الجمهورية العربية السورية

جامعة دمشق

كلية الاقتصاد/قسم المحاسبة

ماجستير تدقيق الحسابات

دورُ ضوابط أمن المعلومات في تفعيلِ نظام الرقابة الداخلية

(دراسةٌ ميدانيّةٌ)

رسالةٌ مقدّمة لاستكمالِ متطلّبات الحصول على درجة الماجستير في تدقيق الحسابات.

إعداد الطالب:

ساريه عبد الرحمن الصواف

إشراف:

أ.د. رشا حمادة

الأستاذ في قسم المحاسبة – كلية الاقتصاد – جامعة دمشق

2021م

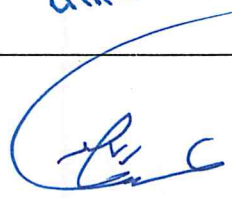
الجمهورية العربية السورية

جامعة دمشق

كلية الاقتصاد/قسم المحاسبة

ماجستير تدقيق حسابات

لقد تم إجراء التعديلات التي طلبت من قبل السادة أعضاء لجنة الحكم على رسالة الماجستير المؤلفة من السادة الأساتذة:

الاسم والمرتبة العلمية	التوقيع
د. رشا حماده **عضواً مشرفاً** الأستاذ في قسم المحاسبة-كلية الاقتصاد-جامعة دمشق.	
د. علي يوسف **عضواً** الأستاذ المساعد في قسم المحاسبة-كلية الاقتصاد-جامعة دمشق.	
د. رياض عبد الرؤوف **عضواً** المدرس في قسم المحاسبة-كلية الاقتصاد-جامعة دمشق.	

الجمهورية العربية السورية

جامعة دمشق

كلية الاقتصاد/قسم المحاسبة

ماجستير تدقيق حسابات

التصريح

دورُ ضوابط أمن المعلومات في تفعيلِ نظام الرقابة الداخلية (دراسةٌ ميدانيّةٌ)

أصرح بأن هذه الرسالة غير مقتبسة أو منقولة أو محرفة من أي عمل علمي آخر، ولم يسبق أن قُبل للحصول على أيه شهادات أو درجة عملية.

التاريخ: 2021/9/20

سارية الصواف

بسم الله الرحمن الرحيم



إهداء

إلى والدي ووالدتي الكريمين حفظهما الله وأدام صحتهما

إلى أخوتي وأخواتي الأعزاء

إلى أصدقائي بل أخوتي الذين لم تلدهم أمي

إلى كلّ من وسعهم قلبي، ولم تسعهم مذكّرتي

إلى كلّ من علّمني، أو دعمني بكلمةٍ طيّبة، أو دعاء خير، أو نصيحة

لكلّ طالبِ علمٍ، أو باحثٍ مجتهد ... أهدي هذا العمل المتواضع

شكرٌ وتقدير

بسم الله الرّحمن الرّحيم، والصّلاة والسّلام على أشرفِ المرسلين سيّدنا محمّد عليه أفضلُ الصّلاةِ وأتمّ التّسليم.

أحمدُ اللهَ تعالى حمداً كثيراً طيّباً مباركاً فيه أن منَّ علي بفضله ونعمه بما لا يُعدّ ولا يُحصى فأكرمني بإتمامِ هذه الدراسة.

وأتقدّمُ بخالصِ الشّكر والتّقدير للأستاذة الدكتورة: رشا حمادة لتفضّلها بالإشراف على هذه الدراسة، ولما قدّمته لي من عونٍ صادقٍ، وإرشادٍ أمين، وتوجيهٍ سديد، إذ لم تبخل عليّ بالنّصائح، والتوجيهات العلميّة، والمنهجيّة في سبيل إنجاز هذه الدراسة.

كما أتقدّمُ بعظيم الشّكرِ للأساتذة الكرام أعضاء لجنةِ المناقشة الموقّرة لتفضّلهم بقبولِ مناقشة هذه الرسالة، وعلى ملاحظاتهم القيّمة التي سيكونُ لها الفضلُ في إثراءِ هذا العمل.

والشكرُ موصولٌ للسّادة المدراء، والعاملين في المصارف المدرجة في سوق دمشق للأوراق المالية، على تعاونهم في سبيل إنجاحِ الجانب العملي لهذه الدراسة.

وخالصُ الشكر والعرفان إلى جامعة دمشق، والهيئة التدريسية في كلية الاقتصاد عامةً، وقسم المحاسبة خاصةً الذين كان لهم الفضلُ في البناء العلميّ للباحث، وإلى كلّ من أبدى نصيحةً، ومشورةً لإتمام هذه الدراسة، وإلى كلّ من علّمني حرفاً ، وألهمني من علمهِ فنفعني به خيرَ منفعةٍ، جزاهم اللهُ عنّي خيرَ الجزاءِ.

فهرس المحتويات:

آية قرآنية ..... أ
إهداء ..... ب
شكرٌ وتقدير ..... ج
فهرس المحتويات: ..... د
قائمة الجداول ..... و
قائمة الأشكال والرسوم البيانية ..... ح
قائمة الاختصارات: ..... ط
الملخص ..... ي
الفصل الأول: الإطارُ العامّ للدراسة 1
1-1 مقدّمةُ الدراسة: 1
2-1 مشكلةُ الدراسة: 2
3-1 أهميةُ الدراسة: 2
4-1 أهدافُ الدراسة: 2
5-1 الدراسات السابقة: 3
6-1 أنموذج الدراسة: 14
7-1 فرضيات الدراسة: 15
الفصل الثاني: الإطار المفاهيمي لأمن المعلومات وضوابطه. 16
المبحث الأول: ماهية أمن المعلومات وخصائصه: 17
1-1-2 تعريف أمن المعلومات: 17
2-1-2 عناصر أمن المعلومات: 18
3-1-2 أهمية أمن المعلومات: 19
4-1-2 خصائص أمن المعلومات: 21
المبحث الثاني: أهداف ومعايير ودورة حياة أمن المعلومات: 23
1-2-2 أهدافُ أمن المعلومات: 23
2-2-2 معايير أمن المعلومات: 23
3-2-2 دورة حياة أمن المعلومات: 29
المبحث الثالث: تهديداتُ أمن المعلومات، والمخاطر المرتبطة بها: 31
1-3-2 تعريف تهديدات أمن المعلومات: 31
2-3-2 المخاطر المرتبطة بتهديدات أمن المعلومات: 35
المبحث الرابع: مفهوم وأنواع ضوابط أمن المعلومات: 38
1-4-2 الضوابط الوقائية لأمن المعلومات: 38

2-4-2 الضوابط الاستكشافية لأمن المعلومات: 45
2-4-3 الضوابط التصحيحية لأمن المعلومات: 47
الفصل الثالث: نظام الرقابة الداخلية في بيئة تكنولوجيا المعلومات 50
المبحث الأول: الإطار المفاهيمي لنظام الرقابة الداخلية: 51
3-1-1 تعريف الرقابة الداخلية: 51
3-1-2 أهداف نظام الرقابة الداخلية: 52
3-1-3 أهمية نظام الرقابة الداخلية: 53
3-1-4 مكونات نظام الرقابة الداخلية: 54
3-1-5 مبادئ الرقابة الداخلية: 57
المبحث الثاني: مقومات نظام الرقابة الداخلية الفعال، والأساليب، والإجراءات، والمعايير المرتبطة به: 59
3-2-1 مقومات نظام الرقابة الداخلية في بيئة تكنولوجيا المعلومات: 59
3-2-2 أساليب وإجراءات الرقابة الداخلية في بيئة تكنولوجيا المعلومات: 61
3-2-3 المعايير، والأطر المرتبطة بنظام الرقابة الداخلية: 66
المبحث الثالث: مواجهة مخاطر تكنولوجيا المعلومات في ظل نظام الرقابة الداخلية: 73
3-3-1 أثر تكنولوجيا المعلومات على نظام الرقابة الداخلية: 73
3-3-2 تطور نظام الرقابة الداخلية لمواجهة مخاطر تكنولوجيا المعلومات: 74
3-3-3 نظام الرقابة الداخلية في ظل استخدام التقنيات الحديثة: 75
الفصل الرابع: الدراسة الميدانية. 77
المبحث الأول: منهجية الدراسة وأدوات جمع وتحليل البيانات: 77
4-1-1 منهجية الدراسة: 77
4-1-2 مجتمع وعينة الدراسة: 77
4-1-3 أداة الدراسة: 78
4-1-4 الأدوات الإحصائية المستخدمة في الدراسة: 79
المبحث الثاني: التحليل الإحصائي الوصفي والاختبارات الإحصائية لأراء عينتي الدراسة: 80
4-2-1 الوصف الإحصائي لعينة الدراسة وفق البيانات العامة: 80
4-2-2 اختبار ثبات وصدق عينتي الدراسة: 84
4-2-3 اختبار كفاية حجم العينة: 85
4-2-4 اختبار التوزيع الطبيعي: 86
4-2-5 نتائج آراء عينتي الدراسة، واختبار الحياد لكل من أسئلة ومحاور الاستبيان: 94
المبحث الثالث: اختبار فرضيات الدراسة: 108
4-3-1 اختبار الفرضية الرابعة: لا يوجد فروقاتٍ ذات دلالة إحصائية بين آراء كلّ من عينتي الدراسة: .. 108
4-3-2 اختبار الفرضية الأولى: لا يوجد علاقةً ذات دلالة إحصائية بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية: 108

3-3-4 اختبارُ الفرضية الثانية: لا يوجد علاقةً ذات دلالةٍ إحصائية بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية: 112
4-3-4 اختبار الفرضية الثالثة: لا يوجد علاقةً ذات دلالة إحصائية بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية: 116
4-4 النتائج والمقترحات: 120
مراجع الدراسة:..... 121
الملحق (1): استبيان الدراسة..... 125
الملحق (2): تحكيم الاستبيان..... 130
Abstract 131

قائمة الجداول

الجدول (2-0): جدولُ المقارنة بين إطار (COBIT 5) وإطار (COBIT 2019). 25
المصدر: www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison 25
الجدول (2-1): جدولُ المقارنة بين المعايير المختلفة لأمن المعلومات. 28
المصدر: من إعداد الباحث. 29
الجدول (2-2): تهديدات أمن المعلومات والمخاطر المرتبطة بها وطرق تجنبها. 37
الجدول (3-1): جدول المقارنة بين المعايير المختلفة للرقابة الداخلية 72
الجدول (4-1) الوصف الإحصائي لكامل مفردات عينتي الدراسة وفق البيانات العامة في الاستبيان..... 83
الجدول (4-2) صدق أداة الدراسة وثباتها لكامل مفردات العينتين..... 84
الجدول (4-3) صدق أداة الدراسة وثباتها لمفردات العينة الأولى. 84
الجدول (4-4) صدق أداة الدراسة وثباتها لمفردات العينة الثانية. 85
الجدول (4-5): اختبار كايزر– مايز– أولكن لكامل مفردات العينتين. 85
الجدول (4-6): اختبار كايزر– مايز– أولكن لمفردات العينة الأولى. 86
الجدول (4-7): اختبار كايزر– مايز– أولكن لمفردات العينة الثانية. 86
الجدول (4-8): نتائج اختبار (Kolmogorov-Smirnov) لكامل مفردات العينتين..... 87
الجدول (4-9): نتائج اختبار (Kolmogorov-Smirnov) لمفردات العينة الأولى. 89
الجدول (4-10): نتائج اختبار (Kolmogorov-Smirnov) لمفردات العينة الثانية. 92
الجدول (4-11): دورُ الضوابطُ الوقائيةُ لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الأولى: 94
الجدول (4-12): دورُ الضوابطُ الاستكشافيةُ لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الأولى: 96

