرت الخماسي، وبدلالة معنوية حيث بلغت قيمة مستوى الدلالة المحسوبة ($P=0.000$)، وهي أقل من مستوى قيمة الدلالة المعنوية المعتمد لهذه الدراسة ($\alpha=0.05$)، ويعني ذلك بشكل عام أن البنوك التجارية العاملة في الجمهورية اليمنية تطبق أساليب وإجراءات لحماية أمن الوصول البرمجي لنظم المعلومات المحاسبية المحسوبة وبدلالة معنوية إحصائياً، ويمكن تعميم هذه النتيجة على المجتمع الكلي للدراسة.

3-4-5: اختبار مدى تطبيق أساليب وإجراءات حماية أمن وسائط التخزين غير

المتصلة: كجزء من اختبار الفرضية الخامسة التي تهدف إلى معرفة مدى تطبيق أساليب وإجراءات حماية أمن نظم المعلومات المحاسبية المحسوبة من قبل البنوك التجارية في الجمهورية اليمنية تم التحقق من مدى تطبيق البُعد الرابع من الأبعاد الخاصة بتلك الأساليب والإجراءات وهو ما يتعلق بحماية أمن وسائط التخزين غير المتصلة بتلك النظم، وقد تم إجراء الاختبار الإحصائي لكل فقرة على حده من فقرات بُعد أساليب وإجراءات حماية أمن وسائط التخزين والواردة في قائمة الاستقصاء حيث كانت النتائج على النحو الآتي:

جدول رقم (3-4-8) نتيجة اختبار (T) لعينة الدراسة على مستوى الفقرات

المتعلقة بحماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية (1)

رقم الفقرة	حماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوبة	دلالة الفرق	نتيجة الفرضية العدمية
121	يقوم البنك بأخذ نسخ احتياطية للبرامج وملفات البيانات الهامة بشكل مستمر ودوري (يومي، أسبوعي، شهري)، وتحفظ في خزان حديدية مغلقة لحمايتها من السرقة أو الحريق، وتوضع نسخة منها في مكان آمن خارج مقر العمل.	4.344	21.531	0.000	معنوية	رفض
122	يتم تشفير النسخ الاحتياطية من قواعد البيانات لحمايتها من التعديل أو الوصول إليها بطريقة غير مشروعة وذلك لفرض الرقابة عليها.	2.459	-8.197	0.000	معنوية	قبول
123	توجد رقابة كافية على وسائط تخزين البيانات غير المتصلة بالنظام، ويتم فحص تلك الوسائط باستمرار للتأكد من صحتها وسلامتها.	3.238	2.977	0.004	معنوية	رفض
124	يتم التخلص من وسائط تخزين البيانات والبرامج بطريقة آمنة معينة وعدم رميها في براميل القمامة، حيث توجد إجراءات رقابية كافية لذلك.	3.607	6.294	0.000	معنوية	رفض
-121 124	المؤشرات العامة لتطبيق حماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية	3.412	7.252	0.000	معنوية	رفض

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS).
• مستوى الدلالة الإحصائية المعنوية المعيارية ($\alpha=0.05$)، عند مستوى الثقة 95 %، ومتوسط أداة القياس الافتراضي = (3)، ودرجة الحرية ($df=121$).

يتبين من الجدول السابق رقم (3-4-8) ما يلي:

- إنَّ قيم مستوى المعنوية المحسوبة لمعاملات (T) لجميع الفقرات تقل عن مستوى الدلالة المعنوية المعتمد في هذه الدراسة والبالغة ($\alpha=0.05$)، مما يدل على أن هناك فروقاً معنوية إحصائية بين المتوسط الحسابي لتلك

الفقرات المتعلقة بحماية أمن الوصول البرمجي لقواعد بيانات نظم المعلومات المحاسبية، والمتوسط الفرضي المعياري لأداة القياس (3)، وبالتالي نستنتج أن أفراد العينة كانوا موافقين أو رافضين لمضمون تلك الفقرات بشكل معنوي، عند مستوى ثقة (95%)، وعليه يمكن تعميم نتيجة تلك الفقرات على مجتمع الدراسة الكلي.

■ تم رفض الفرضية العدمية الخامسة وقبول وتعميم الفرضية البديلة لها على مستوى (3) فقرات في ذلك البُعد والتي كانت قيم المتوسط الحسابي لها أكبر من (3) درجات، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن البنوك التجارية في الجمهورية اليمنية تطبق وسائل وإجراءات حماية أمن الوصول البرمجي المتعلقة بتلك الفقرات، بينما تم قبول وتعميم الفرضية العدمية الخامسة لفقرة واحدة في ذلك البُعد والتي كانت قيمة المتوسط الحسابي لها أصغر من (3) درجات، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن البنوك التجارية في الجمهورية اليمنية لا تطبق وسائل وإجراءات حماية أمن الوصول البرمجي فيما يتعلق بتلك الفقرة.

■ وبشكل عام فقد بلغت قيمة المتوسط الحسابي الإجمالي على مستوى البُعد المتعلق بحماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية المحسوبة لجميع الفقرات (3.412) درجة من أصل خمس درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي الفرضي المعياري لأداة القياس في هذه الدراسة وهي (3) درجات وفقاً لمقياس ليكرت الخماسي، وبدلالة معنوية حيث بلغت قيمة مستوى الدلالة المحسوبة ($P=0.000$)، وهي أقل من مستوى قيمة الدلالة المعنوية المعتمد لهذه الدراسة ($\alpha=0.05$)، ويعني ذلك بشكل عام أن البنوك التجارية العاملة في الجمهورية اليمنية تطبق أساليب وإجراءات لحماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية المحسوبة وبدلالة معنوية إحصائية، ويمكن تعميم هذه النتيجة على المجتمع الكلي للدراسة.

3-4-5: تطبيق أساليب وإجراءات حماية أمن المدخلات: كجزء من اختبار الفرضية الخامسة

التي تهدف إلى معرفة مدى تطبيق أساليب وإجراءات حماية أمن نظم المعلومات المحاسبية المحسوبة من قبل البنوك التجارية في الجمهورية اليمنية تم التحقق من مدى تطبيق البُعد الخامس من الأبعاد الخاصة بتلك الأساليب والإجراءات وهو ما يتعلق بحماية أمن مدخلات تلك النظم، وقد تم إجراء الاختبار الإحصائي لكل فقرة على حده من فقرات بُعد أساليب وإجراءات حماية أمن المدخلات والواردة في قائمة الاستقصاء حيث كانت النتائج على النحو الآتي:

جدول رقم (3-4-9) نتيجة اختبار (T) لعينة الدراسة على مستوى الفقرات

المتعلقة بحماية أمن مدخلات نظم المعلومات المحاسبية المحسوبة (1)

رقم الفقرة	حماية أمن مدخلات نظم المعلومات المحاسبية المحسوبة	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة الفرضية العدمية
125	مستندات إدخال البيانات دقيقة وشاملة لمختلف العمليات، وتساعده على تقليل الأخطاء، ويتم إعدادها وتعبئتها ومصادقتها من الأشخاص المخولين فقط، ويوجد برنامج خاص مصمم لمعرفة من قام بإدخال البيانات.	3.566	7.014	0.000	معنوية	رفض
126	يتم تسجيل بيانات المدخلات أولاً بأول وتوجد رقابة كافية لاكتشاف أي نقص فيها، ويتم توثيق عمليات إدخال البيانات	3.369	5.766	0.000	معنوية	رفض

(1) الجدول من إعداد الباحث اعتماداً على مخرجات برنامج SPSS.

رقم الفقرة	حماية أمن مدخلات نظم المعلومات المحاسبية المحسوبة	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفرق	نتيجة الفرضية العدمية
	بما فيها المحاولات، والمخالفات الخاطئة، ومعرفة مصدرها.					
127	يتم تحديد أخطاء إدخال البيانات وتتبعها حتى يتم تصحيحها وتتضمن برامج النظام ضوابط تمنع إدخال بيانات خاطئة، حيث تظهر رسالة تحذيرية على الشاشة في حال وجود خطأ.	3.434	6.056	0.000	معنوية	رفض
128	توجد مراجعة تفصيلية للبيانات المدخلة للتأكد من دقتها واكتمالها، ويتم إجراء المراجعة الثانية لبيانات المستندات المدخلة للتأكد من سلامتها.	3.721	10.910	0.000	معنوية	رفض
129	تتوفر في نظم المعلومات المحاسبية خاصية تصحيح البيانات الخاطئة التي تم إدخالها في الوقت المناسب ضمن حدود الرقابة المسموح بها.	3.205	2.626	0.010	معنوية	رفض
-125 129	المؤشرات العامة لتطبيق حماية أمن المدخلات	3.459	8.658	0.000	معنوية	رفض

• الجدول من إعداد الباحث/ اعتماداً على نتائج التحليل الإحصائي (SPSS).
• مستوى الدلالة الإحصائية المعنوية المعيارية ($\alpha=0.05$)، عند مستوى الثقة 95 %، ومتوسط أداة القياس الافتراضي = (3)، ودرجة الحرية (df=121).

يتبين من الجدول السابق رقم (3-4-9) ما يلي:

- إنَّ قيم مستوى المعنوية المحسوبة لمعاملات (T) لجميع الفقرات تقل عن مستوى الدلالة المعنوية المعتمد في هذه الدراسة والبالغة ($\alpha=0.05$)، مما يدل على أن هناك فروقاً معنوية إحصائية بين المتوسط الحسابي لتلك الفقرات المتعلقة بحماية أمن مدخلات نظم المعلومات المحاسبية المحسوبة، والمتوسط الفرضي المعياري لأداة القياس (3)، وبالتالي نستنتج أنَّ أفراد العينة كانوا موافقين أو رافضين لمضمون تلك الفقرات بشكل معنوي، عند مستوى ثقة (95%)، وعليه يمكن تعميم نتيجة تلك الفقرات على مجتمع الدراسة الكلي.
- تم رفض الفرضية العدمية الخامسة وقبول وتعميم الفرضية البديلة لها على مستوى جميع الفقرات في ذلك البُعد والتي كانت قيم المتوسط الحسابي لها أكبر من (3) درجات، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن البنوك التجارية في الجمهورية اليمنية تطبق وسائل وإجراءات حماية أمن المدخلات المتعلقة بتلك الفقرات.
- وبشكل عام فقد بلغت قيمة المتوسط الحسابي الإجمالي على مستوى البُعد المتعلق بحماية أمن مدخلات نظم المعلومات المحاسبية المحسوبة لجميع الفقرات (3.459) درجة من أصل خمس درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي الفرضي المعياري لأداة القياس في هذه الدراسة وهي (3) درجات وفقاً لمقياس ليكرت الخماسي، وبدلالة معنوية حيث بلغت قيمة مستوى الدلالة المحسوبة ($P=0.000$)، وهي أقل من مستوى قيمة الدلالة المعنوية المعتمد لهذه الدراسة ($\alpha=0.05$)، ويعني ذلك بشكل عام أن البنوك التجارية العاملة في الجمهورية اليمنية تطبق أساليب وإجراءات لحماية أمن مدخلات نظم المعلومات المحاسبية المحسوبة وبدلالة معنوية إحصائية، ويمكن تعميم هذه النتيجة على المجتمع الكلي للدراسة.

3-4-5-6: اختبار مدى تطبيق أساليب وإجراءات حماية أمن عمليات التشغيل: كجزء من

اختبار الفرضية الخامسة التي تهدف إلى معرفة مدى تطبيق أساليب وإجراءات حماية أمن نظم المعلومات المحاسبية المحسوبة من قبل البنوك التجارية في الجمهورية اليمنية تم التحقق من مدى تطبيق البُعد السادس

من الأبعاد الخاصة بتلك الأساليب والإجراءات وهو ما يتعلق بحماية أمن عمليات تشغيل تلك النظم، وقد تم إجراء الاختبار الإحصائي لكل فقرة على حده من فقرات بُعد أساليب وإجراءات حماية أمن عمليات التشغيل الواردة في قائمة الاستقصاء حيث كانت النتائج على النحو الآتي:

جدول رقم (10-4-3) نتيجة اختبار (T) لعينة الدراسة على مستوى

الفقرات المتعلقة بحماية أمن عمليات التشغيل البرمجي لنظم المعلومات المحاسبية المحوسبة (1)

رقم الفقرة	حماية أمن عمليات التشغيل البرمجي لنظم المعلومات المحاسبية المحوسبة	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة الفرضية العدمية
130	يحتوي برنامج التشغيل على وسائل تحدد صلاحية المستخدمين في تشغيل وتحديث البيانات ومنع قراءتها أو نسخها أو تعديلها من غير المخول لهم ذلك.	3.812	11.116	0.000	معنوية	رفض
131	توجد رقابة آلية مدمجة داخل النظام، من خلا تقارير تحليلية الكترونية لتفاصيل العمليات التشغيلية، تحدد شخص المستخدم ووقت بداية ونهاية الاستخدام، ومكانه وطبيعة الاستخدام، والأخطاء المكتشفة آلياً، ويتم متابعة التقارير بشكل مستمر.	3.369	5.864	0.000	معنوية	رفض
132	توجد إجراءات كافية تضمن تصحيح الأخطاء، وإعادة تشغيل البيانات التي لم يتم تشغيلها بسبب توقف دورة التشغيل والتأكد من تمام معالجتها، ويتم تمييز العمليات التي تمت معالجتها لتتلافى تكرار تشغيلها.	3.418	6.467	0.000	معنوية	رفض
133	توجد إجراءات للتأكد من أن معالجة البيانات قد تمت بشكل كامل عند حد الانقطاع، من نقطة توقف معينة عند توقف دورة التشغيل لسبب من الأسباب.	3.451	5.767	0.000	معنوية	رفض
134	يتم توقيف عمل التطبيقات المحاسبية إجبارياً نهاية الدوام الرسمي، فلا يسمح بتشغيل النظام خارج فترة الدوام المحددة والمبرمجة آلياً، بحيث يتعذر تشغيله النظام خلاف ذلك.	2.393	- 9.133	0.000	معنوية	قبول
-130 134	المؤشرات العامة لتطبيق حماية أمن عمليات التشغيل	3.284	5.802	0.000	معنوية	رفض

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS).
• مستوى الدلالة الإحصائية المعنوية المعيارية ($\alpha=0.05$)، عند مستوى الثقة 95 %، ومتوسط أداة القياس الافتراضي = (3)، ودرجة الحرية (df=121).

يتبين من الجدول السابق رقم (10-4-3) ما يلي:

- إن قيم مستوى المعنوية المحسوبة لمعاملات (T) لجميع الفقرات تقل عن مستوى الدلالة المعنوية المعتمد في هذه الدراسة والبالغة ($\alpha=0.05$)، مما يدل على أن هناك فروقاً معنوية إحصائية بين المتوسط الحسابي لتلك الفقرات المتعلقة بحماية أمن عمليات التشغيل البرمجي لنظم المعلومات المحاسبية المحوسبة، والمتوسط الفرضي المعياري لأداة القياس (3)، وبالتالي نستنتج أن أفراد العينة كانوا موافقين أو رافضين لمضمون تلك الفقرات بشكل معنوي، عند مستوى ثقة (95%)، وعليه يمكن تعميم نتيجة تلك الفقرات على مجتمع الدراسة الكلي.
- تم رفض الفرضية العدمية الخامسة وقبول وتعميم الفرضية البديلة لها على مستوى (4) فقرات في ذلك البُعد والتي كانت قيم المتوسط الحسابي لها أكبر من (3) درجات، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن

(1) الجدول من إعداد الباحث اعتماداً على مخرجات برنامج SPSS.

البنوك التجارية في الجمهورية اليمنية تطبق وسائل وإجراءات حماية أمن التشغيل البرمجي المتعلقة بتلك الفقرات، بينما تم قبول وتعميم الفرضية العدمية الخامسة لفقرة واحدة في ذلك البُعد والتي كانت قيمة المتوسط الحسابي لها أصغر من (3) درجات، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن البنوك التجارية في الجمهورية اليمنية لا تطبق وسائل وإجراءات حماية أمن التشغيل البرمجي فيما يتعلق بتلك الفقرة.

وبشكل عام فقد بلغت قيمة المتوسط الحسابي الإجمالي على مستوى البُعد المتعلق بحماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية المحوسبة لجميع الفقرات (3.284) درجة من أصل خمس درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي الفرضي المعياري لأداة القياس في هذه الدراسة وهي (3) درجات وفقاً لمقياس ليكرت الخماسي، وبدلالة معنوية حيث بلغت قيمة مستوى الدلالة المحسوبة ($P=0.000$)، وهي أقل من مستوى قيمة الدلالة المعنوية المعتمد لهذه الدراسة ($\alpha=0.05$)، ويعني ذلك بشكل عام أن البنوك التجارية العاملة في الجمهورية اليمنية تطبق أساليب وإجراءات لحماية أمن عمليات التشغيل البرمجي لنظم المعلومات المحاسبية المحوسبة وبدلالة معنوية إحصائية، ويمكن تعميم هذه النتيجة على المجتمع الكلي للدراسة.

3-4-5-7: اختبار مدى تطبيق أساليب وإجراءات حماية أمن المخرجات: كجزء من اختبار

الفرضية الخامسة التي تهدف إلى معرفة مدى تطبيق أساليب وإجراءات حماية أمن نظم المعلومات المحاسبية المحوسبة من قبل البنوك التجارية في الجمهورية اليمنية تم التحقق من مدى تطبيق البُعد السابع من الأبعاد الخاصة بتلك الأساليب والإجراءات وهو ما يتعلق بحماية أمن مخرجات تلك النظم، وقد تم إجراء الاختبار الإحصائي لكل فقرة على حده من فقرات بُعد أساليب وإجراءات حماية أمن المخرجات والواردة في قائمة الاستقصاء حيث كانت النتائج على النحو الآتي:

جدول رقم (3-4-11) نتيجة اختبار (T) لعينة الدراسة على مستوى

الفقرات المتعلقة بحماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة (1)

رقم الفقرة	حماية أمن مخرجات نظم المعلومات المحاسبية	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة الفرضية العدمية
135	يتم حصر أنواع المعلومات وتصنيفها إلى فئات وفقاً لدرجة أهميتها وسريتها، وتحديد مستوى الحماية الواجب توفيره لكل فئة منها.	2.836	-2.556	0.012	معنوية	قبول
136	توجد وسائل وإجراءات كافية لعملية توزيع المخرجات، لضمان وصول التقارير والوثائق للجهات المعنية المخولة فقط باستلامها.	2.779	-3.561	0.001	معنوية	قبول
137	يتم إجراء صيانة دائمة لوسائط الإخراج (طابعات، فاكسات، شاشات... الخ)، لضمان سلامة عرض المخرجات.	3.566	7.590	0.000	معنوية	رفض
138	يتم إعداد نسخ مطبوعة لبعض المعلومات المحاسبية الهامة، وتشفير المعلومات الحساسة.	3.393	4.619	0.000	معنوية	رفض
139	يتم النظام مسار معين لمراجعة وتتبع سير المعاملات من مرحلة المدخلات إلى مرحلة المخرجات، والعكس.	3.230	3.050	0.003	معنوية	رفض
140	يقوم البنك بإتلاف المخرجات المهمة والسرية بعد الانتهاء من	3.303	3.765	0.000	معنوية	رفض

(1) الجدول من إعداد الباحث اعتماداً على مخرجات برنامج SPSS.

رقم الفقرة	حماية أمن مخرجات نظم المعلومات المحاسبية	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة الفرضية العدمية
	استخدامها بواسطة لجنة متخصصة ومخولة بذلك، ويتم الإتلاف داخل البنك.					
135-140	المؤشرات العامة لتطبيق حماية أمن المخرجات	3.184	3.449	0.001	معنوية	رفض

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS).
• مستوى الدلالة الإحصائية المعنوية المعيارية ($\alpha=0.05$)، عند مستوى الثقة 95 %، ومتوسط أداة القياس الإحصائي = (3)، ودرجة الحرية (df=121).

يتبين من الجدول السابق رقم (3-4-11) ما يلي:

- إن قيم مستوى المعنوية المحسوبة لمعاملات (T) لجميع الفقرات تقل عن مستوى الدلالة المعنوية المعتمد في هذه الدراسة والبالغة ($\alpha=0.05$)، مما يدل على أن هناك فروقاً معنوية إحصائية بين المتوسط الحسابي لتلك الفقرات المتعلقة بحماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة، والمتوسط الفرضي المعياري لأداة القياس (3)، وبالتالي نستنتج أن أفراد العينة كانوا موافقين أو رافضين لمضمون تلك الفقرات بشكل معنوي، عند مستوى ثقة (95%)، وعليه يمكن تعميم نتيجة تلك الفقرات على مجتمع الدراسة الكلي.
- تم رفض الفرضية العدمية الخامسة وقبول وتعميم الفرضية البديلة لها على مستوى (4) فقرات في ذلك البُعد والتي كانت قيم المتوسط الحسابي لها أكبر من (3) درجات، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن البنوك التجارية في الجمهورية اليمنية تطبق وسائل وإجراءات حماية أمن المخرجات المتعلقة بتلك الفقرات، بينما تم قبول وتعميم الفرضية العدمية الخامسة لفقرتين في ذلك البُعد والتي كانت قيم المتوسط الحسابي لهما أصغر من (3) درجات، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن البنوك التجارية في الجمهورية اليمنية لا تطبق وسائل وإجراءات حماية أمن المخرجات المتعلقة بتلك الفقرتين.
- وبشكل عام فقد بلغت قيمة المتوسط الحسابي الإجمالي على مستوى البُعد المتعلق بحماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة لجميع الفقرات (3.184) درجة من أصل خمس درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي الفرضي المعياري لأداة القياس في هذه الدراسة وهي (3) درجات وفقاً لمقياس ليكرت الخماسي، وبدلالة معنوية حيث بلغت قيمة مستوى الدلالة المحسوبة ($P=0.001$)، وهي أقل من مستوى قيمة الدلالة المعنوية المعتمد لهذه الدراسة ($\alpha=0.05$)، ويعني ذلك بشكل عام أن البنوك التجارية العاملة في الجمهورية اليمنية تطبق أساليب وإجراءات لحماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة وبدلالة معنوية إحصائية، ويمكن تعميم هذه النتيجة على المجتمع الكلي للدراسة.

3-4-5-8: اختبار مدى تطبيق أساليب وإجراءات حماية أمن البيانات المنقولة عبر

شبكات نظم المعلومات المحاسبية: كجزء من اختبار الفرضية الخامسة التي تهدف إلى معرفة مدى

تطبيق أساليب وإجراءات حماية أمن نظم المعلومات المحاسبية المحوسبة من قبل البنوك التجارية في الجمهورية اليمنية تم التحقق من مدى تطبيق البُعد السابع من الأبعاد الخاصة بتلك الأساليب والإجراءات وهو ما يتعلق بحماية أمن البيانات المنقولة عبر شبكات تلك النظم، وقد تم إجراء الاختبار الإحصائي لكل

فقرة على حده من فقرات بُعد أساليب وإجراءات حماية أمن البيانات المنقولة عبر الشبكات والواردة في قائمة الاستقصاء حيث كانت النتائج على النحو الآتي:

جدول رقم (12-4-3) نتيجة اختبار (T) لعينة الدراسة على مستوى الفقرات المتعلقة

بحماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية المحوسبة⁽¹⁾

رقم الفقرة	بحماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفرق	نتيجة الفرضية العدمية
141	تستخدم برامج الجدران النارية لتحديد المعلومات التي يسمح بدخولها أو خروجها من وإلى نظام المعلومات المحاسبي المحسوب للبنك.	3.557	6.908	0.000	معنوية	رفض
142	يتم تشفير البيانات المرسلة عبر الشبكات للتأكد من أنه لم يتم الكشف عنها أو تعديلها وأنها مرسلة من الجهة المعنية، وتتوفر وسائل حماية كافية للحفاظ على سرية مفتاح التشفير.	3.196	3.275	0.001	معنوية	رفض
143	يستخدم البنك التوقيع الرقمي الإلكتروني، كوسيلة للتحقق من موثوقية المستخدمين بشكل غير قابل للتزيف، ولضمان عدم إنكار الأطراف المعنية المشاركة في الوثائق الإلكترونية.	2.680	-4.383	0.000	معنوية	قبول
144	يتم استخدام شهادة رقمية صادرة من جهات فنية معتمدة، عند إرسال أو استلام البيانات عبر الشبكة الخارجية، للتحقق من هوية مرسل الرسائل، وموثوقية المستخدم.	2.459	-11.224	0.000	معنوية	قبول
145	يتم استخدام بروتوكولات أمنية بين البنك والأطراف المتعاملة للحفاظ على سرية المعلومات المحاسبية والتحقق من وصولها للجهة المطلوبة أثناء إجراء المعاملات المالية.	3.279	4.282	0.000	معنوية	رفض
-141 145	المؤشرات العامة لتطبيق حماية أمن البيانات المنقولة عبر الشبكات	3.034	0.750	0.455	غير معنوية	قبول ولا يمكن تعميمها

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS).
• مستوى الدلالة الإحصائية المعنوية المعيارية ($\alpha=0.05$)، عند مستوى الثقة 95 %، ومتوسط أداة القياس الافتراضي = (3)، ودرجة الحرية (df=121).

يتبين من الجدول السابق رقم (12-4-3) ما يلي:

■ إنَّ قيم مستوى المعنوية المحسوبة لمعاملات (T) لجميع الفقرات تقل عن مستوى الدلالة المعنوية المعتمد في هذه الدراسة والبالغة ($\alpha=0.05$)، مما يدل على أن هناك فروقاً معنوية إحصائية بين المتوسط الحسابي لتلك الفقرات المتعلقة بحماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية المحوسبة، والمتوسط الفرضي المعياري لأداة القياس (3)، وبالتالي نستنتج أنَّ أفراد العينة كانوا موافقين أو رافضين لمضمون تلك الفقرات بشكل معنوي، عند مستوى ثقة (95%)، وعليه يمكن تعميم نتيجة تلك الفقرات على مجتمع الدراسة الكلي.

■ تم رفض الفرضية العدمية الخامسة وقبول وتعميم الفرضية البديلة لها على مستوى (3) فقرات في ذلك البُعد والتي كانت قيم المتوسط الحسابي لها أكبر من (3) درجات، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن

(1) الجدول من إعداد الباحث اعتماداً على مخرجات برنامج SPSS.

البنوك التجارية في الجمهورية اليمنية تطبق وسائل وإجراءات حماية أمن البيانات المنقولة عبر الشبكات والمتعلقة بتلك الفقرات، بينما تم قبول وتعميم الفرضية العدمية الخامسة لفقرتين في ذلك البُعد والتي كانت قيم المتوسط الحسابي لهما أصغر من (3) درجات، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن البنوك التجارية في الجمهورية اليمنية لا تطبق وسائل وإجراءات حماية أمن البيانات المنقولة عبر الشبكات المتعلقة بتلك الفقرتين.

■ وبشكل عام فقد بلغت قيمة المتوسط الحسابي الإجمالي على مستوى البُعد المتعلق بحماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية المحوسبة لجميع الفقرات (3.034) درجة من أصل خمس درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي الفرضي المعياري لأداة القياس في هذه الدراسة وهي (3) درجات وفقاً لمقياس ليكرت الخماسي، وبدلالة غير معنوية حيث بلغت قيمة مستوى الدلالة المحسوبة ($P=0.455$)، وهي أكبر من مستوى قيمة الدلالة المعنوية المعتمد لهذه الدراسة ($\alpha=0.05$)، ويعني ذلك بشكل عام أن البنوك التجارية العاملة في الجمهورية اليمنية تطبق أساليب وإجراءات لحماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية المحوسبة ولكن بدلالة غير معنوية إحصائياً، ولا يمكن تعميم هذه النتيجة على المجتمع الكلي للدراسة.

9-5-4-3: تطبيق أساليب وإجراءات حماية أمن تعديل وتطوير نظم المعلومات:

كجزء من اختبار الفرضية الخامسة التي تهدف إلى معرفة مدى تطبيق أساليب وإجراءات حماية أمن نظم المعلومات المحاسبية المحوسبة من قبل البنوك التجارية في الجمهورية اليمنية تم التحقق من مدى تطبيق البُعد التاسع من الأبعاد الخاصة بتلك الأساليب والإجراءات وهو ما يتعلق بحماية أمن تعديل وتطوير تلك النظم، وقد تم إجراء الاختبار الإحصائي لكل فقرة على حده من فقرات بُعد أساليب وإجراءات حماية أمن التعديل والتطوير والواردة في قائمة الاستقصاء حيث كانت النتائج على النحو الآتي:

جدول رقم (3-4-13) نتيجة اختبار (T) لعينة الدراسة على مستوى الفقرات

المتعلقة بحماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة⁽¹⁾

رقم الفقرة	حماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة الفرضية العدمية
146	توجد إجراءات كافية وفعالة لرقابة عمليات تطوير البرامج والتطبيقات المحاسبية، وفق معايير وإجراءات واضحة ومكتوبة ومحددة.	3.246	2.841	0.005	معنوية	رفض
147	لا تتم أية تعديلات في برمج النظام بدون حصول المبرمجين المختصين على موافقات رسمية من الإدارات المعنية المخولة.	3.533	5.279	0.000	معنوية	رفض
148	هناك فريق متخصص لتعديل وتطوير نظم المعلومات المحاسبية من داخل البنك، وتشرف إدارة البنك على تعديل وتطوير النظام.	3.795	10.947	0.000	معنوية	رفض

(1) الجدول من إعداد الباحث اعتماداً على مخرجات برنامج SPSS.

رقم الفقرة	حماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة الفرضية العدمية
149	يتم إجراء الاختبار المبدئي بالتشغيل التجريبي للبرامج الجديدة وتعديلاتها قبل اعتمادها بشكل نهائي للتأكد من سلامتها، وقدرتها على تتبع الأخطاء التي قد تحدث أثناء التنفيذ.	3.615	6.908	0.000	معنوية	رفض
150	يتم توثيق كافة التعديلات التي تتم على البرامج والمعدات، وفق الإجراءات المتبعة.	3.525	5.581	0.000	معنوية	رفض
-146 150	المؤشرات العامة لتطبيق حماية أمن التعديل والتطوير	3.543	7.315	0.000	معنوية	رفض

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS).
• مستوى الدلالة الإحصائية المعنوية المعيارية ($\alpha=0.05$)، عند مستوى الثقة 95 %، ومتوسط أداة القياس الافتراضي = (3)، ودرجة الحرية (df=121).

يتبين من الجدول السابق رقم (3-4-13) ما يلي:

- إن قيم مستوى المعنوية المحسوبة لمعاملات (T) لجميع الفقرات تقل عن مستوى الدلالة المعنوية المعتمد في هذه الدراسة والبالغة ($\alpha=0.05$)، مما يدل على أن هناك فروقاً معنوية إحصائية بين المتوسط الحسابي لتلك الفقرات المتعلقة بحماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة، والمتوسط الفرضي المعياري لأداة القياس (3)، وبالتالي نستنتج أن أفراد العينة كانوا موافقين أو رافضين لمضمون تلك الفقرات بشكل معنوي، عند مستوى ثقة (95%)، وعليه يمكن تعميم نتيجة تلك الفقرات على مجتمع الدراسة الكلي.
- تم رفض الفرضية العدمية الخامسة وقبول وتعميم الفرضية البديلة لها على مستوى جميع الفقرات في ذلك البُعد والتي كانت قيم المتوسط الحسابي لها أكبر من (3) درجات، والفرق معنوي وله دلالة إحصائية، وذلك يعني أن البنوك التجارية في الجمهورية اليمنية تطبق وسائل وإجراءات حماية أمن التعديل والتطوير المتعلقة بجميع تلك الفقرات.
- وبشكل عام فقد بلغت قيمة المتوسط الحسابي الإجمالي على مستوى البُعد المتعلق بحماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة لجميع الفقرات (3.543) درجة من أصل خمس درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي الفرضي المعياري لأداة القياس في هذه الدراسة وهي (3) درجات وفقاً لمقياس ليكرت الخماسي، وبدلالة معنوية حيث بلغت قيمة مستوى الدلالة المحسوبة ($P=0.000$)، وهي أقل من مستوى قيمة الدلالة المعنوية المعتمد لهذه الدراسة ($\alpha=0.05$)، ويعني ذلك بشكل عام أن البنوك التجارية العاملة في الجمهورية اليمنية تطبق أساليب وإجراءات لحماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة وبدلالة معنوية إحصائية، ويمكن تعميم هذه النتيجة على المجتمع الكلي للدراسة.

3-4-5-10: مدى تطبيق أساليب وإجراءات حماية أمن نظم المعلومات المحاسبية المحوسبة ككل:

لاختبار الفرضية الخامسة يمكن تلخيص ما سبق من نتائج فرعية خاصة بها كما هو مبين في الجدول الآتي:

جدول رقم (3-4-14) نتيجة اختبار (T) لعينة الدراسة على مستوى

الأبعاد المتعلقة بأساليب وإجراءات حماية أمن نظم المعلومات المحاسبية المحوسبة⁽¹⁾

رقم الفقرات	الأبعاد الرئيسية لأساليب وإجراءات حماية أمن نظم المعلومات المحاسبية	المتوسط الحسابي	قيمة (T) المحسوبة	مستوى الدلالة المحسوب	دلالة الفروق	نتيجة اختبار الفرضية
100-91	حماية الامن التنظيمي للأفراد.	3.154	3.290	0.001	معنوية	رفض
-100 111	حماية أمن الوصول المادي.	3.342	6.607	0.000	معنوية	رفض
-112 120	حماية أمن الوصول البرمجي.	3.359	5.752	0.000	معنوية	رفض
-121 124	حماية أمن وسائط التخزين غير المتصلة بالنظم.	3.412	7.252	0.000	معنوية	رفض
-125 129	حماية أمن مدخلات النظم.	3.459	8.658	0.000	معنوية	رفض
-130 134	حماية أمن عمليات التشغيل.	3.284	5.802	0.000	معنوية	رفض
-135 140	حماية أمن المخرجات.	3.184	3.449	0.001	معنوية	رفض
-141 145	حماية أمن تبادل البيانات المنقولة عبر الشبكات.	3.034	0.750	0.455	غير معنوية	رفض ولا يمكن تعميمها
-146 150	حماية أمن التعديل والتطوير.	3.543	7.315	0.000	معنوية	رفض
150-91	المؤشرات العامة لتطبيق إجراءات الحماية ككل	3.349	6.971	0.000	معنوية	رفض

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS).
• مستوى الدلالة الإحصائية المعنوية المعيارية ($\alpha=0.05$)، عند مستوى الثقة 95 %، ومتوسط أداة القياس الافتراضي = (3)، ودرجة الحرية (df=121).

يتبين من الجدول السابق (3-4-14) ما يلي:

- إن قيم مستوى المعنوية المحسوبة لمعاملات (T) لمعظم الأبعاد المتعلقة بتطبيق إجراءات الحماية كانت أقل من مستوى الدلالة المعنوية المعتمد في هذه الدراسة والبالغة ($\alpha=0.05$)، مما يدل على أن هناك فروقاً معنوية إحصائية بين المتوسط الحسابي لتلك الأبعاد المتعلقة بإجراءات الحماية، والمتوسط الفرضي المعياري لأداة القياس (3)، وبالتالي نستنتج أن أفراد العينة كانوا موافقين أو رافضين لمضمون تلك الأبعاد بشكل معنوي، عند مستوى ثقة (95%)، وعليه يمكن تعميم النتيجة على مجتمع الدراسة الكلي على مستوى جميع أبعاد المحور الخاص بإجراءات الحماية باستثناء البعد المتعلق بحماية أمن تبادل البيانات المنقولة عبر الشبكات فلا يمكن تعميم نتيجته، حيث كان الفرق غير معنوي ناتجاً عن الحظ والصدفة.

(1) الجدول من إعداد الباحث اعتماداً على مخرجات برنامج SPSS.

- تم رفض الفرضية العدمية الخامسة وقبول وتعميم الفرضية البديلة لها على مستوى جميع الأبعاد التي كانت قيم المتوسط الحسابي لها أكبر من (3)، والفرق معنوي وله دلالة إحصائية.
- بلغت قيمة المتوسط الحسابي الإجمالي على مستوى محور أساليب وإجراءات الحماية لجميع الأبعاد (3.349) درجة من أصل خمس درجات، وهي قيمة أكبر من قيمة المتوسط الحسابي الفرضي المعياري لأداة القياس في هذه الدراسة وهي (3) درجات وفقاً لمقياس ليكرت الخماسي، وبدلالة معنوية حيث بلغت قيمة مستوى الدلالة المحسوبة ($P=0.000$)، وهي أقل من مستوى قيمة الدلالة المعنوية المعتمد لهذه الدراسة ($\alpha=0.05$)، ويعني ذلك بشكل عام أن البنوك التجارية في الجمهورية اليمنية تطبق أساليب وإجراءات كافية لحماية أمن نظم المعلومات المحاسبية المحوسبة وبدلالة معنوية إحصائية، ويمكن تعميم هذه النتيجة على المجتمع الكلي للدراسة.
- وبشكل عام ومن خلال ما سبق من تحليل ودلائل إحصائية فقد تمّ رفض الفرضية العدمية الخامسة التي تنص على أنه: "لا تطبق البنوك التجارية في الجمهورية اليمنية أساليب وإجراءات كافية وفعّالة لحماية أمن نظم المعلومات المحاسبية المحوسبة من المخاطر التي تتهددها وفق القواعد المحلية والأسس والمعايير الدولية"، وتم قبول الفرضية البديلة لها القائلة: "تطبق البنوك التجارية في الجمهورية اليمنية أساليب وإجراءات كافية وفعّالة لحماية أمن نظم المعلومات المحاسبية المحوسبة من المخاطر التي تتهددها وفق القواعد المحلية والأسس والمعايير الدولية".
- ويستنتج الباحث أنه على الرغم من تطبيق البنوك التجارية في الجمهورية اليمنية أساليب وإجراءات كافية وفعّالة لحماية أمن نظم المعلومات المحاسبية المحوسبة من المخاطر التي تتهددها إلا أنها تحتاج إلى تطوير وتحديث، لكي تتلاءم وتتناسب مع حجم المخاطر حسب نتائج تحليل البيانات في هذه الدراسة، وذلك لحماية نظم المعلومات المحاسبية المحوسبة بتلك البنوك بشكل تفصيلي.