الجدول (4-13): دورُ الضوابطُ التصحيحيّة لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الأولى: 98
الجدول (4-14): دورُ الضوابطُ الوقائية لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الثانية: 100
الجدول (4-15): دورُ الضوابطُ الاستكشافية لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الثانية: 103
الجدول (4-16): دورُ الضوابطُ التصحيحية لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الثانية: 105
الجدول (4-17): نتائج اختبار (Mann-Whitney)..... 108
الجدول (4-18): نتائج اختبار الارتباط وفق معامل سبيرمان للفرضية الأولى. 109
الجدول (4-19) جدول مقياس الارتباط (Eta) بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية. 109
الجدول (4-20): جدول (ANOVA) لدراسة العلاقة الخطية بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية..... 110
الجدول (4-21) جدول تحديد أفضل نموذج للعلاقة غير الخطية بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية. 111
الجدول (4-22): نتائج اختبار الارتباط وفق معامل سبيرمان للفرضية الثانية. 112
الجدول (4-23) جدول مقياس الارتباط (Eta) بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية. 113
الجدول (4-24): جدول (ANOVA) لدراسة العلاقة الخطية بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية. 114
الجدول (4-25) جدول تحديد أفضل نموذج للعلاقة غير الخطية بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية. 115
الجدول (4-26): نتائج اختبار الارتباط وفق معامل سبيرمان للفرضية الثالثة. 116
الجدول (4-27) جدول مقياس الارتباط (Eta) بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية. 116
الجدول (4-28): جدول (ANOVA) لدراسة العلاقة الخطية بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية..... 117
الجدول (4-29) جدول تحديد أفضل نموذج للعلاقة غير الخطية بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية. 118

قائمة الأشكال والرسوم البيانية

الشكل (2−1): دورة حياة أمن المعلومات. 30

الشكل (2−2): تهديدات أمن المعلومات..... 32

الشكل (4-1): اختبار التوزع الطبيعي لكامل مفردات عينتي الدراسة، المحور الأول..... 87

الشكل (4-2): اختبار التوزع الطبيعي لكامل مفردات عينتي الدراسة، المحور الثاني..... 88

الشكل (4-3): اختبار التوزع الطبيعي لكامل مفردات عينتي الدراسة، المحور الثالث. 88

الشكل (4-4): اختبار التوزع الطبيعي لكامل مفردات عينتي الدراسة، المحور الرابع. 89

الشكل (4-5): اختبار التوزع الطبيعي لمفردات العينة الأولى، المحور الأول. 90

الشكل (4-6): اختبار التوزع الطبيعي لمفردات العينة الأولى، المحور الثاني. 90

الشكل (4-7): اختبار التوزع الطبيعي لمفردات العينة الأولى، المحور الثالث..... 91

الشكل (4-8): اختبار التوزع الطبيعي لمفردات العينة الأولى، المحور الرابع..... 91

الشكل (4-9): اختبار التوزع الطبيعي لمفردات العينة الثانية، المحور الأول. 92

الشكل (4-10): اختبار التوزع الطبيعي لمفردات العينة الثانية، المحور الثاني. 93

الشكل (4-11): اختبار التوزع الطبيعي لمفردات العينة الثانية، المحور الثالث..... 93

الشكل (4-12): التمثيل البياني لنموذج العلاقة غير الخطية بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية..... 112

الشكل (4-13): التمثيل البياني لنموذج العلاقة غير الخطية بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية..... 115

الشكل (4−14): التمثيل البياني لنموذج العلاقة غير الخطية بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية. 119

قائمة الاختصارات:

الرمز	المعنى باللغة الانكليزية	المعنى باللغة العربية
ISACA	Information Systems Control and Audit Association	جمعية ضبط وتدقيق نظم المعلومات
COBIT	Control Objectives for Information and Related Technologies	إطار أهداف الرقابة على المعلومات والتكنولوجيا ذات الصلة
ISO	International Organization for Standardization	المنظمة الدولية للمعايير
NIST	National Institute of Standards and Technology	المعهد الوطني الأمريكي للمعايير والتكنولوجيا
ITGI	Information Technology Governance Institute	معهد حوكمة تكنولوجيا المعلومات
NIC	Network Interface Card	بطاقة دخول الشبكة
MAC	Media Access Control Address	عنوان التحكم بالوصول إلى الوسائط
IPS	Intrusion Prevention Systems	نظام منع التطفل
LAN	Local Area Network	شبكة الاتصال المحلية (الخاصة بالمنظمة)
IDS	Intrusion Detection Systems	نظام كشف التسلل
CIRT	Computer Incident Response Team	فريق الاستجابة لحوادث الحاسوب
CISO	Chief Information Security Officer	مدير أمن المعلومات
IOT	Internet of Things	انترنت الأشياء
COSO	The Committee of Sponsoring Organizations	لجنة المنظمات الراعية
IFAC	International Federation of Accountants	الاتحاد الدولي للمحاسبين
SAC	Systems Auditability and Control	رقابة وتدقيق الأنظمة

دورُ ضوابط أمن المعلومات في تفعيلِ نظام الرقابة الداخلية (دراسة ميدانية)

إعداد الطالب: ساريه عبد الرحمن الصواف **إشراف: أ. د. رشا حمادة**

الملخص

هدفت الدراسةُ إلى تحديدِ دور ضوابط أمن المعلومات في تفعيلِ نظام الرقابة الداخلية، وذلك من خلال دراسةٍ ميدانيّة على المصارفِ التقليدية المدرجة في سوق دمشق للأوراق المالية، تكوّن مجتمعُ الدراسة من العاملين في المصارف التقليديّة المدرجة في سوق دمشق للأوراق الماليّة، حيثُ تمَّ سحبُ عيّنتين من ذلك المجتمع، كانت العيّنةُ الأولى من المدقّقين الخارجيين المستقلين المكلّفين بالتّدقيق على المصارفِ التقليديّة المدرجة في سوق دمشق للأوراق المالية لعام 2020م، أمّا العيّنةُ الثانية فكانت من لجانِ التّدقيق والموظّفين في المصارف ضمنَ اختصاصات التدقيق الداخلي، ومسؤولي الرّقابة الداخلية، ومسؤولي أمن المعلومات في تلك المصارف، ولأغراضِ الدراسة تمَّ استخدامُ المنهجَ الوصفيّ التحليليّ لملاءمتهِ طبيعة، وأهداف الدراسة، وذلك من أجلِ تكوين إطارٍ معرفيّ واسع حولَ متغيّرات الدراسة، ولإعدادِ الدراسة الميدانيّة تمّ تصميمُ استبانه لجمعِ البياناتِ اللازمة من عينتيّ الدّراسة، إذ وُزِّعَ استبيانُ الدراسة بشكلٍ ورقيّ، وإلكترونيّ على كلّ من عينتيّ الدّراسة، وبلغَ عددُ الإجابات المستردة (224) استبيان تمَّ إلغاء (24) منها لعدمِ جدّية الإجابات، أو لوجودِ تناقضٍ في الإجابات، حيثُ كانَ عددُ الاستبياناتِ المستردة من العينة الأولى (34) استبياناً، أمّا عددُ الاستبياناتِ المستردة من العينة الثانية (166) استبيان، كما تمّ تحليلُ البيانات باستخدامِ برنامجِ الحزمةِ الإحصائيّة للعلوم الاجتماعية (SPSS – 25)، ومن ثمَّ اختبارُ الفرضيات، حيثُ توصّلت الدراسةُ إلى مجموعةٍ من النتائج أهمّها:

1. يوجدُ علاقةً ذات دلالةٍ إحصائيّةٍ بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.
2. يوجدُ علاقةً ذات دلالةٍ إحصائيّةٍ بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.
3. يوجدُ علاقةً ذات دلالةٍ إحصائية بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.

الكلماتُ المفتاحية: ضوابطُ أمن المعلومات، فعاليةُ نظام الرقابة الداخلية، COSO، COBIT2019

الفصل الأول: الإطارُ العامّ للدراسة.

1-1 مقدّمةُ الدراسة:

يشهدُ العالمُ اليوم تطوراتٍ متسارعةٍ في وسائل تقانة المعلومات، وأجهزةِ الاتصالات، ولا يخلو علمُ المحاسبةِ والتّدقيق من تلك التطورات، فقد أصبحَ الحاسوب، والبرامج الالكترونية المختلفة من أهمّ الوسائل الرئيسيّة في معالجةِ البيانات في المنظمة، مما دفعَ منظمات الأعمال إلى استبدالِ نظم المعلومات اليدويّة بنظمِ المعلومات الالكترونية، وهذا ما أوجبَ على منظّماتِ الأعمالِ اكتساب مهاراتٍ، وخبراتٍ متعدّدة في استخدام هذه البرامج، وتغييرِ أساليب الرقابة الداخلية لزيادة الفاعليّة في أداءِ أعمالها.

كما أنَّ هذا التطّور التكنولوجيّ لم يتوقفْ عندَ طبيعةِ نظام المعلومات الذي تتبنّاه المنظّمة فحسب، بل أدّى إلى توسّعِ مفهوم الرقابة الداخلية استجابةً لبيئةِ الأعمال في ظلّ نظم المعلومات الالكترونية، حيثُ تتمثّلُ أهدافُ نظامِ الرقابة الداخلية في ظلّ تكنولوجيا المعلومات في التأكّد من سلامةِ العمليات، والمدخلات، والمخرجات، وسلامةِ البيانات، ومنعِ تعرّضها للسّرقة، أو الوصولِ والتعديلِ غير المصرّح به، بالإضافةِ إلى اعتماد جميعِ العمليات من قبل المستويات الإداريّة المناسبة، أي إنّها لا تعني فقط الضبط الداخلي، والمراجعة الداخلية، بل تمثّلُ نظاماً رقابياً شاملاً لكلّ إدارات المنظمة، وعملياتها ضمنَ سياساتٍ، وإجراءاتٍ رقابيّة محدّدة تتعلقُ بتجنّب المخاطرِ المحتملة عن طريق الإنذار المبكّر لإمكانية حدوثها، أو اكتشافِها في حال حدوثها، ومن ثمّ معالجتِها في الوقت المناسب.

وممّا لا شكَّ فيه أنَّ نظمَ المعلومات الالكترونية توفّرُ مجموعةً من المزايا المختلفة من سرعةٍ في معالجة البيانات، والدقةِ في توصيل المعلومات، والمرونةِ في الاستجابة للمتغيرات، إلا أنَّها تعدُّ ذات مخاطر مرتفعة بحيثُ يمكن أن يتمّ استغلال نقاط الضعف والثغرات الأمنية، بالإضافة إلى الفقدانِ المحتمل للبيانات نتيجة الخطأ، أو ارتكاب أعمال الغش والتلاعب، كما أنَّ استخدام تكنولوجيا المعلومات، والتقنيات الحديثة كالحوسبة السحابية، والمحاكاة الافتراضية، وانترنت الأشياء، فرضت على المنظّمات بذلَ جهودٍ إضافية لتفادي المخاطر التي تنجمُ عن تبنّي تلك التقنيات في المنظمة، لذا كان لابدَّ من تضمين نظم المعلومات المحاسبية وسائل وضوابط رقابية مختلفة تشملُ جميعَ احتمالات التهديدات، والمخاطر المرتبطة بتكنولوجيا المعلومات، والتقنيات الحديثة من أجل تحقيق أهداف ومتطلبات أمن المعلومات.

يتناولُ هذا البحثُ الضوابطَ المختلفة لأمن المعلومات، والمتمثلة بكلّ من الضوابط الوقائية، والضوابط الاستكشافية، والضوابط التصحيحية، من حيثُ الهدف منها، ودورها في الحدّ من المخاطر والتهديدات التي تتعرضُ لها أنظمةُ المعلومات المحاسبية بشكلٍ عامّ، ونظامُ الرقابة الداخلية بشكلٍ خاصّ، وذلك من خلالِ دراسةٍ ميدانية على العاملين في المصارف التقليدية المدرجة في سوق دمشق للأوراق المالية خلال عام 2021م.