3-4-6: نتيجة اختبار الفرضية السادسة:

تنص الفرضية العدمية السادسة (H^0-6) على أنه: "لا تؤثر أساليب وإجراءات الحماية المطبقة في البنوك التجارية في الجمهورية اليمنية على المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى تلك البنوك"، وتنص الفرضية البديلة لها (H^1-6) على أنه: "تؤثر أساليب وإجراءات الحماية المطبقة في البنوك التجارية في الجمهورية اليمنية على المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى تلك البنوك"، وتهدف هذه الفرضية إلى معرفة مدى تأثير أساليب وإجراءات الحماية المطبقة في البنوك التجارية في الجمهورية اليمنية على مخاطر أمن نظم المعلومات المحاسبية المحوسبة في تلك البنوك، وقد لجأ الباحث إلى استخدام اختبار (T)، حيث تم الاعتماد على مستوى الدلالة الإحصائية المعنوية ($\alpha=0.05$) كأساس لقبول الفرضية العدمية أو رفضها (وفق قاعدة القرار المبينة سابقاً)⁽¹⁾، وقد قام الباحث بإجراء الاختبار الإحصائي وقد كانت النتائج كما في الجدول الآتي:

(1) بالعودة إلى آنية وإجراءات تحليل ومعالجة البيانات في المبحث الأول من هذا الفصل.

جدول رقم (3-4-15) نتائج اختبار تحليل الانحدار البسيط لبيان مدى تأثير أساليب وإجراءات الحماية المطبقة في البنوك التجارية في الجمهورية اليمنية على المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة

الفقرات	قيمة (T) المحسوبة	معامل الانحدار (B)	معامل التأثير المعياري (Beta)	معامل ارتباط بيرسون (r)	معامل التحديد (R ²)	احتمال الدلالة المحسوب (P)	نتيجة اختبار الفرضية العدمية
(150-91)	6.298	-0.373	0.498	-0.498	0.248	0.000	رفض

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS)، وقيمة (T) الجدولية (1.96) عند درجة حرية (df = 121).

ويتضح من الجدول السابق أن قيمة (T) المحسوبة (6.298) أكبر من قيمة (T) الجدولية (1.96)، وبدلالة معنوية إحصائية حيث بلغ احتمال الدلالة المحسوب (P=0,000) وهو أقل من مستوى الدلالة المعنوية المعياري ($\alpha=0,05$)، وعليه فإنه يمكن القول بأن أساليب وإجراءات الحماية المطبقة في البنوك التجارية في الجمهورية اليمنية تؤثر على المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى تلك البنوك تأثيراً عكسياً ومباشراً وبشكل إيجابي (أي أن العلاقة عكسية فكلما زادت وسائل الحماية المطبقة انخفضت مخاطر أمن نظم المعلومات المحاسبية المحوسبة) وبدلالة معنوية إحصائية وقوة التأثير قوية نسبياً كون قيمة معامل التأثير المعياري (Beta) قد بلغت (0.498) وهي قيمة دالة إحصائية، وما يعزز هذه النتيجة حصول معامل ارتباط بيرسون (r) بين المتغيرين على نفس القيمة حيث بلغ (0.498)، كما أن قيمة معامل التحديد (R²) قد بلغت (0.248) وهي قيمة دالة إحصائية، وهذا يعني أن أساليب وإجراءات الحماية المطبقة تسهم في تفسير ما نسبته (24.8 %) من التباين أو التغير الحاصل في سلوك (مخاطر أمن نظم المعلومات المحاسبية المحوسبة) إذا أخذت بصورة منفصلة أو منفردة وكحزمة واحدة، وتلك قوة تفسيرية متوسطة نسبياً، وقد يعود ذلك لاستخدام البنوك مجموعة غير متكاملة من أساليب الحماية والتي تحتاج فعلاً إلى تطوير وتحديث وهذه النتيجة تعزز نتيجة اختبار الفرضية الخامسة.

ومن خلال ما سبق من تحليل يستدعي رفض الفرضية العدمية السادسة وقبول الفرضية البديلة القائلة بأنه: "تؤثر أساليب وإجراءات الحماية المطبقة في البنوك التجارية في الجمهورية اليمنية على المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى تلك البنوك".

3-4-7: نتيجة اختبار الفرضية السابعة:

تنص الفرضية العدمية السابعة (H^0-7) على أنه "لا توجد فروق جوهرية بين آراء أفراد عينة الدراسة فيما يتعلق بالمخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية تُعزى للمسمى الوظيفي لهم"، ولاختبار هذه الفرضية استخدم الباحث اختبار تحليل التباين الأحادي (One- Way ANOVA)، لمعرفة ما إذا كان هناك فروق ذات دلالة إحصائية عند مستوى دلالة معنوية (0.05) تعزى للمسمى الوظيفي لأفراد عينة الدراسة حول آرائهم نحو مخاطر أمن نظم المعلومات المحاسبية المحوسبة، والجدول رقم (3-5-16) يوضح ذلك.

جدول رقم (3-4-16) نتائج اختبار تحليل التباين الأحادي (ANOVA)

للفروق بين إجابات أفراد العينة حول مخاطر أمن نظم المعلومات المحاسبية المحوسبة حسب المسمى الوظيفي

م	المسمى الوظيفي	العدد	المتوسط الحسابي	قيمة (F) المحسوبة	مستوى دلالة (F) المحسوبة	نتيجة اختبار الفرضية
1	مدير مالي.	6	2.355	0.968	0.465	قبول (لا يوجد فروق)
2	رئيس قسم حسابات	14	2.361			
3	مدقق داخلي	25	2.403			
4	مدير إدارة مخاطر	7	2.420			
5	رئيس قسم حاسوب	10	2.259			
6	مبرمج نظام	15	2.312			
7	مشغل نظام	9	2.558			
8	مدقق خارجي	29	2.555			
9	مفتش بنك أو مراقب عام	7	2.554			
	الإجمالي	122	2.430			

الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS)، وقيمة (F) الجدولية (2.18) عند درجات حرية (8، 121). (df=121, 8).

يُظهر الجدول السابق عدم وجود فروق ذات دلالة إحصائية بين آراء أفراد العينة تعزى لمتغير المسمى الوظيفي حيث بلغت قيمة (F) المحسوبة (0.968) وهي أصغر من قيمة (F) الجدولية البالغة (2.18) وبدلالة إحصائية (0.348) وهي قيمة غير دالة إحصائياً لأنها أكبر من مستوى الدلالة المعنوية (0.05)، وربما يعود ذلك إلى التقارب الواضح في قيم المتوسطات الحسابية لاستجابة الأفراد المجيبين على أسئلة الاستقصاء، ويعزو الباحث ذلك إلى أن أفراد عينة الدراسة مهما اختلفت مسمياتهم الوظيفية، فإن لديهم رؤية متشابهة نحو مخاطر أمن نظم المعلومات المحاسبية المحوسبة وفقاً لمسمياتهم الوظيفية.

وعليه يتم قبول الفرضية العدمية القائلة: " لا توجد فروق جوهرية بين آراء أفراد عينة الدراسة فيما يتعلق بالمخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية تُعزى للمسمى الوظيفي لهم".

3-4-8: نتيجة اختبار الفرضية الثامنة:

تنص الفرضية العدمية الثامنة (H^0-8) على أنه " لا يوجد اختلاف جوهري بين البنوك التجارية في الجمهورية اليمنية فيما يتعلق بحجم المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة يُعزى لملكية تلك البنوك"، واختبار هذه الفرضية استخدم الباحث اختبار تحليل التباين الأحادي (One-Way ANOVA)، لمعرفة ما إذا كان هناك فروق ذات دلالة إحصائية عند مستوى دلالة معنوية (0.05) لأفراد عينة الدراسة حول آرائهم نحو مخاطر أمن نظم المعلومات المحاسبية المحوسبة، تعزى لملكية البنوك التي ينتمون لها، والجدول الآتي يوضح ذلك.

جدول رقم (3-4-17) نتائج اختبار تحليل التباين الأحادي (ANOVA)

للفروق بين إجابات أفراد العينة حول مخاطر أمن نظم المعلومات المحاسبية المحوسبة حسب ملكية البنوك

م	ملكية البنوك	العدد	المتوسط الحسابي	قيمة (F) المحسوبة	مستوى دلالة (F) المحسوبة	نتيجة اختبار الفرضية
1	ملكية عامة	8	2.651	1.482	0.231	قبول (لا يوجد فروق)
2	ملكية خاصة	88	2.400			
3	ملكية مختلطة	26	2.465			
	الإجمالي	122	2.430			

الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS)، وقيمة (F) الجدولية (2.66) عند درجات حرية (2, 121). (df=121, 2).

يظهر الجدول السابق عدم وجود فروق ذات دلالة إحصائية بين آراء أفراد العينة تعزى لمتغير ملكية البنوك التجارية في الجمهورية اليمنية حيث بلغت قيمة (F) المحسوبة (1.482) وهي أصغر من قيمة (F) الجدولية البالغة (2.66) وبدلالة إحصائية (0.231)، وهي قيمة غير دالة إحصائياً لأنها أكبر من مستوى الدلالة المعنوية (0.05)، وربما يعود ذلك إلى التقارب الواضح في قيم المتوسطات الحسابية لاستجابة الأفراد المجيبين على أسئلة الاستقصاء، ويعزو الباحث ذلك إلى أن البنوك التجارية في الجمهورية اليمنية مهما اختلفت ملكيتها فأنها تتعرض لمخاطر أمن نظم المعلومات المحاسبية المحوسبة متشابهة ومتقاربة.

وعليه يتم قبول الفرضية العدمية القائلة: "لا يوجد اختلاف جوهري بين البنوك التجارية في الجمهورية اليمنية فيما يتعلق بحجم المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة يُعزى لملكية تلك البنوك".

3-4-9: نتيجة اختبار الفرضية التاسعة:

تنص الفرضية العدمية الثامنة (H^0-9) على أنه " لا يوجد اختلاف جوهري بين نظم المعلومات المحاسبية المحوسبة المستخدمة لدى البنوك التجارية في الجمهورية اليمنية فيما يتعلق بحجم المخاطر التي تهدد أمن تلك النظم يُعزى لنوعية تشغيل تلك النظم"، ولاختبار هذه الفرضية استخدم الباحث اختبار تحليل التباين الأحادي (*One- Way ANOVA*)، لمعرفة ما إذا كان هناك فروق ذات دلالة إحصائية عند مستوى دلالة معنوية (0.05) لأفراد عينة الدراسة حول آرائهم نحو مخاطر أمن نظم المعلومات المحاسبية المحوسبة، تعزى لنوعية تشغيل نظم المعلومات المحاسبية المحوسبة التي يعملون عليها، والجدول الآتي يوضح ذلك.

جدول رقم (3-4-18) نتائج اختبار تحليل التباين الأحادي (ANOVA)

للفروق بين إجابات أفراد العينة حول مخاطر أمن نظم المعلومات المحاسبية المحوسبة حسب نوعية تشغيل النظام

م	نوعية تشغيل النظام	العدد	المتوسط الحسابي	قيمة (F) المحسوبة	مستوى دلالة (F) المحسوبة	نتيجة اختبار الفرضية
1	نظام تشغيل على أساس الدفعات	13	2.212	2.745	0.046	رفض (يوجد فروق)
2	نظام تشغيل فوري ومباشر	92	2.438			
3	نظام تشغيل موزع	15	2.489			
4	آخر	2	3.011			
	الإجمالي	122	2.430			

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS)، وقيمة (F) الجدولية (2.66) عند درجات حرية (3, 121). (df=121, 3).

يُظهر الجدول السابق عدم وجود فروق ذات دلالة إحصائية بين آراء أفراد العينة تعزى لمتغير ملكية البنوك التجارية في الجمهورية اليمنية حيث بلغت قيمة (F) المحسوبة (2.745) وهي أكبر من قيمة (F) الجدولية البالغة (2.66) وبدلالة إحصائية (0.046)، وهي قيمة دالة إحصائياً لأنها أصغر من مستوى الدلالة المعنوية (0.05)، وربما يعود ذلك إلى وجود فروق ظاهرة وواضحة في قيم المتوسطات الحسابية لاستجابة الأفراد المجيبين على أسئلة الاستقصاء، ويعزو الباحث ذلك إلى أن مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية تختلف باختلاف نظم التشغيل. وعليه يتم رفض الفرضية العدمية وقبول الفرضية البديلة القائلة: "يوجد اختلاف جوهري بين نظم المعلومات المحاسبية المحوسبة المستخدمة لدى البنوك التجارية في الجمهورية اليمنية فيما يتعلق بحجم المخاطر التي تهدد أمن تلك النظم يُعزى لنوعية تشغيل تلك النظم".

3-4-10: نتيجة اختبار الفرضية العاشرة:

تنص الفرضية العدمية السابعة (H^0-10) على أنه "لا يوجد اختلاف جوهري بين نظم المعلومات المحاسبية المحوسبة المستخدمة لدى البنوك التجارية في الجمهورية اليمنية فيما يتعلق بحجم المخاطر التي تهدد أمن تلك النظم يُعزى لمستوى ارتباط تلك النظم بشبكات الاتصال"، واختبار هذه الفرضية استخدم الباحث اختبار تحليل التباين الأحادي (*One-Way ANOVA*)، لمعرفة ما إذا كان هناك فروق ذات دلالة إحصائية بين إجابات أفراد العينة نحو مخاطر أمن نظم المعلومات المحاسبية المحوسبة عند مستوى دلالة معنوية (0.05) تعزى لمستوى ارتباط النظم التي يعملون بها بشبكات الاتصال، والجدول الآتي يوضح ذلك.

جدول رقم (3-4-19) نتائج اختبار تحليل التباين الأحادي (ANOVA) للفروق بين إجابات أفراد العينة حول مخاطر أمن نظم المعلومات المحاسبية المحوسبة حسب مستوى ارتباط النظم التي يعملون بها بشبكات الاتصال

م	المسمى الوظيفي	العدد	المتوسط الحسابي	قيمة (F) المحسوبة	مستوى دلالة (F) المحسوبة	نتيجة اختبار الفرضية
1	شبكة معلومات محلية بين الأقسام (إنترانت).	20	2.381	1.865	0.159	قبول (لا يوجد فروق)
2	شبكة معلومات محلية بين الفروع (إكسترانت).	88	2.410			
3	شبكة معلومات عالمية (إنترنت).	14	2.627			
	الإجمالي	122	2.430			

• الجدول من إعداد الباحث اعتماداً على نتائج التحليل الإحصائي (SPSS)، وقيمة (F) الجدولية (2.66) عند درجات حرية (2، 121). (df=121, 2).

يُظهر الجدول السابق عدم وجود فروق ذات دلالة إحصائية بين آراء أفراد العينة تعزى لمتغير المسمى الوظيفي حيث بلغت قيمة (F) المحسوبة (1.865) وهي أصغر من قيمة (F) الجدولية البالغة (2.66) وبدلالة إحصائية (0.159) وهي قيمة غير دالة إحصائياً لأنها أكبر من مستوى الدلالة المعنوية (0.05)، وربما يعود ذلك إلى التقارب الواضح في قيم المتوسطات الحسابية لاستجابة الأفراد المجيبين على أسئلة الاستقصاء، ويعزو الباحث ذلك إلى أن الأفراد العاملين على نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية والممثلين في عينة الدراسة لديهم رؤية متشابهة نحو مخاطر أمن نظم المعلومات المحاسبية المحوسبة مهما اختلف مستوى ارتباط تلك النظم بشبكات الاتصالات.

وعليه يتم قبول الفرضية العدمية القائلة: "لا يوجد اختلاف جوهري بين نظم المعلومات المحاسبية المحوسبة المستخدمة لدى البنوك التجارية في الجمهورية اليمنية فيما يتعلق بحجم المخاطر التي تهدد أمن تلك النظم يُعزى لمستوى ارتباط تلك النظم بشبكات الاتصال".

3 5: المبحث الخامس:

النتائج والتوصيات والمقترحات

مقدمة:

إن تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة موضوع كبير وهام ومتعدد الجوانب ولا يمكن تغطيته من خلال هذا الدراسة التي ركزت على تقييم ومعالجة مخاطر نظم المعلومات المحاسبية المحوسبة في بيئة البنوك التجارية لعاملة في الجمهورية اليمنية ومصادرها المختلفة وكذلك التعرف على إجراءات الحماية التي تتبعها تلك البنوك وأيضاً المعايير المستخدمة في معالجة تلك المخاطر، والتي يجب أخذها في الاعتبار في جميع مراحل تطوير نظم المعلومات الموجودة بالمنشأة ويحتاج إلى منهجية منظمة وثابته لأنه يعتمد على تكامل عدد من المجالات والتي تتضمن نظم المعلومات المحاسبية والرقابة الداخلية وأمن المعلومات والاتصالات وتحليل المخاطر إلى غير ذلك من المجالات التي يجب أن تتكامل فيما بينها، بحيث يمكن من خلال ذلك التقييم معالجة مخاطر نظم المعلومات المحاسبية المحوسبة.

وفي ضوء الدراسة التطبيقية من خلال المقابلات الشخصية التي أجراها الباحث مع العديد من الكوادر المصرفية المتخصصة في نظم تكنولوجيا المعلومات والاتصالات، بالإضافة إلى ملاحظات الباحث في دراسة الحالة العملية الاستكشافية، ومن خلال المسح الذي أجراه لمواقع البنوك العاملة بالجمهورية اليمنية على شبكة الانترنت والتقارير ذات العلاقة بهذه الدراسة، ومن خلال ما سبق من تحليل ودلائل إحصائية، يتناول هذا المبحث أهم النتائج التي توصلت إليها الدراسة، وبالتالي يمكن من خلال تلك النتائج إلقاء الضوء على مجموعة من التوصيات والمقترحات بشأنها والتي حاول الباحث أن يرصدها بهدف تعزيز الجوانب المختلفة لعملية التقييم المتعلقة بالدراسة.

3-5-1: نتائج الدراسة:

في ضوء الدراستين النظرية والعملية التي تمت واستناداً إلى تحليل بيانات هذه الدراسة واختبار فرضياتها وتفسير نتائجها، من واقع قوائم الاستقصاء واللقاءات التي أجراها الباحث ببعض المسؤولين لدى البنوك التجارية في الجمهورية اليمنية، فقد توصلت هذه الدراسة التطبيقية إلى مجموعة من النتائج يمكن استخلاص أهمها على النحو التالي:

1. هناك ضعف نسبي في حجم الخدمات المصرفية الالكترونية التي تقدمها البنوك التجارية في الجمهورية اليمنية من خلال أدوات الدفع الإلكترونية بالإضافة إلى ضعف في حجم ما تملكه من تلك الأدوات.

2. تعتمد البنوك التجارية في الجمهورية اليمنية في عملها بشكل كبير على نظم المعلومات المحاسبية المحوسبة وهذا راجع لما تحققه تلك النظم من مزايا متعددة وأهمية متزايدة ولها دور فعّال في تطوير الأداء المحاسبي والرقابي في البنوك التجارية بصفة خاصة ولكن بالمقابل لا يوجد مواكبة للتطورات الحاصلة في تقنية المعلومات الخاصة بحماية تلك النظم من المخاطر التي تتهددها.
3. أغلبية دوائر البنوك التجارية في الجمهورية اليمنية لا يوجد في هياكلها التنظيمية وحدات مستقلة لتقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة، وبشكل عام معظم البنوك لا يتوفر فيها دوائر مختصة ذات كوادر مؤهلة في إدارة وضبط تلك المخاطر الأمنية وإنما يتم إدارة المخاطر من قبل نفس الجهات التي تنفذ العمليات في غالب الأحيان.
4. لا يوجد لدى إدارات تكنولوجيا المعلومات أو إدارات المخاطر لدى البنوك التجارية في الجمهورية اليمنية منهجية علمية تستند إلى معايير وقواعد علمية واضحة في مجال تقييم عمليات إدارة المخاطر.
5. توجد مخاطر تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية بحكم طبيعة العمل في تلك البنوك، وتحدث تلك المخاطر بدرجات متفاوتة تتوقف على كفاءة وفعالية وسائل وإجراءات الحماية والسيطرة المطبقة لدى تلك البنوك، ومستوى التهديدات الداخلية والخارجية الموجودة، وأهم تلك المخاطر هي المخاطر المتعلقة بأمن عمليات المدخلات في تلك النظم بالمرتبة الأولى ثم يليها مخاطر أمن العاملين في تلك النظم بالمرتبة الثانية نتيجة قلة الخبرة والوعي والتدريب، ثم يليها مخاطر أمن الوصول البرمجي لقاعدة بيانات نظم المعلومات المحاسبية، وكانت أقلها أهمية هي مخاطر أمن النسخ في وسائط غير متصلة بقواعد البيانات.
6. كل المخاطر موضوع الدراسة لا يمكن تجنبها أو تقليص حدتها بشكل كامل وذلك ببساطة يعود لوجود عوائق عملية ومالية، لذلك على أي بنك تجاري أن يتقبل مستوى معين من المخاطر (مخاطر متبقية).
7. بالرغم من وجود العديد من المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية إلا أنه لا تحدث مخاطر جوهرية ذات أهمية نسبية تهدد أمن تلك النظم بل كانت محدودة نتيجة محدودية التقنية المستعملة في البيئة اليمنية، ولأن البنوك التجارية في الجمهورية اليمنية تمتلك وسائل وتستخدم مجموعة من إجراءات الحماية المختلفة بشكل أو بآخر للسيطرة على تلك المخاطر.
8. يُعزى حدوث بعض مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية إلى مجموعة من التهديدات الداخلية لدى تلك البنوك، وأهمها هي تلك التهديدات المتعلقة بالأفراد العاملين في نظم المعلومات المحاسبية نتيجة قلة الخبرة والوعي والتدريب، فلا توجد خطط تدريبية أو مجلات ونشرات دورية لرفع الوعي الأمني لدى الأفراد العاملين في تلك النظم، ثم يليها التهديدات المتعلقة بفلسفة الإدارة العليا للبنوك التجارية في اليمن نتيجة لعدم وجود سياسات واضحة ومكتوبة ومطبقة لديها، وإن وجدت تلك السياسات

لدى بعض البنوك التجارية في اليمن إلا أنها لم تقم بإنشاء دوائر – أو تأهيل كوادر- مختصة لإدارة تلك المخاطر، ثم جاءت التهديدات المتعلقة بالتهديدات التنظيمية في المرتبة الثالثة حيث وجد الباحث عدم وجود دائرة خاصة لأمن نظم المعلومات المحاسبية، وندرة وجود الكوادر المختصة والمؤهلة في مجال أمن نظم المعلومات المحاسبية المحوسبة الذي تتوفر فيه الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المتعددة والمطلوبة، هذا بالإضافة إلى صعوبة وعدم كفاية تدريب وتأهيل وتوعية الموظفين في مجال تقنيات وأساليب أمن نظم المعلومات المحاسبية، وعدم توافق التدريب مع التطور المستمر لبرامج أمن نظم المعلومات، بينما كانت التهديدات المتعلقة بالإمكانات التكنولوجية للبنوك التجارية في الجمهورية اليمنية أقل التهديدات أهمية، ولعل مرد ذلك يعود إلى أن كل البنوك التجارية في اليمن سعت لامتلاك أحدث وسائل الاتصالات وتكنولوجيا المعلومات في ظل المنافسة الاقتصادية في الصناعة المصرفية.

9. يُعزى حدوث بعض مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية إلى مجموعة من التهديدات الخارجية لدى تلك البنوك، وأهمها تلك التهديدات التي تتعلق بنقص الوعي الإلكتروني لدى عملاء البنك بالمرتبة الأولى، ولعل ذلك يعود إلى انخفاض وعي العملاء وعدم إلمامهم الكافي بكيفية استخدام نظام الانترنت المصرفي وعدم إحاطتهم بإجراءات التأمين والوقاية، وعدم قيام البنوك بتوعية العملاء وتعريفهم بالاحتياطات الأمنية الواجب اتخاذها وحدود مسؤوليتهم، حيث أن جزء لا يستهان به ليسوا على دراية كافية بهذا المجال، فالتكنولوجيا قد تكون بلا فائدة لمن لا يملك القدرة والمعرفة على التعامل معها، ثم جاءت التهديدات المتعلقة بدخول فيروسات وبرمجيات الحاسوب بالمرتبة الثانية، بينما جاءت التهديدات المتعلقة بضعف التشريعات والقوانين المحلية في مجال تكنولوجيا المعلومات بالمرتبة الثالثة، بينما كانت التهديدات المتعلقة بالمنافسة الاقتصادية بين البنوك أقل التهديدات الخارجية أهمية، ولعل مرد ذلك يعود إلى عدم اكتشاف أي حالة تجسس أو اختراق بين تلك البنوك.

10. يؤثر حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية على العناصر المكونة لأمن تلك النظم المتمثلة ب (إتاحة النظم، وصحة وسلامة وتكامل التشغيل، وسرية وخصوصية المعلومات المحاسبية، وعدم إنكار العمليات) لدى تلك البنوك"، حيث وجد أن تلك التأثيرات مرتفعة بشكل عام وتتسبب في تأثيرات سلبية على أمن تلك النظم لدى البنوك التجارية في الجمهورية اليمنية، فقد كان تأثير المخاطر على سلامة وتكامل تجهيز البيانات في نظم المعلومات المحاسبية أهم التأثيرات لحدوث المخاطر على عناصر أمن تلك النظم والذي جاء في المرتبة الأولى، ثم يليها تأثير المخاطر على خصوصية بيانات الأطراف المتعاملة مع البنك بالمرتبة الثانية، يليها تأثير المخاطر على سرية المعلومات المحاسبية، ثم تأثير المخاطر على إتاحة نظم المعلومات المحاسبية المحوسبة، وكان أقلها أهمية هي تأثير المخاطر على إثبات تصرفات الأطراف المتعاملة خلال تبادل البيانات إلكترونياً.

11. تطبق البنوك التجارية في الجمهورية اليمنية أساليب وإجراءات كافية وفعّالة لحماية أمن نظم المعلومات الحاسوبية المحسوبة من المخاطر التي تتهددها وفق القواعد المحلية والأسس والمعايير الدولية، وكان مستوى تطبيق تلك الإجراءات والوسائل متوسطاً بشكل عام لحماية أمن نظم المعلومات الحاسوبية المحسوبة، وبالتالي، فإننا يمكن القول إن آليات إجراءات الحماية مطبقة نسبياً وبشكل كافي وفعّال، ولكنها ليست مطبقة بالشكل الأمثل، كما أنها تحتاج إلى تطوير وتحديث مستمر لكي تتلاءم وتتناسب مع حجم المخاطر المتغيرة التي يمكن أن تؤثر بشكل كبير على أمن نظم المعلومات الحاسوبية.

12. إن أهم إجراءات ووسائل حماية أمن نظم المعلومات الحاسوبية المحسوبة المطبقة لدى البنوك التجارية في الجمهورية اليمنية هي الإجراءات والوسائل التي تتعلق بحماية أمن تعديل وتطوير نظم المعلومات الحاسوبية المحسوبة بالمرتبة الأولى، ثم يليها إجراءات حماية أمن مدخلات النظم بالمرتبة الثانية، يليها إجراءات حماية أمن وسائط التخزين غير المتصلة بقاعدة البيانات، مما يشير إلى أن إجراءات حماية أمن المخرجات مطبقة وبدرجة مرتفعة ولكن بشكل غير كافٍ، وكان أقلها أهمية هي الإجراءات المتعلقة بحماية أمن تبادل البيانات المنقولة عبر شبكات نظم المعلومات الحاسوبية، ولعل مرد ذلك يعود إلى أن استخدام كلاً من التوقيع الإلكتروني والشهادات الرقمية عند إرسال واستلام البيانات يشوبه الضعف والقصور فإجراءات الحماية غير كافية في ذلك الجانب لدى البنوك التجارية في الجمهورية اليمنية.

13. أظهرت الدراسة وجود تأثير إيجابي لأساليب وإجراءات الحماية المطبقة في البنوك التجارية في الجمهورية اليمنية على المخاطر التي تهدد أمن نظم المعلومات الحاسوبية المحسوبة لدى تلك البنوك، وقوة التأثير قوية نسبياً حيث بلغ قيمة معامل الانحدار التأثيري المعياري (0.498)، كما أن قيمة معامل التحديد (R^2) قد بلغت (0.248) وهي قيمة دالة وذات دلالة إحصائية، وهذا يعني أن أساليب وإجراءات الحماية المطبقة تسهم في تفسير ما نسبته (24.8 %) من التباين أو التغير الحاصل في سلوك (مخاطر أمن نظم المعلومات الحاسوبية المحسوبة) إذا أخذت بصورة منفصلة أو منفردة وكحزمة واحدة، وتلك قوة تفسيرية متوسطة نسبياً، وقد يعود ذلك إلى وجود قصور في التطبيق العملي لتلك الإجراءات واستخدام بعض البنوك مجموعة غير متكاملة من أساليب الحماية والتي تحتاج فعلاً إلى تطوير وتحديث مستمر وهذه النتيجة تعزز ما سبقها من نتائج.

14. لا توجد فروق جوهرية بين آراء أفراد عينة الدراسة فيما يتعلق بالمخاطر التي تهدد أمن نظم المعلومات الحاسوبية المحسوبة لدى البنوك التجارية في الجمهورية اليمنية تُعزى للمسمى الوظيفي لهم، ويعزو الباحث ذلك إلى أن أفراد عينة الدراسة مهما اختلفت مسمياتهم الوظيفية، فإن لديهم رؤية متشابهة نحو مخاطر أمن نظم المعلومات الحاسوبية المحسوبة وفقاً لمسمياتهم الوظيفية.

15. يوجد اختلاف في حجم المخاطر التي تتعرض لها البنوك التجارية في الجمهورية اليمنية باختلاف نوعية القطاع الذي تنتمي لها تلك البنوك، حيث وجد أن المخاطر تزداد بشكل تصاعدي لدى كلاً من (بنوك القطاع

الخاص ثم بنوك القطاع المختلط ثم بنوك القطاع العام) على الترتيب، ولكن بالرغم من ذلك لا يوجد فرق جوهري دال إحصائياً بين تلك البنوك بشكل عام فيما يتعلق بحجم المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة يُعزى لملكية تلك البنوك، ويعزو الباحث ذلك إلى أن البنوك التجارية في الجمهورية اليمنية مهما اختلفت ملكيتها فأنها تتعرض لمخاطر أمن نظم المعلومات المحاسبية المحوسبة متشابهة ومتقاربة.

16. يوجد اختلاف جوهري بين نظم المعلومات المحاسبية المحوسبة المستخدمة لدى البنوك التجارية في الجمهورية اليمنية فيما يتعلق بحجم المخاطر التي تهدد أمن تلك النظم يُعزى لنوعية تشغيل تلك النظم، ويعزو الباحث ذلك إلى أن مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية تختلف باختلاف نظم التشغيل.

17. لا يوجد اختلاف جوهري بين نظم المعلومات المحاسبية المحوسبة المستخدمة لدى البنوك التجارية في الجمهورية اليمنية فيما يتعلق بحجم المخاطر التي تهدد أمن تلك النظم يُعزى لمستوى ارتباط تلك النظم بشبكات الاتصال، ويعزو الباحث ذلك إلى أن الأفراد العاملين على نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية والممثلين في عينة الدراسة لديهم رؤية متشابهة نحو مخاطر أمن نظم المعلومات المحاسبية المحوسبة مهما اختلف مستوى ارتباط تلك النظم بشبكات الاتصالات.

3-5-2: توصيات ومقترحات الدراسة:

انطلاقاً من نتائج الدراسة وفي ضوء ما توصلت إليه من استنتاجات فإنه يمكن الخروج بمجموعة من التوصيات والمقترحات من أجل تحسين وتعزيز الوضع الحالي ورفع فاعلية تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية من خلال اتخاذ العديد من الخطوات وآلية تحديد المخاطر وقياسها ومراقبتها وتخفيضها لتجاوز أثارها السلبية، ولتحقيق فائدة للمهتمين والمتخصصين بأمن نظم المعلومات المحاسبية، ويمكن حصر تلك التوصيات والمقترحات على النحو التالي:

1. ضرورة التزام الإدارات التنفيذية والإدارة العليا في البنوك التجارية اليمنية بالتقييم الدوري والمستمر لمخاطر أمن نظم المعلومات والاهتمام بتأثير تلك المخاطر وضرورة توقعها قبل حدوثها وإيجاد الحلول المناسبة لها في حال وقوعها، وإيجاد السبل الكفيلة باستعادة العمل ووضع خطط الطوارئ اللازمة لضمان أمن نظم المعلومات.
2. ضرورة قيام البنوك التجارية العاملة في اليمن بإدماج تقنيات وبرمجيات أمن نظم المعلومات المحاسبية في مشاريع البنية التحتية لتكنولوجيا الاتصالات المعلومات وتفعيل أساسيات وتطبيقات أمن تلك النظم، وينبغي توافر الدعم الحكومي لتوفير البنية الأساسية لشبكات الاتصالات الأمانة.

3. تشجيع الحوار ما بين البنوك التجارية والسلطات الرقابية لتوفر المعايير الموضوعية الخاصة بالأمان والسلامة للعمليات المصرفية الالكترونية بما لا يؤدي للحد من قدرة البنوك على الإبداع والمنافسة، وتفعيل دور جمعية البنوك اليمنية في هذا الصدد، وأهمية إسهام الهيئات العلمية والمهنية إلى حدٍ بعيد.
4. إصدار كتيب يلخص السياسات والمعايير والإجراءات والمواصفات القياسية التي تبين المسؤوليات والصلاحيات المتعلقة بتنفيذ ومراقبة أمن العمليات المصرفية الالكترونية، وفق الإرشادات الواردة في الممارسات السليمة لإدارة المخاطر، وبيان آليات تنفيذها وعقوبات مخالفتها، مع إقرار وتعهد أمني يوقع عليه جميع الموظفين بمختلف مستوياتهم الإدارية بعد قراءة الكتيب والاطلاع عليه.
5. من الضروري أن تدعم الإدارات العليا للبنوك التجارية مفهوم حوكمة تكنولوجيا المعلومات لديها ومأسسة عملية الرقابة والتوعية والإعلام الخاصة بأمن نظم المعلومات من خلال جهة مؤهلة تتحمل هذه المسؤولية وإنشاء وحدات إدارية (إدارة أو قسم أو شعبة) في الهيكل التنظيمي لتلك البنوك، لتقييم مخاطر أمن نظم المعلومات تخضع لرقابة تدقيق داخلي فعال وردها بكوادر متخصصة ذو خبرة وكفاءة عالية وذلك لتمكين البنوك من تحديد وتعريف وقياس وتحليل تلك المخاطر وبالتالي ضبطها والتحكم فيها وتخفيض الخسائر الناجمة عنها، مع الأخذ في الاعتبار النفقات اللازمة لضبط تلك المخاطر.
6. تطوير واعتماد أدوات حديثة وأنظمة ومنهجية علمية لقياس وتقييم مخاطر أمن نظم المعلومات المحاسبية وتدريب وتأهيل الأفراد ذوي العلاقة لاستخدام تلك الأدوات والأساليب بكفاءة وبما يتوافق مع الممارسات والمعايير الدولية من أجل تحديد تلك المخاطر للسيطرة عليها أو تخفيضها.
7. مراقبة ورفع تقارير دورية حول مخاطر أمن نظم المعلومات المحاسبية المحوسبة، بما فيها بيانات الخسائر والمؤشرات الأخرى للمخاطر المحتملة، وتوضيح إجراءات البنك المتخذة للمعالجة المناسبة والفعالة لأحداث المخاطر ونقاط الضعف، مع إصدار تقرير منفصل ضمن التقرير السنوي المنشور بخصوص تقييم وإدارة تلك المخاطر.
8. ينبغي وجود إستراتيجية شاملة ومتكاملة وواضحة ومكتوبة وقابلة للتطبيق لتقييم وإدارة مخاطر أمن نظم المعلومات المحاسبية، وأن تحدد بوضوح مصادر تلك المخاطر، كما يجب أن تشمل الإستراتيجية مستوى المخاطر التي يتقبلها البنك والذي يعكس تحديد أولويات البنك في إدارته للمخاطر، وفق منهجية علمية تستند إلى معايير وقواعد علمية واضحة في مجال تقييم عمليات إدارة المخاطر.
9. ضرورة المواكبة المستمرة للتطورات المتسارعة في تكنولوجيا الاتصالات والمعلومات الخاصة بحماية أمن نظم المعلومات المحاسبية من المخاطر التي تتهدده، وضرورة قيام الإدارات المصرفية العليا في البنوك التجارية في اليمن بطلب مساعدة من المؤسسات المحلية والدولية المتخصصة لتطوير وتحديث البنية التحتية التقنية المستخدمة، مع الحرص على استخدام أجهزة الحاسوب الحديثة، والبرمجيات المتطورة، والتركيز على نوعيتها ومصدرها، وبما يضمن ويعزز فاعلية أمن نظم المعلومات المحاسبية وزيادة الثقة في مخرجاتها، مع

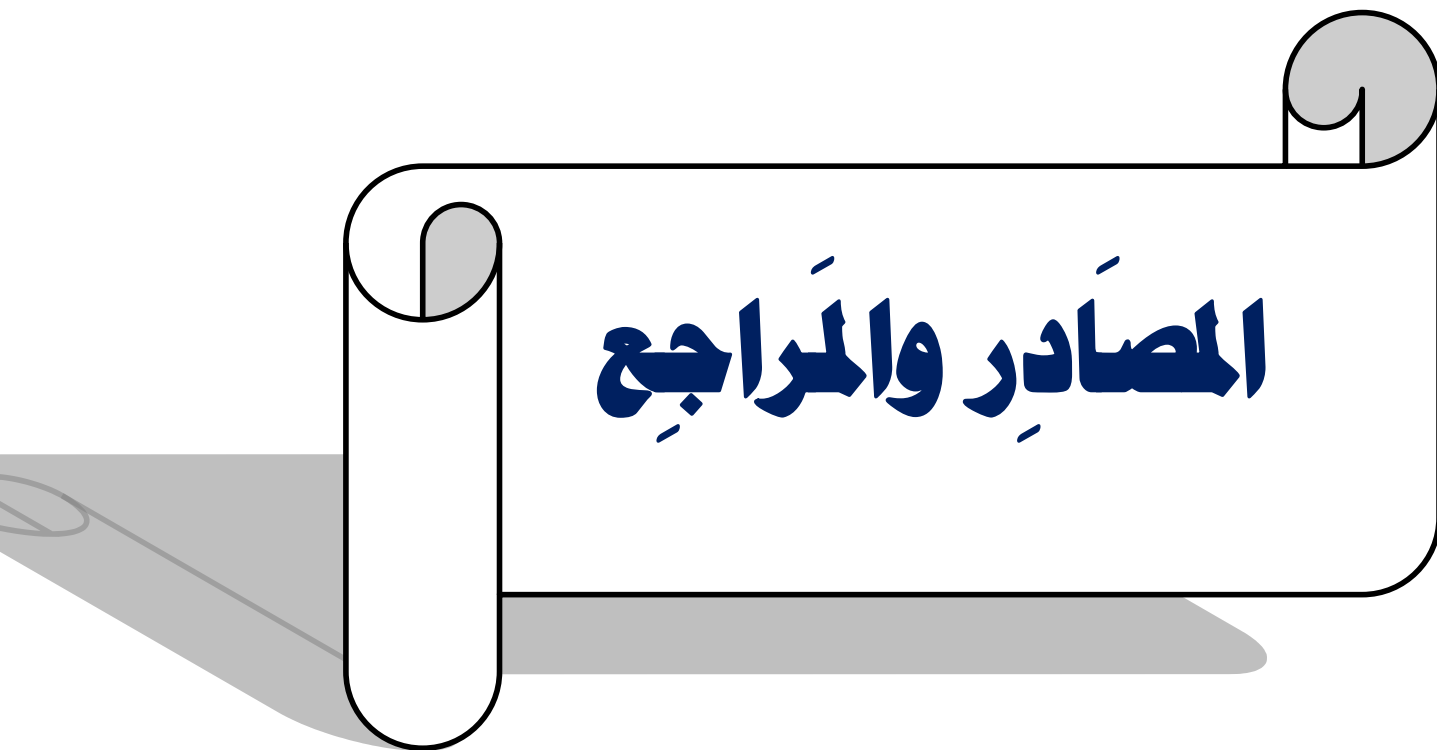
- ضرورة عمل مراجعة دورية لتقنيات المعلومات المستخدمة بغرض تطويرها حسب ظروف العمل، بشكل يضمن الدقة والسرعة عند استخدامها.
10. على البنوك التجارية في الجمهورية اليمنية أن تتقبل مستوى معين من مخاطر أمن نظم المعلومات المحاسبية (مخاطر متبقية)، لأن معظم المخاطر موضوع الدراسة لا يمكن تجنبها أو تقليص حدتها بشكل كامل وذلك ببساطة يعود لوجود عوائق عملية ومالية.
11. التوسع في الخدمات المصرفية الإلكترونية الحديثة وحاجة البنوك للاستثمار في تطوير أدواتها، وتقديم الإرشادات اللازمة للمستخدمين حول مخاطر استخدام تلك الخدمات إلى جانب مزاياها، لضمان رفع مستوى الأداء ونوعية تلك الخدمات على الصعيدين الوطني والدولي.
12. ضرورة تحسين الكفاءة الرقابية لنظم الرقابة الداخلية في البنوك التجارية لتشمل الضوابط الرقابية التطبيقية التي تمنع المخاطر أو تكتشفها وقت حدوثها.
13. التزام البنوك التجارية في الجمهورية اليمنية بالتعليمات الصادرة لها من البنك المركزي اليمني فيما يتعلق بالرقابة على نظم المعلومات وخاصة ما يتعلق بإشعار البنك المركزي بأية اختراقات داخلية أو خارجية تتعرض لها هذه الأنظمة حال حدوثها وكذلك بالتأمين على مخاطر الخدمات المصرفية الإلكترونية التي تقدمها لعملائها.
14. ينبغي على المبرمجين تزويد برامج الحماية في نظم المعلومات المحاسبية المحوسبة بإمكانية إصدار تقارير رقابية خاصة بإدارة المستخدمين تصدر يومياً وبصورة آلية وتعكس كل الأنشطة التي تمت على سجل المستخدمين من إضافة وحذف وتعديل ويراجع ويوقع عليه من قبل المختصين.
15. الاستمرار بتوظيف واستخدام الأفراد الذين يتمتعون بمؤهلات علمية متخصصة في مجال المحاسبة تتناسب مع حجم ومستوى المهام والوظائف المطلوبة منهم، وزيادة الاهتمام بالتدريب والتأهيل العلمي والمهني المتواصل للمحاسبين والقائمين على العمل في نظم المعلومات المحاسبية من مبرمجين ومحلي نظم ومشغلي أجهزة الحاسوب.
16. الاهتمام بالكوادر البشرية التي تستخدم نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية وتطوير قدرات ومهارات الأفراد الوظيفية والتقنية المختصة بأمن نظم تلك النظم وذلك من خلال تدريب وتأهيل وتوعية الموظفين في مجال تقنيات وأسابيب أمن نظم المعلومات المحاسبية، مع إصدار مجلات ونشرات دورية توعوية بالمخاطر محل هذه الدراسة، وينبغي أن يتوافق التدريب مع التطور المستمر لبرامج أمن نظم المعلومات، ويجب متابعة المتدرب بعد الدورة وقياس أثر التدريب على عمله بعد التدريب حتى لا يكون الهدف مجرد عقد دورة تدريبية، مع ضرورة ربط ذلك بحوافز مادية ومعنوية ومكافآت تشجيعية للمتدربين، بالإضافة إلى الاهتمام بالجانب الأخلاقي للعمل المحاسبي وتعزيز الولاء الوظيفي.

17. عقد ندوات ومؤتمرات شهرية لمتابعة التطورات في مجال أمن نظم المعلومات وتقييم المخاطر التي تتهددها، وتكوين ثقافة تخصصية عالية وبدون ذلك فإن الفجوة تزداد بين قدرات ومعارف أفراد عينة الدراسة وما يحصل حولهم في العالم.
18. ضرورة وجود مبرمجين أكفاء تتوفر لديهم الخلفية العلمية والمهارات المتعددة وملمين بأحدث مخاطر أمن نظم المعلومات المحوسبة والإبقاء عليهم لفترات طويلة في أماكنهم لإكساب خبراتهم للغير، وضرورة الاستعانة بخبراء استشاريين أكاديميين ومهنيين ومتخصصين فنيين في نظم المعلومات المحوسبة ضمن الكادر الوظيفي في البنوك لمواجهة أي خلل في تلك النظم.
19. ضرورة قيام الجامعات اليمنية بزيادة الاهتمام بتدريس مادة نظم المعلومات المحاسبية المحوسبة ومساق تكنولوجيا المعلومات لطلبة قسم المحاسبة حتى يكون لهم القدرة على التعامل مع أنظمة معقدة لتطبيقات الحاسوب، ومواجهة التهديدات التي تتعرض نظم المعلومات المحاسبية، وحتى تواكب الخطط الدراسية التطورات العالمية المتلاحقة في هذا الشأن ينبغي أن يكون الإلمام بتقنيات تكنولوجيا المعلومات من أساسيات منح الشهادات العلمية والعملية ومزاولة المهنة.
20. ضرورة زيادة التنسيق بين البنوك التجارية في اليمن والمؤسسات الأكاديمية والمصرفية لتأمين برامج تدريبية وتعليمية مناسبة للأفراد العاملين في نظم المعلومات المحاسبية المحوسبة، مع ضرورة إشراك البنوك التجارية عند تصميم البرامج الجامعية، خاصة مرحلة البكالوريوس في المحاسبة وتكنولوجيا المعلومات، لضمان إدخال احتياجاتها التطبيقية الحقيقية ضمن تلك البرامج.
21. حث البنك المركزي اليمني على تطبيق المعايير الدولية في الرقابة على نظم المعلومات المستخدمة في البنوك التجارية وما يطرأ عليها من تعديلات تتلاءم والبيئة المصرفية اليمنية وخاصة ما يتصل بوسائل الحد من مخاطر العمل المصرفي الإلكتروني عموماً ومخاطر أمن نظم المعلومات لدى البنوك التجارية على وجه الخصوص، بالإضافة إلى الاستمرار في تأهيل كوادره من المفتشين للقيام بهذه المهمة.
22. العمل على تطوير اللوائح والنظم والقوانين المنظمة لعمل البنوك التجارية بشكل عام ولنظم المعلومات المحاسبية المحوسبة بشكل خاص، بما يتفق مع الانفتاح والتطور الذي يشهده القطاع المصرفي في الجمهورية اليمنية، وبما يضمن استقرارية ومرونة العمل، وينعكس إيجاباً على فاعلية أمن نظم المعلومات المحاسبية في تلك البنوك، من خلال وضع أنظمة وتعليمات تساعد على عدم اختراق نظم معلومات البنوك وعدم تداولها إلا بين موظفي البنوك المرخص لهم بذلك.
23. ينبغي إنشاء هيئة وطنية لأمن نظم المعلومات يكون لها الحق في سن تشريعات جديدة وتعديل التشريعات القائمة اللازمة لأمن نظم المعلومات الإلكترونية وردع مرتكبي الجرائم الإلكترونية، وذلك للحفاظ على ما لدى المنشآت الاقتصادية المختلفة - ومنها البنوك - من نظم معلومات قد تكون مؤثرة على الاقتصاد القومي.
24. أهمية وجود معايير محلية لأمن نظم المعلومات المحاسبية تضمن سلامة وسرية وخصوصية البيانات.

25. ينبغي على البنوك التجارية في الجمهورية اليمنية تطبيق إجراءات وضوابط ووسائل حماية أمن نظم المعلومات المحاسبية بالشكل الأمثل، وتطويرها وتحديثها باستمرار لكي تتلاءم وتتناسب مع حجم المخاطر المتغيرة التي يمكن أن تؤثر بشكل كبير على أمن تلك النظم.
26. ينبغي على البنوك التجارية القيام بتوعية العملاء وتعريفهم بالاحتياطات الأمنية الواجب اتخاذها وحدود مسؤوليتهم، عند التعامل مع نظم المعلومات المحوسبة، حيث أن معظم العملاء ليسوا على دراية كافية بهذا المجال، فالتكنولوجيا قد تكون بلا فائدة لمن لا يملك القدرة والمعرفة في التعامل معها.
27. ضرورة قيام البنوك التجارية في الجمهورية اليمنية - خصوصاً البنوك التي تقدم خدمات مصرفية لعملائها من خلال الشبكة - بدور فعّال في توعية عملائها بالإنترنت المصرفي وكيفية استخدامه وكيفية حماية بياناتهم وأجهزتهم من الاختراق.
28. يجب إعداد خطط طوارئ لضمان استمرارية العمل، ومواجهة الكوارث التي تهدد أمن نظم المعلومات المحاسبية، ووضع السيناريوهات الواقعية والممكنة للتطبيق للمعالجة، ويجب أن تشمل هذه الخطط كافة المخاطر المحتمل حدوثها، كما يجب مراجعة تلك الخطط بشكل دوري للتأكد من ملاءمتها لظروف واحتياجات البنك والبيئة المحيطة.
29. تزويد نظم المعلومات المحاسبية بإمكانية إصدار تقارير لكل المستخدمين يعكس كل الأنشطة التي تمت لكل مستخدم، مع ضرورة مراجعة الصلاحيات الممنوحة للمخولين بالدخول إلى نظم المعلومات المحاسبية للتأكد من أن الصلاحيات الممنوحة تتناسب مع الواجبات المنوطة بهم، مع الإلغاء الفوري للصلاحيات الممنوحة للأفراد عند فصلهم أو نقلهم من أماكن عملهم.
30. لا بد من حفظ المعلومات المحاسبية في مكان آمن خارج البنك وخارج المدينة التي يقع فيها المركز الرئيسي إن أمكن، وذلك بوضع خطط لدرء الكوارث وإنشاء مراكز تجهز مسبقاً بالأجهزة ويتم ربطها ما أمكن بشبكة البنك بحيث يتم تحديثها يومياً إلكترونياً عبر الشبكة أو يدوياً وتكون مواكبة للتغيرات التي تحدث في حسابات البنك والعملاء وذلك لضمان استمرارية جاهزية وإتاحة نظم المعلومات المحاسبية الاحتياطية للعمل في حالة حدوث الكوارث المختلفة.
31. يجب تجهيز كل محطة عمل طرفية داخل نظم المعلومات المحاسبية بأفضل البرامج المضادة للفيروسات والمحدّثة باستمرار، ويجب أن تبقى ملفات تعريف الفيروسات المحدّثة في جميع الأوقات، وعدم نقل أو جلب البرامج والبيانات لنظم المعلومات المحاسبية بأي وسيلة ما لم يتم فحصها وتوثيقها من قبل الجهة المختصة بالبنك بخلوها من الفيروسات والبرامج الخبيثة.
32. التركيز على الإجراءات المتعلقة بحماية أمن تبادل البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية، واستخدام كلاً من التوقيع الإلكتروني والشهادات الرقمية عند إرسال واستلام البيانات لدى البنوك التجارية في الجمهورية اليمنية.

33. العمل على تشغيل بروتوكولات التحقق من الهوية، ونظم تشفير البيانات والمعلومات المحاسبية أثناء عملية الحفظ والنقل والتخزين على مختلف الوسائط حتى لا يمكن تدميرها أو اختراقها مع الأخذ في الاعتبار التكلفة والعائد.
34. ربط كافة البنوك التجارية وفروعها المنتشرة في الجمهورية اليمنية بشبكة معلومات حديثة، مع احتفاظ كل بنك بخصوصيته، وبما يمكن تلك البنوك من تقديم خدماتها بسهولة ويسر، ولعل التوصية الأكثر أهمية هنا هي ضرورة زيادة الاهتمام بأمن نظم المعلومات المحاسبية خاصة لدى المنشآت التي تستخدم نظام الشبكات والتي ترتبط بشبكة الانترنت.
35. يتعين على البنوك التجارية في اليمن إجراء اختبارات الاختراق للنظم، ضمن برامج التقييم الدورية لأمن نظم المعلومات المحاسبية، وتشمل اقتحام نقاط الوصول، ومحاولة الوصول إلى قواعد البيانات غير المصرح بها، لتلافي نقاط الضعف إن وجدت وتجنب المخاطر التي قد تنجم عن اختراق تلك النظم، مع الاهتمام بحماية أمن الشبكات الداخلية (الإكسترانت والانترانت) للبنك بنفس درجة أهمية حماية الشبكات الخارجية (الإنترنت).
36. على البنك المركزي اليمني والبنوك التجارية العاملة في اليمن إنشاء مراكز بحوث متخصصة تعنى بقضايا أمن نظم المعلومات لمواكبة أحداث ومستجدات مخاطر أمن نظم المعلومات، لما لذلك من أثر كبير علي تحسين كفاءة وفعالية نظم المعلومات المحاسبية.
37. **ضرورة القيام بدراسات وبحوث أخرى مشابهة:** يمكن تطوير هذه الدراسة واعتبارها نقطة انطلاق لمزيد من الدراسات والبحوث المستقبلية فيما يتعلق بالتنقيب عن المخاطر المتعددة والمتغيرة التي تهدد أمن نظم المعلومات المحاسبية المحوسبة والتي تصاحب التطورات المتسارعة في تكنولوجيا المعلومات، وإجراء مزيداً من الدراسات المتعمقة وإدخال متغيرات أخرى لم تتطرق إليها الدراسة الحالية، وعمل دراسات مقارنة لاختبار الفروق الجوهرية بين معدلات حدوث تلك المخاطر في بيئة الأعمال المختلفة وأيضاً التعرف على موقف المدققين الداخليين والخارجين تجاه تلك المخاطر فهناك جوانب عديدة ملحة وتحتاج إلى مزيد من الدراسات والبحوث منها:
- أ. إجراء دراسة مماثلة لهذه الدراسة بالتطبيق على قطاعات ومؤسسات خاصة وحكومية أخرى بهدف تطوير أمن نظم المعلومات المحاسبية المحوسبة لديها.
- ب. دراسة تلك المخاطر كدراسة حاله لأن لكل بنك خصوصية قد لا يفصح عنها في بحوث مسحية وربطه بواقع العمل البنكي في ظل المنافسة وتحديات العولمة.
- ج. تنفيذ دراسة مقارنة بين البلدان النامية والدول المتقدمة فيما يتعلق بقضايا أمن نظم المعلومات المحاسبية المتقدمة.
- د. دراسة مدى حوكمة تكنولوجيا نظم المعلومات المحاسبية المحوسبة لدى المنشآت المختلفة في الجمهورية اليمنية وفق المعايير والمقاييس الصادرة عن الهيئات والمنظمات الدولية.

- هـ. الوقوف على الصعوبات والمعوقات التي تواجه استخدام تكنولوجيا المعلومات في تطوير نظم المعلومات المتكاملة لدى القطاعات المختلفة في البيئة الاقتصادية اليمنية.
- و. دراسة مدى إمكانية تطبيق المعايير الدولية لأمن نظم المعلومات الحاسوبية المحوسبة في البيئة اليمنية والجدوى الاقتصادية لذلك التطبيق.
- ز. استخدام برنامج بريمافيرا (Primavera) وهو برنامج متكامل لأعمال التخطيط والجدولة وتوزيع الموارد للمشاريع وإدارتها وذلك لأن هذا البرنامج وضع أساساً لمساعدة الإدارة على أساس علمي قوي في التخطيط وإدارة ومراقبة المشاريع ومخاطرها وتكاليف تأثيرات حدوث تلك المخاطر على عدة مستويات كلية وجزئية.
- ح. تطوير نموذج للعوامل التي تؤثر على العلاقة بين مهام المراجعة الداخلية وأمن نظم المعلومات الحاسوبية.
- ط. استخدام خرائط التدفق في تصوير أمن نظم المعلومات الحاسوبية الالكترونية ومكوناته وعلاقاته مع النظم الأخرى فمن خلالها يمكن تحديد المشكلات والاختناقات التي تحدث في نظام الأمن الواجب تحليله وذلك بهدف تحقيق الكفاءة والفعالية لتلك النظم.
- ي. التركيز على المشاكل التي تواجه مستخدم ومصمم نظم المعلومات الحاسوبية المحوسبة في البنوك التجارية في الجمهورية اليمنية.
- ك. استخدام تقنيات الذكاء الاصطناعي ونظم الخبرة والتنقيب عن البيانات والشبكات العصبية والمنطق الضبابي بالإضافة إلى الطرق والأساليب الإحصائية في إدارة أمن نظم المعلومات الحاسوبية الالكترونية واكتشاف عمليات التلاعب والاختلاسات وربط وتحليل الأحداث الناتجة عن نظم المعلومات الحاسوبية المحوسبة.
- ل. دراسة العوامل المؤثرة على فاعلية أمن نظم المعلومات الحاسوبية من خلال بيانات تطبيقية حية كأداة للدراسة.
- م. أفراد دراسات خاصة تركز على العناصر المكونة لنظام المعلومات الحاسوبي وخاصة: الأفراد، والإجراءات، والبيانات، والأجهزة والبرمجيات.
- ن. بحث كيفية معالجة مشكلة التخطيط في بيئة تكنولوجيا المعلومات، والاستحواذ على أدوات تكنولوجيا المعلومات وعلى مشكلة مراقبة أنظمة تكنولوجيا المعلومات، وأخيراً مشكلة أخلاقيات تكنولوجيا المعلومات.
- س. دراسة مدى انعكاسات تبني أنظمة تكنولوجيا المعلومات على نموذج التعليم الحاسوبي في الألفية الثالثة.
- ع. ضرورة استمرار جهود الباحثين في مجال تأثير بيئة تكنولوجيا المعلومات على أنظمة الرقابة الداخلية وخصوصاً البحث عن آثار تكنولوجيا المعلومات على إجراءات التدقيق الداخلية وإجراءات التدقيق الخارجية، ودراسة اتجاهات التطور في معايير التدقيق الداخلية ومعايير التدقيق الخارجية عند تبني أنظمة تكنولوجيا المعلومات.



المصادر والمراجع

قائمة المصادر والمراجع

أولاً: المصادر والمراجع باللغة العربية

المصادر:

- القرآن الكريم، سورة المجادلة، آية (11).

المراجع باللغة العربية

أولاً: الكتب:

1. أحمد، طارق عبد العظيم، (2010)، "استخدام الحاسبات في المؤسسة"، مكتبة الجامعة بأكتوبر - القاهرة، مصر.
2. البياتي، محمود مهدي (2005)، تحليل البيانات الإحصائية باستخدام البرنامج الإحصائي SPSS، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، الأردن.
3. توريه، حمدون، (2011)، "البحث عن السلام السيبراني"، الاتحاد الدولي للاتصالات (ITU)، جنيف، سويسرا.
4. الجواد، دلال صادق & والفتال، حميد ناصر، (2008)، "أمن المعلومات"، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن.
5. الحاج علي، عوض & وحسين، عبد الأمير، (2005)، أمنية نظم المعلومات وتقنيات التشفير، الطبعة الثانية، مطبعة جامعة النيلين، الخرطوم، السودان.
6. حجر، عبد الملك إسماعيل، (2009)، نظم المعلومات المحاسبية، الطبعة الثانية، الأمين للنشر والتوزيع، صنعاء، اليمن.
7. الحبيطي، قاسم محسن & والسقا، زياد هاشم، (2011)، نظام المعلومات المحاسبية، وحدة الحداية للطباعة والنشر، كلية الحداية الجامعة، الموصل، العراق.
8. الحميد، محمد دباس & ونيو، ماركو إبراهيم، (2007)، "حماية أنظمة المعلومات"، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، الأردن.
9. الحداد، وسيم وآخرون، (2011)، "الخدمات المصرفية الإلكترونية"، دار المسيرة للنشر والتوزيع والطباعة، عمان، الأردن.
10. حريز، سامي & وعبودي، زيد، (2008)، "إدارة الكوارث والمخاطر الأسس النظرية والتطبيقية"، الطبعة الأولى، دار الراية، عمان، الأردن.

11. الحمامي، علاء و العاني، (2007)، سعد، تكنولوجيا أمنية المعلومات وأنظمة الحماية، الطبعة الأولى، دار وائل للنشر والتوزيع، عمان، الأردن.
12. خالد، أبو ذر عثمان، (2011)، "سياسات أمن المعلومات"، الطبعة الأولى، المركز القومي للمعلومات، الخرطوم، السودان.
13. الدلاهمة، سليمان مصطفى، (2008)، "أساسيات نظم المعلومات المحاسبية وتكنولوجيا المعلومات"، الطبعة الأولى، مؤسسة الوراق للنشر والتوزيع، عمان، الأردن.
14. داود، حسن طاهر، (2004)، "أمن شبكات المعلومات"، مركز البحوث، معهد الإدارة العامة، الرياض، السعودية.
15. الذبيبة، زياد & الرمحي، نضال & الجعدي، عمر، (2011)، "نظم المعلومات في الرقابة والتدقيق"، الطبعة الأولى، دار المسيرة للنشر والتوزيع والطباعة، عمان، الأردن.
16. رملي، فياض حمزة، (2011)، "نظم المعلومات المحاسبية المحوسبة – مدخل معاصر لأغراض ترشييد القرارات الإدارية"، شركة مطابع السودان للعملة المحدودة، الأباي للنشر والتوزيع، الخرطوم، السودان.
17. الزعبي، محمد بلال & الطلافحة، عباس، (2004)، النظام الإحصائي SPSS- فهم وتحليل البيانات الإحصائية، الطبعة السادسة، دار وائل للنشر والتوزيع، عمان، الأردن.
18. السقا، زياد هاشم يحيى، (2011)، "نظام المعلومات المحاسبية"، الطبعة الثانية، دار الطارق للنشر والتوزيع، الموصل، العراق.
19. الشبلي، هيثم حمود، (2009)، "إدارة مخاطر الاحتيال في قطاع الاتصالات"، الطبعة الأولى، دار صفاء للنشر والتوزيع، عمان، الأردن.
20. شحادة، حسين خليل، (2012)، "مذكرات في اقتصاديات البيانات والمعلومات المحاسبية"، كلية الإدارة والاقتصاد، الأكاديمية العربية المفتوحة في الدنمارك، فرع الموصل، العراق.
21. طه، طارق، (2007)، "نظم المعلومات والحاسبات الآلية والإنترنت"، دار الفكر الجامعي، الإسكندرية، مصر.
22. الطيطي، خضر مصباح، (2010)، "أساسيات أمن المعلومات والحاسوب"، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، الأردن.
23. عاطف، عبد المنعم & الكاشف، محمد & سيد، كاسب، (2008)، "تقييم وإدارة المخاطر"، الطبعة الأولى، مركز تطوير الدراسات العليا والبحوث، جامعة القاهرة، مصر.
24. عبد الفتاح، محمد نجيب، وآخرون، (2009)، التحليل المعمق للبيانات باستخدام حزمة البرامج الجاهزة (SPSS)، جامعة الدول العربية، القاهرة، مصر.
25. الغنبر، خالد سليمان، & القحطاني، محمد عبد الله، (2009)، "أمن المعلومات بلغة ميسرة"، الطبعة الأولى، مركز التميز لأمن المعلومات، جامعة الملك سعود، الرياض، السعودية.
26. اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، (2009)، "بناء الثقة بالخدمات الإلكترونية في منطقة الإسكوا"، 10 مارس 2009.

27. منسي، محمود & و الشريف، خالد (2014)، التحليل الإحصائي للبيانات باستخدام برنامج SPSS- الجزء الأول، الطبعة الأولى، دار الجامعة الجديدة، الإسكندرية، مصر.
28. النجار، فايز جمعه، (2010)، "نظم المعلومات الإدارية: منظور إداري"، الطبعة الثالثة، دار الحامد للنشر والتوزيع، عمان، الأردن.
29. ياسين، سعد غالب، (2010)، تحليل وتصميم نظم المعلومات، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان، الأردن.

ثانياً: الدوريات:

1. أبوشيبة، إبراهيم علي & والفطيمي، محمد مفتاح، (2017)، "مخاطر استخدام نظم المعلومات المحاسبية الالكترونية - دراسة ميدانية على المصارف التجارية في بلدية مصراتة"، مجلة دراسات الاقتصاد والأعمال، المجلد (5)، عدد خاص، كلية الاقتصاد والعلوم السياسية، جامعة مصراتة، ليبيا، ص: 80-97.
2. أمرو، إسماعيل، (2006)، "أسباب ضعف الإجراءات الرقابية في نظم المعلومات المحاسبية - دراسة تحليلية"، مجلة تنمية الرفادين، المجلد (82)، العدد (28)، جامعة الموصل، العراق، ص: 21-42.
3. البحيصي، عصام محمد، (2011)، "استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة في الشركات الفلسطينية العاملة في قطاع غزة: دراسة تطبيقية"، مجلة الجامعة الإسلامية سلسلة الدراسات الإنسانية، المجلد (19)، العدد (1)، الجامعة الإسلامية، غزة، فلسطين، يناير 2011م، ص: 1147-1177.
4. البحيصي، عصام، (2014)، "مدى فعالية نظام الرقابة الداخلية في ظل نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على البنوك العاملة في قطاع غزة"، مجلة جامعة فلسطين للأبحاث والدراسات - العدد (6)، غزة، فلسطين، ص: 78-95.
5. بن علي، بلعوز، (2010)، "استراتيجيات إدارة المخاطر في المعاملات المالية"، مجلة الباحث، العدد (7)، جامعة الشلف، الجزائر، ص: 331-344.
6. الجبوري، ندى، (2011)، "حماية أمن أنظمة المعلومات دراسة حالة في مصرف الرفادين - فرع شارع فلسطين"، مجلة تكريت للعلوم الإدارية، العدد (21)، جامعة تكريت، العراق، ص: 72-94.
7. الجزراوي، إبراهيم & سعيد، لقمان، (2009)، "أدوات تكنولوجيا المعلومات ودورها في كفاءة وفاعلية المعلومات المحاسبية"، مجلة الإدارة والاقتصاد، العدد (75)، الجامعة المستنصرية، بغداد، العراق، ص: 1-36.
8. الجوهر، كريمة & والبلداوي، شاكر & والبياتي، محمود جلال، (2011)، "دور المدقق الداخلي والخارجي في إدارة مخاطر التكنولوجيا - دراسة تحليلية مقارنة"، مجلة الإدارة والاقتصاد، العدد (89)، الجامعة المستنصرية، بغداد، العراق، ص: 22-35.
9. الجوهر، كريمة & والعقده، صالح & وأبو سردانة، جمال، (2010)، "أثر مخاطر استخدام التكنولوجيا في جودة عمل المدقق الخارجي دراسة ميدانية في بعض مكاتب التدقيق الأردنية"، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد (10)، العدد (2)، جامعة الزرقاء، الأردن، ص: 14-32.
10. الحافظ، علي عبد الستار & والنعمي، أحمد هاني، (2010)، " دور (ISO 27001:2005) في تعزيز مفهوم إدارة دورة حياة المعلومات (نموذج مقترح)"، مجلة تكريت للعلوم الإدارية والاقتصادية، المجلد (6)، العدد (17)، جامعة تكريت، العراق، ص: 56-73.

11. الحسبان، عطا الله أحمد، (2009)، "مدى تعامل مدققي أنظمة تكنولوجيا المعلومات بمعايير التدقيق الدولية الخاصة ببيئة أنظمة المعلومات للمحافظة على أمن وسرية المعلومات في البنوك التجارية الأردنية"، مجلة كلية بغداد للعلوم الاقتصادية، الإصدار (20)، كلية بغداد للعلوم الاقتصادية، بغداد، العراق، ص ص: 341-385.
12. حسين، وسام نعمة & وزياب، محمد أحمد، (2018)، "مخاطر استخدام نظم المعلومات المحاسبية الالكترونية وأثرها على خصائص جودة المعلومات المحاسبية - دراسة استطلاعية"، مجلة تكريت للعلوم الإدارية والاقتصادية، المجلد (3)، العدد (43)، كلية الإدارة والاقتصاد، جامعة تكريت، العراق، ص ص: 45 - 65.
13. الحكيم، سليم، (2010)، "إمكانية الرقابة على نظم المعلومات المحاسبية المؤتمتة للمؤسسات العامة ذات الطابع الاقتصادي من قبل مفتشي الجهاز المركزي للرقابة المالية"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد (26)، العدد (1)، دمشق، سوريا، 2010، ص ص: 563-592.
14. حمادة، رشا، (2010)، "أثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الالكترونية في زيادة موثوقية المعلومات المحاسبية"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 26، العدد 1، جامعة دمشق، دمشق، سوريا، ص ص: 305-334.
15. حوري، زينب & وخضراوي، ساسية، (2013)، "معالجة مخاطر التكنولوجيا في أعمال المحاسبة والتدقيق"، مجلة العلوم الإنسانية، العدد (30-31)، جامعة محمد خيضر، بسكرة، الجزائر، مايو 2013، ص ص: 379-396.
16. خطاب، محمد & وأبو موسى، أحمد (2012)، "عوامل نجاح برامج أمن نظم المعلومات المحاسبية ودورها في تفعيل حوكمة الشركات: دراسة ميدانية على الشركات السعودية"، مجلة كلية التجارة للبحوث العلمية، العدد (1)-المجلد (49)، جامعة الإسكندرية، مصر.
17. الخضير، سليمان، (2013)، الشامل، مجلة دورية تصدر عن إدارة التسويق في مصرف اليمن البحرين الشامل، العدد (8)، صنعاء، اليمن، ص ص: 16-18.
18. الخطيب، محمد، (2012)، أمن المعلومات، الاجتماع الثاني لرؤساء الإدارات المختصة بتقنية المعلومات بالنيابات العامة العربية، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، بيروت، لبنان، 5-7 أيار مايو 2012.
19. خليل، عطا الله ورّاد، (2011)، "آليات أمن المعلومات في ظل الانفتاح المعلوماتي"، مجلة الفكر القانوني والاقتصادي، العدد 4، يوليو 2011، كلية الحقوق، جامعة بنها، مصر، ص ص: 589 - 641.
20. الدباغ، رائد & وزينل، بشرى، (2012)، "فاعلية التدريب في تحقيق نجاح أمن نظم المعلومات دراسة استطلاعية لآراء عينة من العاملين في نظم المعلومات بجامعة الموصل"، تنمية الرافيدين، مجلد 34، ملحق العدد 11، كلية الإدارة والاقتصاد، جامعة الموصل، العراق، ص ص: 123-140.
21. الدلاهمة، سليمان مصطفى، (2013)، "أثر مخاطر استخدام تكنولوجيا المعلومات على أداء نظم المعلومات المحاسبية من وجهة نظر مراجعي الحسابات في المملكة العربية السعودية"، مجلة جامعة القدس المفتوحة للأبحاث والدراسات، العدد (30)، فلسطين، ص ص: 11-36.

22. الدوغجي، علي حسين & والخيرو، إيمان، (2013)، "تحسين فاعلية نظام الرقابة الداخلية وفق أنموذج COSO"، مجلة العلوم الاقتصادية والإدارية، مجلد (19)، الإصدار (70)، كلية الإدارة والاقتصاد، جامعة بغداد، العراق، ص ص: 398-433.
23. الدوغجي، علي حسين، (2008)، "دور مراقب الحسابات في ظل تكنولوجيا المعلومات المعقدة ومخاطر التدقيق"، مجلة العلوم الاقتصادية والإدارية، المجلد (14)، العدد (52)، كلية الإدارة والاقتصاد، جامعة بغداد، العراق، ص ص: 285-304.
24. دهيرب، محمد سمير، (2012)، "تقييم أنظمة الرقابة الداخلية وفق مفهوم لجنة (COSO)"، مجلة الكوت للعلوم الاقتصادية والإدارية، العدد (6)، جامعة واسط، العراق، ص ص: 255-278.
25. الربيدي، محمد علي، (2012)، "تقييم نظام الرقابة الداخلية في المنشآت المستخدمة لتكنولوجيا المعلومات – دراسة ميدانية في مكاتب المراجعة اليمنية"، المجلة العربية للمحاسبة، العدد (15)، جامعة البحرين، تشرين أول (أكتوبر) 2012، ص ص: 89-122.
26. الربيدي، محمد علي، (2010)، "حماية المعلومات المحاسبية في ظل مخاطر التكنولوجيا للعمليات المصرفية الإلكترونية: دراسة ميدانية في البنوك العاملة في اليمن"، مجلة كلية التجارة والاقتصاد، العدد (33)، كلية التجارة والاقتصاد، جامعة صنعاء، صنعاء، اليمن، مارس 2010، ص ص: 1-46.
27. رشيد، ناظم حسن، (2011)، "دور مراقب الحسابات في إضفاء الثقة بالبيانات المحاسبية المنشورة على الانترنت في بيئة التجارة الإلكترونية"، مجلة تكريت للعلوم الإدارية والاقتصادية، المجلد (7)، العدد (23)، كلية الإدارة والاقتصاد، جامعة تكريت، ص ص: 173-197.
28. زبار، سلمان عبود، (2010)، "معايير تطوير نظام المعلومات الإدارية عبر شبكة المعلومات الدولية دراسة تطبيقية في شركة الفرات العامة للصناعات الكيماوية"، مجلة جامعة بابل للعلوم الإنسانية، المجلد 18، العدد (2)، 2010، ص ص: 343-367.
29. زويلف، إنعام، " (2009)، طبيعة تهديدات أمن نظم المعلومات المحاسبية الإلكترونية – دراسة تطبيقية على شركات التأمين الأردنية، المجلة العربية للمحاسبة، العدد (12)، جامعة البحرين، المنامة، البحرين، ص ص: 46-77.
30. الساكني، سعد عبد الكريم & والعواد، حنان علي، (2012)، "مخاطر استخدام تكنولوجيا المعلومات وأثرها على أداء نظم المعلومات المحاسبية – دراسة تطبيقية لعينة من الشركات المساهمة المدرجة في بورصة عمان للأوراق المالية، دراسات المعلومات، العدد (14)، جامعة الإمام محمد بن سعود، الرياض، السعودية، أيار (مايو) 2012، ص ص: 207-257.
31. شاهين، علي عبدالله، (2010)، "نظم الدفع الإلكترونية ومخاطرها ووسائل الرقابة عليها دراسة تطبيقية على بنك فلسطين"، مجلة جامعة الأزهر بغزة، مجلد (12)، العدد (1)، غزة، فلسطين، ص ص: 511-546.
32. شتيوي، أيمن أحمد، (2006)، "قياس تأثير بعد الصناعة على دور المراجع الداخلي في إدارة المخاطر المرتبطة بنظم المعلومات المحاسبية الآلية"، مجلة كلية التجارة للبحوث العلمية، كلية التجارة، جامعة الإسكندرية، المجلد 34، العدد 2، الإسكندرية، مصر، سبتمبر 2006، ص ص: 1-52.