1-2 مشكلةُ الدراسة:

إنَّ التطورَ الكبيرَ في تكنولوجيا المعلومات على المستوى العالميّ في المجالات الحياتية المختلفة أصبحَ أمراً ضرورياً لا بد من مواكبته، فعلمُ المحاسبة والتدقيق كغيره من العلوم الأخرى مرتبط ارتباطاً حتمياً بهذا التطور، وقد أشارت معظمُ الدراسات إلى ضعفِ، ومحدوديةِ اهتمام المنظمات بتبنّي ضوابطَ محددة لحماية أمن المعلومات، مما قد يؤثّرُ على نظم الرقابة الداخلية وفعاليته، تأتي هذه الدراسةُ للإجابة على التساؤلات الآتية:

1. هل تساهمُ الضوابطُ الوقائيّة لأمنِ المعلومات في تفعيلِ نظامِ الرقابة الداخلية؟
2. هل تساهمُ الضوابطُ الاستكشافيّة لأمنِ المعلوماتِ في تفعيلِ نظامِ الرقابة الداخلية؟
3. هل تساهمُ الضوابطُ التصحيحيّة لأمنِ المعلومات في تفعيلِ نظامِ الرقابة الداخلية؟

1-3 أهميةُ الدراسة:

يمكنُ إيضاحُ أهميةِ الدراسة من خلال الآتي:

الأهميةُ العلميّة: تتمثّلُ الأهميةُ العلميّةُ للدراسة في محاولةِ بيان مخاطر وتهديدات أمن المعلومات في ظل تكنولوجيا المعلومات، والتطورات التي فرضتها التقنيات الحديثة المختلفة كالحوسبة السحابية، والمحاكاة الافتراضية وانترنت الأشياء، و مدى إمكانية استخدام الضوابط المختلفة لأمن المعلومات وتبنّيها من قبل المنظّمات في سبيل الحدِّ من تلكَ المخاطر والتهديدات، وتدعيمِ نظم الرقابة الداخلية ليحققَ أهدافَه بفعالية.

الأهميةُ العملية: تتضحُ الأهميّةُ العمليّة من خلالِ الحصول على دليلٍ ميدانيّ من بيئةِ الأعمال السورية حولَ المخاطرِ والتهديدات التي تتعرّضُ لها نظم المعلومات المحاسبية، والوسائل والأساليب التي تتبناها المنظمات السورية متمثلةً بأداء العاملين بالمصارف التقليدية المدرجة في سوق دمشق للأوراق المالية للتعامل مع مخاطر أمن المعلومات للحفاظ على الأصول، وبخاصة الأصول الالكترونية لديها، بالإضافة إلى تحقيقِ الأهداف المختلفة لنظام الرقابة الداخلية.

1-4 أهدافُ الدراسة:

تهدفُ هذه الدراسة إلى بيانِ الدور الذي تقومُ به ضوابطُ أمن المعلومات في تفعيل نظام الرقابة الداخلية، ويتحققُ هذا الهدفُ من خلال الأهداف الفرعية التالية:

1. بيانُ دور الضوابط الوقائيّة لأمن المعلومات في تفعيل نظام الرقابة الداخلية.
2. بيانُ دور الضوابط الاستكشافيّة لأمن المعلومات في تفعيل نظام الرقابة الداخلية.
3. بيانُ دور الضوابط التصحيحيّة لأمن المعلومات في تفعيلِ نظام الرقابة الداخلية.

1-5 الدراسات السابقة:

أولاً: الدراسات باللغة العربية:

1) دراسةُ (المطيري، 2013)[1] بعنوان "أثر استخدام تكنولوجيا المعلومات على فاعلية نظام الرقابة الداخلية في شركات النفط الكويتية":

هدفت هذه الدراسةُ إلى التعرّفِ على أثرِ استخدام تكنولوجيا المعلومات على فعالية نظام الرقابة الداخلية في شركات النفط الكويتية، وذلك من وجهةِ نظر المديرين الماليين، والمحاسبين في شركات النفط الكويتية، ولتحقيق هذا الهدف فإنَّ الباحثَ تعاملَ مع نوعين من البيانات هما: البياناتُ الثانويّة، والبياناتُ الأوليّة، تمَّ استخدامُ استبانة تم توزيعها على عينة شملت (206) مديراً مالياً ومحاسباً يعملون في الشركات المشمولة بالدراسة.

توصّلت الدراسةُ إلى عددٍ من النتائج أهمها: أنَّه يوجدُ أثراً لاستخدام تكنولوجيا المعلومات (أجهزة الحاسوب، العناصر البرمجية، قواعد البيانات، فرق الدعم، وشبكات الاتصال) على فعالية نظام الرقابة الداخلية في شركات النفط الكويتية من وجهةِ نظرِ المديرين الماليين والمحاسبين.

2) دراسة (زهيري، 2015)[2] بعنوان "مخاطر أمن نظم المعلومات المحاسبية الالكترونية، واستراتيجيات مواجهتها (دراسةٌ وصفية في المصارف السورية):

هدفت هذه الدراسةُ إلى التعرّف على المخاطرِ التي تواجهُ نظم المعلومات المحاسبية الالكترونية في المصارف العاملة في سورية، وأهمُّ الأسباب التي تؤدّي إلى حدوثِها، واستراتيجيات مواجهتها.

فمن خلال المراجعة الأدبيّة للكتب، والمقالات النظرية، والتطبيقية المتعلّقة بالموضوع، تمَّ تصميمُ استبانةٍ وُزّعَت على مجموعةٍ من الموظفين العاملين في المصارف السورية الموجودة في الساحل السوري، وقد توصّلت الدراسةُ إلى النتائج التالية وهي: قلّةُ عدد موظفي تكنولوجيا المعلومات في المصارف العاملة في سورية، وجودُ نسبةٍ كبيرةٍ من المصارف السورية لا تعدّ خطة لمواجهة المخاطر، عدمُ حدوثِ مخاطر نظم المعلومات المحاسبية الالكترونية بشكلٍ متكررٍ في المصارف السورية، إنَّ المصارفَ العاملة في سورية تتّبعُ إجراءات حمايةٍ كافية لمواجهة مخاطر أمن نظم المعلومات المحاسبية الالكترونية، وأفضت نتائجُ الدراسة إلى أنَّ أهمّ المخاطر التي تواجهُ المصارف السورية تتمثّلُ في الإدخال العرضي للبيانات الخاطئة من قبل الموظفين، والمشاركة في كلمات المرور.

---

[1] المطيري، ناصر، 2013، **أثر استخدام تكنولوجيا المعلومات على فاعلية نظام الرقابة الداخلية في شركات النفط الكويتية**، رسالة ماجستير، جامعة الشرق الأوسط، الأردن.

[2] زهيري، ماهر، 2015، **مخاطر أمن نظم المعلومات المحاسبية الالكترونية واستراتيجيات مواجهتها**، رسالة ماجستير، جامعة تشرين، سورية.

3) دراسة (النعامي، سمور، 2015)[3] بعنوان "دور تقنية المعلومات المحاسبية في تطوير نظم الرقابة الداخلية (دراسةٌ تطبيقيّة على الجامعات الفلسطينية العاملة في قطاع غزة)":

هدفت هذه الدراسةُ إلى توضيحِ دورِ تقنيّة المعلومات المحاسبية في تطوير نظم الرقابة الداخلية، وذلك من خلالِ دراسةٍ تطبيقيّةٍ على الجامعات الفلسطينية العاملة في قطاع غزة، و لتحقيق أهداف هذه الدراسة، فقد صُمِّمت استبانة مكوّنة من أربعة أجزاءٍ اعتماداً على الإطار النظريّ، و الدراسات السابقة، وُزّعت على العاملين في الدوائر المالية ، ودوائر الرقابة والتدقيق في الجامعات الفلسطينية العاملة في قطاع غزة ، و عددها (60) استبانة، وبلغت الردودُ (51) استبانة صالحة للتحليل، أي بنسبةِ إرجاع قدرها 85%.

لقد استخدمَ الباحثان المنهجَ الوصفيّ التحليليّ، ولتحليلِ النتائج أُستخدم البرنامج الإحصائي (SPSS) في التحليل، كما أُستخدمت المعالجات الإحصائية الملائمة لهذا الغرض.

وقد قدّمت الدراسةُ مجموعةً من النتائج أهمها: وجودُ دور لتقانة المعلومات المحاسبي عند مستوى دلالة (0.05) في تطوير نظم الرقابة الداخلية للجامعات الفلسطينية العاملة في قطاع غزة، و جاءت هذه النتيجةُ الرئيسة من خلال مجموعةٍ من النتائج الفرعية، والمتمثّلة في أنَّ تقنيةَ المعلومات المحاسبية لها دورٌ في حماية الأصول. كما لها دورٌ في الحدِّ من أخطاء التقارير المالية. واتباع اللوائح، والسياسات التنظيمية، وإنَّ تقنيةَ المعلومات المحاسبية لها دورٌ في تطوير الإجراءات الرقابيّة على الأنشطة التشغيليّة.

4) دراسة (حرب، 2016)[4] بعنوان "أثر التدقيق الداخلي في حماية أنظمة المعلومات المحاسبية في البنوك التجارية في الأردن":

هدفت هذه الدراسةُ للتعرف على أثرِ التدقيق الداخلي في حماية أنظمة المعلومات المحاسبية في البنوك التجارية في الأردن، فقد قامَ الباحثُ بتصميم استبانةٍ مكونة من (28) فقرة، تمَّ توزيعُها على مجتمعِ الدراسة المكونة من البنوكِ التّجارية في الأردن، وعددها (5) بنوك تجارية مع نهاية عام 2015، علماً بأنّ الدراسة لا يوجدُ فيها اختيار للعينة من المجتمع، فعيّنة الدراسة شملت جميعَ أفراد المجتمع، وتمثّلت وحدةُ التحليل بالأفراد العاملين في أقسام المحاسبة (المدراء الماليين والمحاسبين)، والدوائرِ، والأقسام الأخرى في قطاع البنوك التجارية مع نهاية عام 2015، حيثُ تمَّ توزيع (100) استبانة على الأفراد العاملين في هذه الدوائر، والأقسام.

وقد توصّلت هذه الدراسةُ إلى أنّه يوجدُ تأثيراً ذات دلالةٍ إحصائية (للفرضية الأولى) لتأثيرِ التدقيق الداخلي في حماية أنظمة المعلومات المحاسبية في البنوك التجارية في الأردن.

---

[3] النعامي، علي، سمور، حمدي، حزيران 2015، **دور تقنية المعلومات المحاسبية في تطوير نظم الرقابة الداخلية**، مجلة جامعة القدس المفتوحة للأبحاث والدراسات الإدارية والاقتصادية، المجلد الأول، العدد 2.

[4] حرب، أيمن، **أثر التدقيق الداخلي في حماية أنظمة المعلومات المحاسبية في البنوك التجارية في الأردن**، Journal of Business & Management (COES&RJ-JBM), 4(4), pp. 151-171.

وكذلك توصّلت هذه الدراسةُ إلى أنّه يوجدُ تأثير ذات دلالةٍ إحصائية (للفرضية الثانية) لتأثير التدقيق الداخلي في قواعد أمن المعلومات المحاسبية في البنوك التجارية في الأردن.

وكذلك توصّلت هذه الدراسةُ إلى أنّه يوجدُ تأثير ذات دلالةٍ إحصائية (للفرضية الثالثة) لتأثير التدقيق الداخلي في تعزيز إدراك، ووعي الموظفين في البنوك التجارية في الأردن.