33. الشحادة، عبدالرزاق & العاصي، سعد، (2009)، "إطار متكامل لتقييم كفاءة نظم المعلومات المحاسبية في المؤسسات المصرفية في ظل الأزمة المالية العالمية - دراسة ميدانية على المصارف العاملة بمدينة حلب"، مجلة كلية بغداد للعلوم الاقتصادية، العدد (20)، كلية بغداد للعلوم الاقتصادية، 2009، ص: 15-48.
34. الشرايري، عادل، (2009)، "سياسات وإجراءات التدقيق الداخلي في ظل بيئة تكنولوجيا المعلومات في البنوك الأردنية"، مجلة جامعة تشرين للبحوث والدراسات العلمية- سلسلة العلوم الاقتصادية والقانونية، المجلد (31)، العدد (1)، جامعة تشرين، اللاذقية، سوريا، ص: 47-72.
35. صيام، وليد زكريا، (2010)، "الرقابة الداخلية على تطبيقات نظم المعلومات المحاسبية الالكترونية"، مجلة المدقق، العدد 85-86، جمعية المحاسبين القانونيين الأردنيين، عمان، الأردن، أغسطس 2010، ص: 17-19.
36. الطنملي، سهير، (2009)، "دور الرقابة الداخلية في دعم وتفعيل أمن وسلامة المعلومات في البنوك الالكترونية والخلوية: الجزء الأول"، مجلة المال والتجارة، العدد (478)، نادي التجارة بشبين الكوم، المنوفية، مصر، ص: 27-48.
37. العبيدي، أسامة، (2012)، "جريمة الدخول غير المشروع إلى النظام المعلوماتي - دراسة قانونية في ضوء القوانين المقارنة"، دراسات المعلومات، العدد (14)، جامعة الإمام محمد بن سعود، الرياض، السعودية، أيار (مايو) 2012، ص: 9-68.
38. العرود، شاهر & والخاتنة، وحيد & والشرفاء، أمجد، (2011)، "تأثير تطبيق مدققي الحسابات لأساليب تكنولوجيا المعلومات على إتمام عملية التدقيق الالكتروني في الأردن"، مجلة المحاسبة والإدارة والتأمين، العدد رقم (78)، كلية التجارة، جامعة القاهرة، مصر، ص: 1-28.
39. عمران، جمال، (2008)، "أساليب الرقابة الداخلية في نظم المعلومات المحاسبية الإلكترونية"، مجلة تشرين للدراسات والبحوث العلمية سلسلة العلوم الاقتصادية والقانونية، المجلد 28 العدد 1، اللاذقية، سوريا.
40. عيسى، علا & وعاشور، عصافيت، (2010)، "مخاطر نظم المعلومات المحاسبية وحوكمة الشركات ومواجهة الأزمة المالية العالمية"، مجلة الفكر المحاسبي، المجلد (14)، العدد (2)، كلية التجارة، جامعه عين شمس، القاهرة، مصر، ص: 408-434.
41. الغنبر، خالد & والصبيح، أمل، (2012)، "حال أمن المعلومات في المملكة العربية السعودية"، دراسات المعلومات، العدد (14)، جامعة الإمام محمد بن سعود، الرياض، السعودية، أيار (مايو) 2012، ص: 189-205.
42. غنوم، أيمن، (2009)، "أمن المعلومات"، مجلة البنوك، جمعية البنوك في الأردن، عمان، الأردن، نسخة إلكترونية.
43. فاضل، عبدالكريم محمد يحيى، (2012)، "مدى تأثير استخدام الصيرفة الإلكترونية على فاعلية الرقابية التطبيقية لنظم المعلومات المحاسبية المحوسبة - دراسة ميدانية لدى البنوك التجارية اليمنية"، بحث مقبول للنشر، مجلة الباحث الجامعي، جامعة إب، اليمن.
44. القاسم، عبد الرزاق & العلي، أحمد، (2012)، "أثر تقانة المعلومات في تطوير نظم عمليات المصارف العامة في سوريا"، مجلة جامعة دمشق، مجلد (28)، العدد (1)، 2012، ص: 301-326.

45. قاسم، عبدالرزاق & الردايدة، مراد، (2010)، " أمن البيانات ونظم المعلومات المحاسبية في بيئة تكنولوجيا المعلومات في البنوك الأردنية -دراسة ميدانية "، المجلة العربية للعلوم الاقتصادية والإدارية، العدد (5)، كلية إدارة الأعمال والعلوم التجارية، جامعة الروح القدس، الكسليك، بيروت، لبنان، تشرين الأول (أكتوبر)، ص ص: 111-91.
46. قدومي، ثائر عدنان، (2010)، "الصيرفة الإلكترونية في المصارف التجارية الأردنية - دراسة تطبيقية لدور الخصائص الشخصية: المعوقات ومقومات النجاح"، المجلة العربية للإدارة، المجلد (30)، العدد (1)، يونيو 2010، عمان، الأردن، ص ص: 142-113.
47. القطناني، خالد محمود، (2007)، "أثر خصائص البيئة التقنية وتكنولوجيا المعلومات في مخاطر الرقابة التشغيلية- دراسة تحليلية في المصارف الأردنية"، مجلة المنارة، المجلد (13)، العدد (2)، جامعة آل البيت، المفرق، الأردن، ص ص: 39-9.
48. محمد، طارق مختار، (2011)، "تفعيل دور الرقابة الداخلية في الأنشطة المصرفية في ظل نظام المعلومات المحاسبية الإلكترونية"، المجلة العلمية للاقتصاد والتجارة، العدد (1)، كلية التجارة، جامعة عين شمس، القاهرة، مصر، ص ص: 665-578.
49. مشتهى، صبري ماهر & حمدان، علاء محمد & شكر، طلال حمدون، (2011)، "مدى موثوقية نظم المعلومات المحاسبية وأثرها في تحسين مؤشرات الأداء المصرفي دراسة مقارنة على المصارف الأردنية والفلسطينية المدرجة ببورصتي عمان ونابلس"، دراسات - العلوم الإدارية، المجلد 38، العدد 1، الجامعة الأردنية، عمان، الأردن، ص ص: 46-21.
50. الهادي، محمد، (2006)، " توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية "، cybrarians journal العدد (9)، أكاديمية السادات للعلوم الإدارية، القاهرة، مصر، حزيران (يونيو 2006)، <http://www.journal.cybrarians.org>
51. وادي، رشدي عبداللطيف، (2008)، "أهمية ومزايا البنوك الالكترونية في قطاع غزة بفلسطين ومعوقات انتشارها"، مجلة الجامعة الإسلامية- سلسلة الدراسات الإنسانية، مجلد(16)، العدد(2)، غزة، فلسطين، يونيو 2008، ص ص: 893-855.

ثالثاً: الأطروحات والرسائل الجامعية غير المنشورة:

1. حسين، أماني حسين، (2006)، " إطار مقترح لتقييم الرقابة الداخلية لأنشطة التجارة الإلكترونية"، أطروحة دكتوراه غير منشورة، جامعة حلوان، حلوان، مصر.
2. محمد، حيدر صاحب، (2011)، "مسؤولية مراقب الحسابات في تحديد وتقييم مخاطر تكنولوجيا نظم المعلومات المحاسبية لرفع جودة أدائه"، بحث مقدم كجزء من متطلبات نيل شهادة المحاسبة القانونية، هيئة أمناء المعهد العربي للمحاسبين القانونيين، الاتحاد العام للمحاسبين والمراجعين العرب، بغداد، العراق.
3. محمد، عصام الدين، (2017)، "مخاطر نظم المعلومات المحاسبية الالكترونية وأثرها على المراجعة الداخلية - دراسة حالة هيئة الموانئ البحرية"، رسالة ماجستير غير منشورة، كلية الاقتصاد والعلوم الإدارية، جامعة البحر الأحمر، السودان.

رابعاً: المؤتمرات والندوات العلمية:

1. أبو شنب، عماد، (2009)، "إدارة وتحليل مخاطر أمن المعلومات"، مؤتمر أمن المعلومات والحكومة الإلكترونية، كوالالمبور، ماليزيا، 12 - 16 ابريل (نيسان) 2009م. 1-18
2. الجوهر، كريمة & وجاسم، أحمد، (2013)، " إجراءات حوكمة تقنية المعلومات (نموذج مقترح في ضوء أهداف إطار COBIT)"، المؤتمر العلمي الدولي التاسع، "الوضع الاقتصادي العربي وخيارات المستقبل"، كلية الاقتصاد والعلوم الإدارية، جامعة الزرقاء، الأردن، للفترة 24 - 25 نيسان (أبريل) 2013م.
3. دبيان، السيد عبد المقصود، كشك، وليد السيد، (2002)، "الاتجاهات الحديثة في الرقابة الداخلية على أمن نظم المعلومات في ظل التجارة الإلكترونية ودور المعايير الدولية"، مؤتمر التجارة الإلكترونية: الأفاق والتحديات، كلية التجارة - جامعة الإسكندرية، مصر، 25-27 يوليو 2002، ص ص: 513-524.
4. الرضا، عقبة كامل، (2008)، "تدقيق الحسابات في ظل نظم المعلومات المحاسبية"، ورقة بحث ضمن الفعاليات العلمية لجمعية المحاسبين القانونيين السوريين، دمشق، سوريا، أيار (مايو) 2008، ص ص: 1-13.
5. زيدان، محمد & وحمو، محمد، (2010)، "متطلبات أمن المعلومات المصرفية في بيئة الإنترنت"، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية بعنوان "البيئة المعلوماتية الآمنة - المفاهيم والتشريعات والتطبيقات"، الرياض، السعودية، 6-7 نيسان (أبريل) 2010.
6. صقر، ممدوح الشحات، (2007)، "أمن المعلومات"، ندوة أمن وحماية نظم المعلومات في المؤسسات العربية، القاهرة، مصر، 3 - 7 يونيو 2007.
7. عبد القادر، عصماني، (2009)، "أهمية بناء أنظمة لإدارة المخاطر لمواجهة الأزمات في المؤسسات المالية"، الملتقى العلمي الدولي - "الأزمة المالية والاقتصادية الدولية والحوكمة العالمية"، كلية العلوم الاقتصادية وعلوم التسيير، جامعة فرحات عباس، سطيف، الجزائر، 20-21 تشرين الأول (أكتوبر)، 2009.
8. عميش، رحاب، (2009)، "الجريمة المعلوماتية"، المؤتمر العلمي المغربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ليبيا، 28 - 29 تشرين أول (أكتوبر).
9. مريم، بن الشريف، (2011)، "الأعمال المصرفية الالكترونية: الرهانات والتحديات وإشكالية الإشراف والرقابة المصرفية"، الملتقى العلمي الدولي الرابع "عصرنة نظام الدفع في البنوك الجزائرية وإشكالية اعتماد التجارة الإلكترونية في الجزائر - عرض تجارب دولية"، معهد العلوم الاقتصادية، المركز الجامعي خميس مليانة، الجزائر، 26-27 نيسان (أبريل) 2011.
10. المنصور، كاسر نصر، (2007)، " إدارة المخاطر واستراتيجية التأمين في ظل تكنولوجيا المعلومات"، المؤتمر العلمي الدولي السنوي السابع، إدارة المخاطر واقتصاد المعرفة، جامعة الزيتونة الأردنية، عمان، الأردن، 16-18 نيسان 2007.
11. يوسف، عبد الستار، (2007)، "تقدير المخاطرة في ظل تحليل (SWOT) في المؤسسات الصناعية- دراسة تحليلية"، المؤتمر العلمي الدولي السنوي السابع- إدارة المخاطر واقتصاد المعرفة، كلية الاقتصاد والعلوم الإدارية، جامعة الزيتونة الأردنية، الزرقاء، الأردن، 16-18 نيسان (أبريل) 2007.

خامساً: الوثائق الرسمية والمنشورات الحكومية:

1. الأمم المتحدة، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الأسكوا) ESCWA، (2009)، "بناء الثقة بالخدمات الإلكترونية في منطقة الإسكوا"، 10 آذار (مارس).
2. البنك المركزي اليمني، الإدارة العامة للبحوث والإحصاء، مجموعة تقارير ربع سنوية عن الأعوام : 2016-2012م، الإدارة العامة للبحوث والإحصاء، مطابع اليمن العصرية، صنعاء، اليمن.
3. البنك المركزي اليمني، (2003)، التعليمات الصادرة عن البنك المركزي اليمني إلى البنوك وشركات الصرافة، البنك المركزي اليمني، صنعاء، اليمن.
4. الجمهورية اليمنية، (2006)، القانون رقم (40) لعام 2006م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية، وزارة الشؤون القانونية، الجريدة الرسمية، العدد (24)، ديسمبر 2006، صنعاء، اليمن.
5. _____، القانون رقم (38) لسنة 1998م بشأن البنوك التجارية.
6. _____، القانون رقم (14) لسنة 2000م بشأن البنك المركزي اليمني.
7. _____، القانون رقم (35) لسنة 2003م بشأن غسل الأموال.
8. _____، القانون رقم (1) لسنة 2010م بشأن مكافحة غسل الأموال وتمويل الإرهاب.
9. _____، القانون رقم (13) لسنة 2012م بشأن حق الحصول على المعلومات.
10. الجمهورية اليمنية، وزارة الشؤون القانونية، (قانون رقم 38 لعام 1998 بشأن البنوك، الجريدة الرسمية، العدد 24، ج 2، & قانون رقم 14 لعام 2000 بشأن البنك المركزي اليمني، الجريدة الرسمية، العدد 12، ج 2).
11. الجمهورية اليمنية، (2016)، منشورات وبروشورات مختلفة، البنوك التجارية العاملة في الجمهورية اليمنية، صنعاء، اليمن.
12. البنك المركزي اليمني، (2013)، هيكل الجهاز المصرفي في اليمن، و مجموعة تقارير ربع سنوية عن العام 2012م، الإدارة العامة للبحوث والإحصاء، صنعاء، اليمن، www.ybrd.com.ye
13. جمعية البنوك اليمنية، (2012)، مجلة المصارف، العدد (6)، صنعاء، اليمن، كانون الأول (ديسمبر) 2012.
14. المنشورات والسجلات والتقارير السنوية لدى البنوك التجارية محل الدراسة من كانون ثاني 2012م وحتى نهاية كانون الأول (ديسمبر) 2016م.
15. النخبة للعلاقات العامة والإعلان، (2010)، الدليل المصرفي اليمني وشركات التأمين، صنعاء، اليمن، صفحات متفرقة.

سادساً: مواقع الكترونية من الانترنت:

1. البنك المركزي اليمني، موقع البنك على الشبكة العالمية للمعلومات (الانترنت):
<http://www.mpicyemen.org> 22/ 12/ 2012: 15:22:49 GMT
2. بن يحيى، عماد، (2012)، الهجمات الإلكترونية كأبزر المخاطر التي تهدد قطاع الأعمال، عالم التقنية، من الموقع: <http://www.tech-wd.com/wd/2012/09/08/kaspersky-global-it-security-risks-survey-report>

3. البواب، احمد إسماعيل، (2016)، "البنوك اليمنية ومواكبتها للعمليات المصرفية الإلكترونية"، تاريخ الاطلاع 2016/8/20 الساعة 11:33 صباحاً، من الموقع الإلكتروني لصحيفة 26 سبتمبر، <http://www.26sep.net/newsweekarticle.php?sid=6526>
4. حسنين، رجب عبد الحميد، (2012)، "أمن شبكات المعلومات الإلكترونية: المخاطر والحلول"، Cybrarians Journal، ع 30 (ديسمبر 2012). - تاريخ الاطلاع 30 - 7 - 2013 م، متاح في: http://www.journal.cybrarians.org/index.php?option=com_content&view=article&id=629:networks&catid=257:studies
5. عبدالرحيم، شريفة، (2013)، سباق القط والفأر بين البنوك والهاكرز، جريدة الاهرام الاقتصادي، القاهرة، مصر، 16 أيلول (سبتمبر)، 14:24، <http://economic.ahram.org.eg>
6. عبيد، أحمد يوسف (2008)، "إدارة مخاطر أمن المعلومات"، مقالة علمية متاحة على: <http://www.secureminds.net/Pages/articleRiskManagement.asp> تم الدخول بتاريخ 23 / 2 / 2011م الساعة 25 : 09 صباحاً.
7. القرني، ميسون محمد، (2007)، "أمن المعلومات المحاسبية"، كلية الحاسبات وتقنية المعلومات، جامعة الملك عبد العزيز، الرياض، السعودية، من الموقع: www.maysoon.ws/archives/420 ، بتاريخ 1-2-2014، س: 6:06 صباحاً.
8. قطينة، عدنان، (2016)، "الخدمات المصرفية الإلكترونية في اليمن والرقابة عليها"، دراسات وافكار، بتاريخ 2012/6/30، 5:14 مساءً، <http://adnanqatinah.blogspot.com/2010/06/electronic-banking-services-in-yemen.html>
9. المدرع، فهد فايز، (2012)، "المعايير العالمية لأمن المعلومات"، مركز التميز لأمن المعلومات، الرياض، السعودية، نسخة الكترونية، مستخرجة بتاريخ 2012-9-25، 8:36 مساءً.
10. المري، عايض، (2011)، امن المعلومات ماهيتها وعناصرها واستراتيجياتها، الدراسات والاستشارات القانونية، 6 نوفمبر 2011، http://www.dralmarri.com/show.asp?field=res_a&id=205
11. الهادي، محمد، (2006)، "توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية"، cybrarians journal، العدد (9)، أكاديمية السادات للعلوم الإدارية، القاهرة، مصر، حزيران (يونيو) 2006، <http://www.journal.cybrarians.org>
12. هوارى، معراج & عبيرات، مقدم "إدارة مخاطر الأمن وشفافية المعلومات لنظم المعلومات فى ظل البيئة الرقمية"، كلية الاقتصاد وعلوم التسيير، جامعة الأغواط، من الموقع: <http://www.docstoc.com/docs/145138300>

المراجع باللغة بالإنجليزية

Foreign References

FIRST: The Books:

1. Arens, Alvin A., Elder, Randal J., & Beasley, Mark S.,(2014), **Auditing & Assurance Services: An Integrated Approach**, 15th Edition, International Edition, Inc, Pearson Education, Inc. Prentice Hall, Upper Saddle Rivers: New Jersey, USA.
2. Bagranoff , Nancy A. & Simkin, Mark G. & Norman, Carolyn Strand,(2010), **Core Concepts of Accounting Information Systems** , 11th Edition , John Wiley & Sons, INC., U.S.A.
3. Bodnar , George H. & Hopwood, William S.,(2012), **Accounting Information Systems**, 11th Edition, Prentice Hall, New Jersey, USA.
4. Boczeko, T, (2012), **Introduction to Accounting Information Systems**, Pearson Education, England.
5. Calder, Alan & Watkins, Steve, (2008),**"IT Governance: A Manager's Guide to Data Security and ISO27001/ISO 27002"**, 4th Edition, KOGANPAGE, London, United Kingdom and Philadelphia, USA.
6. Dennis, Alan (2012), **Systems Analysis and Design with UML**, 5th Ed., John-Wiley & Sons, Inc. USA.
7. Federal Financial Institutions Examination Council (FFIEC),(2012), **"Audit"**, HANDBOOK, April 2012.
8. Gelinas, Ulric J. & Sutton, Steven G. & Hunton , James E.,(2012), **Accounting Information Systems** , 9th Edition, Thomson South-Western, Mason, Ohio, USA.
9. Hall, James A., (2013), **Accounting Information Systems**, 8th Edition, CENGAGE Learning, Lehigh University, Thomson, South-Western, Mason, Ohio, USA, THOMSON, South-Western, USA.
10. Jessup, Leonardand & Valanch, Joseph, (2008),**"Information Systems Today- Managing the Digital World"**, Pearson Prentice Hall, Inc, New Jersey, USA.
11. Laudon Kenneth C. & Laudon Jane P.,(2011), **"Management Information Systems- Managing The Digital Firm"** , 12th Ed., Prentice - Hall, Inc, New Jersey, USA.
12. Macedo, F., & Da Silva, M. M., (2016), **Comparative Study of Information Security Risk Assessment Models**. Universidad Técnica de Lisboa, Lisboa.
13. Miller, David R. et. al, (2011),**"Security Information and Event Management (SIEM) Implementation"**, McGraw Hill, Network Pro Library, New York, USA.
14. O'Brien. J. A, (2010),**"Management Information systems: Managing Information Technology in the E-Business Enterprise"**, 15th Ed., Boston: Irwin: Mc Graw-Hill Companies, Inc., USA.

15. Romney, Marshall B. & Steinbart, Paul J., (2015), "Accounting Information Systems", 13th Edition, England: Pearson Education (Pearson International Edition), Prentice Hall, New Jersey, USA.
16. Rose, Peter S. (2002), "Commercial Bank Management", 5th Edition, McGraw-Hill, Companies, Inc., Boston, USA.
17. Sekaran, Uma, (2003), "Research Methods for Business: A Skill-Building Approach", 4th Edition, John Wiley & Sons Inc., New York, USA.
18. Senft, Sandra & Gallegos, Frederick, (2009), "Information Technology Control and Audit", 3rd Edition, Taylor & Francis Group, LLC, Boca Raton – London – New York, USA.
19. Turner, Leslie & Weickgenannt, Andrea, (2013), "Accounting Information Systems: Controls and Processes", 2nd Edition, John Wiley & Sons, New Jersey, USA, <http://my.safaribooksonline.com/book/accounting/9781118162309>
20. Vacca, John R., (2009), "Computer and Information Security Handbook", 3RD Edition, Morgan Kaufmann Publishers is an imprint of Elsevier, USA.
21. Vaassen, Eddy H. J., (2005), "Accounting Information System- A managerial Approach", John Wiley & Sons Ltd, Chichester, England.

SECOND: The Periodicals:

1. Abdelhak, Djenane & Dalel, Hammoudi (2010), "Evaluation of the performance of the Financial and Accounting Computerized Information Systems in the Jordanian Banking Sector: An Empirical Study", Laboratoire Finances, Banques et Management, N0. 26, Université de Biskra, Algeria, PP: 1-17.
2. Abu-Khadra, Husam & Chan, Joseph & Pavelka, Deborah, (2012), "Incorporating the COBIT Framework for IT Governance in Accounting Education", Communications of the IIMA, Vol.12, No. 2, 2012, PP: 81-92.
3. Abu-Musa, Ahmad A., (2009), "Exploring COBIT Processes for ITG in Saudi Organizations: An empirical Study", The International Journal of Digital Accounting Research, Vol.9, PP: 99-126.
4. Abu-Musa, Ahmad A., (2010), "Investigating Adequacy of Security Controls in Saudi Banking Sector: An Empirical Study", Journal of Accounting-Business & Management, Vol. 17, No.1, PP:1-41.
5. Abu-Musa A. A., (2007), "Evaluating the Security Controls of CAIS in Developing Countries an Examination of Current Research", Information Management & Computer Security, Vol.15, No.1&2, PP: 46-63 & PP: 128-148, PDF Copy.
6. Abu-Musa, Ahmad A., (2006), "Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations", King Saud University Journal, Vol. 18, Computer and Information Science, Riyadh, Saudi Arabia, 2006, PP: 1-26.

7. Al-Ahmad, Walid & Mohammad, Bassil,(2013), "Addressing Information Security Risks by Adopting Standards", **International Journal Of Information Security Science**, Vol. 2, No 2, June 2013, PP: 28-43.
8. Anderson, Evan E. & Choobineh, Joobin, (2008),"Enterprise Information Security Strategies", **Computers & Security**, Vol. 27, No. (1-2), March 2008, PP: 22-29.
9. Anomah, Sampson & Agyabeng, Owusu, (2013), "Evaluating Internal Controls in A Computerized Works Environment – A Risk to Audit Professionals and A Challenge to Accountancy Training Providers", **Research Journal of Finance and Accounting**, Vol.4, No.1, PP: 132- 143. , www.iiste.org
10. Arsenie-Samoil, M. D. (2011). Security of the Accounting Information System Infrastructure. Ovidius University Annals, **Economic Sciences Series**, Vol. 11, No.1, PP: 1339-1345.
11. Ashenden, Debi, (2008), "Information Security management: A human challenge?", **Information Security Technical Report**, Vol.13, No.4, PP: 195 – 201.
12. Bafghi, A. A. S. T., (2014), "Status and Security of Accounting Information Systems in Iranian Organizations", **International Journal of Economy, Management and Social Sciences**, Vol. 3, No. 12, PP: 71-76.
13. Basharat, Iqra & Azam, Farooque & Muzaffar, Abdul Wahab, (2012)," Database Security and Encryption: A Survey Study", **International Journal of Computer Applications**, Volume 47– No.12, June 2012, National University of Sciences and Technology (NUST), Islamabad, Pakistan, PP: 888-975.
14. Al-Bashtawi, S. H., & Al-Husban, A. (2013). Determinants of Auditing Electronic Accounting Information Systems, A Case Study in the Jordanian Commercial Banks. **European Scientific Journal**, ESJ, Vol. 9, No. 10.
15. Belkhamza, Zakariya & Wafa, Syed Azizi, (2009), "The Effect of Perceived Risk on the Intention to Use E-commerce: The Case of Algeria", **Journal of Internet Banking and Commerce**, Vol. 14, No.1., April 2009, PP:1-9, available at <http://www.arraydev.com/commerce/jibc>
16. Beard, Deborah & Wen, H. Joseph, (2007),"Reducing the Threat Levels for Accounting Information System, Challenge for Management, Accountants, Auditors and Academicians", **The CPA Journal**, Publication of the New York state society of CPA, New York, USA, Vol. 77, No. 5, May 2007, PP: 34-42.
17. Benaroch, Michel & Chernobai, Anna & Goldstein, James, (2012),"An Internal Control Perspective on the Market Value Consequences of IT Operational Risk Events", **International Journal of Accounting Information Systems**, Vol.13, PP:357- 381, Contents lists Elsevier Available at: SciVerse ScienceDirect. <http://dx.doi.org/10.1016/j.accinf.2012.03.001>

18. Brandas, C. & Stirbu, D. & Didraga, O., (2013), "Integrated Approach Model of Risk, Control and Auditing of Accounting Information Systems", **Informatica Economică**, Vol. 17, No. 4, West University of Timisoara, Romania, PP: 87-95.
19. Brender, Nathalie & Markov, Iliya, (2013), "Risk perception and risk management in cloud computing: Results from a case study of Swiss companies", (2013), **International Journal of Information Management**, No.33 2013, PP:726– 733, <http://www.elsevier.com/locate/ijinfomgt>
20. Breier, Jakub & Hudec, Ladislav, (2012), "Towards a Security Evaluation Model Based on Security Metrics ", **International Conference on Computer Systems and Technologies , CompSysTech'12**, 22-23 June 2012, Ruse, Bulgaria.
21. Chen, Pei-yu et al., (2011), "Correlated Failures, Diversification and Information Security Risk Management", **MIS Quarterly**, Vol. 35 No. 2, June 2011, U.S.A., PP: 397-422.
22. Christopher, Joe & Sarens, Gerrit & Leung, Philomena, (2009), "A critical Analysis of the Independence of the Internal Audit Function: Evidence from Australia", **Accounting, Auditing & Accountability Journal**, Vol. 22, No.2, PP: 200-220.
23. Choi, M., & Lee, C., (2015), " Information security management as a bridge in cloud systems from private to public organizations", **Sustainability**, Vol.7, No.9, PP: 12032-12051.
24. Colwill, Carl, (2009), "Human Factors in Information Security: The Insider Threat e Who Can You Trust These Days?", **Information Security Technical Report**, Vol. 14, No.4, November 2009, PP: 186-196.
25. Dalci, I. & Tanis, V. (2009), "Benefits of Computerized Accounting Information Systems on the JIT Production Systems", **Review of Social Economic & Business Studies**, Vol.2, PP: 45-64.
26. Dai, Weihui, (2012), "Risk Management Model of Information Security in IC Manufacturing Industry", **Journal of Computers**, Vol. 7, No. 2, February 2012, PP: 317-324.
27. Daru, M. U., (2015), "Role of computerized accounting in banking sector", **International Journal of Advanced Research in Management and Social Sciences**, Vol. 4, No.2, PP: 26-34.
28. Da Veiga, A & Eloff, J.H.P, (2010), "A framework and Assessment Instrument for Information Security Culture", **Computer & Security**, Vol.29, No.4: 196-207.
29. Disterer, Georg, (2013), "ISO/IEC 27000, 27001 and 27002 for Information Security Management", **Journal of Information Security**, No.4, PP: 92-100.

30. Drew, Jeef,(2013), "Data, security take top two spots in AICPA technology priorities survey: Organizations must know where their critical information is stored, moved, and processed", **Journal of Accountancy**, AICPA, USA.,
<http://www.journalofaccountancy.com/News/20137879> (accessed on 13 September 2013).
31. Drtil , Jan, . (2013)" Impact of Information Security Incidents - Theory and Reality", **Journal of Systems Integration**, NO.1, University of Economics, Prague, Czech Republic, PP: 44-52.
32. Eloff, J. H. P. & Eloff M. M., (2005), "Information Security Architecture", **Computer Fraud & Security**, Vol. 2005, No.11, November 2005, PP: 10-16.
33. Fardinal,(2013), "The Quality of Accounting Information and The Accounting Information System through The Internal Control Systems: A Study on Ministry and State Agencies of The Republic of Indonesia", **Research Journal of Finance and Accounting**, Vol.4, No.6, PP: 156-161.
34. Fang, J., & Shu, L. (2016). Modern Accounting Information System Security (AISS) Research Based on IT Technology, **Advanced Science and Technology Letters**, Vol.121 (AST 2016)
35. Feng, Nan & Wang, Harry & Li, Minqiang,(2013), "A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis", **Information Sciences**, Vol. xxx, 2013, PP: 1-17,
<http://dx.doi.org/10.1016/j.ins.2013.02.036>
36. French, Aaron M., (2012), "A Case Study on E-Banking Security – When Security Becomes Too Sophisticated for the User to Access Their Information", **Journal of Internet Banking and Commerce**, Vol. 17, No.2, August 2012, PP: 1-15.
37. Gerić, Sandro & Hutinski, Željko, (2007), Information System Security Threats Classifications, **Journal of Information and Organizational Sciences**, Vol. 31, No. 1, University of Zagreb, Croatia, PP: 59-60.
38. Gehrmann, Maico,(2012), "Combining ITIL, COBIT and ISO/IEC 27002 for Structuring Comprehensive Information Technology for Management in Organizations", **Navus - Revista de Gestão e Tecnologia. Florianópolis**, SC, Vol. 2, No. 2, Jul. 2012, PP: 66-77.
39. Greenberg, Robert & Li, Wei & Wong-On-Wing, Bernard, (2012), "The effect of trust in system reliability on the intention to adopt online accounting systems", **International Journal of Accounting and Information Management**, Vol. 20, No. 4, PP: 363-376.

40. Hamdan, M. N., & Hosban, A. (2015). *The Role of the Auditor in Planning and Reduce the Risk of IT Environment in Commercial Jordanian Banks*. **International Journal of Economics and Finance**, 7(11), 222, PP:295-304.
41. Al Hanini , Eman , (2015), *Evaluating the Reliability of the Internal Control on the Computerized Accounting Information Systems: An Empirical Study on Banks Operating in Jordan*. **Research Journal of Finance and Accounting**, ISSN 2222-1697 (Paper) ISSN 2222-2847 (Online) www.iiste.org
42. Al Hanini, Eman,(2012), "*The Risks of Using Computerized Accounting Information Systems in the Jordanian Banks: Their Reasons and Ways of Prevention*", **European Journal of Business and Management**, Vol. 4, No.20, PP: 53-63, www.iiste.org
43. Hayale, Talal H. & Abu-Khadra, Husam A., (2008), "*Investigating Perceived Security Threats of Computerized Accounting Information Systems an Empirical Research applied on Jordanian banking sector* ", **Journal of Economic & Administrative Sciences**, Vol. 24, No. 1, UAE, June 2008, PP: 41-67.
44. Hayale, Talal H. & Abu-khadra, Husam A., (2006), "*Evaluation of the Effectiveness of Control Systems in Computerized Accounting Information Systems: An Empirical Research Applied on Jordanian Banking Sector*", **Journal of Accounting – Business & Management**, No. 13, PP:39-68.
45. Hossin, A. M. & Ayedh, A. M. , (2016) , "*The Risks of Electronic Accounting Information System in The Central Bank of Libya*", **South East Asia Journal of Contemporary Business, Economics and Law**, Vol. 10, Issue 1 (Aug.2016), ISSN: 2289-1560 , PP:74-79.
46. Hunker, J. & Probst, C., (2011), "*Insiders and Insider Threats – An Overview of Definitions and Mitigation Techniques*," **Journal of Wireless Mobile Networks**, Ubiquitous Computing and Dependable Applications, Vol. 2, No. 1, March 2011, PP: 4-27.
47. Hulitt, Elaine & Vaughn, Rayford B., (2010), "*Information system Security Compliance to FISMA Standard: A Quantitative Measure*", **Telecomm un Syst** , No. 45, PP: 139–152.
48. Joseph, Rhoda & Jeffers, Patrick, (2009), "*E-Government in the Caribbean Nations*", **Journal of Global Information Technology Management**, Vol. 12, No. 1, PP: 52-71.
49. Kasasbeh, F. I. O., & Thuneibat, N. S. M. (2018). *The Ability of Computerized Accounting Information Systems in Saudi Public Universities to Face Cyber Threats*, **International Review of Management and Marketing**, Vol. (8), No. (3), PP: 19-25.
50. Kazemi, Mehdi et al., (2012), "*Evaluation of Information Security Management System Success Factors: Case Study of Municipal Organization*", **African Journal of Business Management** , Vol. 6, No. 14, April 2012, PP: 4982-4989, Available online at <http://www.academicjournals.org/AJBM>

51. Khambhammettu, Hemanth, et al., (2013), "A framework for risk assessment in access control systems", **computers & Security**, Vol. xxx, 27 February 2013, PP: 1-18.
52. Knapp, Kenneth J. et al., (2009), "Information Security Policy: An Organizational-Level Process Model", **Computers & Security**, Vol. 28, No. 7, PP: 493-508, available at www.sciencedirect.com
53. Kolb, Nancy & Abdullah, Faisal, (2009), "Developing an Information Security Awareness Program for a Non-Profit Organization", **International Management Review**, Vol. 5, No. 2, PP: 105-110.
54. Koskosas, Ioannis & Koskosa, Maria-Mirela, (2011), "Internet Banking Security Management through Trust Management", **World of Computer Science and Information Technology Journal (WCSIT)**, Vol. 1, No. 3, PP:79-87.
55. Kritzinger, E & Smith, E., (2008), "Information Security Management: An Information Security Retrieval and Awareness Model for Industry", **Computer & Security**, Vol.27, No.5-6, PP:224 – 231.
56. Al-Laith, Ali, (2012), "Adaptation of the Internal Control Systems with the Use of Information Technology and its Effects on the Financial Statements Reliability: An Applied Study on Commercial Banks", **International Management Review**, Vol. 8, No. 1, 2012, PP: 12-19.
57. Lendle, Klaus, (2008), "Performance Management in Internal Audit: Implementation, Merits and Challenges in A Medium-Sized Audit Department", **Journal of Securities Law, Regulation & Compliance**, Nov, Vol. 2 Issue 1, 2008, PP: 62-67.
58. Lo, Chi-Chun & Chen, Wan-Jia, (2012), "A Hybrid Information Security Risk Assessment Procedure Considering Interdependences Between Controls", **Expert Systems with Applications**, No.39, PP:247-257, <http://www.elsevier.com/locate/eswa>
59. Lin, Fengyi & Sheng, Olivia R.L. & Wu, Soushan, (2005), "An integrated Frame-work For E-Chain Bank Accounting Systems", **Industrial Management & Data Systems**, Vol. 105, No. 3, Emerald Group Publishing Limited, PP:291-306.
60. Madani, Haider H.,(2009), "The Role of Internal Auditors in ERP-Based Organizations", **Journal of Accounting & Organizational Change**, Vol. 5 No. 4, PP: 514-526, available at: www.emeraldinsight.com/1832-5912.htm

61. Malami, Abu Bakar & Zainol, Zaini & Nelson, Sherliza, (2012), "Security Threats of Computerized Banking Systems (CBS): The Manager's Perception in Malaysia", **International Journal of Economics and Finance Studies**, Vol. 4, No. 1, 2012, PP: 21-30.
62. Maram, Venkata et al., (2012), "A Study of Risk Management of an Information System by Assessing Threat, Vulnerability and Countermeasure", **International Journal of Advanced Research in Computer Science and Software Engineering**, Vol. 2, No. 12, December 2012, PP: 51-53.
63. Mihalache, Arsenie, (2011), "Security of the Accounting Information System Infrastructure", **Annals of the "Ovidius" University, Economic Sciences Series**, Volume XI, No.1, PP:1339-1345, <http://ideas.repec.org/a/ovi/oviste/v11y2011i1p1339-1345.html>
64. Mohamed, Intan Salwani et. al, (2012), "Assessing Drivers for Organizational Commitment Towards the Security Controls Implementation in The Malaysian Online Service in Computer-Based Accounting System", **Advances in Natural and Applied Sciences**, 6 (8), PP: 1223-1237.
65. Muhrtala, Tijani & Ogundeji, Mathias, (2013), "Computerized Accounting Information Systems and Perceived Security Threats in Developing Economies: The Nigerian Case. **Universal Journal of Accounting and Finance**, Vol.1, No.1, PP: 9-18.
66. Murtaza, Mirza B. (2007), "Developing An IT Risk Assessment Framework", **Review of Business Information Systems**, Vol.11, No.4, Middle Tennessee State University, USA, PP:69-75.
67. Năstase, Pavel & Unchiașu, Simona, (2013), "Implications of the Operational Risk Practices Applied in the Banking Sector on the Information Systems Area", **Accounting and Management Information Systems**, Vol. 12, No. 1, PP: 101-117.
68. Nikolić, Božo & Ružić-Dimitrijević, Ljiljana, (2009), "Risk Assessment of Information Technology Systems", **Issues in Informing Science and Information Technology**, Vol. 6, PP:1-21.
69. Olasanmi, Omoneye & Olufunke, Lecturer, (2010), "Computer Crimes and Counter Measures in the Nigerian Banking Sector", **Journal of Internet Banking and Commerce**, Vol. 15, No.1, April 2010, PP: 1-10.
70. Orakzai, T. (2014). **COBIT, ITIL and ISO 27002 Alignment for Information Security Governance in Modern Organisations**, Electronic copy available at: <http://ssrn.com/abstract=2385845>
71. Osunmuyiwa, Olufolabi, (2013), "Online Banking and the Risks Involved", **Research Journal of Information Technology**, Vol. 5, No. (2), June 2013, PP: 50-54.

72. Parakkattu, Sindhuja & Kunnathur, Anand. S., (2010), "A Framework for Research in Information Security Management", **Northeast Decision Sciences Institute Proceedings (NEDSI)**, March 2010, PP: 318-323.
73. Palfi, Cristina & Mureşan, Mariana, (2009), "Survey on Weaknesses of Banks Internal Control Systems", **Journal of International Finance & Economics**, Vol. 9, Issue 1, PP: 106-116.
74. Pandey, Santosh K., (2012), "A Comparative Study of Risk Assessment Methodologies for Information Systems", **Buletin Teknik Elektro dan Informatika**, Vol.1, No.2, June 2012, PP: 111-122, <http://journal.uad.ac.id/index.php/EEI/index>
75. Alramahi, N. M., Barakat, A. I., & Haddad, H. (2014), Information Technology Governance Control Level in Jordanian Banks Using: Control Objectives for Information and Related Technology (COBIT 5), **Information Technology**, Vol. 6, No.5, PP: 194-206.
76. Rees, Jackie & Allen, Jonathan, (2008), "The State of Risk Assessment Practices in Information Security: An Exploratory Investigation, **Journal of Organizational Computing and Electronic Commerce**, No. 18, USA, PP: 255–277.
77. Rubino, M., et. Al., (2017), "How IT controls improve the control environment", **Management Research Review**, Vol.40, No.2, PP: 218-234.
78. Ross, Steven, (2011), "Information Security Matters", **SACA Journal**, Vol.6, PP: 1-2, Available Online: www.isaca.org/journal
79. Saleh, Mohamed & Alfantookh, Abdulkader, (2011), "A New Comprehensive Framework for Enterprise Information Security Risk Management", **Applied Computing and Informatics**, Vol. 9, King Saud University, Riyadh, Saudi, PP:107-118, <http://www.sciencedirect.com/science/journal/22108327>
80. Saleh, Zakaria I. & Refai, Heba & Mashhour, Ahmad, (2011), "Proposed Framework for Security Risk Assessment", **Journal of Information Security**, No.2, PP:85-90 doi:10.4236/jis.2011.22008 Published Online April 2011, <http://www.scirp.org/journal/jis>
81. Samukri, (2015), Influence Effectiveness of Internal Control System and Implementation of Financial Accounting Information System on the Quality of Accounting Information, **Research Journal of Finance and Accounting**, Vol.6, No.11, (Online) www.iiste.org
82. Sani, Alireza & Chaharmahalie, Shahram, (2012), "Internal Accounting Controls", **Engineering and Technology**, World Academy of Science, No. 62, 2012, PP: 54-57.
83. Shamszadeh, Bagher & Sharif, Abolfazl Azizi, (2012), "Computerized Accounting Information Systems (CAIS) Versus Security Threats", **Journal of Academic Research in Economics**, Vol. 4, No.1, March 2012, Islamic Azad University - Hamadan Branch, Iran, PP: 69-80.

84. Shahri, Ahmad & Ismail, Zuraini & Rahim, Nor, (2012), "Security Effectiveness in Health Information System: Through Improving the Human Factors by Education and Training", **Australian Journal of Basic and Applied Sciences**, Vol. 2, No. 12, 2012, PP: 226-233.
85. Shamala, Palaniappan & Ahmad, Rabiah & Yusoff, Mariana, (2013), "A conceptual Framework of Info Structure for Information Security Risk Assessment (ISRA)", **Information Security and Applications**, Vol. 18, No. 1, PP: 45-52.
86. Sharairi, Jamal & Lababidi, Mohammad, (2011), "Factors Affecting the Role of Internal Auditor in the Protection of Computerized Accounting Information Systems from Electronic Penetration-A Field Study on Banks Operating in Jordan", **International Research Journal of Finance and Economics**, Issue 68, EuroJournals Publishing, Inc. 2011, PP:140-161.
87. Al-Shbiel, Mohanad & Bani Ahmad, Audeh, (2013), "The Risks of Communication Between Department of Internal Control & Computer and Its Impact on the Efficiency of the Accounting Information Systems in the Commercial Banks", **Interdisciplinary Journal of Contemporary Research in Business**, Vol 4, No 11, PP:297-303.
88. Siponen, Mikko & Willison, Robert, (2009), "Information Security Management Standards: Problems and Solutions", **Information & Management**, Vol.46, No.5, PP: 267–270.
89. Soudani, Siamak, (2013), "The Impact of Implementation of E-Accounting System on Financial Performance with Effects of Internal Control Systems", **Research Journal of Finance and Accounting**, Vol.4, No.11, PP:17-27, <http://www.iiste.org>
90. Steinbart, Paul John, (2012), "The Relationship Between Internal Audit and Information Security: An Exploratory Investigation", **International Journal of Accounting Information Systems**, Vol. 13, No. 3, September 2012, PP: 228-243.
91. Stroie, E. R. & Rusu, A. C., (2011), "Security Risk Management - Approaches and Methodology", **Informatica Economica**, Vol. 15, No.1, Academy of Economic Studies, Bucharest, Romania, PP: 228- 240.
92. Sun, L. & Srivastava, R. & Mock, T.J., (2015), "An Information Systems Security Risk Assessment Model Under Dempster-Shafer Theory of Belief Functions", **Journal of Management Information systems**, Vol. 22, No.4, PP:109-142.
93. Tarmidi, M., et al., (2013), "Computerized Accounting Systems Threats in Malaysian Public Services", **International Journal of Finance and Accounting**, Vol. 2, No.2, PP: 109-113.
94. Teru, S. P., & Hla, D. T. (2015). Appraisal of Accounting Information System and Internal Control Frameworks. **International Journal of Scientific and Research Publications**, Volume 5, Issue 9, ISSN 2250-3153, www.ijsrp.org

95. Tofan, Dan, (2011), "Information Security Standards", **Journal of Mobile, Embedded and Distributed Systems**, Vol. III, No.3, Academy of Economic Studies Bucharest, Romania, PP:128-135.
96. Tuttle, Brad & Vandervelde, Scott D., (2007), "An Empirical Examination of Cobit As An Internal Control Framework for Information Technology", **International Journal of Accounting Information Systems**, Vol.8, PP:240-263.
97. Van Niekerk, J.F. & Von Solms, R., (2010), "Information security culture: A management perspective", **Computer & Security**, Vol.29, No.4, PP: 476-486.
98. Veiga, A. Da & Eloff, J.H.P., (2010), "A Framework and Assessment Instrument for Information Security Culture", **Computers & Security**, No. 29, PP:196-207.
99. Von Solms, Rossouw & Niekerk, Johan van, (2013), "From information security to cyber security", **Computers & Security**, No. 38, Elsevier Ltd. All rights reserved, PP: 97-102.
100. Wahyudi, Ilham, (2016), "Do Risk Controls and User's Competence Affecting Accounting Information System Quality?." **I J A B E R**, Vol. 14, No. 3, PP: 1561-1569.
101. Wallace, Linda et al., (Spring 2011), Information Security and Sarbanes-Oxley Compliance: An Exploratory Study, **Journal of Information System**, Vol. 25, No. 1, American Accounting Association, USA, PP: 185-211.
102. Warkentin, Merrill & Willison, Robert, (2009), "Behavioral and Policy Issues in Information Systems Security: The Insider Threat", **European Journal of Information Systems**, Vol. 18, PP: 101-105, www.palgrave-journals.com/ejis/
103. Werlinger, R. & Hawkey, K. & Beznosov, K, (2009), "An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management", **Information Management & Computer Security**, Vol. 17, No.1, PP: 4-19.
104. Wood, C.C. & Banks, W.W., (2003), "Human error: an overlooked but significant information security problem", **Computers & Security**, Vol.12, No.1,2003, PP: 51-60.
105. Yang , L.H.,(2011), "Information Security in Network Finance and Its Countermeasures", **Engineering Education and Management**, LNEE, Springer-Verlag Berlin Heidelberg , PP: 651-656. <http://aisel.aisnet.org/pacis2007/74> ACCESSED ON 8/2012
106. Zafar, Humayun, (2013), "Human resource information systems: Information security concerns for organizations", **Human Resource Management Review**, No. 23, PP: 105-113, <http://dx.doi.org/10.1016/j.hrmr.2012.06.010>

107. Zainol, Zaini & Nelson, Sherliza & Malami, AbuBakar, (2012), "Internal Human Based Threats and Security Controls in Computerized Banking Systems: Evidence from Malaysia", **Procedia - Social and Behavioral Sciences**, No. 65, PP: 199 –204, Available Online at: www.sciencedirect.com
108. Zhiwei, Yu & Zhongyuan, Ji, (2012), "A Survey on the Evolution of Risk Evaluation for Information Systems Security", **Energy Procedia**, Vol. 17, PP:1288-1294.
109. Zimucha, Tafadzwa et. al, (2012), "An Evaluation of the Effectiveness of E-banking Security Strategies in Zimbabwe: A Case Study of Zimbabwean Commercial Banks", **Journal of Internet Banking and Commerce**, Vol. 17, No.3, December 2012, PP: 1-16.
110. Al-Zwyalif, Inaam M., (2013), "IT Governance and its Impact on the Usefulness of Accounting Information Reported in Financial Statements", **International Journal of Business and Social Science**, Vol. 4, No. 2, February 2013, PP: 83-94.

THIRD: Unpublished PhD. and Master's theses

1. Al-Awadi, Maryam, (2009), "A Study of Employees' Attitudes Towards Organizational Information Security Policies in the UK and Oman", **PhD thesis**, Glasgow University, Glasgow, UK.
2. Darragh, Warren J., (2009), "An Analysis of Information Security in Selected Australian Organizations", **Master of Information Technology (Research)**, University of Southern Queensland, Australia
3. Rafique, Rajia & Mehmood, Furhan, (2010), "Management of Operational Risks Related to Information Security in Financial Organizations", **Master Thesis in IT Management**, School of Sustainable Development of Society and Technology (HST).
4. Tayeh, A., (2008), "Effectiveness of Information Security Management at the Palestinian Information Technology Companies", **Master Thesis**, Islamic University of Gaza, Palestinian.

FIFTH: : Conferences Proceedings, Reports and Surveys

1. Černá, Marie, (2012), "Information Risks and Their Connection with Accounting", **6th European Conference on Information Management and Evaluation**, Faculty of Economics - University of West Bohemia, Pilsen, Czech Republic, 2012.
2. Dahbur, Kamal & Mohammad, Bassil & Tarakji, Ahmad, (2011), "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing", **International Conference on Intelligent Semantic Web-Services and Applications**, New York, USA.

3. Gunawardana, K. D. (2015). *An empirical investigation of the computerized accounting information systems frauds in licensed banks in Sri Lanka*. **Proceedings of the 1st International Conference in Accounting Researchers and Educators (ICARE 2015)**, October 09, 2015. Department of Accountancy, University of Kelaniya, Sri Lanka. pp 1-21.
4. Hypponen, Mikko, (2013), "Cyber Threats Unlikely to Disappear, Says Security Researcher", **INFOSEC 2013**, 23-25 April 2013, London, UK.
5. Jouini, M., & Rabai, L. B. A. (2016). *Comparative Study of Information Security Risk Assessment Models for Cloud Computing systems*. *Procedia Computer Science*, 83, **The 6th International Symposium on Frontiers in Ambient and Mobile Systems**, PP: 1084-1089.
6. Mansour, Ebrahim et. Al., (2009), "Examine the Existence of (Sys Trust) Model and its Impact on Jordanian Commercial Banks Performance", **European And Mediterranean Conference on Information Systems**, 13~14 July 2009, Crown Plaza Hotel, Izmir, Turkey.
7. Mihalache, Arsenie, (2011), "**Risk Analysis of Accounting Information System Infrastructure**", Working Papers Series, Faculty of Economics and Business Administration Alexandru Ioan Cuza University, Iași România, 10 February 2011.
8. Mishra, Sushma & Dhillon, Gaurpreet, (2008), "Defining Internal Control Objectives for Information Systems Security: A Value Focused Assessment", **Virginia Commonwealth University, ECIS 2008 Proceedings**. Paper 210,
<http://aisel.aisnet.org/ecis2008/210>
9. Munteanu, Adrian, (2006), "Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma", *Managing Information in Digital Economy: Issues & Solutions*, **Proceedings of the 6th International Business Information Management Association (IBIMA) Conference**, Faculty of Economics and Business Administration, Alexandru Ioan Cuza University, Romanian, 19-21 June, PP: 227-232.
10. Munteanu, A. & Fotache, D. & Dospinescu, O., (2008), "Information Systems Security Risk Assessment. Harmonization with International Accounting Standards", **International Conference on Innovation in Software Engineering –ISE'2008**, 10 – 12 December 2008, University of Canberra, Vienna – Austria.
11. Olivia, (2011), **Difference Between Standard and Framework**. Available to:
<http://www.differencebetween.com/difference-between-standard-and-vs-framework/> , (3-5-2011).

12. Poepjes, Robert & Lane, Michael, (2012), "An Information Security Awareness Capability Model (ISACM)", **10th Australian Information Security Management Conference (SECAU 2012)**, 3-5 Dec 2012, Perth, Western Australia.
13. Whitman, M. E. & Mattord, H. J., (2010), "The Enemy Is still at the Gates: Threats to Information Security Revisited", **the 2010 Information Security Curriculum Development Conference**, Kennesaw State University, USA, 1-3 October 2010, PP:95-99.

Sixth: Government

1. Bonnette, Cynthia A., (2006), **"Assessing Threats to Information Security in Financial Institutions"**, SANS Technology Institute, 31 May 2006, USA.
2. The Office of the Government Chief Information Officer, (2012), **"Security Risk Assessment & Audit Guidelines"**, Version:5.0, The Government of the Hong Kong Special Administrative Region, September 2012.

Seventh: WEB SITE

1. American Institute of Certified Public Accountants & Canadian Institute of Chartered Accountants, (AICPA), (2012), **COBIT 5 for Information Security - Preview Version**, Printed in the United States of America, USA, <http://www.isaca.org/cobit5info-sec>
2. Basel Committee on Banking Supervision (BCBS), (2012), **"Core Principles for Effective Banking Supervision"**, Bank for International Settlement (BIS), Basel, Switzerland, September 2012, PP: 1-85, www.bis.org
3. Basel Committee on Banking Supervision (BCBS), (2003), **Risk Management Principles for Electronic Banking**, Bank for International Settlement (BIS), Basel, Switzerland, July 2003, PP: 6-22. www.bis.org
4. Committee of Sponsoring Organization of the Tread-way Commission (COSO), (2004), **Enterprise Risk Management- Integrated Framework: Executive Summary**, AICPA, New York, USA, September 2004, PP: 1-7, http://www.coso.org/IC-Integrated_Framework-summary.htm
5. Committee of Sponsoring Organization of the Tread-way Commission (COSO), (2013), **"Internal Control-Integrated Framework"**, Tread-way Commission, New Jersey, USA, Available from http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf
6. DELOITTE, (2009), **International Financial Reporting Standards**, Electronic Version, Available at: <http://www.Iasplus.com/fs/29modelfs.pdf>

7. Denis, Elizabeth Gasiorowski, (2011), "**Are Information Security Risks Threatening Your Business? New and Improved ISO/IEC 27005 Standard Beefs Up Protection**", http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref145
8. Humphreys, Edward, (2010), "**Information Security Risk Management, Handbook for ISO/IEC 27001**", British Standards Institution (BSI), Available at: <http://shop.bsigroup.com/bip0076> (Accessed May 14, 2012).
9. IFAC, IAASB, (2009), Handbook of International Auditing, Assurance, and Ethics pronouncements, International Federation of Accountants, New York, USA.
10. International Federation of Accountants (IFAC), (2012), "**Effective Governance, Risk Management, and Internal Control**", <https://www.ifac.org/publications-resources/effective-governance-risk-management-and-internal-control> node-19388 (Accessed on 25 December 2012).
11. Information Systems Audit and Control Association (ISACA), (2012), "**COBIT 5 for Information Security - Preview Version**", Printed in the United States of America, USA, <http://www.isaca.org/cobit5info-sec>
12. Information Systems Audit and Control Association (ISACA), (2009), "**An Introduction to the Business Model for Information Security**", Printed in the United States of America, USA, Available at: <http://www.isaca.org> Accessed on 8-12-2012.
13. ISACA (Information Systems Audit and Control Association) (2009) "**The Risk IT Practitioner Guide**", Printed in the United States of America.
14. The ISO 27000 Directory (2013), "**An Introduction to ISO 27001, ISO 27002....ISO 27008, ISO /IEC**", available at: <http://www.27000.org> (Accessed July 14, 2013).
15. ISO/IEC 27000, (2012), "**Information Technology - Security techniques -Information security management systems - Overview and vocabulary**", ISO /IEC, Available at: <http://www.27000.org> (Accessed July 14, 2013).
16. ISO/IEC 27001:2005, (2013), "**Information Technology - Security Techniques - Information Security Management Systems - Requirements**", 2nd Ed., International Standards Organization and International Electro technical Commission (ISO/IEC), Geneva, Switzerland.
17. ISO/IEC 27005, (2008), "**Information Technology - Security Techniques -Information Security Risk Management**", International Standards Organization and International Electro technical Commission (ISO/IEC), Geneva, Switzerland.

18. Jaisingh, Jeevan & Rees, Jackie, (2001), "**Value at Risk: A Methodology for Information Security Risk Assessment**", Krannert Graduate School of Management, Purdue University, West Lafayette, PP:3-4. Available at:
https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/bibtex_archive/2001-127.pdf
19. National Institute of Standards and Technology: NIST, (2012), "**Guide for Conducting Risk Assessments**", Special Publication (SP) 800-30 Revision. 1, July 2012
20. National Institute of Standards and Technology (NIST), (2011), "**Managing Information Security Risk-Organization, Mission, and Information System View**", Special Publication (SP) 800-39, March 2011, Available at <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>
21. National Institute of Standards and Technology (NIST), (2006), "**Risk Management Guide for Information Technology Systems**", Special Publication (SP) 800-30, USA.
22. National Institute of Standards and Technology (NIST), (2010), "**Standards for Security Categorization of Federal Information and Information Systems**", February Available at <http://www.Nist.Gov> as 19/2/ 2010 at 08:15:00 PM GMT, PDF Copy.
23. Organization For Economic Co-Operation And Development (OECD), (2002), "**OECD Guidelines for the Security of Information Systems and Network: Towards a Culture of Security**", The Council of the OECD, Paris, France, 25 July 2002, PP:1-30, Retrieved 22 April 2013, at <http://www.oecd.org/dataoecd/16/22/15582260.pdf>
24. Wikipedia, (2014), http://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Information_Security_and_Risk_Management Accessed 26/02/2014, in 08:33 GMT.

الملاحق

ملحق رقم (1) قائمة الاستقصاء



الجمهورية العربية السورية

جامعة دمشق

كلية الاقتصاد

قسم المحاسبة

--	--	--

رقم استمارة الاستقصاء:

الأخوة/ القائمون بالعمل في الإدارات المالية والرقابة الداخلية وإدارة المخاطر والتشغيل الإلكتروني في البنك الأكارم
الأخ / المراجع الخارجي لنظام المعلومات المحاسبي للبنك..... المحترم

تحية طيبة واحتراماً وبعد:

يتعلق هذه الاستقصاء بأطروحة دكتوراه في المحاسبة يُجرى تحضيرها حالياً والموسومة ب:

« تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية »

في الجمهورية اليمنية – "دراسة تطبيقية"

وكما هو العهد بكم دوماً الاهتمام الكبير والاستعداد الدائم لموازرة الأبحاث العلمية التي تخدم تطور المجتمع، فإننا نأمل في تعاونكم من خلال الإجابة على الأسئلة المرفقة لما لذلك من أهمية في تحقيق أهداف الدراسة والوصول إلى نتائج واقعية ومن ثم الخروج بتوصيات تساعد في الارتقاء بفعالية وكفاءة أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية.

لذا يُرجى مُنكم التكرم بالإجابة على أسئلة الاستقصاء بدقة وعناية وموضوعية، ونؤكد لكم بأن كافة الإجابات ستعامل بسرية تامة ولن تُستخدم إلا ضمن إطار البحث العلمي فقط، كما أنه سيتم تزويدكم بنسخة من نتائج هذه الدراسة إن شاء الله تعالى إذا رغبتم بذلك.

شاكرين لكم حسن تعاونكم سلفاً وتفضلوا بقبول فائق الاحترام والتقدير،،،،،

الباحث :

عبد الكريم محمد يحيى فاضل

طالب دكتوراه في قسم المحاسبة

كلية الاقتصاد – جامعة دمشق

Fathel_Karem4@hotmail.com

Fathel_Karem4@yahoo.com

GSM: 00967711797934

* ملاحظة: فيما يلي توضيح لمفهوم بعض المصطلحات التي قد ترد في الاستقصاء:

- **نظام التشغيل على أساس الدفعات:** هو النظام الذي يتم فيه تشغيل البيانات بالدفعات بعد استكمال جميع البيانات ذات العلاقة خلال فترة محددة، ويعرف باسم التغذية البعيدة، حيث يتم تجميع مجموعات من البيانات وتحويلها إلى وسط إدخال ما، في مواقع بعيدة عن الحاسوب، وأجهزة الإدخال والإخراج بهذه المواقع تسمى محطات الإدخال والإخراج البعيدة.
- **نظام التشغيل الفوري والمباشر:** هو النظام الذي يتم فيه تشغيل البيانات بشكل مباشر وفي نفس الوقت، حيث تتم تغذية البيانات من الطرفيات مباشرة إلى نظام الحاسوب، ويتم استرجاعها بشكل مباشر، وتتميز هذه المعالجة بأن مخرجاتها تكون متاحة وبسرعة كافية لمواجهة احتياجات الإدارة للمعلومات.
- **نظام التشغيل الموزع:** هو النظام الذي يتم فيه معالجة البيانات بشكل متكامل عن طريق قاعدة البيانات المشتركة والمتصلة بشبكة البنك، وبرامج المعالجة الخاصة بالمستفيد، ويتم إنجازها عن طريق عدة حاسبات متصلة اتصالاً داخلياً بواسطة شبكة اتصالات خاصة، بالإضافة إلى الاعتماد على حاسب مركزي كبير أو على حاسبات مستقلة تماماً (لا مركزية) ولكنها متناسقة بخطة شاملة لإدارة موارد المعلومات.
- **الصيرفة الإلكترونية عبر الهاتف:** تقديم الخدمات المصرفية على مدار الساعة ومن خلال التليفون المحمول باستخدام العميل لرقم سري يتيح له الدخول إلى حسابه للاستعلام عن أرصده وكذلك للخصم منه تنفيذاً لأي من الخدمات المصرفية المطلوبة، والحصول على معلومات تخص الحساب من خلال الرسائل القصيرة، ومن هنا ظهر البنك الخليوي (أو البنك الناطق)، وبنوك مرسل (SMS).
- **الصيرفة عبر شبكة الانترنت:** تقديم الخدمات المصرفية بواسطة شبكة الإنترنت، حيث يقوم العميل بإدارة حساباته أو إنجاز أعماله المتصلة بالبنك عبر شبكة الانترنت من أي مكان وفي أي وقت، والحصول على الخدمات المختلفة بواسطة رقم سري يمكنه من الدخول على حسابه وإجراء استعلام أو عمليات مالية، وتندرج هنا الخدمات المصرفية الفورية أو الخدمات المصرفية من المنزل.
- **الصيرفة الإلكترونية عبر نقاط البيع:** تقديم خدمة مصرفية تمكن العميل من أداء مدفوعات من خلال الخصم على حسابه إلكترونياً بتمرير بطاقات ذكية داخل الآلات المتصلة إلكترونياً بحاسب البنك والمنشرة لدى المنشآت التجارية والخدمية بمختلف أنواعها وأنشطتها.
- **جدران النار (Fire-Walls):** هي عبارة عن مجموعة من الأجهزة والبرمجيات التي تقوم بعملية فصل الشبكات الخاصة للبنك عن الشبكات العامة حيث تقوم بعملية تصفية البيانات التي تنتقل من الشبكة العالمية (الإنترنت) إلى الشبكة المحلية للبنك حيث تتلقى البيانات والمعلومات المسموح بها فقط، بعد فحص مصدرها وغايتها، لضمان أمن تدفق البيانات من وإلى النظام.
- **الشهادة الرقمية (Digital Certificate):** عبارة عن وثيقة إلكترونية يتم إعدادها والتوقيع عليها رقمياً من قبل طرف ثالث موضع ثقة، يشهد في تلك الوثيقة بهوية مالك المفتاح العام الذي يظهر اسمه في تلك الشهادة.
- **تشفير البيانات (Data Encryption):** هو عبارة عن تحويل البيانات ومحتويات الملفات إلى شفرة سرية من أجل حفظها في قاعدة البيانات أو نقلها عبر الشبكات، ويتم ذلك من خلال تحويل البيانات من صورة نصية عادية إلى كلام غير مقروء لتحقيق سرية البيانات.
- **التوقيع الرقمي (Digital Signature):** هو عبارة عن جزء مشفر يتخذ هيئة حروف أو أرقام أو رموز إشارات أو غيرها ويمكن التعرف من خلاله على المنشأة وتمييزه وتحديد هويته وتأكيد على موافقته على محتوى البيانات المرسله ويستخدم للتأكد من أن الرسالة قد جاءت من مصدرها دون تعرضها لأي تغيير أثناء عملية النقل، وبذلك يتم تأمين سلامة الرسالة والتحقق من صحتها.
- **بروتوكولات التبادل الآمن للمعلومات:** هي مجموعة الأسس والقواعد والإجراءات التي يجب الالتزام بها عند تنفيذ التراسل ما بين أجهزة شبكة معينة.

الجزء الأول: معلومات أساسية عن المُجيب:

* يُرجى التَّكْرَمُ بوضع إشارة (✓) في المكان الذي تراه مناسباً:

1- مؤهلك العلمي:

ثانوية عامة فما دون	دبلوم متوسط	بكالوريوس	دبلوم عالي	ماجستير	دكتوراه	مؤهل آخر (يرجى تحديده)
						

2- تَفْصُّكُ العلمي:

محاسبة	إدارة أعمال	إدارة عامة	تمويل ومصارف	اقتصاد	علوم حاسوب	تخصص آخر (يرجى تحديده)
						

3 - المسمى الوظيفي الذي تشغله:

مدير مالي أو نائبه	رئيس قسم حسابات	مراجع داخلي	مدير إدارة المخاطر	رئيس قسم الحاسوب	مبرمج النظام	مشغل النظام	مراجع خارجي	مفتش بنك مركزي أو مراقب عام	وظيفة أخرى (يرجى تحديدها)
									

4- عمرك يقع في الفئة العمرية:

أقل من 25 سنة	من 25 إلى أقل من 35 سنة	من 35 إلى أقل من 45 سنة	من 45 إلى أقل من 55 سنة	55 سنة فأكثر

5- عدد سنوات خبرتك في التعامل مع نظم المعلومات الحاسوبية:

أقل من 3 سنوات	من 3 إلى أقل من 6 سنوات	من 6 إلى أقل من 10 سنوات	من 10 إلى أقل من 15 سنة	15 سنة فأكثر

6- عدد الدورات التدريبية التي تلقيتها في نظم المعلومات الحاسوبية وتكنولوجيا المعلومات:

أقل من 3 دورات	من 3 إلى أقل من 6 دورات	من 6 إلى أقل من 10 دورات	من 10 إلى أقل من 15 دورة	15 دورة فأكثر

الجزء الثاني: معلومات أساسية عن البنك ونظام المعلومات الحاسبي المستخدم فيه:

يرجى التكرم بوضع إشارة (✓) في المكان الذي تراه مناسباً:

1- إسم البنك الذي تعمل به: 2. سنة تأسيس البنك الذي تعمل فيه:

3- جنسية البنك:	أ. يمني	ب. عربي غير يمني	ج. أجنبي
4- ملكية البنك:	أ. عام	ب. خاص	ج. مختلط
5- الشركة المصممة للنظام المستخدم:	أ. يمنية	ب. عربية غير يمنية	ج. أجنبية

6- نسبة عدد العاملين في تشغيل النظام الحاسبي إلى إجمالي عدد العاملين في البنك:

أقل من 10%	من 10% إلى أقل من 20%	من 20% إلى أقل من 30%	من 30% إلى أقل من 40%	أكثر من 40%

7- الفترة الزمنية التي مضت على استخدام الحاسوب وبرمجياته في تشغيل نظام المعلومات الحاسبي لديكم:

أقل من 4 سنوات	من 4 إلى أقل من 8 سنوات	من 8 إلى أقل من 12 سنة	من 12 إلى 16 سنة	أكثر من 16 سنة

8- يتوفر في بنككم دائرة لإدارة مخاطر أمن نظم المعلومات الحاسبية تتبع مباشرة:

مجلس الإدارة	الإدارة التنفيذية	التدقيق الداخلي	إدارة أخرى (يرجى ذكرها)	لا توجد إدارة لمخاطر أمن نظم المعلومات
				

9 - الخدمة المصرفية الالكترونية الأكثر تعرضاً لمخاطر أمنية في البنك هي المقدمة باستخدام:

موظفي النظام مباشرة	الصراف الآلي	الهاتف الخليوي	شبكة الإنترنت	نقاط البيع	خدمة أخرى (يرجى تحديدها)
					

10-- عدد أجهزة الحاسوب العاملة على الشبكة الداخلية لنظام المعلومات الحاسبي في البنك:

أقل من 20 جهاز	من 20 إلى أقل من 40 جهاز	من 40 إلى أقل من 60 جهاز	من 60 إلى أقل من 80 جهاز	80 حاسوب فأكثر

11- نظام المعلومات الحاسبي الحوسب المستخدم في البنك هو:

نظام تشغيل على أساس الدفعات	نظام تشغيل فوري ومباشر	نظام تشغيل موزع	نظام آخر (يرجى ذكره).
			

12- نظام المعلومات الحاسبي الخاص في البنك مرتبط بشبكة على مستوى:

شبكة معلومات محلية تربط بين الأقسام (إنترنت)	شبكة معلومات محلية تربط بين الفروع (إكسترنال)	شبكة معلومات عالمية (إنترنت)

الجزء الثالث: بيانات تتعلق بمتغيرات الدراسة:

المحور الأول: مخاطر أمن نظم المعلومات المحاسبية المحوسبة: يُرجى قراءة الفقرات التالية جيداً ووضع إشارة (✓) في الخانة التي تُعبّر عن رأيك وبما يعكس الواقع الحالي والقائم لديكم.

مخاطر أمن نظم المعلومات المحاسبية المحوسبة					درجة حدوث الخطر
عالية جداً	عالية	متوسطة	منخفضة	منخفضة جداً	
أولاً: مخاطر أمن الأفراد العاملين في نظم المعلومات المحاسبية:					
					1 قيام بعض موظفي نظم المعلومات باستغلال صلاحياتهم في هذه النظم في خدمة أغراضهم الشخصية بما يتعارض والسياسات الموضوعية من قبل الإدارة والمختصين.
					2 انتحال صلاحيات شخص مخول بأي طريقة من الطرق نتيجة إهمال المستخدم، والثقة المتبادلة بين الموظفين التي تجعلهم يستخدمون كلمات السر فيما بينهم.
ثانياً: مخاطر الأمن المادي لنظم المعلومات المحاسبية المحوسبة:					
					3 حدوث تلف جزئي أو تدمير كلي لأجهزة ومعدات النظام المادية.
					4 حدوث أعطال في المكونات المادية والبرمجية للنظام.
ثالثاً: مخاطر أمن الوصول البرمجي لقاعدة بيانات نظم المعلومات المحاسبية المحوسبة:					
					5 الوصول البرمجي غير المصرح به إلى برامج النظام والملفات في قاعدة البيانات بواسطة أفراد من داخل البنك بقصد الإضرار والتخريب.
					6 الوصول البرمجي، غير المصرح به إلى برامج النظام والملفات في قاعدة البيانات بواسطة أفراد أو جهات من خارج البنك، لإنجاز عمليات (تعديل/تدمير/كشف/نسخ وسرقة/استخدام) بطريقة غير مشروعة.
					7 تلف بعض ملفات البيانات والبرامج ونظم التشغيل نتيجة تعرض قاعدة البيانات لنظم المعلومات المحاسبية المحوسب للإصابة بالبرامج الخبيثة مثل (الفيروسات، والديدان، وبرامج التجسس).
رابعاً: مخاطر أمن النسخ في وسائط غير متصلة بقاعدة بيانات النظام:					
					8 ضياع أو سرقة وسائط تخزين البيانات والبرامج الاحتياطية غير المتصلة بقاعدة بيانات نظام المعلومات المحاسبية المحوسب.
					9 الوصول غير المصرح به للبيانات والبرامج المخزنة في وسائط غير متصلة بنظام المعلومات المحاسبية المحوسب.
خامساً: مخاطر تهديد أمن عمليات مدخلات نظم المعلومات المحاسبية:					
					10 الحذف أو التعديل المتعمد لمصادر بيانات مدخلات صحيحة بواسطة الأفراد العاملين في نظام المعلومات المحاسبية.
					11 الحذف أو التعديل غير المتعمد لمصادر بيانات مدخلات صحيحة بواسطة الأفراد العاملين في نظام المعلومات المحاسبية.
					12 الإدخال المتعمد لبيانات غير سليمة أو مكررة من قبل العاملين في نظام المعلومات المحاسبية، للقيام بعمليات غير مصرح بها.
					13 الإدخال غير المتعمد لبيانات غير سليمة أو مكررة من قبل العاملين في نظام المعلومات المحاسبية، نتيجة السهو وعدم المعرفة.
					14 التأخير المقصود في إدخال بعض البيانات بواسطة العاملين في نظام المعلومات المحاسبية.
					15 التأخير غير المقصود في إدخال بعض البيانات بواسطة العاملين في نظام المعلومات المحاسبية.

مخاطر أمن نظم المعلومات الحاسوبية					درجة حدوث الخطر				
					عالية جداً	عالية	متوسطة	منخفضة	منخفضة جداً
سادساً: مخاطر أمن عمليات تشغيل نظم المعلومات الحاسوبية المحوسبة:									
16	إهدار وسرقة وقت تشغيل بعض أجهزة الحاسوب المستخدمة في نظام المعلومات الحاسوبي من خلال استغلالها في الأغراض الشخصية.								
17	تعديل أو حذف البيانات بطريقة مقصودة نتيجة حدوث احتيال وغش من قبل مستخدم نظام المعلومات الحاسوبي أثناء عمليات التشغيل.								
18	تعديل أو حذف البيانات بطريقة غير مقصودة نتيجة حدوث أخطاء من قبل مستخدم نظام المعلومات الحاسوبي أثناء عمليات التشغيل.								
19	حدوث عمليات تشغيلية غير مكتملة لبيانات محاسبية تم إدخالها.								
سابعاً: مخاطر أمن مخرجات نظم المعلومات الحاسوبية المحوسبة:									
20	حذف وإخفاء بنود معينة من مخرجات نظام المعلومات الحاسوبي وإنتاج مخرجات مظلمة غير سليمة.								
21	الكشف غير المخول به للمعلومات الحاسوبية أثناء عرضها على الشاشات أو طباعتها على الورق أو أثناء التخلص منها بعد استخدامها								
22	توجيه وتوزيع وتسليم بعض البيانات والمعلومات الحاسوبية لأشخاص غير مخولين باستلام نسخة منها أو لا تتوفر فيهم الأمانة.								
23	سرقة وسوء استخدام مخرجات النظام (المعلومات الحاسوبية) من قبل القائمين على النظام واستغلالها في أغراض شخصية.								
ثامناً: مخاطر أمن تبادل البيانات عبر شبكات نظم المعلومات الحاسوبية المحوسبة:									
24	انقطاع وتوقف تدفق البيانات والمعلومات المحولة إلكترونياً عبر شبكات الحاسوب من المركز الرئيسي للبنك إلى الفروع أو العكس.								
25	اعتراض وصول البيانات المرسله عبر الشبكات من أجهزة الخوادم لأجهزة المستخدمين، وتعرضها أحياناً للكشف أو التعديل، أو السرقة.								
26	اختراق مواقع الويب الخاص ببيانات البنك والتجسس على خطوط الاتصالات الخاصة بنقل البيانات.								
27	إنكار بعض الأطراف المتعاملة مع البنك للبيانات والمعلومات الحاسوبية المتبادلة إلكترونياً.								
28	حدوث أخطاء معينة غير مقصودة أثناء نقل البيانات كإرسال بيانات أو معلومات عن طريق الخطأ إلى موقع آخر.								
تاسعاً: مخاطر أمن تعديل وتطوير نظم المعلومات الحاسوبية المحوسبة:									
29	يتم إجراء تغييرات للنظام وبرامجه بطريقة غير مسموح بها، من قبل أشخاص غير مخولين بذلك، للقيام بعمليات تلاعب واحتيال لاحقة.								
30	حدوث أخطاء في عدم استكمال التعديلات المطلوبة أثناء عمليات التعديل والتطوير.								