5) دراسة (الموسوي، 2016)[5] بعنوان "نظام المعلومات المحاسبي الالكتروني ودوره في تعزيز أمن المعلومات المالية":

هدفت هذه الدراسةُ إلى تقييمِ نظام المعلومات المحاسبي الإلكتروني في الشركة العراقية، وتعيينِ الأساليب والخطوات التي يمكنُ اتّباعها للاستجابة بكفاءةٍ لمخاطرِ أمن المعلومات المحاسبية، كما هدفت إلى تحديدِ الإجراءات التي يمكنُ استخدامها في إجراءات الأمن، والرقابة على المعلومات المالية في ظل نظام المعلومات المحاسبي الإلكتروني.

تمَّ استخدامُ أسلوب الاستقصاء، وإجراء المقابلات مع الموظفين للتعرّف على واقعِ حالِ شركة الطيف للتحويل المالي من خلال الخدمات التي تقدّمُها، والمشاكلِ التي وُجدت، وقد تمّ معالجتها وفقاً للمصادر والمراجع الخاصّة بأمن نظم المعلومات المحاسبية الإلكترونية.

وقد توصّلت الدراسةُ إلى مجموعةٍ من الاستنتاجاتِ أهمّها ما يأتي:

إنَّ عمليةَ الشراء لنظام المعلومات المحاسبي تمّت على اختيارِ فرصةٍ واحدة، وليس الاختيارُ من بين عدّة بدائل، كما أنّه لا توجدُ إجراءاتٍ معينة لاستعادةِ النسخ الاحتياطية الخاصّة بالبيانات المخزونة عندَ حصولِ حوادث، كما أنَّ التخزينَ يحفظُ على قرصٍ صلب، ويوضعُ في شعبة نظم المعلومات، وليس في موقعٍ آمن خارج شعبة نظم المعلومات، ولم تحدد مدّةُ الاحتفاظِ بتلك النسخ مما قد يتيحُ فرصةً للموظفين غير المصرّح لهم للوصولِ إلى تلك البيانات.

6) دراسة (الحسين، 2017)[6] بعنوان "أثر مخاطر نظم المعلومات المحاسبية الالكترونية على فاعلية عملية المراجعة":

هدفت هذه الدراسة إلى تحديدِ مخاطرِ نظم المعلومات المحاسبية الالكترونية، وأثرها على فعالية عملية المراجعة في السودان، حيثُ تمثّلت مشكلةُ البحث في ماهيّة المخاطر التي تهدّدُ نظم المعلومات المحاسبية الإلكترونية، وما مدى توفّر مراجعي حسابات خارجيين مؤهلين لمراجعةِ نظم المعلومات المحاسبية الالكترونية، وقد هدفَ البحثُ

[5] الموسوي، علي، 2016، **نظام المعلومات المحاسبي الالكتروني ودوره في تعزيز أمن المعلومات المالية**، رسالة ماجستير، جامعة القادسية، العراق.

[6] الحسين، إشراقة، 2017، **أثر مخاطر نظم المعلومات المحاسبية الالكترونية على فاعلية عملية المراجعة**، رسالة ماجستير، جامعة شندي، السودان.

إلى توضيحِ أثرِ مخاطر استخدام نظم المعلومات المحاسبية على فعالية عملية المراجعة، وقد اعتمدَ البحثُ على عدةّ مناهج متعدّدةِ الجوانب منها: المنهجُ التاريخيّ، والمنهجُ الوصفيّ التحليليّ، والمنهجُ الاستقرائيّ، توصّلَ البحثُ إلى مجموعةٍ من النتائجِ منها: الاستفادةُ من الخبرات العالمية في مجال أمن المعلومات يرفعُ من درجة الثقة في المعلومات المحاسبية، إجراءات الحماية الموجودة الآن في مجال أمن المعلومات المحاسبية الالكترونية تحتاجُ للتحديث الدوري.

7) دراسة (غزال، سعيد، 2018)[7] بعنوان "أثر تكنولوجيا المعلومات على فاعلية نظام الرقابة الداخلية":

هدفت هذه الدراسةُ للإجابة عن الإشكاليةِ الرئيسة: إلى أي مدى يمكنُ لتكنولوجيا المعلومات أن تدعمَّ فاعلية نظام الرقابة الداخلية؟ وذلك لأنّ استخدامَ تكنولوجيا المعلومات أصبحَ في العديد من المجالات، وهذا لما تحقّقه من سرعةٍ ودقةٍ في الأداء خاصّة مع تطّور، وتعقّد مختلفِ العمليات الإدارية، والتشغيليةن وصعوبة مراقبتها، ومن هنا أصبحَ الاعتمادُ عليها لتسهيلِ، وتسريعِ عمليات الرقابة.

ولتحقيق هذا الهدف جاءت الدراسةُ في شقّيها النظريّ، والتطبيقيّ تحملُ في طيّاتها على مقدمةٍ، وفصلين، وخاتمة.

اعتمدت الدراسةُ في الجانب النظري على المنهجِ التحليليّ الوصفيّ لتبيينِ أثر المتغيّر المستقلّ تكنولوجيا المعلومات، على المتغيّر التابع لفاعلية نظام الرقابة الداخلية، كما أنَّ استخدامَ طريقة الاستبيان في الجانب التطبيقيّ لجمعِ البيانات استهدفنا من خلاله مجموعةً من الأكاديميين، والأخصّائيين في مجال الاختصاص، وعُولجت وفقَ البرنامج الإحصائي (SPSS 21). وقد خَلُصت الدراسة إلى مجموعةٍ من النتائج أهمّها: إنَّ تكنولوجيا المعلومات لها دورٌ أساسيّ في تدعيمِ فاعلية نظام الرقابة الداخلية، وتحسينِ إجراءاتها، وأساليبها.

8) دراسة (الجعبري، 2018)[8] بعنوان "أثر الأمن المعلوماتي على أداءِ شركات التأمين العاملة في فلسطين":

هدفت هذه الدراسةُ إلى تحديدِ واقع تطبيق الأمن المعلوماتي، وتأثيره على أداءِ شركات التأمين العاملة في فلسطين وفقاً لأبعادِ بطاقة الأداء المتوازن (الأداء المالي، وبعد العمليات الداخلية، وبعد خدمة الزبائن/ العملاء، بعد خدمة الموظفين)، تكوّنَ مجتمعُ الدراسة من موظفي، ومدراء شركات التأمين العاملة في فلسطين، والبالغ عددهم (1112) موظفاً، ومديراً، ولأغراض هذه الدراسة تمَّ استخدامُ طريقة العيّنة العشوائية مكونة من (157) فرداً، واستخدامُ المنهج الوصفيّ التحليليّ لملائمتهِ، وطبيعة وأهداف الدراسة، وأُستخدمت كلاً من أداتي المقابلة الهاتفية، والاستبانة لجمع البيانات اللازمة.

تمّ تحليلُ البيانات باستخدام برنامج الرزم الإحصائية للعلوم الاجتماعية (SPSS)، وتوصّلت الدراسةُ إلى مجموعةٍ من النتائج أهمها: وجودُ تطبيقٍ للأمن المعلوماتي في شركات التأمين، ووجودُ أثرٍ ذو دلالةٍ إحصائية لتطبيق الأمن

---

[7] غزال، مصباح، سعيد، عمر، مهاوه، صدام حسين، 2018، **أثر تكنولوجيا المعلومات على فاعلية نظام الرقابة الداخلية**، رسالة ماجستير، جامعة الشهيد حمه لخضر-الوادي، الجزائر.

[8] الجعبري، هناء، 2018، **أثر الأمن المعلوماتي على أداء شركات التأمين العاملة في فلسطين**، رسالة ماجستير، جامعة الخليل، فلسطين.

المعلوماتي على أداء شركات التأمين العاملة في فلسطين بأبعاده الأربعة (الأداء المالي، وبعد العمليات الداخلية، وبعد خدمة الزبائن/ العملاء، بعد خدمة الموظفين).

9) دراسة (عوكل، 2018)[9] بعنوان "إمكانية تطبيق إطار كوبت COBIT لتحسين أداء منظمات الأعمال في سورية":

هدفت الدراسةُ إلى تحديدِ إمكانيةِ تطبيقِ إطار كوبت في منظمات الأعمال السورية لتحسينِ أداءها الأمر الذي يرتبطُ بمعرفة متطلّبات التطبيق، والتعرف على الإطار بحدّ ذاته، وصعوباتِ تطبيقهِ، ومعرفةِ آلياتِ القياس الخاصة به من خلالِ نموذجِ النضوج المرتبط ببطاقة الأهداف المتوازنة الاستراتيجية الخاصّة بتقانة المعلومات، حيثُ وجدَ الباحثُ أنَّ إطارَ كوبت مطبّقٌ في منظمات الأعمال في سورية، وبمستوياتٍ مختلفة، وأدى تطبيقُ الإطار إلى تحسينِ أداءِ عمليات التقييم، والتوجيه، والمراقبة الخاصة بحوكمةِ تقانة المعلومات، وإلى تحسين أداء عمليات الموائمة، والتخطيط، والتنظيم والاستحواذ، والبناء، والتنفيذ ،وتقديم الخدمات، والصّيانة والدعم أو للمراقبةِ والتقييم وتقديرِ التوافقية الخاصّة بإدارة تقانة المعلومات.

تمّت الدراسةُ على ثلاثِ شركات من قطاع الاتصالات، والمصارف والتّأمين حيثُ تمَّ تقييمُ متطلباتِ التطبيق المقترحة من إطارِ كوبت، وكذلك من خلال نموذجِ الإجراءات التمكينية المكون من 37 عملية، والتي تحقق 271 هدفاً رقابيّاً، وربطِه مع نموذجِ النّضج المرتبط بأهدافِ بطاقة الأهداف المتوازنة الخاصّة بتقانة المعلومات.

10) دراسة (خرخاش، 2018)[10] بعنوان "أثر تطبيق حوكمة الشركات في تفعيل أنظمة الرقابة الداخلية لدى البنوك التجارية الجزائرية":

هدفت هذه الدراسةُ إلى معرفةِ أثرِ تطبيقِ حوكمة الشركات في تفعيلِ أنظمةِ الرقابة الداخلية بالبنوك التجارية الجزائرية، لأجلِ تحقيقِ ذلك تمَّ تصميمُ استبياناً وتوزيعه على 22 بنكاً بالولايات التالية :المسيلة، برج بوعريريج، سطيف، الجلفة، حيثُ شملت البياناتُ المطلوبة لأجل تحليلِ موضوعِ الاستبيان باستخدامِ برنامجِ الحزمة الإحصائية للعلوم إصدار رقم 22، توصّلت الدراسةُ إلى مجموعةٍ من النتائج من بينها البنوك التجارية SPSS الاجتماعية الجزائرية تُطبّق مبادئَ حوكمة الشركات عند مستوى معنوية .% 0,05 تمتازُ البنوكُ التّجارية الجزائرية بأنظمة رقابةٍ داخلية فعّالة عندَ مستوى معنوية .% 0,05 إنّ تطبيقَ مبادئ حوكمة الشركات يؤثّرُ على فاعلية أنظمة الرقابة الداخلية لدى البنوك التجارية الجزائرية عند مستوى معنوية .% 0,05 البنوك التجارية الجزائرية لا تعاني من مشكلة الإفصاح، والشفافية عند مستوى معنوية .% 0,05.

---

[9] عوكل، محمد، 2018، **إمكانية تطبيق إطار كوبت COBIT لتحسين أداء منظمات الأعمال في سورية**، أطروحة دكتوراه، جامعة دمشق، سوريا.

[10] خرخاش، جميلة، 2018، **اثر تطبيق حوكمة الشركات في تفعيل أنظمة الرقابة الداخلية لدى البنوك التجارية الجزائرية**، أطروحة دكتوراه، جامعة محمد بوضياف بالمسيلة، الجزائر.

11) دراسة (دهيليس، بوطريفة، 2018)[11] بعنوان "دور المراجع الداخلي في تحسين نظام الرقابة الداخلية في المؤسسات الاقتصادية ":

هدفت هذه الدراسةُ إلى بيان دورِ المراجع الداخلي في تحسين نظام الرقابة الداخلية في المؤسسات الاقتصادية، تمَّ إجراءُ الدراسةِ في شركة الإسمنت بسور الغزلان، من خلال تقييم نظام الرقابة الداخلية على دورة المشتريات من خلال زياراتٍ ميدانية بالاعتمادِ على الملاحظة، والمقابلات الشخصية، وقائمة استقصاء، ومن ثمَّ استنتاجُ نقاط القوة، والضعف للنظام، وقد توصّلت الدراسةُ إلى مجموعةِ نتائج أهمها: – يساعدُ نظامُ الرقابة الداخلية على التحكّم في المنظمة من أجلِ تحقيقِ أهدافها، المراجعة الداخلية تعملُ على الحكم، و التقييم لخدمةِ أهدافِ الإدارة في مجال الرقابة عن طريقِ مراجعةِ جميع العمليات، و حمايةِ ممتلكات المؤسسة من السرقة، و التلاعبات، و الأخطاء المحتملة ، وبالتالي إظهارُ الثغرات السلبية للمؤسسة، المراجعةُ الداخلية هي أداةٌ من أدوات الرقابة الداخلية يقومُ بها المراجعُ الداخلي باختبار مدى تماشي النظام مع متطلباتِ الإدارة، و العمل على تحسينه.

12) دراسة (فيلالي، 2019)[12] بعنوان "مستوى أمن المعلومات في المؤسسة الجزائرية ومدى تأثره بطبيعة التهديدات وطبيعة الحماية المطبقة":

هدفت هذه الدراسةُ إلى تحليلِ مستوى أمن المعلومات على مستوى المؤسسات الجزائرية، ومدى تأثّرِهِ بطبيعة التهديدات التي تتعرّضُ لها المؤسسةُ بصفةٍ عامّة، ونظام المعلومات بصفة خاصّة، ومدى تأثّرِهِ أيضاً بطبيعةِ الحماية المطبّقة.

خَلُصت الدراسةُ التي تمّت على مستوى (35) مؤسسة إلى أنَّ مستوى أمن المعلومات في المؤسسات الجزائرية متوسط، وأنّه يتأثّرُ بطبيعةِ الحماية المطبقة، بحيثُ كلما ارتفعَ مستوى الحماية وتطوّرت أيضاً الوسائل، والاستراتيجيات الخاصّة بالحماية كلما ارتفعَ مستوى أمن المعلومات، وعليه بما أنّ مستوى الحماية المطبقة متوسط فإنَّ مستوى أمن المعلومات متوسط أيضاً، أما بالنسبة للتهديدات فتوصّلت الدراسةُ إلى أنَّ أمنَ المعلومات في المؤسسات الجزائرية لا يتأثّرُ بطبيعة التهديدات التي تتعرضُ لها المؤسسات وأنظمتها، ماعدا التهديدات التنظيمية المتمثلة خصوصاً في كفاءة العامل البشري على مستوى المؤسسة.

---

[11] دهيليس، أيوب، بوطريفة، أيوب، 2018، **دور المراجع الداخلي في تحسين نظام الرقابة الداخلية في المؤسسات الاقتصادية**، رسالة ماجستير، جامعة أكلي محند أولحاج، الجزائر.

[12] فيلالي، أسماء، 2019، **مستوى أمن المعلومات في المؤسسات الجزائرية ومدى تأثره بطبيعة التهديدات وطبيعة الحماية المطبقة**، أطروحة دكتوره، جامعة ابي بكر بلقايد، الجزائر.

13) دراسة (آقبيق، 2020)[13] بعنوان " دور الضوابط الرقابية وفق إطار COBIT في الحد من مخاطر أمن نظم المعلومات المحاسبية في شركات التأمين السورية":

هدفت الدراسةُ إلى تعريّف دور العمليات التمكينية، كأحدِ أشكال الضوابط الرقابية وفق إطاري COBIT5 للمخاطر وأمن المعلومات، في الحد من مخاطر أمن نظم المعلومات المحاسبية في شركات التأمين السورية.

حيثُ اعتمدت الدراسةُ المنهجَ الوصفيّ التحليليّ من خلال وصف ما جاء في الدراسات السابقة العربيّة، والأجنبيّة ذات الصلة بأطر COBIT5 ومخاطر أمن نظم المعلومات المحاسبية، لتكوينِ إطارٍ فكريّ واسع حولَ مشكلة الدراسة. ولاختبارِ فرض الدراسة تمَّ تصميمُ قائمة استقصاء، وتوزيعها على العاملين وفقَ مستوياتٍ وظيفيةٍ معيّنة في شركات التأمين السورية، حيثُ أُستخدِم برنامج (SPSS) لتحليلِ بيانات قوائم الاستقصاء المستردة. وتوصّلت الدراسة إلى أنّ مستوى تطبيق العمليات التمكينية، كأحد أشكال الضوابط الرقابية وفق إطاري COBIT5 للمخاطر وأمن المعلومات، ليس له دورٌ في الحدّ من مخاطرِ أمن نظم المعلومات المحاسبية التي تتعرّضُ لها شركاتُ التّأمين السورية.

14) دراسة (بوعبدالله، منومس، 2020)[14] بعنوان " دور نظام المعلومات المالي في تحقيق فعالية الرقابة الداخلية":

هدفت هذه الدراسةُ إلى التعرّف على دورِ نظام المعلومات المالي في تحقيق فعالية الرقابة الداخلية ببنك الفلاحة والتنمية الريفية، ولغرضِ، معالجة إشكالية الدراسة و الإجابة على تساؤلاتها، واختبار فرضياتها، تمّت الاستعانةُ بالمنهجِ الوصفيّ التحليليّ فيما يخصّ الجانبَ النظريّ، أما في الجانب التطبيقيّ منها فقد تمَّ تصميمُ استمارة كأداةٍ لجمعِ البيانات بلغت عدد فقراتها (31 فقرة) وُزّعت على جميع الموظفين العاملين في بنك محل الدراسة وبلغ عددهم 33 موظفاً تمّ استرجاعُ جميع الاستمارات، حيثُ تمَّ استخدامُ أسلوبَ حزم الإحصائية للعلوم الاجتماعية(SPSS) من أجلِ تحليل بيانات الاستمارات بالاعتماد على المتوسطات الحسابية ، تكرارات، الانحراف المعياري، التباين الاحادي، وأسلوب الانحدار البسيط، توصّلنا من خلال هذه الدراسة إلى مجموعةٍ من النتائج من أبرزها: وجودُ دورٍ ذو دلالةٍ إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لنظام المعلومات المالي في تفعيل الرقابة

الداخلية، كما أنّه لا يوجدُ دوراً ذو دلالةٍ إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لمتغيرات الديموغرافية (العمر، الجنس، المؤهل العلمي، المستوى الوظيفي، مدة الخدمة في الوظيفة).

---

[13] آقبيق، نور، 2020، **دور الضوابط الرقابية وفق إطار COBIT في الحد من مخاطر أمن نظم المعلومات المحاسبية في شركات التأمين السورية- دراسة ميدانية**، رسالة ماجستير، جامعة دمشق، سورية.

[14] بوعبد الله، فريدة، منومس، شيماء، 2020، **دور نظام المعلومات المالي في تحقيق فعالية الرقابة لداخلية**، رسالة ماجستير، معهد العلوم الاقتصادية والتجارية وعلم التسيير، الجزائر.

ثانياً: الدراسات باللغة الانكليزية:

1) دراسة (Steinbart, et al, 2012)[15]: بعنوان "العلاقة بين التدقيق الداخلي وأمن المعلومات: دراسة استكشافية":

هدفت هذه الدراسةُ إلى تحديدِ العلاقة بين التدقيق الداخلي، وأمن المعلومات، وقد توصّلت من خلال المنهج الاستكشافي إلى أنّه يجبُ أن تعملَ وظائفُ التدقيق الداخلي، وأمن المعلومات معاً بشكلٍ مشتركٍ، وتصميمِ ضوابط لأمن المعلومات، وتنفذ مختلف الإجراءات والتقنيات لحماية موارد معلومات المنظمة، ومع ذلك، تشيرُ التقاريرُ في الأدبيات المهنية إلى أنّ الوظيفتين لا تربطُهما دائماً علاقة متناغمة، تقدّم هذه الدراسة المرحلةَ الأولى من برنامجٍ بحثي مُصَمّم لدراسةِ طبيعةِ العلاقة بين أمن المعلومات، ووظائف التدقيق الداخلي، و تقدّمُ النتائجُ من خلال سلسلةٍ من المقابلاتِ شبه المنظّمة مع كلّ من المدققين الداخليين، ومحترفي أنظمة المعلومات، كما تمّ تطويرُ نموذجٍ استكشافي للعوامل التي تؤثّرُ على طبيعةِ العلاقة بين التدقيق الداخلي، ووظائفِ أمن المعلومات، والفوائدِ المحتملة التي يمكنُ للمنظمات الحصول عليها من تلك العلاقة، وتقديمِ المقترحات لتوجيهِ البحوث المستقبلية.

2) دراسة (Alqahtani, 2017)[16]: بعنوان: " تطوير سياسة أمن المعلومات: منهج دراسة الحالة":

هدفت هذه الدراسةُ إلى دراسةِ طرقِ تطوير سياسات أمن المعلومات، حيثُ استكشفت هذه الدراسةُ مُزودي خدمات الإنترنت في أندونيسيا لتقييمِ مدى كفاية السياسات، وتحديدِ وعي المستخدم، والامتثال لهذه السياسات. من خلال استخدام نهج دراسة الحالة، توصّلت هذه الدراسةُ إلى مجموعةٍ من النتائجِ أهمها: أنّ مجالات التركيز على أمن المعلومات المضمنة في هذه المؤسسة هي مزودي إدارة الكلمات، استخدامُ البريد الإلكتروني، والإنترنت، ومواقع الشبكات الاجتماعية، الحوسبة المتنقلة ومعالجة المعلومات. ومع ذلك، تفاوتت مستوياتُ نضج هذه العناصر بين مجالات التركيز بسبب نقصِ الوعي، والامتثال بين المستخدمين.

كما قدّمت الدراسةُ مجموعةً من المقترحات أهمها: أنّه يجبُ حمايةُ المعلومات، والبيانات التنظيمية من الهجمات النشطة، والسلبيّة وتأمينها من الوصول غير القانوني، أو الانقطاع غير المرغوب فيه، أو التغيير غير المُصرّح به أو الحذف من خلال سياساتِ أمنِ المعلومات، تقعُ العديدُ من المؤسسات ضحي لمثل هذه الهجمات بسبب سياسات أمن المعلومات الضعيفة. كما أنّ تعطيلَ سياسات أمن المعلومات هذه بواسطةِ مستخدمي تقنية المعلومات يجعلُ المؤسسات تحتَ تهديداتِ أمن المعلومات.