المحور الثاني: الأسباب الداخلية لمخاطر أمن نظم المعلومات المحاسبية: يُرجى قراءة الفقرات التالية جيداً ووضع إشارة (✓) في الخانة التي تُعبّر عن رأيك وبما يعكس الواقع الحالي والقائم لديكم.

الأسباب الداخلية للمخاطر التي تهدد أمن نظم المعلومات المحاسبية					موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
أولاً: فلسفة الإدارة العليا للبنك:									
31	لا تدرك الإدارة العليا للبنك أهمية أمن نظم المعلومات المحاسبية، فلا تدعم الجهة المعنية بتطبيق السياسات الأمنية مادياً أو معنوياً.								
32	عدم وجود سياسات وخطط إدارية واضحة ومعتمدة ومعلنة وموثقة لإدارة مخاطر أمن نظم المعلومات المحاسبية في البنك.								
33	عدم قيام إدارة البنك بإصدار قرارات وتشريعات خاصة فعالة للحد من مخاطر أمن نظم المعلومات المحاسبية، ومعاينة الموظفين المخلين بتلك القواعد.								
34	شعور إدارة البنك بعدم جدوى تقييم مخاطر أمن نظم المعلومات المحاسبية، لاعتقادها بأن تكلفة تطبيق إجراءات الحماية أكبر من عوائدها المتوقعة.								
35	لا تقوم الإدارة بمشاركة الأقسام المختصة لبحث أفضل السبل لمواجهة تلك المخاطر.								
36	امتناع الإدارة العليا للبنك عن الإفصاح عن تلك المخاطر والخسائر المترتبة عنها، خوفاً من اهتزاز الثقة بسمعة البنك وبمركزه المالي.								
ثانياً: أسباب وعوامل تنظيمية:									
37	عدم وجود إدارة أو قسم أو لجنة مستقلة، لها صلاحيات كافية لتقييم ومتابعة مخاطر أمن نظم المعلومات المحاسبية، بهدف حماية تلك النظم.								
38	غياب التوصيف الدقيق للوظائف والذي يحدد المسؤوليات والصلاحيات لكل موظف داخل الهيكل التنظيمي للبنك.								
39	الفصل غير الواضح بين المهام المتعلقة بنظم المعلومات المحاسبية في البنك، كإشراك بعض العاملين باستخدام نفس كلمات السر أو تبادلها بينهم، مما قد يهدر مبدأ تقسيم العمل.								
40	النقص الكبير في الموظفين المختصين بأمن نظم المعلومات والذي تتوفر فيهم الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المتعددة والمطلوبة لذلك.								
41	صعوبة وعدم كفاية تدريب وتأهيل وتوعية الموظفين في مجال تقنيات وأساليب أمن نظم المعلومات، وعدم توافق التدريب مع التطور المستمر لبرامج أمن نظم المعلومات.								
42	الاهتمام غير الكافي بفحص التاريخ الوظيفي والمهني للموظفين الجدد مما قد يؤثر على قاعدة وضع الرجل المناسب في المكان المناسب.								
ثالثاً: أسباب متعلقة بإمكانات البنك التكنولوجية:									
43	تقدم الأجهزة والبرامج المستخدمة وضعف فاعليتها في حفظ وتشغيل البيانات وإنتاج المعلومات وتدقيقها وتخزينها واسترجاعها بسهولة ودقة وسرعة.								
44	الصعوبة في إيجاد التوليفة المثلى للأجهزة والبرامج وأجهزة الدعم المساندة لها بعناية، لتحديث وتطوير الأنظمة، بما يؤمن تحقيق أهداف النظام وتأمين عناصر الرقابة.								
45	وجود أخطاء في تصميم البرامج والتطبيقات المحاسبية المستخدمة تؤدي إلى إنتاج معلومات خاطئة أو غير دقيقة لفترات طويلة.								
46	عدم كفاية عمليات الصيانة الدورية لأجهزة الحاسوب والبرمجيات المستخدمة في تشغيل وحماية نظم المعلومات المحاسبية المحوسبة.								
47	اعتماد البنك في الحصول على الأجهزة والبرامج، والدعم الفني لها على مزودين قليلي الخبرة، ولا يتم التقييم المستمر لوضعهم في السوق.								

الأسباب الداخلية للمخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة					موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
48	عدم التوافق والتوافق ما بين الأنظمة والتطبيقات الموجودة لدى البنك مع الأنظمة والتطبيقات الخاصة بالمنشآت التي قد يتم ربط أنظمة البنك معها.								
رابعاً: أسباب تتعلق بالأفراد العاملين في نظم المعلومات المحاسبية المحوسبة:									
49	سوء استخدام الصلاحيات الواسعة المخولة لبعض الأفراد المسؤولين عن تشغيل النظام ممن لديهم معرفة واسعة بتفاصيل النظام، وعدم التزامهم بالإجراءات المحددة لحمايته.								
50	ضعف إدراك بعض العاملين بالنظام لمهامهم الموكلة لهم (كنسيان كلمة المرور للدخول للنظام، أو السماح لزملاء باستخدامها)، مما يترتب عليها أخطاء فادحة عند التشغيل.								
51	إهمال بعض العاملين بنظام المعلومات المحاسبي وعدم بذلهم العناية المهنية الكافية لأداء العمل، لنقص التأهيل والخبرة والوعي الرقابي.								
52	ارتفاع مستوى خبرة بعض العاملين في مجال التشغيل الإلكتروني، وزيادة معرفتهم أكثر من غيرهم بنقاط الضعف في الضوابط الرقابية المطبقة، مما ينتج عن ذلك مخاطر للنظام.								
53	التصرفات الانتقامية للأفراد الغاضبين سواء أثناء عملهم بسبب معاقبتهم أو بعد إنهاء خدماتهم بسبب فصلهم من العمل، حيث يقوموا بالكشف عن بعض المعلومات السرية.								
54	انخفاض معدل دوران موظفي أنظمة المعلومات لدى البنك، واحتفاظهم بأسرار الأنظمة ومفاتيح الحل وعدم تعاونهم مع زملائهم في تبادل المعرفة والخبرة.								
خامساً: أسباب متعلقة بضعف الرقابة الداخلية وإدارة المخاطر في البنك:									
55	عجز التدابير الأمنية لنظم المعلومات، وعدم كفاية وفعالية الأدوات والضوابط والإجراءات الرقابية المطبقة في البنك لحماية أمن نظام المعلومات المحاسبي.								
56	ضعف كفاءة وفعالية نظم الرقابة الداخلية للبنك وعدم إصدار تقارير رقابية دورية حول الأنظمة الآلية، ليتم متابعتها وتقييمها لمواكبة التطورات التي تجري لمواجهة المخاطر.								
57	عدم كفاءة وفعالية إجراءات إدارة المخاطر، وعدم القيام بالتقييم الذاتي لمخاطر أمن نظم المعلومات بحيث يقوم كل موظف بتحديد المخاطر التي يواجهها وتقييم إجراءات مواجهتها.								
58	غياب المسار المرئي للمراجعة فعدم رؤية عمليات إدخال البيانات وتشغيلها سهل من تغيير أو إضافة أو حذف أي بيانات دون ترك أثر يدل على ذلك، وصعوبة اكتشاف ذلك.								
سادساً: أسباب تتعلق بحدوث كوارث داخلية في البنك غير طبيعية:									
59	حدوث كوارث غير طبيعية من البيئة الداخلية للبنك (كالتخريب، والحريق، وانقطاع الكهرباء، وتسريب المياه)، تسبب تلك الكوارث تلف جزئي أو تدمير كلي لموارد النظام.								

المحور الثالث: الأسباب الخارجية لمخاطر أمن نظم المعلومات المحاسبية المحوسبة: يُرجى قراءة الفقرات التالية جيداً ووضع إشارة (✓) في الخانة التي تُعبر عن رأيك وبما يعكس الواقع الحالي والقائم لديكم.

الأسباب الخارجية للمخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة					موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
أولاً: التغيير التكنولوجي غير المتوازن:									
60	التطورات التكنولوجية السريعة والهائلة والمتلاحقة والتي تلي وضع الإجراءات الرقابية في البنك، فتقدم التقنية خارجياً أسرع من ممارسة الأمن داخل البنك.								
61	عدم وجود استقرار نسبي لنظام المعلومات، بسبب ارتفاع معدلات التغيير في تكنولوجيا المعلومات، مقابل ضعف إمكانيات البنك المالية والبشرية لمجاراتها واستيعابها.								
62	تصميم أساليب للتلاعب تبنى داخل النظام المحاسبي الإلكتروني يصعب اكتشافها، تؤدي إلى إنتاج معلومات محاسبية خاطئة.								
63	عدم توفر بنية تحتية تكنولوجية قوية في الجمهورية اليمنية.								
ثانياً: الكوارث الطبيعية والسياسية:									
64	حدوث الكوارث الطبيعية والبيئية كالزلازل، والبراكين، والفيضانات والسيول، والرياح العاتية والأعاصير، والصواعق، والحرائق الطبيعية وانقطاع التيار الكهربائي لأسباب طبيعية خارجية، يؤدي الى حدوث تلف جزئي أو تدمير كلي لموارد النظام (أجهزة، وبرامج، وملفات بيانات، وأفراد).								
65	حدوث كوارث غير طبيعية (بشرية)، كالاضطرابات السياسية المحلية والإقليمية، والحروب، والتهديدات الإرهابية.								
ثالثاً: المخترقون والقرصنة:									
66	من أسباب المخاطر التي يتعرض لها نظام المعلومات المحاسبي المحسوب، جرائم وقرصنة الحاسوب نتيجة تصرفات غير آمنة من قبل أطراف خارجية كالقرصنة والمتطفلين الذين يخترقون نظم الحماية، رغبة في التحدي، أو لنوايا إجرامية وتجسسية.								
رابعاً: دخول فيروسات وبرمجيات الحاسوب الخبيثة للنظام:									
67	من أسباب المخاطر التي يتعرض لها نظام المعلومات المحاسبي المحسوب، الإصابة بالبرامج الخبيثة (الفيروسات والديدان، وبرامج التجسس)، التي قد تتلف البيانات أو تعطل النظام وتؤثر على عملية تشغيل البيانات.								
خامساً: المنافسة الاقتصادية بين البنوك:									
68	من أسباب حدوث مخاطر أمن نظم المعلومات رغبة منافسي البنك في الوصول إلى المعلومات السرية كعملاء البنك، وحجم النشاط وغيرها من المعلومات الهامة.								
69	من أسباب حدوث المخاطر زيادة المنافسة بين البنوك والذي جعلتها تقوم بتقديم الخدمات المصرفية الإلكترونية دون مراعاة الآثار التي يمكن أن تحدث عند الاستخدام الفعلي.								
سادساً: ضعف الرقابة الخارجية على نظم المعلومات المحوسبة للبنوك:									
70	عدم إيلاء المراجع الخارجي الأهمية الكافية لمخاطر أمن نظم المعلومات المحاسبي في البنك، عند قيامه بمهامه للتأكد من أن النظام قد تم تصميمه وتشغيله بطريقة ملائمة.								
71	عدم قيام البنك المركزي والسلطات الرقابية الرسمية بتكثيف حملات تفتيشية مفاجئة لتقييم مخاطر أمن نظم المعلومات المحاسبية لدى البنوك، وإلزامها برفع تقارير بهذا الشأن.								
سابعاً: ضعف التشريعات والقوانين المحلية في مجال تكنولوجيا المعلومات:									

الأسباب الخارجية للمخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة					موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
72	عدم تحديث القوانين المحلية النافذة التي تهدف إلى حماية أمن نظم المعلومات، سواء كانت قوانين جنائية أو مدنية أو تجارية، فهي تفتقد إلى كثير من النصوص اللازمة.								
73	الغموض التشريعي بشأن اختصاص وانطباق القوانين واللوائح المعمول بها لتحديد الحقوق والالتزامات الناتجة عن العمليات المصرفية الالكترونية.								
74	اختلاف التشريعات القانونية التي تنظم التعاملات المصرفية الالكترونية بين الدول مما يؤدي إلى تنازع القوانين واختصاصات المحاكم في فض النزاعات التي تنشأ عنها.								
75	عدم وجود أطر تشريعية وقانونية متناسقة ومتجانسة على المستوى المحلي والإقليمي والدولي لمعاقبة مرتكبي جرائم الحاسوب والانترنت.								
ثامناً: نقص الوعي الإلكتروني لدى عملاء البنك:									
76	نقص الوعي الإلكتروني لدى عملاء البنك وعدم اتباعهم إجراءات التأمين الوقائية الواجبة لبياناتهم الشخصية، وضعف دور البنك في القيام بتوعيتهم.								

المحور الرابع: الآثار المترتبة لحدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة: يُرجى قراءة الفقرات التالية جيداً ووضع إشارة (✓) في الخانة التي تُعبّر عن رأيك وبما يعكس وجهة نظرك إذا حدثت المخاطر لديكم.

الآثار الناتجة عن مخاطر أمن نظم المعلومات المحاسبية المحوسبة					درجة التأثير الناجمة عن المخاطر				
					عالية جداً	عالية	متوسطة	منخفضة	منخفضة جداً
أولاً: تأثير المخاطر على إتاحة نظم المعلومات المحاسبية:									
77	تعرض نظام المعلومات المحاسبي بالبنك للتعطيل بسبب المخاطر يؤثر على استرجاع البيانات والمعلومات ويترتب على ذلك خسائر مالية كبيرة، وقد يؤدي ذلك إلى خروج البنك من السوق وإفلاسه.								
78	تدمير البنية التحتية لنظم المعلومات المحاسبية وتوقفها لفترات طويلة يؤدي إلى إعاقة وصول المستخدمين والأطراف المستفيدة، مما يفقد البنك فرص نشاط حقيقية.								
79	حالات التعطيل والتوقف المفاجئ لنظام المعلومات المحاسبي للبنك لبعض الوقت يؤدي إلى اهتزاز مكانة البنك أمام عملائه وتكبد البنك خسائر تجارية ومالية كبيرة.								
ثانياً: تأثير المخاطر على سلامة وتكامل تجهيز البيانات في نظم المعلومات المحاسبية:									
80	حدوث مخاطر أمن نظم المعلومات المحاسبية يؤثر على سلامة تجهيز البيانات وعمليات التشغيل والمخرجات، بالدقة والشمولية المطلوبة وفي الوقت المناسب.								
81	تشغيل النظام بشكل خاطئ وباستخدام برامج غير ملائمة يؤدي إلى حصول البنك لمخرجات غير دقيقة وغير سليمة، يؤثر على صحتها ومصداقيتها.								
82	تعرض نظم المعلومات المحاسبية المحوسبة بالبنك إلى أي خطر يخفض من تكامل تلك النظم مع بعضها البعض على مستوى الأقسام والفروع، ففوق خطأ ما يؤدي إلى وقوع سلسلة من الأخطاء نتيجة التحديث الفوري للملفات.								
ثالثاً: تأثير المخاطر على سرية المعلومات المحاسبية:									
83	إن اقتحام نظام المعلومات المحاسبي من أطراف غير مخولة بالدخول، يؤدي إلى إمكانية								

الآثار الناتجة عن مخاطر أمن نظم المعلومات المحاسبية المحوسبة					درجة التأثير الناجمة عن المخاطر				
					عالية جدا	عالية	متوسطة	منخفضة	منخفضة جدا
سرقة أو تسرب معلومات هامة على درجة عالية من السرية لجهات غير مرغوب فيها.									
إن حدوث مخاطر أمن نظم المعلومات المحاسبية يؤدي إلى إطلاع المنافسين على المعلومات المرتبطة بالبنك والتي قد يترتب عليها الإضرار بالموقف التنافسي.									
إن حدوث المخاطر يؤدي إلى عدم قدرة نظام المعلومات المحاسبي في البنك على التعامل مع الأطراف المستفيدة المختلفة وفقاً لأصول السرية والفائدة المرجوة.									
رابعاً: تأثير المخاطر على خصوصية بيانات الأطراف المتعاملة مع البنك:									
إن حدوث مخاطر أمن نظم المعلومات المحاسبية يؤدي إلى ضعف قدرة البنك في حماية خصوصيات وأسرار عملائه، نتيجة سرقة أو كشف المعلومات الشخصية لهم والتي يتم جمعها واستخدامها والاحتفاظ بها من قبل نظام المعلومات المحاسبي للبنك.									
إن تعرض البنك لمخاطر أمن نظم المعلومات المحاسبية يهدد سمعته نتيجة فقدان الثقة وفشل البنك في تحقيق متطلبات العملاء بتقديم خدمة مصرفية إلكترونية متطورة وأمنة.									
إن حدوث مخاطر أمن نظم المعلومات المحاسبية يؤدي إلى عدم إتاحة الفرصة للعملاء للوصول إلى المعلومات المخزنة الشخصية لتعديلها أو إلغائها.									
خامساً: تأثير المخاطر على إثبات تصرفات الأطراف المتعاملة خلال تبادل البيانات إلكترونياً:									
حدوث المخاطر يؤدي إلى تهرب بعض أطراف المعاملات الإلكترونية من الالتزامات، عن طريق إنكار وقوع أحداث وقعت أو ادعاء وقوع أحداث لم تقع، وقد يؤدي ذلك إلى تحمل البنك لخسائر مالية وفقدان الثقة في مخرجات نظم المعلومات المحاسبية.									
رفض بعض الجهات الحكومية لحجية مخرجات نظم المعلومات المحاسبية المحوسبة استناداً لنصوص تشريعية، كالقانون التجاري وقانون البنوك.									

المحور الخامس: إجراءات ووسائل الحماية المطبقة لمواجهة مخاطر أمن نظم المعلومات المحاسبية المحوسبة:
يُرجى قراءة الفقرات التالية جيداً ووضع إشارة (✓) في الخانة التي تُعبر عن رأيك وبما يعكس الواقع القائم لديكم.

إجراءات ووسائل الحماية المطبقة لمواجهة مخاطر أمن نظم المعلومات المحاسبية المحوسبة					درجة تطبيق إجراءات الحماية الأمنية				
					عالية جدا	عالية	متوسطة	منخفضة	منخفضة جدا
أولاً: حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية:									
يوجد في البنك قسم خاص ومستقل بشكل كافٍ وبإمكانيات مناسبة مسؤول عن تنفيذ أمن نظم المعلومات المحاسبية وحمايتها، ووضع معايير وأسس وضوابط أمنية.									
يوجد دليل عمل مكتوب يتضمن إجراءات أداء العمل لكافة وظائف نظم المعلومات المحاسبية، محدد فيه السلطات والمسئوليات والكفاءات الملائمة لكل وظيفة داخل النظام.									
يوجد نظام صلاحية مبرمج بحيث يسمح النظام لكل مستخدم بإدارة نظام المعلومات المحاسبي حسب صلاحياته في التعامل مع ملفات النظام، (مثل قراءة البيانات أو نسخها أو تعديلها...الخ)، من خلال الوصول إلى أجزاء معينة وبيانات محددة.									
كل مستخدم للنظام له كلمة سر خاصة، فلا يتشارك اثنان بكلمة سر واحدة، ويتم إيقاف صلاحيات المستخدم إذا تم إدخال كلمة المرور خطأ أكثر من العدد المسموح به للمحاولات.									

درجة تطبيق إجراءات الحماية الأمنية					إجراءات ووسائل الحماية المطبقة لمواجهة مخاطر أمن نظم المعلومات المحاسبية المحوسبة	
منخفضة جدا	منخفضة	متوسطة	عالية	عالية جدا		
					95	هنالك فصل سليم بين الوظائف والمهام المختلفة والمتعارضة لمعالجة البيانات بين المبرمجين والمشغلين والمراقبين والمستخدمين بطريقة تسمح بمراقبة تنفيذ المهام.
					96	يعمل البنك على تنفيذ سياسة التدوير الوظيفي للمهام الأساسية لنظم المعلومات المحاسبية، بإجراء تنقلات بين الموظفين من حين لآخر، والزامهم بأخذ إجازاتهم السنوية دفعة واحدة.
					97	يعقد البنك برامج بواسطة مختصين في أمن نظم المعلومات لتوعية العاملين بالمخاطر التي تهدد أمن نظم المعلومات المحاسبية، وتدريبهم على إتباع الإجراءات الملائمة لمواجهةها.
					98	يتم تشجيع الأفراد على اتخاذ مبادرات لحل المشكلات، ومكافأة من يقوم بعمل إيجابي نحو تجسيد نظام الحماية، ومعاقبة من يتعامل سلباً مع المخاطر ويخالفون سياسات الأمن.
					99	يعين البنك شخص مسؤول عن حماية النظام يسمى ضابط أمن المعلومات، ويتم تكوين فريق طوارئ، من فنيين وإداريين فاعلين، لمواجهة أي ظرف طارئ يمس بحماية النظام.
					100	يتم اختيار موظفي نظم المعلومات المحاسبية بحرص شديد وإجراء تحريات عنهم وعن ماضيهم الوظيفي، والحرص على أن يكونوا ذوي خبرة وثقة وأمانة ويعملون لمصلحة البنك، وعدم إعطاء الموظف حديث التعيين صلاحيات عالية لاستخدام النظام.
					ثانياً: حماية الأمن المادي لنظم المعلومات المحاسبية المحوسبة:	
					101	توجد خطة طوارئ معلنة وموثقة خاصة لمواجهة الكوارث تتضمن إعداد وحدة متكاملة من تجهيزات الحاسوب والشبكات، ونسخة احتياطية من قاعدة البيانات، في موقع آخر بديل غير الموقع الرئيسي لضمان استمرارية العمل، واستئناف النشاط بصورة سريعة.
					102	تتضمن خطة الطوارئ مصفوفة مخاطر أمن نظم المعلومات المحاسبية المتوقعة، والاثار الناتج، والجهة المتأثرة، والتصرف اللازم لمواجهةها.
					103	يتعاقد البنك مع شركات تأمين متخصصة للتأمين على الأجهزة والبرمجيات وشبكات المعلومات والموظفين في نظام المعلومات المحاسبي المحوسب، ضد كافة المخاطر.
					104	يتم تصميم مواقع العمل وأماكن الأجهزة والمعدات، بصورة تتلاءم مع التغيرات الطبيعية، ويتم وضع أجهزة النظام في غرف محمية وآمنة، وعدم السماح بالدخول إليها لأي كان.
					105	يتم استخدام جميع الوسائل المادية التي تمنع الوصول غير المخول إلى نظم المعلومات المحاسبية وقواعدها كرجال الحراسة، والأقفال والحواجز والغرف المحصنة وغيرها.
					106	يستخدم موظفي البنك بطاقات دخول إلكترونية ذكية ممغنطة عليها صورهم الشخصية، للدخول إلى أماكن عملهم عبر البوابات المقفلة المبرمجة وفق الصلاحيات المخولة لهم، ويصدر إنذار مبكر فور الدخول المادي غير المخول.
					107	يقوم البنك بتثبيت كاميرات تلفزيونية على خارج مبنى دائرة النظام والممرات الداخلية فيها، وتعمل على مراقبة المستخدمين والأماكن التي توجد تجهيزات النظام، من موقع مركزي.
					108	يتم استخدام منظم كهربائي، وبطاريات إضافية، وخزانات طاقة، ومولد كهربائي لتجنب ارتفاع أو انخفاض الطاقة الكهربائية أو انقطاعها، وتعطلها بشكل مفاجئ، والذي يؤدي إلى تلف أجهزة وبرامج الحاسوب أو توقفها عن العمل.
					109	يتم تركيب أجهزة كشف الحريق في الأماكن المعرضة للخطر وتجهيزها بالشكل المناسب الذي يساعد على كشف الحريق بأسرع وقت ممكن وسرعة القيام بمقاومة الحريق.

درجة تطبيق إجراءات الحماية الأمنية					إجراءات ووسائل الحماية المطبقة لمواجهة مخاطر أمن نظم المعلومات المحاسبية
عالية جدا	عالية	متوسطة	منخفضة	منخفضة جدا	
					110 يتم استخدام أسقف وحوائط وأرضيات تمنع تسرب المياه، مع استخدام أغطية واقية من الأتربة والماء، وتركيب أجهزة إنذار من المياه والرطوبة.
					111 يتم إجراء صيانة دورية ومستمرة لأجهزة النظام ووسائل حمايته بما فيها أجهزة التكييف، لضمان استمرار عملها بفاعلية، ويتم توفير قطع ومعدات بديلة للأجهزة العاملة بشكل سريع فور تعطلها، بما يضمن سلامة الحواسيب وحمايتها.
					ثالثاً: حماية أمن الوصول البرمجي لقاعدة البيانات المتصلة بنظم المعلومات المحاسبية:
					112 يتم التحقق من هوية الشخص أو المعدات التي تحاول الدخول للنظام من خلال خليط من (كلمات مرور/ كروت ذكية/ معرفات بيولوجية/ أجهزة أخرى).
					113 يتم استخدام مستويات متتالية من الرقابة على دخول قاعدة البيانات بكلمات مرور متعددة ومختلفة للدخول إلى (الشبكة أو الحاسوب أو سيرفر البيانات أو قاعدة البيانات)، ويتم التنبيه للموظفين بعدم إفشاء كلمات المرور السرية، وتكون من الصعب تخمينها.
					114 يوجد سجل خاص لجميع الصلاحيات الممنوحة للموظفين المخولين بالدخول للنظام، ويتم برمجة مصفوفة الرقابة على الوصول آلياً، فيتم تحديد كلمة سر خاصة لكل موظف، والملفات أو البرامج التي يصرح له بالوصول إليها.
					115 يتم تغيير كلمات السر بشكل دوري ومستمر وخاصة بعد نقل الموظفين ويتم إلغاء كلمة السر الخاصة بالموظف الذي استقال أو أقيل من العمل بشكل فوري.
					116 يتم استخدام برامج الجدران النارية العازلة لمنع الوصول غير المصرح به إلى النظام، ومنع المستخدم من استخدام برامج أو ملفات لا يملك الصلاحية للدخول إليها، ويتم تحديث تلك البرامج وتعديلها باستمرار.
					117 يوثق النظام كافة محاولات الوصول غير المصرح بها، ويصدر تقرير حولها يتضمن وقت المحاولة والموقع الذي تمت من خلاله، ويتم معالجة ذلك بإغلاق الفجوات المكتشفة.
					118 يتم إجراء اختبار اختراق النظام بصورة دورية من قبل المراجعين الداخليين أو الخارجيين، أو بواسطة خبرات متخصصة لمعرفة نقاط الضعف في نظم المعلومات المحاسبية.
					119 يحرص البنك على تحميل واستخدام برامج متطورة وأصلية وفعالة مضادة لفيروسات الحاسوب وبرمجياته الخبيثة، ويتم تحديثها بشكل دوري ومستمر.
					120 يتم استخدام وسيلة التشفير لكافة البيانات والمعلومات الهامة المحفوظة في قاعدة البيانات.
					رابعاً: حماية أمن وسائط التخزين غير المتصلة بنظم المعلومات المحاسبية:
					121 يقوم البنك بأخذ نسخ احتياطية للبرامج وملفات البيانات الهامة بشكل مستمر ودوري (يومي، أسبوعي، شهري)، وتحفظ في خزائن حديدية مقفلة لحمايتها من السرقة أو الحريق، وتوضع نسخة منها في مكان آمن خارج مقر العمل.
					122 يتم تشفير النسخ الاحتياطية من قواعد البيانات لحمايتها من التعديل أو الوصول إليها بطريقة غير مشروعة وذلك لفرض الرقابة عليها.
					123 توجد رقابة كافية على وسائط تخزين البيانات غير المتصلة بالنظام، ويتم فحص تلك الوسائط باستمرار للتأكد من صحتها وسلامتها.

إجراءات ووسائل الحماية المطبقة لمواجهة مخاطر أمن نظم المعلومات المحاسبية المحوسبة					درجة تطبيق إجراءات الحماية الأمنية
عالية جدا	عالية	متوسطة	منخفضة	منخفضة جدا	
					124
يتم التخلص من وسائط تخزين البيانات والبرامج بطريقة آمنة معينة وعدم رميها في براميل القمامة، حيث توجد إجراءات رقابية كافية لذلك.					
خامساً: حماية أمن مدخلات نظم المعلومات المحاسبية المحوسبة:					
					125
مستندات إدخال البيانات دقيقة وشاملة لمختلف العمليات، وتساعد على تقليل الأخطاء، ويتم إعدادها وتعبئتها ومصادقتها من الأشخاص المخولين فقط، ويوجد برنامج خاص مصمم لمعرفة من قام بإدخال البيانات.					
					126
يتم تسجيل بيانات المدخلات أولاً بأول وتوجد رقابة كافية لاكتشاف أي نقص فيها، ويتم توثيق عمليات إدخال البيانات بما فيها المحاولات، والمخالفات الخاطئة، ومعرفة مصدرها.					
					127
يتم تحديد أخطاء إدخال البيانات وتتبعها حتى يتم تصحيحها وتتضمن برامج النظام ضوابط تمنع إدخال بيانات خاطئة، حيث تظهر رسالة تحذيرية على الشاشة في حال وجود خطأ.					
					128
توجد مراجعة تفصيلية للبيانات المدخلة للتأكد من دقتها واكتمالها، ويتم إجراء المراجعة الثنائية لبيانات المستندات المدخلة للتأكد من سلامتها.					
					129
تتوفر في نظم المعلومات المحاسبية خاصية تصحيح البيانات الخاطئة التي تم إدخالها في الوقت المناسب ضمن حدود الرقابة المسموح بها.					
سادساً: حماية أمن عمليات التشغيل البرمجي لنظم المعلومات المحاسبية المحوسبة:					
					130
يحتوي برنامج التشغيل على وسائل تحدد صلاحية المستخدمين في تشغيل وتحديث البيانات ومنع قراءتها أو نسخها أو تعديلها من غير المخول لهم ذلك.					
					131
توجد رقابة آلية مدمجة داخل النظام، من خلا تقارير تحليلية إلكترونية لتفاصيل العمليات التشغيلية، تحدد شخص المستخدم ووقت بداية ونهاية الاستخدام، ومكانه وطبيعة الاستخدام، والأخطاء المكتشفة آلياً، ويتم متابعة تلك التقارير بشكل مستمر.					
					132
توجد إجراءات كافية تضمن تصحيح الأخطاء، وإعادة تشغيل البيانات التي لم يتم تشغيلها بسبب توقف دورة التشغيل والتأكد من تمام معالجتها، ويتم تمييز العمليات التي تمت معالجتها لتلافي تكرار تشغيلها.					
					133
توجد إجراءات للتأكد من أن معالجة البيانات قد تمت بشكل كامل عند حد الانقطاع، من نقطة توقف معينة عند توقف دورة التشغيل لسبب من الأسباب.					
					134
يتم توقيف عمل التطبيقات المحاسبية إجبارياً نهاية الدوام الرسمي، فلا يسمح بتشغيل النظام خارج فترة الدوام المحددة والمبرمجة آلياً، بحيث يتعذر تشغيله النظام خلاف ذلك.					
سابعاً: حماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة:					
					135
يتم حصر أنواع المعلومات وتصنيفها إلى فئات وفقاً لدرجة أهميتها وسريتها، وتحديد مستوى الحماية الواجب توفيره لكل فئة منها.					
					136
توجد وسائل وإجراءات كافية لعملية توزيع المخرجات، لضمان وصول التقارير والوثائق للجهات المعنية المخولة فقط باستلامها.					
					137
يتم إجراء صيانة دائمة لوسائط الإخراج (طابعات، فاكسات، شاشات...الخ)، لضمان سلامة عرض المخرجات.					

درجة تطبيق إجراءات الحماية الأمنية					إجراءات ووسائل الحماية المطبقة لمواجهة مخاطر أمن نظم المعلومات المحاسبية المحوسبة	
عالية جدا	عالية	متوسطة	منخفضة	منخفضة جدا		
					138	يتم إعداد نسخ مطبوعة لبعض المعلومات المحاسبية الهامة، وتشفير المعلومات الحساسة.
					139	يتيح النظام مسار معين لمراجعة وتتبع سير المعاملات من مرحلة المدخلات إلى مرحلة المخرجات، والعكس.
					140	يقوم البنك بإتلاف المخرجات المهمة والسرية بعد الانتهاء من استخدامها بواسطة لجنة متخصصة ومخولة بذلك، ويتم الإتلاف داخل البنك.
					ثامناً: حماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية المحوسبة:	
					141	تستخدم برامج الجدران النارية لتحديد المعلومات التي يسمح بدخولها أو خروجها من وإلى نظام المعلومات المحاسبي المحوسب للبنك.
					142	يتم تشفير البيانات المرسلّة عبر الشبكات للتأكد من أنه لم يتم الكشف عنها أو تعديلها وأنها مرسلّة من الجهة المعنية، وتتوفر وسائل حماية كافية للحفاظ على سرية مفتاح التشفير.
					143	يستخدم البنك التوقيع الرقمي الإلكتروني، كوسيلة للتحقق من موثوقية المستخدمين بشكل غير قابل للتزيف، ولضمان عدم إنكار الأطراف المعنية المشاركة في الوثائق الإلكترونية.
					144	يتم استخدام شهادة رقمية صادرة من جهات فنية معتمدة، عند إرسال أو استلام البيانات عبر الشبكة الخارجية، للتحقق من هوية مرسل الرسائل، وموثوقية المستخدم.
					145	يتم استخدام بروتوكولات أمنية بين البنك والأطراف المتعاملة للحفاظ على سرية المعلومات المحاسبية والتحقق من وصولها للجهة المطلوبة أثناء إجراء المعاملات المالية.
					تاسعاً: حماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة:	
					146	توجد إجراءات كافية وفعالة لرقابة عمليات تطوير البرامج والتطبيقات المحاسبية، وفق معايير وإجراءات واضحة ومكتوبة ومحددة.
					147	لا تتم أية تعديلات في برمج النظام بدون حصول المبرمجين المختصين على موافقات رسمية من الإدارات المعنية المخولة.
					148	هناك فريق متخصص لتعديل وتطوير نظام المعلومات المحاسبي من داخل البنك، وتشرف إدارة البنك على تعديل وتطوير النظام.
					149	يتم إجراء الاختبار المبدئي بالتشغيل التجريبي للبرامج الجديدة وتعديلاتها قبل اعتمادها بشكل نهائي للتأكد من سلامتها، وقدرتها على تتبّع الأخطاء التي قد تحدث أثناء التنفيذ.
					150	يتم توثيق كافة التعديلات التي تتم على البرامج والمعدات، وفق الإجراءات المتبعة.

- 

.....@.....