---

[15] Paul John Steinbart, Robyn L. Raschke, Graham Gal, William N. Dilla, 2012, **The relationship between internal audit and information security: An exploratory investigation**, International Journal of Accounting Information 228–243

[16] Fayez Hussain Alqahtani, 2017, **Developing an Information Security Policy: A Case Study Approach,** Information Systems International Conference 2017, ISICO 2017, , Bali, Indonesia

3) دراسة (Steinbart, et al, 2018)[17]: بعنوان " تأثير العلاقة الجيدة بين التدقيق الداخلي، ووظائف أمن المعلومات على نتائج أمن المعلومات":

هدفت هذه الدراسةُ للوقوفِ على تأثيرِ العلاقة الجيدة بين التدقيق الداخليّ، ووظائفِ أمن المعلومات على المقاييس الموضوعيّة للفعالية الكليّة لجهودِ أمن المعلومات الخاصّة بالمنظمة، وذلك باستخدامِ مجموعةِ بياناتٍ فريدة، حيثُ أُجرِيَت دراسةً استقصائية على شبكةِ الإنترنت لمراجعي تكنولوجيا المعلومات الذين كانوا أعضاءً في قسم إدارة المعلومات، وضمان التكنولوجيا IMTA من جمعية المحاسبين القانونيين الدوليين المعتمدين AICPA. كان المسحُ جزءاً من دراسةٍ أكبر تضمنّت أسئلةً إضافية لا تتعلقُ بأسئلة البحث التي تمّ استكشافهُا في هذه الدراسة. أرسلت اللجنة التنفيذية لقسم إدارة المعلومات وضمان التكنولوجيا IMTA رسالةَ بريدٍ إلكتروني إلى أعضائها لتشجيعِ مشاركتِهم في الدراسة.

توصّلت هذه الدراسةُ إلى مجموعةِ نتائج أهمها: تؤثّرُ جودةُ هذه العلاقة بشكلٍ إيجابي على عدِد نقاطِ ضعف الرقابة الداخلية المبلغ عنها، وحوادث عدم الامتثال، وكذلك على عددِ الحوادث الأمنية التي تمَّ اكتشافُها، سواءً قبلَ أو بعد أن تسبَّب حدوثَ ضررٍ مادي للمنظمة. إضافةً إلى ذلك، نجدُ أنَّ الدَّعمَ الإداري من المستويات العليا لأمن المعلومات ، ووجود تقريرِ مدير أمن المعلومات (CISO) بشكلٍ مستقل عن وظيفة تكنولوجيا المعلومات له تأثيرٌ إيجابيٌّ على جودةِ العلاقة بين التدقيق الداخلي، ووظائف أمن المعلومات.

كما تضمنّت الدراسةُ مجموعةً من النتائجِ أهمها: أصبحَ من الأهمية بمكان بالنسبة للشركات إدارة مخاطر أمن المعلومات، ناقشت أدبيات ممارسة المهنة منذ فترة طويلة أنَّ وظيفةَ التدقيق الداخلي (IAF) يمكنُ أن تلعبَ دوراً مهماً في توفيرِ الضمان فيما يتعلّقُ بأمن المعلومات، وفي تكوين رؤىً حولَ كيفيةِ تحسينِ أمن معلومات المنظمة.

4) دراسة (Stafford, Deitz, Li 2018)[18]: بعنوان " دور التدقيق الداخلي وتدريب المستخدم في الامتثال لسياسة أمن المعلومات":

هدفت هذه الدراسةُ إلى استكشافِ دور الامتثال لسياسة أمن المعلومات، ودور تدقيق نظم المعلومات في تحديد عدمِ الامتثال في مكان العمل، مع التّركيز بشكلٍ خاصٍّ على دورِ المطّلعين غير الخبيثين الذين يحبطون أمن معلومات الشركة بشكلٍ غير مدروسٍ، أو بغير علم.

تُطبّق هذه الدراسةُ دراسة الحالة لمفاهيم أمن مستخدم تكنولوجيا المعلومات، مقترنةً بالتحليل الوصفيّ للمقابلات العميقة مع المدقّقين لفحص، وشرح قواعد سلوكيات مستخدمي التكنولوجيا غيرِ الضّارة في انتهاكِ توجيهات أمن

[17] Paul John Steinbart, Robyn L. Raschke, Graham Gal, William N. Dilla, 2018, **The influence of a good relationship between the internal audit and information security functions on information security outcomes,** Accounting, Organizations and Society

[18] Thomas Stafford, George Deitz, Yaojie Li, 2018, **The role of internal audit and user training in information security policy compliance**, Managerial Auditing Journal, Volume: 33 Issue: 4

المعلومات، لتحديد الطّرق التي يمكنُ بها للمدقّق مساعدة الإدارة على أفضلِ وجهٍ في التغلّب على المشاكل المرتبطة بالرضى الأمني بين المستخدمين.

5) دراسة (Niekerk, Rudman 2019)[19] بعنوان " مخاطر، وضوابط، وحوكمة تقنيات إنترنت الأشياء في المعلومات المحاسبية ":

هدفت هذه الدراسةُ إلى تحديدِ مخاطرِ، وضوابطِ التّحكم المرتبط بإنترنت الأشياء في تقنيات المعلومات المحاسبية، حيثُ تمَّ إجراءُ مراجعةً منهجيةً للأدبيات لتحديدِ مفهوم إنترنت الأشياء، واكتساب فهمٍ للتقنيات التمكينية لإنترنت الأشياء. من أجلِ تحديدِ المخاطر الكامنة وراءَ التقنيات التي تُمكّنُ إنترنت الأشياء بشكلٍ شامل، وكان من الضروري اختيارُ إطارِ عمل للحوكمة يمكنُ استخدامه كمعيارٍ كامل من الضوابط. تمَّ تعيينُ الفهم المكتسب لتقنيات إنترنت الأشياء مقابلَ عمليات COBIT 5 المتعلقة بمخاطر المعلومات المحاسبية لتحديدِ التهديدات ذات الصلة والتوصية بضوابط محتملة. تمَّ تطويرُ مصفوفةِ المخاطر لتحديدِ المخاطر الرئيسية، وتخفيفها من خلال الضوابط. تركّزُ المخاطرُ المحددة للمعلومات المالية على تكاملِ البيانات، والسرية، وتوافرِ الشبكة، ونقاطِ الضعف في تكنولوجيا المعلومات. تمّت صياغةُ نهجٍ متعدّدِ الطبقات للضوابط الداخلية الفنية، وغير الفنية، للتخفيفِ من المخاطر المحدّدة إلى مستوى مقبول.

توصّلت الدراسةُ إلى مجموعةٍ من النتائج أهمها: يمكن أن يؤدي اعتمادُ إنترنت الاشياء (IoT) كجزءٍ من عمليات الشركة إلى توليد قيمة للأعمال من خلال توليد البيانات وتكاملها، فضلاً عن تحسينِ جودة المعلومات، من خلال جمعِ المعلومات في الوقت الفعلي باستخدام تقنيات الاستشعار المدمجة في كائناتٍ مادية، أو افتراضية يمكنُ التعرفُ عليها بشكلٍ فريد من أجل تعزيز الأعمال التجارية لقدراتها المعلوماتية، قد يؤدي اعتمادُ إنترنت الأشياء إلى تحقيق السرعةِ في المعالجة، دونَ فهمٍ كاملٍ لتقنياتها التمكينية، والمخاطر المرتبطة بها.

كما تمَّ تبنّي مجموعةً من التوصيات أهمها: من الضروري أن تحتفظَ المعلومات المالية بخصائص الدقةِ، والاكتمال والتوقيت المناسب عندَ نشرِ إنترنت الأشياء في الأعمال التجارية. وتوصي الدراسة باستخدامِ الضوابطِ المناسبة التي يمكنُ تنفيذُها للتّخفيف من المخاطر.

[19] Anja van Niekerk, Riaan Rudman, 2019, **Risks, controls and governance associated with internet of things technologies on accounting information,** Southern African Journal of Accountability and Auditing Research, Volume 21 Number 1, p. 15 - 30

6) دراسة (Li, Chang, et al 2019)[20] بعنوان: "عناصر الرقابة الداخلية لتكنولوجيا المعلومات لمرحلة ما بعد التنفيذ لأنظمة تخطيط موارد المؤسسة ":

هدفت هذه الدراسةُ إلى تحديدِ عناصرِ الرقابة الداخلية لتكنولوجيا المعلومات لمرحلةِ ما بعد التنفيذ لأنظمة تخطيطِ مواردِ المؤسسة، في هذه الدراسةُ، استناداً إلى إطار COBIT 5، قامَ الباحثُون بمراجعة 56 دراسة من المجلات الأكاديمية ذات الصلة من عام 1998 إلى عام 2014 لتشكيلِ قائمةٍ أوليّة بعناصر الرقابة الداخلية لتكنولوجيا المعلومات (IT) لمرحلةِ ما بعد التنفيذ لأنظمةِ تخطيطِ مواردِ المؤسسة (ERP). تمَّ إجراءُ مسحٍ للتحقّقِ من صحة القائمة، وتمَّ تصنيفُ 45 عنصراً للتحكّم باستخدامِ طريقة دلفي. قد تساعدُ العناصرُ المقترحة الشركات، والمدققين في التركيز على قضايا الرقابة الداخلية الأساسية خلالَ مرحلةِ ما بعدَ تنفيذِ نظام تخطيط موارد المؤسسات.

توصّلت الدراسةُ إلى نتائجَ أهمها: لا يزالُ فهمنا للضوابط الداخلية ذات الصلة في مرحلة ما بعدَ التنفيذ محدوداً على الرغم من التوجيه العامّ من الأطر المهنيةِ، أو المعايير إلى تطبيق ضوابطٍ محدّدة.

7) دراسة (Ismail, Islam 2020)[21] بعنوان: "إطار عمل موحد لشفافية وتدقيق أمن السحابة":

هدفت هذه الدراسةُ إلى تقديمِ إطارِ عملٍ لمواجهةِ التّحدي المُلحّ لشفافية أمن السحابة، حيثُ تتضمنُ عمليات وأدوات تدقيقٍ داعمة لفحص مزودي الخدمات السحابية، وتمكينِ الشفافية الأمنية بناءً على متطلّبات المستخدم المحددة مسبقاً، حيثُ قامَ الباحثُ بتطوير أدواتِ تدقيقٍ شفافية أمنية يمكنُ من خلالها للمستخدمين جمعُ الأدلة من موفري الخدمات السحابية، وتحليلُها لتحديد التوافق مع المتطلبات، كما تمَّ تصميمُ الأداة لتكونَ مكوناً تكميلياً لإطارِ العمل المقترح الذي يسمحُ بالتحققِ، والفحص المستمر لمزوّد الخدمات السحابية الذي يفي بمتطلبات المستخدم ، وبالتالي تعزيزُ الشفافية الأمنية، العملُ الجديدُ الذي قدّمته الدراسةُ أنّه تمّ دمجُ عناصر مختلفة لتوفير طريقةٍ مبسّطة للمنظمات، لتحقيقِ الشفافيةِ الأمنية.

[20] Hsing-Jung Li, She-I Chang, Tawei (David) Wang and Li-Min Chang, 2019, **Information Technology Internal Control Items for the Post-Implementation Phase of Enterprise Resource Planning Systems,** Journal of Information Systems.

[21] Ismail, Umar, Islam, Shareef, 2020**, A unified framework for cloud security transparency and audit**, Journal of Information Security and Applications.

8) دراسة (Sun, 2020)[22] بعنوان: " حماية الأمن والخصوصية في الحوسبة السحابية: المناقشات والتحديات"

تهدفُ الدراسةُ إلى تقديمِ مراجعةٍ حولَ قضايا الأمن والخصوصية من خلال العديدِ من تقنيات حماية الأمن والخصوصية في الحوسبة السحابية، حيثُ تقُدّمُ أولاً عرضاً لمخاطرِ أمن، وخصوصية الحوسبة السحابية، وتقترحُ إطاراً شاملاً لحماية الأمن والخصوصية في الحوسبة السحابية.

ثمَّ تعرضُ وتناقش العديدَ من التقنيات المستخدمة لتحقيقِ أمن، وخصوصية الحوسبة السحابية، ثمّ مقارنة وتحليل خصائص، ونطاق تطبيق المخططات النموذجية لأمن وخصوصية الحوسبة السحابية، أخيراً تناقشُ التحديات الحالية، وتبرزُ اتجاهات البحثِ المستقبليّة المحتملة.

<u>ما تتميز به الدراسة الحالية عن الدراسات السابقة:</u>

تأتي هذه الدراسةُ استكمالاً للدراسات السابقة التي ركّزت على أثرِ استخدام تكنولوجيا المعلومات بشكلٍ عامّ على نظام الرقابة الداخلية، كما ركّزت دراسات أخرى على مخاطرِ أمن المعلومات وأثرِها على عملية التدقيق، في حين تناولت بعضُ الدراساتِ نظامَ المعلومات المحاسبي الالكتروني، ودورهِ في تعزيزِ أمن المعلومات المالية.

أمّا الدراسةُ الحاليّة، فتتميزُ بأنّها تسعى إلى بيانِ مدى إسهامِ ضوابط أمن المعلومات المختلفة التي تتبنّاها المنظمة في رفعِ أداء نظام الرقابة الداخلية، ودفعه لتحقيقِ أهداف المنظمة في مواجهةِ مختلفِ المخاطر من فقدان الأصول أو الوصول غير المصرّح به، وكافّة المخاطر التي تتعرّضُ لها سواءً في البيئة الداخلية، أو الخارجية للمنظمة، حيثُ بحثت الدراسةُ بشكلٍ محدّدٍ حولَ دورِ ضوابط أمن المعلومات في تفعيل نظام الرقابة الداخلية في البيئة السورية، للوصول إلى نظامِ رقابة داخلية متناغماً مع أهدافِ حماية المنظمة من المخاطر المختلفة لاسيما مخاطر أمن المعلومات.

1-6 أنموذج الدراسة:

بناءً على هدفِ الدراسة، صُمّمَ الأنموذجُ الآتي لدراسةِ دورِ ضوابطِ أمن المعلومات في تفعيلِ نظامِ الرقابة الداخلية.

[22] Sun, PanJun, 2020, **<u>Security and privacy protection in cloud computing: Discussions and challenges</u>**, Journal of Network and Computer Applications 160

المتغير المستقل:	المتغير التابع:
ضوابط أمن المعلومات:	**نظام الرقابة الداخلية:**
الضوابطُ الوقائيّة. **الضوابطُ الاكتشافيّة.** **الضوابطُ التصحيحيّة.**	**الفصلُ بين المسؤوليات، والاختصاصات.** **وضوحُ خطوط السلطة، والمسؤولية.** **كفاءةُ الموظفين.** **سلامةُ السجلات، والتصديق على العمليات.** **حمايةُ الأصول والسجلات.** **متابعةُ الالتزام بنظم الرقابة الداخلية.**

1-7 فرضيات الدراسة:

انطلاقاً من مشكلة الدراسة، ولتحقيقِ أهدافِها يمكنُ للباحث تحديدَ الفرضيات الآتية:

1. لا توجدُ علاقةً ذات دلالةٍ إحصائية بين الضوابط الوقائيّة لأمن المعلومات، وتفعيلِ نظام الرقابة الداخلية.
2. لا توجدُ علاقةً ذات دلالةٍ إحصائية بين الضوابط الاستكشافيّة لأمن المعلومات، و تفعيل نظام الرقابة الداخلية.
3. لا توجدُ علاقةً ذات دلالةٍ إحصائية بين الضوابط التصحيحيّة لأمن المعلومات، و تفعيل نظام الرقابة الداخلية.
4. لا توجدُ فروقاتٍ ذات دلالةٍ إحصائية بين آراء عينتيّ الدراسة.

الفصل الثاني: الإطار المفاهيمي لأمن المعلومات وضوابطه.

تمهيد:

مرَّ مفهومُ أمنِ المعلومات بمراحل تطورٍ متلاحقة، ففي ستينيات القرن الماضي كانت أجهزةُ الحاسوب وعملها هي شغلُ العاملين في أقسام المعلومات، حيثُ كانَ همُّهم هو كيفيةُ تنفيذ البرامج، والأنشطة المحوسبة، ولم يكونوا مشغولينَ بأمنِ المعلومات بقدرِ انشغالهم بعملِ الأجهزة، وكانَ مفهومُ الأمن يدورُ حولَ تحديدِ الوصولِ أو الاطلاع على البيانات من خلال منعِ كلّ غريبٍ من التلاعب في الأجهزة، لذلك ظهرَ مصطلحُ أمن الحاسوب، والذي يعني حماية الحاسوب، وقواعد البيانات.

ونتيجةً للتوسع في استخدم أجهزة الحاسوب، وما تؤدّيه من منافعَ تتعلقُ باتساعِ أحجام معالجة البيانات تغيّرَ الاهتمامُ ليمثّلَ السيطرةَ على البيانات وحمايتها، وفي سبعينيات القرن الماضي تمَّ الانتقالُ إلى مفهومِ أمن البيانات، ورافقَ ذلك استخدامَ كلماتِ السر البسيطة للسيطرة على الوصول للبيانات، إضافةً إلى وضعِ إجراءات الحماية لمواقع الحواسيب من الكوارث، واعتمادَ خططٍ لتخزينِ نسخٍ إضافية من البيانات والبرمجيات بعيداً عن موقع الحاسوب، ومع بداية القرن الحالي ازدادت أهميةُ استخدامِ البيانات، وساهمت التطورات في مجال تكنولوجيا المعلومات بالسماحِ لأكثرِ من مستخدمٍ المشاركةُ في قواعد البيانات، كلّ هذا أدى إلى الانتقال من مفهوم أمن البيانات إلى أمن المعلومات، وأصبحَ من الضروري المحافظةُ على المعلومات، وتكاملها، وتوفرها، ودرجة موثوقيتها، حيث إنَّ الإجراءات الأمنية المناسبة يمكن أن تساهمَ في ضمانِ النتائج المرجوّة، وتقلّصُ اختراقَ نظم المعلومات، والتلاعبَ بها.[23]

وتشكّلُ المعلومات البنيةَ التحتيّة للمنظمات حيثُ تُمكّنُها من أداءِ مهامِها، والمساعدةِ في اتخاذ قراراتها الإدارية، والتمويلية والاستثمارية، إذ إنّ نوعَ المعلومات، وكميّتَها، وطريقةَ عرضها ، تعتبرُ الأساسَ في نجاح عملية صنع القرارات داخل المنظمات وخارجها، وعليه تمثّلُ المعلومات اليوم أحدَ الأصولِ الهامّة في العديد من المنظمات، فبدون معلوماتٍ موثوقة، ومحمية بشكلٍ صحيح، فمن المرجّح أن تتوقفَ المنظمةُ عن العمل، وعلى الرغم من أنَّ الاستثمارَ في أمن المعلومات يمكن أن يجلبَ للمنظمة العديدَ من الفوائد من حيثُ إنّه يساعدُ في حماية أصول المعلومات القيّمة، ومنعِ العواقب المدمرة في حالِ تعرّضِها لخطرِ التهديدات المحيطة، فإنّ العديدَ من المنظمات لا تستثمرُ ما يكفي من أموالها في سبيل تحقيق أمن المعلومات، وذلك لصعوبةِ إثباتِ قيمة الاستثمارات في أمن

[23] فيلالي، أسماء، 2019، **مستوى أمن المعلومات في المؤسسات الجزائرية ومدى تأثره بطبيعة التهديدات وطبيعة الحماية المطبقة**، أطروحة دكتوراه، جامعة أبي بكر بلقايد، الجزائر، ص 62.

المعلومات، و نظراً لما للمعلوماتِ من قيمةٍ عاليةٍ، فإنَّه يتوجبُ على إدارة المنظمة وضعَ الضوابط اللازمة لاستخدامها، وتداولها، ووضعَ السُّبلِ الكفيلةِ بحيازتها.[24]

يتناولُ الباحثُ في هذا الفصلِ ماهيّةَ أمنِ المعلومات، وعناصرها ، وأهميتها، وخصائصها، وأهدافها، كما نوضّحُ بعضَ المعاييرِ العالميّة التي من الممكن تبنّيها جزئياً أو كلياً من قبل المنظمات لضمانِ أمن المعلومات على نحوٍ موثوق، إضافةً لمصادر الإخلالِ بأمن المعلومات، و التهديدات المحيطة بها، ونوضّحُ في ضوء تلكَ المعايير والأطر العالمية، والتشريعات المختلفة بصورةٍ أكثر تفصيلاً ضوابطَ أمن المعلومات التي من الممكن أن تحقّقَ مستوىً عالٍ لأمن المعلومات في المنظمة.

المبحث الأول: ماهية أمن المعلومات وخصائصه:

2-1-1 تعريف أمن المعلومات:

يُعرّفُ أمنِ المعلومات على أنّه "استراتيجيةٌ شاملةٌ لجميعِ أقسامِ الشّركة، ونواحي العمل بهدفِ حماية المعلومات الخاصّة بالشركة بغضّ النظر عن نوعِ هذه المعلومات (داخليّةٌ، أم خارجية) حماية تقنية، وقانونية من خلال وضع السياسات، والضوابط اللازمة لذلك، وتطبيقها بفعالية مع توجيهها ، ومراقبتها بشكلٍ مستمرّ ضماناً لحماية المعلومات من أيّ تهديداتٍ تعرّضُها للخطر".[25]

كما يمكنُ تعريفُ أمنُ المعلومات بأنّه " عبارةٌ عن مجموع الوسائل التقنية، والإدارية التي يتمُّ استخدامُها لمنعِ الوصول غير المُصرّح، وسوء استخدام المعلومات الإلكترونية، ونظم الاتصالات والمعلومات التي تحتويها بهدفِ ضمانِ توافر، واستمرارية عمل نظم المعلومات، وتأمين حماية، وسرية، وخصوصية البيانات الشخصيّة، وحماية المواطنين من المخاطر في الفضاء السيبراني".[26]

أمّا (اللجنة التنفيذية لخدمات الثقة Trust Services) فقد أكّدت على أنّ أمنَ المعلومات يعني أنّ " المعلومات والأنظمة محميةٌ ضدَ الوصول غير المصرّح به، والكشفِ غير المصرّح به عن المعلومات، والأضرارِ التي تلحق بالأنظمة التي يمكنُ أن تضرَّ بتوافِر، وسلامةِ، وسرية، وخصوصية المعلومات، أو الأنظمة، وتؤثّرُ على قدرةِ المنظمة على تحقيق أهدافِها، وبالتالي يشيرُ أمنُ المعلومات إلى حماية: [27]

- المعلومات أثناءَ جمعِها، أو إنشائِها، واستخدامِها، ومعالجتها، ونقلها، وتخزينها.

---

[24] Otero, Angel R., 2019, **Information Technology Control and Audit**, Fifth Edition, CRC Press Taylor & Francis Group, USA, p: 316.

[25] الجعبري، هناء، 2018، **أثر الأمن المعلوماتي على أداء شركات التأمين العاملة في فلسطين**، رسالة ماجستير، جامعة الخليل، فلسطين، ص 18.

[26] اللجنة العربية للرقابة المصرفية، 2017، **سلامة وأمن المعلومات المصرفية الإلكترونية**، صندوق النقد العربي، أبو ظبي، ص 10

[27] The Assurance Services Executive Committee, , March 2020, **2017 Trust Services Criteria**, AICPA, p: 6.

- الأنظمة التي تستخدمُ المعلومات الإلكترونية لمعالجتِها، ونقلِها، وتخزينِها لتمكينِ الكيان من تحقيق أهدافه.