مع جزيل الشكر والتقدير،،،،،،،،،،

الباحث :

عبد الكريم محمد يحيى فاضل

طالب دكتوراه في قسم المحاسبة

كلية الاقتصاد – جامعة دمشق

Fathel_Karem4@hotmail.com

Fathel_Karem4@yahoo.com

GSM: 00967711797934

ملحق رقم (2)

قائمة بأسماء الأساتذة المحكمين لصدق وصلاحيّة قائمة الاستقصاء
(مرتبة حسب الألقاب العلمية ثم الحروف الأبجدية)

م	الاسم	الجامعة	الكلية / الوظيفة	القسم
1	أ.د. حسين القاضي	جامعة دمشق	الاقتصاد	المحاسبة
2	أ.د. رشا حمادة	جامعة دمشق	الاقتصاد	المحاسبة
3	أ.د. عبد الملك إسماعيل حبر	جامعة صنعاء	التجارة والاقتصاد رئيس جمعية المحاسبين القانونيين اليمنيين وشريك ديلويت آند توتش الشرق الأوسط في اليمن.	المحاسبة
4	أ.د. عدنان الغانم	جامعة دمشق	الاقتصاد عميد كلية الاقتصاد	الإحصاء
5	د. تيسير المصري	جامعة دمشق	الاقتصاد	المحاسبة
6	د. عبد الرزاق محمد قاسم	جامعة دمشق	الاقتصاد المدير التنفيذي لسوق دمشق للأوراق المالية	التمويل والمصارف
7	د. عبد العزيز العززي	جامعة عمران	التجارة والاقتصاد	المحاسبة
8	د. قاسم محمد النعيمي	جامعة دمشق	الاقتصاد	الإحصاء
9	د. محمد أحمد السياني	جامعة صنعاء	التجارة والاقتصاد نائب محافظ البنك المركزي اليمني	المحاسبة
10	د. منذر حسين العوّاد	جامعة دمشق	الاقتصاد	الإحصاء

ملحق رقم (3)

البنوك التجارية في الجمهورية اليمنية مرتبة وفقاً لسنة التأسيس
موضحاً فيه مجتمع الدراسة وحجم العينة المختارة *

م	إسم البنك	جنسية البنك	سنة التأسيس (ميلادي)	نوع الشركة	نسب ملكية رأس المال %			مجتمع الدراسة		عينة الدراسة	
					عام يمني	خاص يمني	خاص خارجي	عدد	نسبة %	عدد	نسبة %
1	البنك اليمني للإنشاء والتعمير.	يمني	1962	مختلطة	51	49		198	13.71	29	13.81
2	البنك الأهلي اليمني.	يمني	1969	عامة	100			65	4.50	9	4.29
3	يوناييتد بنك ليمنت	أجنبي	1971	مساهمة مقفلة			100	26	1.80	4	1.90
4	البنك العربي	عربي	1972	مساهمة مقفلة			100	50	3.46	7	3.33
5	بنك الـيمن والكويت للتجارة والاستثمار.	يمني	1977	مساهمة مقفلة		100		119	8.24	17	8.10
6	بنك اليمن الدولي.	يمني	1979	مساهمة مقفلة		85	15	79	5.47	11	5.24
7	مصرف الرافدين.	عربي	1982	عامة			100	25	1.73	4	1.90
8	بنك التسليف التعاوني والزراعي	يمني	1982	مختلطة	99	1		138	9.55	20	9.52
9	البنك التجاري اليمني	يمني	1993	مساهمة مقفلة	10	90		97	6.71	14	6.67
10	البنك الإسلامي اليمني للتمويل والاستثمار	يمني	1996	مساهمة مقفلة	4.5	73.5	22	66	4.57	10	4.76
11	بنك التضامن الإسلامي الدولي	يمني	1995	مساهمة مقفلة		96.7	3.3	145	10.03	21	10.00
12	بنك سبأ الإسلامي	يمني	1997	مساهمة مقفلة		85	15	152	10.51	22	10.47
13	بنك الـيمن والخليج	يمني	2001	مساهمة مقفلة	1	77	22	73	5.05	11	5.24
14	مصرف الـيمن البحرين الشامل	يمني	2002	مساهمة مقفلة		57	43	113	7.82	16	7.63
15	بنك قطر الوطني	عربي	2007	مساهمة مقفلة			100	53	3.67	8	3.81
16	مصرف الكريمي للتمويل الأصغر الإسلامي	يمني	2010	مساهمة مقفلة		100		46	3.18	7	3.33
الإجمالي								1445	%100	210	%100

* الجدول من إعداد الباحث معتمداً على:

- جمعية البنوك اليمنية، (2012)، مجلة المصارف، العدد (6)، صنعاء، اليمن، كانون الأول (ديسمبر) 2012.
- والنخبة للعلاقات العامة والإعلان، (2010)، الليل المصرفي اليمني وشركات التأمين، صنعاء، اليمن، صفحات متفرقة.
- البنك المركزي، التقارير الربع سنوية، حتى شهر ديسمبر (كانون الأول) 2012م.
- إدارات الموارد البشرية لدى البنوك التجارية في الجمهورية اليمنية، إحصائيات وبيروشورات مختلفة، حتى شهر كانون الأول (ديسمبر) 2012م.

ملحق رقم (4)

توزيع أفراد مجتمع وعينة الدراسة على البنوك التجارية في الجمهورية اليمنية
موضحاً فيه الاستقصاءات الموزعة والمستردة والمستبعدة والخاضعة للتحليل مصنفة وفقاً لاسم البنك *

م	اسم البنك	الاستقصاءات الموزعة (العينة)		الاستقصاءات المستردة		نسبة الاستجابة من العينة %	الاستقصاءات المستبعدة (غير صالحة)		الاستقصاءات الخاضعة للتحليل		نسبة الخاضع للتحليل من العينة %
		نسبة %	عدد	نسبة %	عدد		نسبة %	عدد	نسبة %	عدد	
1	البنك اليمني للإتشاء والتعمير	13.81	29	12.34	19	65.52	15.62	5	11.48	14	48.28
2	البنك الأهلي اليمني.	4.29	9	4.55	7	77.78	3.13	1	4.92	6	66.67
3	يونايتد بنك ليمتد	1.90	4	2.60	4	100.00	6.25	2	1.64	2	50.00
4	البنك العربي	3.33	7	4.55	7	100.00	6.25	2	4.10	5	71.43
5	بنك السيمن والكويت للتجارة والاستثمار.	8.10	17	7.79	12	70.59	6.25	2	8.20	10	58.82
6	بنك اليمن الدولي.	5.24	11	5.84	9	81.82	6.25	2	5.74	7	63.64
7	مصرف الرافدين.	1.90	4	1.95	3	75.00	3.13	1	1.64	2	50.00
8	بنك التسليف التعاوني والزراعي.	9.52	20	8.44	13	65.00	3.13	1	9.84	12	60.00
9	البنك التجاري اليمني.	6.67	14	5.19	8	57.14	6.25	2	4.92	6	42.86
10	البنك الإسلامي اليمني للتمويل والاستثمار.	4.76	10	5.19	8	80.00	9.37	3	4.10	5	50.00
11	بنك التضامن الإسلامي الدولي.	10.00	21	11.04	17	80.95	9.37	3	11.48	14	66.67
12	بنك سبأ الإسلامي.	10.47	22	10.39	16	72.73	6.25	2	11.48	14	63.64
13	بنك اليمن والخليج.	5.24	11	5.84	9	81.82	6.25	2	5.74	7	63.64
14	مصرف اليمن والبحرين الشامل.	7.63	16	7.14	11	68.75	3.13	1	8.20	10	62.50
15	بنك قطر الوطني	3.81	8	3.90	6	75.00	3.13	1	4.10	5	62.50
16	مصرف الكريمي للتمويل الأصغر الإسلامي.	3.33	7	3.25	5	71.43	6.25	2	2.46	3	42.86
الإجمالي		%100	210	%100	154	73.33	%100	32	%100	122	58.10

* الجدول من إعداد الباحث معتمداً على:

- جمعية البنوك اليمنية، مجلة المصارف، العدد (6)، صنعاء، اليمن، كانون الأول (ديسمبر) 2012.
- والنخبة للعلاقات العامة والإعلان، (2010)، الدليل المصرفي اليمني وشركات التأمين، صنعاء، اليمن، صفحات متفرقة.
- البنك المركزي، (2012)، التقارير الربع سنوية، حتى شهر ديسمبر (كانون الأول) 2012م.
- إدارات الموارد البشرية في البنوك التجارية اليمنية، (2012)، إحصائيات وبروشورات مختلفة، حتى شهر كانون الأول (ديسمبر) 2012م.

ملحق رقم (5)

مخرجات ونتائج التحليل بواسطة برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS)

One-Sample Statistics & One-Sample Test (Test Value = 3)

رقم الفقرة	متغيرات الدراسة	المتوسط الحسابي Mean	الانحراف المعياري Std. Deviation	معامل الاختلاف	قيمة (t) المحسوبة	القيمة المعنوية Sig. (2-tailed)	نتيجة اختبار الفرضية العدمية
1	قيام بعض موظفي نظم المعلومات باستغلال صلاحياتهم في هذه النظم في خدمة أغراضهم الشخصية بما يتعارض والسياسات الموضوعة من قبل الإدارة والمختصين.	2.23	.831	37.26	-10.240-	.000	رفض
2	انتحال صلاحيات شخص مخول بأي طريقة من الطرق نتيجة إهمال المستخدم، والثقة المتبادلة بين الموظفين التي تجعلهم يستخدمون كلمات السر فيما بينهم.	2.75	.696	25.3	-3.902-	.000	رفض
	أولاً: مخاطر أمن الأفراد العاملين في نظم المعلومات المحاسبية:						
3	حدوث تلف جزئي أو تدمير كلي لأجهزة ومعدات النظام المادية.	2.00	.813	40.6	-13.584-	.000	رفض
4	حدوث أعطال في المكونات المادية والبرمجية للنظام.	2.71	.732	27.0	-4.325-	.000	رفض
	ثانياً: مخاطر الأمن المادي لنظم المعلومات المحاسبية:						
5	الوصول البرمجي غير المصرح به إلى برامج النظام والملفات في قاعدة البيانات بواسطة أفراد من داخل البنك بقصد الإضرار والتخريب.	2.02	.807	40.0	-13.340-	.000	رفض
6	الوصول البرمجي، غير المصرح به إلى برامج النظام والملفات في قاعدة البيانات بواسطة أفراد أو جهات من خارج البنك، لإنجاز عمليات (تعديل/تدمير/كشف/نسخ وسرقة/استخدام) بطريقة غير مشروعة.	1.83	.746	40.8	-17.349-	.000	رفض
7	تلف بعض ملفات البيانات والبرامج ونظم التشغيل نتيجة تعرض قاعدة البيانات لنظام المعلومات المحاسبي المحوسب للإصابة بالبرامج الخبيثة مثل (الفيروسات، والديدان، وبرامج التجسس).	3.58	.860	24.0	7.467	.000	قبول
	ثالثاً: مخاطر أمن الوصول البرمجي لقاعدة بيانات نظم المعلومات المحاسبية:						
8	ضياح أو سرقة وسائط تخزين البيانات والبرامج الاحتياطية غير المتصلة بقاعدة بيانات نظام المعلومات المحاسبي المحوسب.	2.20	.832	37.8	-10.548-	.000	رفض
9	الوصول غير المصرح به للبيانات والبرامج المخزنة في وسائط غير متصلة بنظام المعلومات المحاسبي المحوسب.	2.11	.713	33.8	-13.829-	.000	رفض
	رابعاً: مخاطر أمن النسخ في وسائط غير متصلة بقاعدة بيانات النظام:						
10	الحذف أو التعديل المتعمد لمصادر بيانات مدخلات صحيحة بواسطة الأفراد العاملين في نظام المعلومات المحاسبي.	2.01	.886	44.0	-12.364-	.000	رفض
11	الحذف أو التعديل غير المتعمد لمصادر بيانات مدخلات صحيحة بواسطة الأفراد العاملين في نظام المعلومات المحاسبي.	3.26	.811	24.9	3.572	.001	قبول
12	الإدخال المتعمد لبيانات غير سليمة أو مكررة من قبل العاملين في نظام المعلومات المحاسبي، للقيام بعمليات غير مصرح بها.	2.30	.726	31.6	-10.600-	.000	رفض
13	الإدخال غير المتعمد لبيانات غير سليمة أو مكررة من قبل العاملين في نظام المعلومات المحاسبي، نتيجة السهو وعدم المعرفة.	3.19	.903	28.3	2.306	.023	قبول
14	التأخير المقصود في إدخال بعض البيانات بواسطة العاملين في نظام المعلومات المحاسبي.	2.77	.831	30.0	-3.050-	.003	رفض
15	التأخير غير المقصود في إدخال بعض البيانات بواسطة العاملين في نظام المعلومات المحاسبي.	3.44	.692	20.1	7.055	.000	قبول
	خامساً: مخاطر تهدد أمن عمليات مدخلات نظم المعلومات المحاسبية:						
16	إهدار وسرقة وقت تشغيل بعض أجهزة الحاسوب المستخدمة في نظام المعلومات المحاسبي من خلال استغلالها في الأغراض الشخصية.	2.75	.932	33.9	-3.011-	.003	رفض
17	تعديل أو حذف البيانات بطريقة مقصودة نتيجة حدوث احتيال وغش من قبل مستخدم نظام المعلومات المحاسبي أثناء عمليات التشغيل.	2.13	.760	35.7	-12.626-	.000	رفض
18	تعديل أو حذف البيانات بطريقة غير مقصودة نتيجة حدوث أخطاء من قبل مستخدم نظام المعلومات المحاسبي أثناء عمليات التشغيل.	2.84	.856	30.1	-2.115-	.037	رفض
19	حدوث عمليات تشغيلية غير مكتملة لبيانات محاسبية تم إدخالها.	2.19	.672	30.7	-13.335-	.000	رفض
	سادساً: مخاطر أمن عمليات تشغيل نظم المعلومات المحاسبية:						
20	حذف وإخفاء بنود معينة من مخرجات نظام المعلومات المحاسبي وإنتاج مخرجات مظلة غير سليمة.	1.95	.870	44.6	-13.311-	.000	رفض
21	الكشف غير المخول به للمعلومات المحاسبية أثناء عرضها على الشاشات أو طباعتها على الورق أو أثناء التخلص منها بعد استخدامها.	3.49	.794	22.8	6.719	.000	قبول

رقم الفقرة	متغيرات الدراسة	المتوسط الحسابي Mean	الانحراف المعياري Std. Deviation	معامل الاختلاف	قيمة (t) المحسوبة	القيمة المعنوية Sig. (2-tailed)	نتيجة اختبار الفرضية العدمية
22	توجيه وتوزيع وتسليم بعض البيانات والمعلومات المحاسبية لأشخاص غير مخولين باستلام نسخة منها أو لا تتوفر فيهم الأمانة.	2.52	.784	31.1	-6.809-	.000	رفض
23	سرقة وسوء استخدام مخرجات النظام (المعلومات المحاسبية) من قبل القائمين على النظام واستغلالها في أغراض شخصية.	1.81	.795	44.0	-16.492-	.000	رفض
سابعاً: مخاطر أمن مخرجات نظم المعلومات المحاسبية المحوسبة:							
24	انقطاع وتوقف تدفق البيانات والمعلومات المحولة إلكترونياً عبر شبكات الحاسوب من المركز الرئيسي للبنك إلى الفروع أو العكس.	2.77	.713	25.7	-3.554-	.001	رفض
25	اعتراض وصول البيانات المرسله عبر الشبكات من أجهزة الخوادم لأجهزة المستخدمين، وتعرضها أحياناً للكشف أو التعديل، أو السرقة.	2.30	.870	37.8	-8.836-	.000	رفض
26	اختراق مواقع الويب الخاص ببيانات البنك والتجسس على خطوط الاتصالات الخاصة بنقل البيانات.	2.08	.984	47.3	-10.304-	.000	رفض
27	إنكار بعض الأطراف المتعاملة مع البنك للبيانات والمعلومات المحاسبية المتبادلة إلكترونياً.	1.83	.789	43.1	-16.402-	.000	رفض
28	حدوث أخطاء معينة غير مقصودة أثناء نقل البيانات كإرسال بيانات أو معلومات عن طريق الخطأ إلى موقع آخر.	2.62	.875	33.4	-4.759-	.000	رفض
ثامناً: مخاطر أمن تبادل البيانات عبر شبكات نظم المعلومات المحاسبية المحوسبة:							
29	يتم إجراء تغييرات للنظام وبرامجه بطريقة غير مسموح بها، من قبل أشخاص غير مخولين بذلك، للقيام بعمليات تلاعب واحتيال لاحقة.	1.97	.978	49.6	-11.657-	.000	رفض
30	حدوث أخطاء في عدم استكمال التعديلات المطلوبة أثناء عمليات التعديل والتطوير.	2.67	.866	32.4	-4.179-	.000	رفض
تاسعاً: مخاطر أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة:							
مخاطر أمن نظم المعلومات المحاسبية المحوسبة							
31	لا تترك الإدارة العليا للبنك أهمية أمن نظم المعلومات المحاسبية، فلا تدعم الجهة المعنية بتطبيق السياسات الأمنية مادياً أو معنوياً.	3.32	.989	29.8	3.567	.001	قبول
32	عدم وجود سياسات وخطط إدارية واضحة ومعتمدة ومعلنة وموثقة لإدارة مخاطر أمن نظم المعلومات المحاسبية في البنك.	3.31	1.099	33.2	3.130	.002	قبول
33	عدم قيام إدارة البنك بإصدار قرارات وتشريعات خاصة فعالة للحد من مخاطر أمن نظم المعلومات المحاسبية، ومعاينة الموظفين المخلين بتلك القواعد.	3.52	1.030	29.2	5.536	.000	قبول
34	شعور إدارة البنك بعدم جدوى تقييم مخاطر أمن نظم المعلومات المحاسبية، لاعتمادها بأن تكلفة تطبيق إجراءات الحماية أكبر من عوائدها المتوقعة.	2.76	.987	35.8	-2.658-	.009	قبول
35	لا تقوم الإدارة بمشاركة الأقسام المختصة ليبحث السبل أفضل لمواجهة تلك المخاطر.	3.63	.873	24.0	7.977	.000	قبول
36	امتناع الإدارة العليا للبنك عن الإفصاح عن تلك المخاطر والخسائر المترتبة عنها، خوفاً من اهتزاز الثقة بسمعة البنك ومركزه المالي.	3.71	.913	24.6	8.623	.000	قبول
أولاً: فلسفة الإدارة العليا للبنك:							
37	عدم وجود إدارة أو قسم أو لجنة مستقلة، لها صلاحيات كافية لتقييم ومتابعة مخاطر أمن نظم المعلومات المحاسبية، بهدف حماية تلك النظم.	3.32	1.108	33.4	3.187	.002	قبول
38	غياب الوصف الدقيق للوظائف والذي يحدد المسؤوليات والصلاحيات لكل موظف داخل الهيكل التنظيمي للبنك.	3.28	1.207	36.8	2.549	.012	قبول
39	الفصل غير الواضح بين المهام المتعلقة بنظم المعلومات المحاسبية في البنك، كإشراك بعض العاملين باستخدام نفس كلمات السر أو تبادلها بينهم، مما قد يهدد مبدأ تقسيم العمل.	2.71	1.229	45.3	-2.577-	.011	رفض
40	النقص الكبير في الموظفين المختصين بأمن نظم المعلومات والذي تتوفر فيهم الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المتعددة المطلوبة لذلك.	3.30	1.082	32.9	3.095	.002	رفض
41	صعوبة وعدم كفاية تدريب وتأهيل وتوعية الموظفين في مجال تقنيات وأساليب أمن نظم المعلومات، وعدم توافق التدريب مع التطور المستمر لبرامج أمن نظم المعلومات.	3.88	.905	23.3	10.701	.000	قبول
42	الاهتمام غير الكافي بفحص التاريخ الوظيفي والمهني للموظفين الجدد مما قد يؤثر على قاعدة وضع الرجل المناسب في المكان المناسب.	3.34	1.104	33.1	3.444	.001	قبول
ثانياً: أسباب وعوامل تنظيمية:							
43	تقدم الأجهزة والبرامج المستخدمة وضعف فاعليتها في حفظ وتشغيل البيانات وإنتاج المعلومات وتحققها وتخزينها و استرجاعها بسهولة وسرعة.	2.70	.908	33.6	-3.689-	.000	رفض
44	الصعوبة في إيجاد التوثيق الدئلي للأجهزة والبرامج وأجهزة الدعم المساندة لها بعناية، لتحديث وتطوير الأنظمة، بما يؤمن تحقيق أهداف النظام وتأمين عناصر الرقابة.	2.54	.892	35.1	-5.683-	.000	رفض
45	وجود أخطاء في تصميم البرامج والتطبيقات المحاسبية المستخدمة تؤدي إلى إنتاج معلومات خاطئة أو غير دقيقة لفترات طويلة.	2.71	.999	36.9	-3.169-	.002	رفض
46	عدم كفاية عمليات الصيانة الدورية لأجهزة الحاسوب والبرمجيات المستخدمة في تشغيل وحماية نظم المعلومات المحاسبية المحوسبة.	2.75	.696	25.3	-3.902-	.000	رفض
47	اعتماد البنك في الحصول على الأجهزة والبرامج، والدعم الفني لها على مزودين قليلي الخبرة، ولا يتم التقييم المستمر لوضعهم في السوق.	2.88	.799	27.7	-2.377-	.019	رفض
48	عدم التوائم والتوافق ما بين الأنظمة والتطبيقات الموجودة لدى البنك مع الأنظمة والتطبيقات الخاصة بالمنشآت التي قد يتم ربط أنظمة البنك معها.	2.39	1.008	42.8	-6.642-	.000	رفض
ثالثاً: أسباب متعلقة بإمكانات البنك التكنولوجية:							
		2.65	.606	22.9	-6.298-	.000	رفض

رقم الفقرة	متغيرات الدراسة	المتوسط الحسابي Mean	الانحراف المعياري Std. Deviation	معامل الاختلاف	قيمة (t) المحسوبة	القيمة المعنوية Sig. (2-tailed)	نتيجة اختبار الفرضية العدمية
49	سوء استخدام الصلاحيات الواسعة المخولة لبعض الأفراد المسؤولين عن تشغيل النظام ممن لديهم معرفة واسعة بتفاصيل النظام، وعدم التزامهم بالإجراءات المحددة لحماية.	3.156	1.128	35.7	1.525	.130	رفض.....
50	ضعف إدراك بعض العاملين بالنظام لمهامهم الموكولة لهم (كنسيان كلمة المرور للدخول للنظام، أو السماح لملاء باستخدامها)، مما يترتب عليها أخطاء فادحة عند التشغيل.	3.75	.895	23.9	9.196	.000	قبول
51	إهمال بعض العاملين بنظام المعلومات المحاسبي وعدم بذلهم العناية المهنية الكافية لأداء العمل، لنقص التأهيل والخبرة والوعي الرقابي.	4.07	.800	19.7	14.709	.000	قبول
52	ارتفاع مستوى خبرة بعض العاملين في مجال التشغيل الإلكتروني، وزيادة معرفتهم أكثر من غيرهم بنقاط الضعف في الضوابط الرقابية المطبقة، مما ينتج عن ذلك مخاطر للنظام.	3.31	.927	28.0	3.708	.000	قبول
53	التصرفات الانتقامية للأفراد الغاضبين سواء أثناء عملهم بسبب معاقبتهم أو بعد إنهاء خدماتهم بسبب فصلهم من العمل، حيث يقوموا بالكشف عن بعض المعلومات السرية.	3.20	1.003	31.3	2.255	.026	قبول
54	انخفاض معدل دوران موظفي أنظمة المعلومات لدى البنك، واحتفاظهم بأسرار الأنظمة ومفاتيح الحل وعدم تعاونهم مع زملائهم في تبادل المعرفة والخبرة.	3.64	.900	24.7	7.842	.000	قبول
	رابعاً: أسباب تتعلق بالأفراد العاملين في نظم المعلومات المحاسبية المحوسبة:						
55	عجز التدابير الأمنية لنظم المعلومات، وعدم كفاية وفعالية الأدوات والضوابط والإجراءات الرقابية المطبقة في البنك لحماية أمن نظام المعلومات المحاسبي.	2.46	.762	31.0	-7.840	.000	رفض
56	ضعف كفاءة وفعالية نظم الرقابة الداخلية للبنك وعدم إصدار تقارير رقابية دورية حول الأنظمة الآلية، ليتم متابعتها وتقييمها لمواكبة التطورات التي تجري لمواجهة المخاطر.	2.68	.718	26.8	-4.912	.000	رفض
57	عدم كفاءة وفعالية إجراءات إدارة المخاطر، وعدم القيام بالتقييم الذاتي لمخاطر أمن نظم المعلومات بحيث يقوم كل موظف بتحديد المخاطر التي يواجهها وتقييم إجراءات مواجهتها	3.30	.768	23.2	4.244	.000	قبول
58	غياب المسار المرئي للمراجعة لعدم رؤية عمليات إدخال البيانات وتشغيلها سهل من تغيير أو إضافة أو حذف أي بيانات دون ترك أثر يدل على ذلك، وصعوبة اكتشاف ذلك.	3.05	.7255	23.8	.749	.456	قبول
	خامساً: أسباب متعلقة بضعف الرقابة الداخلية وإدارة المخاطر في البنك:						
59	حدوث كوارث غير طبيعية من البيئة الداخلية للبنك (كالتخريب، والحريق، وانقطاع الكهرباء، وتسريب المياه)، تسبب تلك الكوارث تلف جزئي أو تدمير كلي لموارد النظام.	3.17	1.237	39.0	1.536	.127	قبول
	سادساً: أسباب تتعلق بحدوث كوارث داخلية في البنك غير طبيعية:						
	الأسباب الداخلية للمخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة						
60	التطورات التكنولوجية السريعة والهائلة والمتلاحقة والتي تلي وضع الإجراءات الرقابية في البنك، فتتقدم التقنية خارجياً أسرع من ممارسة الأمن داخل البنك.	4.03	.781	19.4	14.600	.000	قبول
61	عدم وجود استقرار نسبي لنظام المعلومات، بسبب ارتفاع معدلات التغيير في تكنولوجيا المعلومات، مقابل ضعف إمكانيات البنك المالية والبشرية لمجاراتها واستيعابها.	3.64	.936	25.7	7.540	.000	قبول
62	تصميم أساليب للتلاعب تبني داخل النظام المحاسبي الإلكتروني يصعب اكتشافها، تؤدي إلى إنتاج معلومات محاسبية خاطئة.	2.74	.821	3.0	-3.528	.001	رفض
63	عدم توفر بنية تحتية تكنولوجية قوية في الجمهورية اليمنية.	3.75	1.006	26.8	8.274	.000	قبول
	أولاً: التغيير التكنولوجي غير المتوازن:						
64	حدوث الكوارث الطبيعية والبيئية كالزلازل، والبراكين، والفيضانات والسيول، والرياح العاتية والأعاصير، والصواعق، والحرائق الطبيعية وانقطاع التيار الكهربائي لأسباب طبيعية خارجية، يؤدي إلى حدوث تلف جزئي أو تدمير كلي لموارد النظام (أجهزة، وبرامج، وملفات بيانات، وأفراد).	3.22	.857	26.6	2.850	.005	قبول
65	حدوث كوارث غير طبيعية (بشرية)، كالاضطرابات السياسية المحلية والإقليمية، والحروب، والتهديدات الإرهابية.	3.74	.968	25.9	8.409	.000	قبول
	ثانياً: الكوارث الطبيعية والسياسية:						
66	من أسباب المخاطر التي يتعرض لها نظام المعلومات المحاسبي المحوسب، جرائم وقرصنة الحاسوب نتيجة تصرفات غير آمنة من قبل أطراف خارجية كالقرصنة والمتطفلين الذين يخترقوا نظم الحماية، رغبة في التحدي، أو لنوايا إجرامية وتجسسية.	3.30	.770	23.3	4.349	.000	قبول
	ثالثاً: المخترقون والقرصنة:						
67	من أسباب المخاطر التي يتعرض لها نظام المعلومات المحاسبي المحوسب، الإصابات بالبرامج الخبيثة (الفيروسات والديدان، وبرامج التجسس)، التي قد تلتف البيانات أو تعطل النظام وتؤثر على عملية تشغيل البيانات.	4.07	.746	18.3	15.761	.000	قبول
	رابعاً: دخول فيروسات وبرمجيات الحاسوب الخبيثة للنظام:						
68	من أسباب حدوث مخاطر أمن نظم المعلومات رغبة منافسي البنك في الوصول إلى المعلومات السرية كعملاء البنك، وحجم النشاط وغيرها من المعلومات الهامة.	2.61	.787	30.1	-5.516	.000	رفض
69	من أسباب حدوث المخاطر زيادة المنافسة بين البنوك والذي جعلتها تقوم بتقديم الخدمات المصرفية الإلكترونية دون مراعاة الآثار التي يمكن أن تحدث عند الاستخدام الفعلي.	3.11	.677	21.8	1.736	.085	قبول
	خامساً: المنافسة الاقتصادية بين البنوك:						
70	عدم إيلاء المراجع الخارجي الأهمية الكافية لمخاطر أمن نظام المعلومات المحاسبي في البنك، عند قيامه بمهامه للتأكد من أن النظام قد تم تصميمه وتشغيله بطريقة ملائمة.	3.74	.769	20.6	10.592	.000	قبول
71	عدم قيام البنك المركزي والسلطات الرقابية الرسمية بتكثيف حملات تفتيشية مفاجئة لتقييم مخاطر أمن نظم المعلومات المحاسبية لدى البنوك، والزامها برفع تقارير بهذا الشأن.	3.84	.953	24.8	9.779	.000	قبول

رقم الفقرة	متغيرات الدراسة	المتوسط الحسابي Mean	الانحراف المعياري Std. Deviation	معامل الاختلاف	قيمة (t) المحسوبة	القيمة المعنوية Sig. (2-tailed)	نتيجة اختبار الفرضية العدمية
	سادساً: ضعف الرقابة الخارجية على نظم المعلومات المحوسبة للبنوك:						
72	عدم تحديث القوانين المحلية النافذة التي تهدف إلى حماية أمن نظم المعلومات، سواء كانت قوانين جنائية أو مدنية أو تجارية، فهي تفقد إلى كثير من النصوص اللازمة.	4.05	.790	19.5	14.651	.000	قبول
73	الغموض التشريعي بشأن اختصاص وانطباق القوانين واللوائح المعمول بها لتحديد الحقوق والالتزامات الناتجة عن العمليات المصرفية الالكترونية.	4.14	.633	15.2	19.850	.000	قبول
74	اختلاف التشريعات القانونية التي تنظم التعاملات المصرفية الالكترونية بين الدول مما يؤدي إلى تنازع القوانين واختصاصات المحاكم في فض النزاعات التي تنشأ عنها.	3.82	.909	23.8	9.957	.000	قبول
75	عدم وجود أطر تشريعية وقانونية متناسقة ومتجانسة على المستوى المحلي والإقليمي والدولي لمعالجة مرتكبي جرائم الحاسوب والانترنت.	3.90	.856	21.9	11.624	.000	قبول
	سابعاً: ضعف التشريعات والقوانين المحلية في مجال تكنولوجيا المعلومات:						
76	نقص الوعي الالكتروني لدى عملاء البنك وعدم إتباعهم إجراءات التأمين الوقائية الواجبة لبياناتهم الشخصية، وضعف دور البنك في القيام بتوعيتهم.	4.12	.744	18.0	16.649	.000	قبول
	ثامناً: نقص الوعي الإلكتروني لدى عملاء البنك:						
	الأسباب الخارجية للمخاطر التي تهدد أمن نظم المعلومات المحاسبية						
77	تعرض نظام المعلومات المحاسبي بالبنك للتعطيل بسبب المخاطر يؤثر على استرجاع البيانات والمعلومات ويترتب على ذلك خسائر مالية كبيرة، وقد يؤدي ذلك إلى خروج البنك من السوق وإفلاسه.	2.76	.987	35.8	-2.658	.009	قبول
78	تدمير البنية التحتية لنظم المعلومات المحاسبية وتوقفها لفترات طويلة يؤدي إلى إعاقة وصول المستخدمين والأطراف المستفيدة، مما يفقد البنك فرص نشاط حقيقية.	3.27	1.028	31.4	2.904	.004	قبول
79	حالات التعطيل والتوقف المفاجئ لنظام المعلومات المحاسبي للبنك لبعض الوقت يؤدي إلى اهتزاز مكانة البنك أمام عملائه وتكبد البنك خسائر تجارية ومالية كبيرة.	3.47	.980	28.2	5.262	.000	قبول
	أولاً: تأثير المخاطر على إتاحة نظم المعلومات المحاسبية:						
80	حدوث مخاطر أمن نظم المعلومات المحاسبية يؤثر على سلامة تجهيز البيانات وعمليات التشغيل والمخرجات، بالدقة والشمولية المطلوبة وفي الوقت المناسب.	3.39	.913	27.0	4.660	.000	قبول
81	تشغيل النظام بشكل خاطئ وباستخدام برامج غير ملائمة يؤدي إلى حصول البنك لمخرجات غير دقيقة وغير سليمة، يؤثر على صحتها ومصداقيتها.	3.89	.910	23.4	10.735	.000	قبول
82	تعرض نظم المعلومات المحاسبية المحوسبة بالبنك إلى أي خطر يخفض من تكامل تلك النظم مع بعضها البعض على مستوى الأقسام والفروع، ففوق خطأ ما يؤدي إلى وقوع سلسلة من الأخطاء نتيجة التحديث الفوري للملفات.	3.54	.854	24.1	6.995	.000	قبول
	ثانياً: تأثير المخاطر على سلامة وتكامل تجهيز البيانات في نظم المعلومات المحاسبية:						
83	إن اقتحام نظام المعلومات المحاسبي من أطراف غير مخولة بالدخول، يؤدي إلى إمكانية سرقة أو تسرب معلومات هامة على درجة عالية من السرية لجهات غير مرغوب فيها.	3.66	1.147	31.3	6.393	.000	قبول
84	إن حدوث مخاطر أمن نظم المعلومات المحاسبية يؤدي إلى إطلاع المنافسين على المعلومات المرتبطة بالبنك والتي قد يترتب عليها الإضرار بالموقف التنافسي.	2.83	.664	23.5	-2.862	.005	رفض
85	إن حدوث المخاطر يؤدي إلى عدم قدرة نظام المعلومات المحاسبي في البنك على التعامل مع الأطراف المستفيدة المختلفة وفقاً لأصول السرية والفائدة المرجوة.	3.53	1.005	28.5	5.852	.000	قبول
	ثالثاً: تأثير المخاطر على سرية المعلومات المحاسبية:						
86	إن حدوث مخاطر أمن نظم المعلومات المحاسبية يؤدي إلى ضعف قدرة البنك في حماية خصوصيات وأسرار عملائه، نتيجة سرقة أو كشف المعلومات الشخصية لهم والتي يتم جمعها واستخدامها والإحتفاظ بها من قبل نظام المعلومات المحاسبي للبنك.	3.69	.882	24.0	8.621	.000	قبول
87	إن تعرض البنك لمخاطر أمن نظم المعلومات المحاسبية يهدد سمعته نتيجة فقدان الثقة وفشل البنك في تحقيق متطلبات العملاء بتقديم خدمة مصرفية إلكترونية متطورة وأمنة.	3.60	.924	25.7	7.152	.000	قبول
88	إن حدوث مخاطر أمن نظم المعلومات المحاسبية يؤدي إلى عدم إتاحة الفرصة للعملاء للوصول إلى المعلومات المخزنة الشخصية لتعديلها أو إلغائها.	3.42	.879	25.7	5.248	.000	قبول
	رابعاً: تأثير المخاطر على خصوصية بيانات الأطراف المتعاملة مع البنك:						
89	حدوث المخاطر يؤدي إلى تهرب بعض أطراف التعاملات الالكترونية من الالتزامات، عن طريق إنكار وقوع أحداث وقعت أو إدعاء وقوع أحداث لم تقع، وقد يؤدي ذلك إلى تحمل البنك لخسائر مالية وفقدان الثقة في مخرجات نظم المعلومات المحاسبية.	2.88	.766	26.6	-1.771	.079	رفض
90	رفض بعض الجهات الحكومية لحجية مخرجات نظم المعلومات المحاسبية المحوسبة استناداً لنصوص تشريعية، كالقانون التجاري وقانون البنوك.	2.79	.815	29.2	-2.887	.005	رفض
	خامساً: تأثير المخاطر على إثبات تصرفات الأطراف المتعاملة خلال تبادل البيانات إلكترونياً:						
	الآثار الناتجة عن مخاطر أمن نظم المعلومات المحاسبية المحوسبة						
91	يوجد في البنك قسم خاص ومستقل بشكل كافي وبإمكانيات مناسبة مسؤول عن تنفيذ أمن نظم المعلومات المحاسبية وحمايتها، ووضع معايير وأسس وضوابط أمنية.	2.64	.739	28.0	-5.388	.000	قبول
92	يوجد دليل عمل مكتوب يتضمن إجراءات أداء العمل لكافة وظائف نظم المعلومات المحاسبية، محدد فيه السلطات والمسؤوليات والكفاءات اللازمة لكل وظيفة داخل النظام.	3.49	.893	25.5	6.083	.000	رفض

رقم الفقرة	متغيرات الدراسة	المتوسط الحسابي Mean	الانحراف المعياري Std. Deviation	معامل الاختلاف	قيمة (t) المحسوبة	القيمة المعنوية Sig. (2-tailed)	نتيجة اختبار الفرضية العدمية
93	يوجد نظام صلاحية مبرمج بحيث يسمح النظام لكل مستخدم بإدارة نظام المعلومات المحاسبي حسب صلاحياته في التعامل مع ملفات النظام، (مثل قراءة البيانات أو نسخها أو تعديلها...الخ)، من خلال الوصول إلى أجزاء معينة وبيانات محددة.	3.79	.845	23.0	10.282	.000	رفض
94	كل مستخدم للنظام له كلمة سر خاصة، فلا يتشارك اثنان بكلمة سر واحدة، ويتم إيقاف صلاحيات المستخدم إذا تم إدخال كلمة المرور خطأ أكثر من العدد المسموح به للمحاولات.	4.18	.85	20.3	14.918	.000	رفض
95	هناك فصل سليم بين الوظائف والمهام المختلفة والمتعارضة لمعالجة البيانات بين المبرمجين والمشغلين والمراقبين والمستخدمين بطريقة تسمح بمراقبة تنفيذ المهام.	3.77	.831	22.0	10.240	.000	رفض
96	يعمل البنك على تنفيذ سياسة التوفير الوظيفي للمهام الأساسية لنظم المعلومات المحاسبية، بإجراء تنقلات بين الموظفين من حين لآخر، وإلزامهم بأخذ أجازاتهم السنوية دفعة واحدة.	2.43	.667	27.4	-9.501	.000	قبول
97	يعقد البنك برامج بواسطة مختصين في أمن نظم المعلومات لتوعية العاملين بالمخاطر التي تهدد أمن نظم المعلومات المحاسبية، وتدريبهم على إتباع الإجراءات الملزمة لمواجهتها.	2.44	.862	35.3	-7.134	.000	قبول
98	يتم تشجيع الأفراد على اتخاذ مبادرات لحل المشكلات، ومكافأة من يقوم بعمل إيجابي نحو تبسيط نظام الحماية، ومعاينة من يتعامل سلباً مع المخاطر ويخالفون سياسات الأمن.	2.78	.766	27.6	-3.191	.002	قبول
99	يعين البنك شخص مسؤول عن حماية النظام يسمى ضابط أمن المعلومات، ويتم تكوين فريق طوارئ، من فنيين وإداريين فاعلين، لمواجهة أي ظرف طارئ يمس بحماية النظام.	2.76	.680	24.6	-3.856	.000	قبول
100	يتم اختيار موظفي نظم المعلومات المحاسبية بحرص شديد وإجراء تحريات عنهم وعن ماضيهم الوظيفي، والحرص على أن يكونوا ذوي خبرة وثقة وأمانة ويعملون لمصلحة البنك، وعدم إعطاء الموظف حديث التعيين صلاحيات عالية لاستخدام النظام.	3.30	.984	29.8	3.309	.001	رفض
أولاً: حماية الأمن التنظيمي للأفراد العاملين في نظم المعلومات المحاسبية:							
101	توجد خطة طوارئ معلنة وموثقة خاصة لمواجهة الكوارث تتضمن إعداد وحدة متكاملة من تجهيزات الحاسوب والشبكات، ونسخة احتياطية من قاعدة البيانات، في موقع آخر بعيد غير الموقع الرئيسي لضمان استمرارية العمل، واستئناف النشاط بصورة سريعة.	2.66	.745	28.0	-4.980	.000	قبول
102	تتضمن خطة الطوارئ مصفوفة مخاطر أمن نظم المعلومات المحاسبية المتوقعة، والأثر الناتج، والجهة المتأثرة، والتصرف اللازم لمواجهتها.	2.51	.695	27.0	-7.813	.000	قبول
103	يتعاقد البنك مع شركات تأمين متخصصة للتأمين على الأجهزة والبرمجيات وشبكات المعلومات والموظفين في نظام المعلومات المحاسبي المحسوب، ضد كافة المخاطر.	3.40	1.041	30.6	4.258	.000	رفض
104	يتم تصميم مواقع العمل وأماكن الأجهزة والمعدات، بصورة تتلاءم مع التغيرات الطبيعية، ويتم وضع أجهزة النظام في غرف محمية وأمنة، وعدم السماح بالدخول إليها لأي كان.	3.16	.816	25.8	2.217	.028	رفض
105	يتم استخدام جميع الوسائل المادية التي تمنع الوصول غير المخول إلى نظم المعلومات المحاسبية وقواعدها كرجال الحراسة، والأقفال والحواجز والغرف المحصنة وغيرها.	3.69	.988	26.8	7.696	.000	رفض
106	يستخدم موظفي البنك بطاقات دخول الكترونية ذكية مغطاة عليها صورهم الشخصية، للدخول إلى أماكن عملهم عبر البوابات المقفلة المبرمجة وفق الصلاحيات المخولة لهم، ويصدر إنذار مبكر فور الدخول المادي غير المخول.	2.11	.800	37.9	-12.322	.000	قبول
107	يقوم البنك بتثبيت كاميرات تلفزيونية على خارج مبنى دائرة النظام والممرات الداخلية فيها، وتعمل على مراقبة المستخدمين والأماكن التي توجد تجهيزات النظام، من موقع مركزي.	3.76	.872	23.1	9.651	.000	رفض
108	يتم استخدام منظم كهربائي، وبطاريات إضافية، وخازنات طاقة، ومولد كهربائي لتجنب ارتفاع أو انخفاض الطاقة الكهربائية أو انقطاعها، وتعطلها بشكل مفاجئ، والذي يؤدي إلى تلف أجهزة وبرامج الحاسوب أو توقفها عن العمل.	4.12	.744	18.1	16.649	.000	رفض
109	يتم تركيب أجهزة كشف الحريق في الأماكن المعرضة للخطر وتجهيزها بالشكل المناسب الذي يساعد على كشف الحريق بأسرع وقت ممكن وسرعة القيام بمقاومة الحريق.	4.16	.753	18.1	17.059	.000	رفض
110	يتم استخدام أسقف وحواظ وأرضيات تمنع تسرب المياه، مع استخدام أغطية واقية من الأتربة والماء، وتركيب أجهزة إنذار من المياه والرطوبة.	3.52	1.107	31.4	5.232	.000	رفض
111	يتم إجراء صيانة دورية ومستمرة لأجهزة النظام ووسائل حماية بما فيها أجهزة التكييف، لضمان استمرار عملها بفاعلية، ويتم توفير قطع ومعدات بديلة للأجهزة العاملة بشكل سريع فور تعطلها، بما يضمن سلامة الحواسيب وحمايتها.	3.65	.951	26.1	7.612	.000	رفض
ثانياً: حماية الأمن المادي لنظم المعلومات المحاسبية المحوسبة:							
112	يتم التحقق من هوية الشخص أو المعدات التي تحاول الدخول للنظام من خلال خليط من (كلمات مرور / كروت ذكية / معرفات بيولوجية / أجهزة أخرى).	3.73	.872	23.4	9.237	.000	رفض
113	يتم استخدام مستويات متتالية من الرقابة على دخول قاعدة البيانات بكلمات مرور متعددة ومختلفة للدخول إلى (الشبكة أو الحاسوب أو سيرفر البيانات أو قاعدة البيانات)، ويتم التنبيه للموظفين بعدم إقضاء كلمات المرور لسرية، وتكون من الصعب تخمينها.	3.69	1.012	27.4	7.507	.000	رفض

رقم الفقرة	متغيرات الدراسة	المتوسط الحسابي Mean	الانحراف المعياري Std. Deviation	معامل الاختلاف	قيمة (t) المحسوبة	القيمة المعنوية Sig. (2-tailed)	نتيجة اختبار الفرضية العدمية
114	يوجد سجل خاص لجميع الصلاحيات الممنوحة للموظفين المخولين بالدخول للنظام، ويتم برمجة مصفوفة الرقابة على الوصول الآلي، فيتم تحديد كلمة سر خاصة لكل موظف، والملفات أو البرامج التي يصرح له بالوصول إليها.	3.76	.909	24.2	9.257	.000	رفض
115	يتم تغيير كلمات السر بشكل دوري ومستمر وخاصة بعد نقل الموظفين ويتم إلغاء كلمة السر الخاصة بالموظف الذي استقال أو أقيل من العمل بشكل فوري.	3.87	.926	24.0	10.356	.000	رفض
116	يتم استخدام برامج الجدران النارية العازلة لمنع الوصول غير المصرح به إلى النظام، ومنع المستخدم من استخدام برامج أو ملفات لا يملك الصلاحية للدخول إليها، ويتم تحديث تلك البرامج وتعديلها باستمرار.	3.45	1.004	29.1	4.955	.000	رفض
117	يوثق النظام كافة محاولات الوصول غير المصرح بها، ويصدر تقرير حولها يتضمن وقت المحاولة والموقع الذي تمت من خلاله، ويتم معالجة ذلك بإغلاق الفجوات المكتشفة.	3.45	1.053	30.6	4.728	.000	رفض
118	يتم إجراء اختبار اختراق النظام بصورة دورية من قبل المراجعين الداخليين أو الخارجيين، أو بواسطة خبرات متخصصة لمعرفة نقاط الضعف في نظم المعلومات الحاسوبية.	2.30	.726	31.6	-10.600	.000	قبول
119	يحرص البنك على تحميل واستخدام برامج متطورة وأصلية وفعالة مضادة لفيروسات الحاسوب وبرمجياته الخبيثة، ويتم تحديثها بشكل دوري ومستمر.	3.19	.865	27.1	2.406	.018	رفض
120	يتم استخدام وسيلة التشفير لكافة البيانات والمعلومات الهامة المحفوظة في قاعدة البيانات.	2.79	.864	31.0	-2.722	.007	قبول
	ثالثاً: حماية أمن الوصول البرمجي لقاعدة البيانات المتصلة بنظم المعلومات الحاسوبية:	3.35	.689	21.0	5.752	.000	رفض
121	يقوم البنك بأخذ نسخ احتياطية للبرامج وملفات البيانات الهامة بشكل مستمر ودوري (يومي، أسبوعي، شهري)، وتحفظ في خزائن حديدية مقللة لحمايتها من السرقة أو الحريق، وتوضع نسخة منها في مكان آمن خارج مقر العمل.	4.34	.689	15.9	21.531	.000	رفض
122	يتم تشفير النسخ الاحتياطية من قواعد البيانات لحمايتها من التعديل أو الوصول إليها بطريقة غير مشروعة وذلك لفرض الرقابة عليها.	2.46	.728	29.6	-8.197	.000	قبول
123	توجد رقابة كافية على وسائط تخزين البيانات غير المتصلة بالنظام، ويتم فحص تلك الوسائط باستمرار للتأكد من صحتها وسلامتها.	3.24	.881	27.2	2.977	.004	رفض
124	يتم التخلص من وسائط تخزين البيانات والبرامج بطريقة آمنة معينة وعدم رميها في براميل القمامة، حيث توجد إجراءات رقابية كافية لذلك.	3.61	1.064	29.5	6.294	.000	رفض
	رابعاً: حماية أمن وسائط التخزين غير المتصلة بنظم المعلومات الحاسوبية:	3.41	.627	18.4	7.252	.000	رفض
125	مستندات إدخال البيانات دقيقة وشاملة لمختلف العمليات، وتساعد على تقليل الأخطاء، ويتم إعدادها وتعبئتها ومصادقتها من الأشخاص المخولين فقط، ويوجد برنامج خاص مصمم لمعرفة من قام بإدخال البيانات.	3.57	.890	24.9	7.014	.000	رفض
126	يتم تسجيل بيانات المخلات أولاً بأول وتوجد رقابة كافية لاكتشاف أي نقص فيها، ويتم توثيق عمليات إدخال البيانات بما فيها المحاولات، والمخالفات الخاطئة، ومعرفة مصدرها.	3.37	.706	20.9	5.766	.000	رفض
127	يتم تحديد أخطاء إدخال البيانات وتتبعها حتى يتم تصحيحها وتتضمن برامج النظام ضوابط تمنع إدخال بيانات خاطئة، حيث تظهر رسالة تحذيرية على الشاشة في حال وجود خطأ.	3.43	.792	23.1	6.056	.000	رفض
128	توجد مراجعة تفصيلية للبيانات المدخلة للتأكد من دقتها واكتمالها، ويتم إجراء المراجعة الثانية لبيانات المستندات المدخلة للتأكد من سلامتها.	3.72	.730	19.6	10.910	.000	رفض
129	تتوفر في نظم المعلومات الحاسوبية خاصية تصحيح البيانات الخاطئة التي تم إدخالها في الوقت المناسب ضمن حدود الرقابة المسموح بها.	3.20	.861	26.9	2.626	.010	رفض
	خامساً: حماية أمن مدخلات نظم المعلومات الحاسوبية:	3.46	.585	16.9	8.658	.000	رفض
130	يحتوي برنامج التشغيل على وسائل تحدد صلاحية المستخدمين في تشغيل وتحديث البيانات ومنع قراءتها أو نسخها أو تعديلها من غير المخول لهم ذلك.	3.81	.806	21.1	11.116	.000	رفض
131	توجد رقابة آلية مدمجة داخل النظام، من خلا تقارير تحليلية إلكترونية لتفاصيل العمليات التشغيلية، تحدد شخص المستخدم ووقت بداية ونهاية الاستخدام، ومكانه وطبيعة الاستخدام، والأخطاء المكتشفة آلياً، ويتم متابعة تلك التقارير بشكل مستمر.	3.37	.694	20.6	5.864	.000	رفض
132	توجد إجراءات كافية تضمن تصحيح الأخطاء، وإعادة تشغيل البيانات التي لم يتم تشغيلها بسبب توقف دورة التشغيل والتأكد من تمام معالجتها، ويتم تمييز العمليات التي تمت معالجتها لتلافي تكرار تشغيلها.	3.41	.713	20.9	6.467	.000	رفض
133	توجد إجراءات للتأكد من أن معالجة البيانات قد تمت بشكل كامل عند حد الانقطاع، من نقطة توقف معينة عند توقف دورة التشغيل لسبب من الأسباب.	3.45	.863	25.0	5.767	.000	رفض
134	يتم توقيف عمل التطبيقات الحاسوبية إجبارياً نهاية الدوام الرسمي، فلا يسمح بتشغيل النظام خارج فترة الدوام المحددة والمبرمجة آلياً، بحيث يتعذر تشغيله النظام خلاف ذلك.	2.39	.733	30.7	-9.133	.000	قبول
	سادساً: حماية أمن عمليات التشغيل البرمجي لنظم المعلومات الحاسوبية:	3.28	.539	16.4	5.802	.000	رفض
135	يتم حصر أنواع المعلومات وتصنيفها إلى فئات وفقاً لدرجة أهميتها وسريتها، وتحديد	2.84	.708	24.9	-2.556	.012	قبول

رقم الفقرة	متغيرات الدراسة	المتوسط الحسابي Mean	الانحراف المعياري Std. Deviation	معامل الاختلاف	قيمة (t) المحسوبة	القيمة المعنوية Sig. (2-tailed)	نتيجة اختبار الفرضية العدمية
	مستوى الحماية الواجب توفيره لكل فئة منها.						
136	توجد وسائل وإجراءات كافية لعملية توزيع المخرجات، لضمان وصول التقارير والوثائق للجهات المعنية المخولة فقط باستلامها.	2.78	.686	24.7	-3.561	.001	قبول
137	يتم إجراء صيانة دائمة لوسائل الإخراج (طابعات، فاكسات، شاشات... الخ)، لضمان سلامة عرض المخرجات.	3.57	.823	23.0	7.590	.000	رفض
138	يتم إعداد نسخ مطبوعة لبعض المعلومات المحاسبية الهامة، وتشفير المعلومات الحساسة.	3.39	.940	27.7	4.619	.000	رفض
139	يتيح النظام مسار معين لمراجعة وتتبع سير المعاملات من مرحلة المدخلات إلى مرحلة المخرجات، والعكس.	3.23	.831	25.7	3.050	.003	رفض
140	يقوم البنك بإتلاف المخرجات المهمة والسرية بعد الانتهاء من استخدامها بواسطة لجنة متخصصة ومخولة بذلك، ويتم الإتلاف داخل البنك.	3.30	.889	26.9	3.765	.000	رفض
	سابعاً: حماية أمن مخرجات نظم المعلومات المحاسبية المحوسبة:	3.18	.590	18.6	3.449	.001	رفض
141	تستخدم برامج الجدران النارية لتحديد المعلومات التي يسمح بدخولها أو خروجها من وإلى نظام المعلومات المحاسبي المحسوب للبنك.	3.56	.891	25.0	6.908	.000	رفض
142	يتم تشفير البيانات المرسلة عبر الشبكات للتأكد من أنه لم يتم الكشف عنها أو تعديلها وأنها مرسلة من الجهة المعنية، وتتوفر وسائل حماية كافية للحفاظ على سرية مفتاح التشفير.	3.20	.663	20.7	3.275	.001	رفض
143	يستخدم البنك التوقيع الرقمي الإلكتروني، كوسيلة للتحقق من موثوقية المستخدمين بشكل غير قابل للتزيف، ولضمان عدم إنكار الأطراف المعنية المشاركة في الوثائق الإلكترونية.	2.68	.805	30.0	-4.383	.000	قبول
144	يتم استخدام شهادة رقمية صادرة من جهة فنية معتمدة، عند إرسال أو استلام البيانات عبر الشبكة الخارجية، للتحقق من هوية مرسل الرسائل، وموثوقية المستخدم.	2.46	.532	21.6	-11.224	.000	قبول
145	يتم استخدام بروتوكولات أمنية بين البنك والأطراف المتعاملة للحفاظ على سرية المعلومات المحاسبية والتحقق من وصولها للجهة المطلوبة أثناء إجراء المعاملات المالية.	3.28	.718	21.9	4.282	.000	رفض
	ثامناً: حماية أمن البيانات المنقولة عبر شبكات نظم المعلومات المحاسبية المحوسبة:	3.03	.506	16.7	.750	.455	رفض
146	توجد إجراءات كافية وفعالة لمراقبة عمليات تطوير البرامج والتطبيقات المحاسبية، وفق معايير وإجراءات واضحة ومكتوبة ومحددة.	3.25	.956	29.4	2.841	.005	رفض
147	لا تتم أية تعديلات في برمج النظام بدون حصول المبرمجين المختصين على موافقات رسمية من الإدارات المعنية المخولة.	3.53	1.114	31.6	5.279	.000	رفض
148	هناك فريق متخصص لتعديل وتطوير نظام المعلومات المحاسبي من داخل البنك، وتشرف إدارة البنك على تعديل وتطوير النظام.	3.80	.802	21.1	10.947	.000	رفض
149	يتم إجراء الاختبار المبدئي بالتشغيل التجريبي للبرامج الجديدة وتعديلاتها قبل اعتمادها بشكل نهائي للتأكد من سلامتها، وقدرتها على تتبّع الأخطاء التي قد تحدث أثناء التنفيذ.	3.61	.982	27.3	6.908	.000	رفض
150	يتم توثيق كافة التعديلات التي تتم على البرامج والمعدات، وفق الإجراءات المتبعة.	3.52	1.038	29.9	5.581	.000	رفض
	تاسعاً: حماية أمن تعديل وتطوير نظم المعلومات المحاسبية المحوسبة:	3.54	.819	23.1	7.315	.000	رفض
	إجراءات ووسائل الحماية المطبقة لمواجهة مخاطر أمن نظم المعلومات المحاسبية المحوسبة	3.35	.553	16.5	6.971	.000	رفض

درجة الحرية (df=121)

نبذة عن الباحث

- من مواليد 27 تشرين أول (أكتوبر) 1972م، بمديرية حَمَر محافظة عمران في الجمهورية اليمنية.
- متزوج وله سبعة أبناء: (عبير، أكرم، طارق، عمَّار، عبدالرحمن، شام، أريج).
- درس التعليم الأساسي (الابتدائية والإعدادية) بمدرسة السلام بمديرية حَمَر - بمحافظة عمران وكان ترتيبه الأول على المركز التعليمي بتلك المديرية في الشهادتين الإبتدائية والإعدادية.
- درس المرحلة الثانوية في ثانوية الزعيم جمال عبدالناصر بأمانة العاصمة صنعاء وحصل على شهادة الثانوية العامة في عام 1992م بمعدل 87 % (القسم العلمي).
- ألتحق في العام 1993/1994م، بجامعة صنعاء كلية التجارة والاقتصاد قسم المحاسبة والمراجعة وكان خلال دراسته من أوائل الطلبة على النحو التالي:

العام الجامعي	المستوى	عدد الطلبة	الترتيب	التقدير
1994 /93	الأول	3372	الثالث	جيد جداً
1995 /94	الثاني	1488	الأول	ممتاز
1996 /95	الثالث	874	الثاني	جيد جداً
1997/96	الرابع	493	الثالث	جيد جداً مع مرتبة الشرف

- تعين معيداً بقسم المحاسبة بكلية التجارة والاقتصاد في جامعة صنعاء في العام الجامعي 1999/98م.
- في عام 2000 م صدر قرار إيفاده إلى الهند وكذلك إلى مصر 2002م ولم يسافر لظروف اجتماعية خاصة، واستمر بالعمل معيداً بقسم المحاسبة لمدة (6) سنوات من 1998 حتى نهاية 2004 م.
- في نهاية العام 2004 م سنحت الفرصة وتم إيفاده من جامعة صنعاء إلى جامعة آل البيت في المملكة الأردنية الهاشمية لنيل درجة الماجستير في المحاسبة.
- وفي 21 أيار (مايو) 2007 م حصل على درجة الماجستير في المحاسبة من كلية إدارة المال والأعمال بجامعة آل البيت في الأردن بتقدير " إمتياز " عن رسالته الموسومة: "مدى تأثير العوامل البيئية والتنظيمية والسلوكية والتكنولوجية على فاعلية نظم المعلومات المحاسبية لدى البنوك التجارية في الجمهورية اليمنية – دراسة ميدانية"، وبمعدل تراكمي لجميع الساعات التدريسية المعتمدة 91.88%، وكان ترتيبه الأول على طلاب الفوج التاسع لماجستير المحاسبة.
- عمل مدرس مساعد بقسم المحاسبة بكلية التجارة والاقتصاد في جامعة عمران للعامين 2008م و2009م.
- في العام 2010 م تم إيفاده من جامعة عمران إلى جامعة دمشق لنيل درجة الدكتوراه في المحاسبة.

- وفي 7 أيار (مايو) 2018 م حصل على درجة الدكتوراه في المحاسبة من كلية الاقتصاد بجامعة دمشق بتقدير "إمتياز" وبعلامة قدرها (91) درجة عن أطروحته الموسومة: " تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية - دراسة تطبيقية".

▪ الخبرات المهنية:

1. عمل متدرب على أعمال المحاسبة في بعض مكاتب التدقيق بصنعاء 1996م.
2. رئيس قسم بالإدارة المالية لإحدى الشركات الخاصة في صنعاء للفترة من 1997/8 حتى 1998/10.
3. مساعد مدقق خارجي بمكتب مراجعة وتدقيق في صنعاء للفترة من 2001م - 2004 م.

▪ الخبرات الأكاديمية:

1. معيد في جامعتي صنعاء وعمران من 1998م وحتى العام 2004 م.
2. مدرس مساعد متفرغ في جامعة عمران للعامين 2008 و 2009 م.
3. مدرس غير متفرغ في جامعات خاصة في اليمن للفترة 2009/2008 م.

▪ المواد التي تم تدريسها:

1. مبادئ المحاسبة المالية.
2. محاسبة شركات أشخاص وأموال، ومحاسبة المنشآت المالية.
3. محاسبة ضريبية، ومحاسبة إدارية، ومحاسبة المنشآت المتخصصة.
4. نظم المعلومات المحاسبية، ونظرية المحاسبة.

▪ أبحاث منشورة:

1. " قدرة المراجعة الداخلية على رفع فاعلية إدارة المخاطر المصرفية لدى البنوك التجارية اليمنية - دراسة ميدانية"، بحث مقبول للنشر، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، جامعة دمشق، سوريا، 2011 م.
2. " مدى تأثير استخدام تكنولوجيا المعلومات على فاعلية نظم المعلومات المحاسبية لدى البنوك التجارية اليمنية - دراسة ميدانية"، بحث مقبول للنشر، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، جامعة دمشق، سوريا، 2011 م.
3. " مدى تأثير العوامل التنظيمية والسلوكية على فاعلية الرقابة الداخلية التطبيقية في بيئة تكنولوجيا المعلومات - دراسة استطلاعية لدى البنوك التجارية اليمنية"، بحث مقبول للنشر، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، جامعة دمشق، سوريا، 2011 م.
4. " مدى تأثير استخدام الصيرفة الإلكترونية على فاعلية الرقابية التطبيقية لنظم المعلومات المحاسبية المحوسبة - دراسة ميدانية لدى البنوك التجارية اليمنية"، بحث مقبول للنشر، مجلة الباحث الجامعي، جامعة إب، اليمن، 2012 م.

وبالله التوفيق والسداد،،،

SUMMARY OF THE STUDY

***« Evaluating the Risks of the Security Computerized
Accounting Information Systems
at the Commercial Banks in Republic of Yemen »
" An Applied Study"
Thesis Submitted for PhD Degree in Accounting***

Prepared By: *Abdul-karim Mohammed Yahya Fadhel*

Scientific Supervisor: *Prof. Dr. Atta-Allah Warrad Khalil*

Damascus University - 2018

This study aimed to assess the risks to the Security of computerized accounting information systems in The Republic of Yemen by:

Identifying the most important fundamental risks that occur and threaten the security of those systems, Recognizing the internal and external threats that cause risks to the security of those systems, Measuring the impact of these risks on the main components of those system, which are represented by (availability of systems, operation safety, healthiness and integration, confidentiality and privacy of the outputs of those systems, and the denial of transacting parties); Verifying the compliance of commercial banks in Republic of Yemen with the methods and procedures of protection according to the local rules and international norms and standards with regard to the security of information systems; Evaluating the impact of these methods and procedures on security risks at those banks with the aim of identifying the weaknesses and strengths at computerized accounting information systems; and Showing how those risks differs among commercial banks in the Republic of Yemen pursuant to bank ownership, quality of used system and level of correlation of accounting information systems with the network of communications.

To achieve these objectives, the study has adopted the analytical descriptive approach, taking into consideration the previous relevant studies, the researcher has performed an exploratory surveying study at three commercial banks representing different economic sectors (public, private and mixed one) depending on practical statements extracted from the interviews and observations.

This was supported also by a surveying study for all commercial banks in the Republic of Yemen through designing and developing a scientific inquiry-based and well-organized questionnaire, The analysis of statements and the test of presumptions on Statistical Packages for Social Sciences (SPSS).

According to applied study - with its two exploratory and field parts – the research has found many results. The most important of those conclusions are the following:

- 1. In spite of the existence of many risks threatening the security of computerized accounting information systems at commercial banks in the Republic of Yemen, there weren't any serious risks which could threaten the security of those systems. On the contrary, they were very limited in view of the limitedness of technology used in the Republic of Yemen and due to the fact that commercial banks in Republic of Yemen have and use protection procedures that differ in one way or another to control those risks.*
- 2. The occurrence of security risks in the computerized accounting information systems at commercial banks in the Republic of Yemen has influences on the elements constituting the security of those systems which are represented by (availability of systems, operation safety, healthiness and integration, confidentiality and privacy of accounting information and denial of operations) at these banks, where it was found that those influences are high in general and cause negative impacts on the security of those systems.*
- 3. There is a difference in the amount of risks that commercial banks expose to in the Republic of Yemen which differs according to the type of sector to which these banks belong. It was found that risks increase progressively at each of (private, mixed and public sector banks) successively. However, in spite of all this, there is no essential difference of a statistical indication between those banks in general with respect to the amount of risks that threaten the security of computerized accounting information systems which can be attributed to the ownership of these banks.*

In the light of results reached by this study, researcher suggested a number of recommendations and suggestions. The following are the most significant:

- 1. Necessity of the commitment of executive managements and supreme administration at commercial banks of Yemen to perform a periodic and continuous assessment to the risks to the security of information systems and to give more attention to these risk, and also the importance of predicting them before their happening to find the most suitable solutions for them in the case of their occurrence, to identify the ways that can restore work balance, and to put emergency plans for ensuring the security of computerized accounting information systems.*
- 2. There must be an integral, comprehensive, written and applicable strategy for assessing and managing the risks to the security of accounting information systems and to clearly identify the sources of those risks. This strategy must include the level of risks that is accepted by bank and reflects the priorities of bank in managing the risks according to a scientific methodology and based on clear scientific rules in the field of evaluating and management of those risks.*

■ **Key words:** *Assessing Risks, Security of Information Systems, Computerized Accounting Information Systems, Commercial Banks, Republic of Yemen.*

*The Syrian Arab Republic
Damascus University
College of Economics
Accounting Department*



*Evaluating Risks of the Security Computerized
Accounting Information Systems
at the Commercial Banks in Republic of Yemen
"An Applied Study"*

Thesis Submitted for PhD Degree in Accounting

Prepared By

Abdul-karim Mohammed Yahya Fadhel

Scientific Supervisor

Prof. Dr. Atta-Allah Warrad Khalil

Damascus University

Participant Supervisor

Prof. Dr. Abdul-malek Esmail Hajar

Sana'a University

2018

ملخص الدراسة

« تَقْيِيمُ مَخَاطِرِ أَمْنِ نُظْمِ الْمَعْلُومَاتِ الْمَحَاسِبِيَّةِ الْمُحَوَّسَةِ لدى البنوك التجارية في الجمهورية اليمنية » - "دراسة تطبيقية"

أطروحة مُقدِّمة لِنَيْلِ دَرَجَةِ الدُّكُورَاهِ فِي الْمَحَاسَبَةِ

إعداد الباحث: عبدالكريم محمد يحيى فاضل

إشراف الأستاذ الدكتور: عطا الله وراد خليل

جامعة دمشق: 2018

هدفت هذه الدراسة إلى تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية، من خلال التعرف على أهم المخاطر الجوهرية التي تحدث وتهدد أمن تلك النظم، وتحديد التهديدات الداخلية والخارجية المسببة لحدوث مخاطر أمن تلك النظم، وقياس مدى تأثير تلك المخاطر على العناصر الرئيسية المكونة لأمن تلك النظم الممتثلة ب (إتاحة النظم، وصحة وسلامة وتكامل التشغيل، وسرية وخصوصية مخرجات تلك النظم، وعدم إنكار حدوث العمليات من الأطراف المتعاملة)، والتحقق من مدى تطبيق البنوك التجارية في الجمهورية اليمنية لأساليب وإجراءات الحماية وفق القواعد المحلية والأسس والمعايير الدولية لأمن نظم المعلومات، وقياس تأثير تلك الأساليب والإجراءات على المخاطر الأمنية في تلك البنوك، بهدف تشخيص نقاط القوة والضعف في أمن نظم المعلومات المحاسبية المحوسبة، بالإضافة إلى بيان مدى اختلاف تلك المخاطر بين البنوك التجارية في اليمن باختلاف ملكية البنك ونوعية النظام المستخدم ومستوى ارتباط نظم المعلومات المحاسبية بشبكة الاتصالات.

ولتحقيق تلك الأهداف فقد اعتمدت الدراسة على المنهج الوصفي التحليلي، فبعد أن قام الباحث بالاطلاع على الدراسات السابقة، وعلى الخلفية النظرية للدراسة، قام بإجراء دراسة حالة عملية تطبيقية لدى ثلاثة بنوك تجارية تمثل القطاعات الاقتصادية المختلفة (العامة والخاصة والمختلطة)، من خلال بيانات عملية، وتم تعزيز ذلك بدراسة مسحية شاملة لجميع البنوك التجارية العاملة في الجمهورية اليمنية، من خلال تصميم وتطوير قائمة استقصاء محكمة، وقد تم تحليل البيانات واختبار الفرضيات باستخدام الأساليب الوصفية والتحليلية المناسبة، اعتماداً على الحزمة الإحصائية للعلوم الاجتماعية (SPSS).

واستناداً للدراسة التطبيقية - بشقيها الاستكشافية والميدانية - فقد توصلت الدراسة إلى الكثير من النتائج كان من أبرزها ما يلي:

1. بالرغم من وجود العديد من المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية إلا أنه لا تحدث مخاطر جوهرية ذات أهمية نسبية تهدد أمن تلك النظم بل كانت محدودة نتيجة محدودية التقنية المستخدمة في البيئة اليمنية، ولأن البنوك التجارية في الجمهورية اليمنية تمتلك وسائل وتستخدم مجموعة من إجراءات الحماية المختلفة بشكل أو بآخر للسيطرة على تلك المخاطر.
2. يؤثر حدوث مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في الجمهورية اليمنية على العناصر المكونة لأمن تلك النظم المتمثلة ب (إتاحة النظم، وصحة وسلامة وتكامل التشغيل، وسرية وخصوصية المعلومات المحاسبية، وعدم إنكار العمليات) لدى تلك البنوك، حيث وجد أن تلك التأثيرات مرتفعة بشكل عام وتتسبب في تأثيرات سلبية على أمن تلك النظم.
3. يوجد اختلاف في حجم المخاطر التي تتعرض لها البنوك التجارية في الجمهورية اليمنية باختلاف شكل ملكية البنك للقطاعات المختلفة التي تنتمي لها تلك البنوك، حيث وجد أن المخاطر تزداد بشكل تصاعدي لدى كلاً من (بنوك القطاع الخاص ثم بنوك القطاع المختلط ثم بنوك القطاع العام) على الترتيب، ولكن بالرغم من ذلك لا يوجد فرق جوهري دال إحصائياً بين تلك البنوك بشكل عام فيما يتعلق بحجم المخاطر التي تهدد أمن نظم المعلومات المحاسبية المحوسبة يُعزى لملكية تلك البنوك.

وفي ضوء النتائج التي توصلت لها الدراسة قدم الباحث مجموعة من التوصيات والمقترحات، فيما يلي أهمها:

1. ضرورة التزام الإدارات التنفيذية والإدارة العليا لدى البنوك التجارية في الجمهورية اليمنية بالتقييم الدوري والمستمر لمخاطر أمن نظم المعلومات والاهتمام بتأثير تلك المخاطر وضرورة توقعها قبل حدوثها وإيجاد الحلول المناسبة لها في حال وقوعها، وإيجاد السبل الكفيلة باستعادة العمل ووضع خطط الطوارئ اللازمة لضمان أمن نظم المعلومات المحاسبية المحوسبة.
2. ينبغي وجود إستراتيجية شاملة ومتكاملة وواضحة ومكتوبة وقابلة للتطبيق لتقييم وإدارة مخاطر أمن نظم المعلومات المحاسبية، وأن تحدد بوضوح مصادر تلك المخاطر، كما يجب أن تشمل الإستراتيجية مستوى المخاطر التي يتقبلها البنك والذي يعكس تحديد أولويات البنك في إدارته للمخاطر، وفق منهجية علمية تستند إلى معايير وقواعد علمية واضحة في مجال تقييم عمليات إدارة المخاطر.

■ **كلمات مفتاحية:** تقييم مخاطر، أمن نظم المعلومات، نظم المعلومات المحاسبية المحوسبة، البنوك التجارية، الجمهورية اليمنية.

SUMMARY OF THE STUDY

**« Evaluating the Risks of the Security Computerized
Accounting Information Systems
at the Commercial Banks in Republic of Yemen »
" An Applied Study"
Thesis Submitted for PhD Degree in Accounting**

Prepared By: *Abdul-karim Mohammed Yahya Fadhel*

Scientific Supervisor: *Prof. Dr. Atta-Allah Warrad Khalil*

Damascus University - 2018

This study aimed to assess the risks to the Security of computerized accounting information systems in The Republic of Yemen by:

Identifying the most important fundamental risks that occur and threaten the security of those systems, Recognizing the internal and external threats that cause risks to the security of those systems, Measuring the impact of these risks on the main components of those system, which are represented by (availability of systems, operation safety, healthiness and integration, confidentiality and privacy of the outputs of those systems, and the denial of transacting parties); Verifying the compliance of commercial banks in Republic of Yemen with the methods and procedures of protection according to the local rules and international norms and standards with regard to the security of information systems; Evaluating the impact of these methods and procedures on security risks at those banks with the aim of identifying the weaknesses and strengths at computerized accounting information systems; and Showing how those risks differs among commercial banks in the Republic of Yemen pursuant to bank ownership, quality of used system and level of correlation of accounting information systems with the network of communications.

To achieve these objectives, the study has adopted the analytical descriptive approach, taking into consideration the previous relevant studies, the researcher has performed an exploratory surveying study at three commercial banks representing different economic sectors (public, private and mixed one) depending on practical statements extracted from the interviews and observations.

This was supported also by a surveying study for all commercial banks in the Republic of Yemen through designing and developing a scientific inquiry-based and well-organized questionnaire, The analysis of statements and the test of presumptions on Statistical Packages for Social Sciences (SPSS).

According to applied study - with its two exploratory and field parts – the research has found many results. The most important of those conclusions are the following:

- 1. In spite of the existence of many risks threatening the security of computerized accounting information systems at commercial banks in the Republic of Yemen, there weren't any serious risks which could threaten the security of those systems. On the contrary, they were very limited in view of the limitedness of technology used in the Republic of Yemen and due to the fact that commercial banks in Republic of Yemen have and use protection procedures that differ in one way or another to control those risks.*
- 2. The occurrence of security risks in the computerized accounting information systems at commercial banks in the Republic of Yemen has influences on the elements constituting the security of those systems which are represented by (availability of systems, operation safety, healthiness and integration, confidentiality and privacy of accounting information and denial of operations) at these banks, where it was found that those influences are high in general and cause negative impacts on the security of those systems.*
- 3. There is a difference in the amount of risks that commercial banks expose to in the Republic of Yemen which differs according to the type of sector to which these banks belong. It was found that risks increase progressively at each of (private, mixed and public sector banks) successively. However, in spite of all this, there is no essential difference of a statistical indication between those banks in general with respect to the amount of risks that threaten the security of computerized accounting information systems which can be attributed to the ownership of these banks.*

In the light of results reached by this study, researcher suggested a number of recommendations and suggestions. The following are the most significant:

- 1. Necessity of the commitment of executive managements and supreme administration at commercial banks of Yemen to perform a periodic and continuous assessment to the risks to the security of information systems and to give more attention to these risk, and also the importance of predicting them before their happening to find the most suitable solutions for them in the case of their occurrence, to identify the ways that can restore work balance, and to put emergency plans for ensuring the security of computerized accounting information systems.*
- 2. There must be an integral, comprehensive, written and applicable strategy for assessing and managing the risks to the security of accounting information systems and to clearly identify the sources of those risks. This strategy must include the level of risks that is accepted by bank and reflects the priorities of bank in managing the risks according to a scientific methodology and based on clear scientific rules in the field of evaluating and management of those risks.*

■ ***Key words:*** *Assessing Risks, Security of Information Systems, Computerized Accounting Information Systems, Commercial Banks, Republic of Yemen.*