وقد عرّفَ آخرون أمنَ المعلومات بأنّه "هو كلُّ السياسات، والإجراءاتِ المطبّقة بهدفِ حمايةِ المعلومات عن طريق توفير الأمن لكلّ المكونات المادية من محلات، وأجهزة، و المكونات التقنية كالبرمجيات، والشبكات، والاتصالات، وكلّ التكنولوجيات المستعملة في تداولِ المعلومات، دونَ نسيان أهمّ عنصرٍ وهو العنصرُ البشريّ الذي كلما زادت حمايته تطوّرَ تعامله مع المعلومات لأنَّ التقنيةَ مهما بلغت مستوياتُها لا يمكن أن تحلَّ محلَّ العنصرَ البشريّ".[28]

كما عرّفت السياسات الوطنية لأمن المعلومات الصادرة عن الهيئة الوطنية لخدمات الشبكة أمن المعلومات بأنّه: "الوسائلُ والتدابيرُ الخاصة بالحفاظِ على سرية وتوافرية، وسلامة المعلومات، وحمايتِها من الأنشطة غير المشروعة التي تستهدفُها".[29]

في ضوءِ التعريفاتِ السابقة يمكنُ القول أنَّ أمنَ المعلومات هو استراتيجيةٌ شاملةٌ تتبنّى مجموعةً من الإجراءات والسياسات، بهدفِ ضمان حماية، وسرية، وخصوصية المعلومات أثناءَ كافةِ مراحل إنتاجِ المعلومات في نظام المعلومات، وتوفيرِ الأمن على كافة العناصر المكوّنة لنظام المعلومات، من أصولٍ مادية كالأجهزة، والمعدات، والأصول المعنوية كالبرمجيات، والتقانات التي تعالجُ، وتنقلُ وتخزّنُ المعلومات، والأصول البشرية التي تديرُ وتستخدمُ أنظمة المعلومات، ويشيرُ الباحثُ إلى أنّه في ظلِّ التطورات الأخيرة الحاصلة في بيئة الأعمال من استخدام التقنيات الحديثة كالحوسبة السحابية، والمحاكاة الافتراضية، وانترنت الأشياء وغيرها، فقد تتعرّضُ المعلومات إلى مخاطرَ جديدة في المستقبل تؤثّرُ على استراتيجية، وإجراءات أمن المعلومات.

2-1-2 عناصر أمن المعلومات: يقومُ أمنُ المعلومات على ثلاث ركائز أساسية:

1. **السرية Confidentiality:** تشيرُ السّرية إلى حمايةِ المعلومات من الوصول إليها من قبل أطرافٍ غير مصرّح لها، وضمانِ حفظِ المعلومات المخزّنة أو المنقولة، وعدمِ الاطلاع عليها، أو استخدامها إلا بموجب إذن، حيثُ إنَّ النظامَ الآمن هو الذي يضمنُ سريةَ، وخصوصيةَ البيانات المخزنة فيه، فلا يسمحُ بكشفها بدون ترخيص، أو الاطلاعِ عليها من قبل أشخاصٍ غير مخول لهم بالاطلاع على تلك البيانات، إضافةً إلى تأمين الطرقِ المناسبة لحمايتها من القراءة أثناءَ نقلِها عبرَ شبكةِ الاتصال، والسرعة في نقلها، وتحديد حدود، وصلاحية الاستخدام سواءً كان كلياً أم جزئياً، مع تحديدِ من له صلاحيةُ التعديل، أو الإدخال، أو الحذف، أو الإضافة.[30]

---

[28] فيلالي، أسماء، 2019، **مرجع سبق ذكره**، ص 60.

[29] الهيئة الوطنية لخدمات الشبكة، 2014، **السياسات الوطنية لأمن المعلومات**، وزارة الاتصالات والتقانة، سوريا، ص 2.

[30] Chopra, Abhishek, Chaudhary, Mukund, 2020, **Implementing an Information Security Management System Security Management Based On ISO 27001 Guidelines**, APRESS, USA, p: 8.

2. **التكاملية والسلامة Integrity**: تشيرُ سلامةُ المعلومات إلى اتّساقها، ودقتها، وموثوقيتها طوالَ دورةِ حياتها بأكملها، وعدمِ إمكانية تغييرها أو التلاعب بها[31]، والتأكّد أنَّ هذه المعلومات لم تتعرض لأيّ عمليةِ حذفٍ أو تخريب أو تلفٍ كليّ، أو جزئيّ سواءً بصفةٍ متعمّدة، أو غير متعمّدة في أيّ مرحلةٍ من مراحل المعالجة، أو التبادلِ وإلا يكونُ قد تمَّ ضياعُ تكامل المعلومات.[32]
3. **التوفر والإتاحة Availability**: أي أن تكونَ البيانات متاحةً بسهولةٍ للمستخدمين المصرّح لهم، فإذا كانت البيانات مؤمنةً، ولكنّها غيرُ متاحةٍ عند طلبها، فقد يمثّلُ ذلك خطراً كبيراً على المنظمة، و لهذا العنصرُ مجموعة من الخصائص متمثلة في: [33]

- المقاومة: وهي قدرةُ النظام على الحفاظ على نفسه من العمليات التي تجعلُه غير متاحٍ للمستخدمين المخولين باستخدامه.
- سهولة الاستخدام: أي إنَّ المعلومات متاحةٌ للاستخدام من قبل الأشخاص العاديين، ولا تحتاجُ إلى مستويات عليه من المعرفة والخبرة للوصول إليها.
- المرونة: والمتمثلةُ في توفّر الإمكانياتِ و الأدوات التي تمكّن من إدارة النظام دون أن يستدعي ذلك توقّفه.
- المقدرة على التوسّع لسدِّ الحاجيات المستقبلية.

حتى يستمر تطبيقٌ ما بالتوفر يجب أن تكونَ جميعُ مكوّنات النظام متوفرةً أيضاً بحيثُ تتضمنُ التطبيقَ، و قاعدة البيانات، و الخادم، و أجهزةَ التخزين، وسلامةَ الشبكة من البداية إلى النهاية.

كما نلاحظُ فإنَّ الأبعادَ الأساسية الثلاثة لإدارة أمن المعلومات (السرية، السلامة، و التوفر) لابدَّ من توفّرها في كلّ نظام، و لكن قد يغلبُ أحدها على الآخر حسبَ طبيعة المعلومات، و المنظمة، و الظروفِ المحيطة بها، و الأهمُّ من ذلك كلّه التوازنُ بين المنع، والاستخدام، فمنعُ استخدامِ المعلومات يحقّقُ أقصى درجاتِ السرية لكن يحجبُ إمكانية التوفّر للمعلومات في المنظمة، أما إتاحةُ المعلومات للاستخدام يحقّقُ أعلى درجاتِ التوفّر لكنّ ذلك سيؤثّرُ حتماً على سريّة المعلومات، فمن المعروف أنَّ اتخاذَ قرار المنع الكلي سهلٌ جداً ،و لكنّه غيرُ مناسبٍ، وغيرُ مفيدٍ، والعكسُ بالعكس.

2-1-3 أهمية أمن المعلومات:

تمثّلُ المعلومات أحد الأصول الهامة في العديدِ من المنظمات اليوم، وبالتالي فبدون معلوماتٍ موثوقةٍ، ومحميةٍ بشكلٍ صحيحٍ فمن المرجّح أن تتوقفَ المنظّمةُ عن العمل، كما يرتبطُ الحفاظُ على سمعةِ المنظمة، وتعزيزِها ارتباطاً

---

[31] Chopra, Abhishek, Chaudhary, Mukund, 2020, **Op cit.**, p: 8.

[32] البركي، أحمد، 2020، **واقع تطبيق مُتطلبات نُظم إدارة أمن المعلومات المتوافقة مع المواصفة (ISO 27001) بالمصارف العاملة بمدينتي بنغازي والبيضاء، مجلة الاقتصاد الدولي والعولمة**، العدد (2)، المجلد (3)، ليبيا، ص: 146.

[33] Chopra, Abhishek, Chaudhary, Mukund, 2020, **Op cit.**, p: 8.

مباشراً بالطريقة التي تُدارُ بها المعلومات، وبالتالي يساعدُ التنفيذُ الفعّال لأمن المعلومات على ضمانِ تلبيةِ أهدافِ العمل الاستراتيجية للمنظمة.[34]

فمع تزايدِ حدّةِ التنافسِ بين المنظمات، وازديادِ حجمِ الأسواق باتت عمليةُ حماية الأصول بما فيها المعلومات التي تنتجُها أنظمة المعلومات المختلفة في المنظمة من الأولويات التي لا يجب التغافل عنها، حيثُ يتمُّ ذلك من خلال وضعِ الضوابط والتوجيهات اللازمة للحفاظ على أمن المعلومات من أيّ تهديدٍ قد تتعرّضُ له، واتخاذِ التدابير والإجراءات اللازمة لذلك، إذ إنَّ فقدانَ أو تسريب المعلومات قد يكونُ الحدَّ الفاصل للربح أو الخسارة للمنظمات، ولا يكون ذلك الخطرُ على المستوى المالي فحسب، وإنما سبباً في فقدانِ ثقة العملاء، والزبائن، وتوقّفهم عن التعامل مع المنظمة ، وتراجعِ أداء المنظمة بشكلٍ عامّ.[35]

ويمكنُ عرض أهمية أمن المعلومات من خلال النقاط الآتية:[36]

- اعتمادُ مختلف المنظمات على فعالية المعلومات.
- النمو المضطردُ في الاستخدامات، والتطبيقات الالكترونية، وظهورُ التجارة الالكترونية، والحكومة الالكترونية، الإدارة الالكترونية التي تحتاجُ إلى بيئةٍ معلوماتية آمنة.
- الحاجةُ إلى حماية البنية التحتية للشبكة المعلوماتية، وذلك من أجلِ استمرارية الأعمال التجارية.
- تقليلُ الخسائر المالية التي قد تنتجُ عن الوقوع في مهدّدات أمن المعلومات.

يمكننا انطلاقاً من التّعاريف السّابقة لأمن المعلومات إضافةَ مجموعةٍ أخرى من النقاط التي من الممكن أن توضّحَ أهميةَ قيام المنظمة بالاستثمار في أمن المعلومات:

- تقليلُ المخاطر المختلفة المحيطة بالمنظمة إلى مستوى مقبول.
- رفعُ كفاءةِ اتخاذ القرارات الإدارية بالاعتماد على معلوماتٍ موثوقة.
- تشكّلُ المعلومات اليوم أصولاً معنويةً يمكنُ بيعها، وتداولها، وبالتالي فإنَّ أمنَ المعلومات لا يقلُّ أهميةً عن أمن الأصول المادية الأخرى في المنظمة.
- يزيدُ أمنُ المعلومات من القيمة السوقية للمنظمات التي تتبنّى معاييراً واضحةً لسلامةِ معلومات العملاء، مما يدفعُ لزيادةِ حصّتها السوقية مقارنةً مع منظمات أخرى لا تأخذ ضوابط أمن المعلومات على محمل الجدّ.

---

[34] Otero, Angel R., 2019, **Op Cit.**, p: 317.

[35] الجعبري، هناء، 2018، **مرجع سبق ذكره**، ص 19.

[36] الشوابكة، عدنان، 2019، **دور إجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلومات في جامعة الطائف**، المجلة العربية للأبحاث والدراسات في العلوم الأنسانية والأجتماعية، العدد 4، المجلد 11، المملكة العربية السعودية، ص: 168.

2-1-4 خصائص أمن المعلومات:

يرى خبراءُ أمن المعلومات أنَّ أهمَّ الخصائص التي يجبُ أن يتمتعَ بها أمن المعلومات في المنظمة تتمثّل في أنَّ:

1. **أمن المعلومات يجب أن يُحقّقَ رؤيةَ و أهدافَ المنظمة:** قد يُنظر إلى أمن المعلومات أحياناً على أنّه يعيقُ عملَ المنظمة من خلال فرضِ قواعد وإجراءات تؤثّرُ على المستخدمين، والمديرين، والأنظمة بشكلٍ عامّ، لكنّ الحقيقة أنّ تلكَ القواعد والإجراءات في حال تمَّ اختيارُها بالشكلِ المناسب فإنَّها تساهمُ إلى حدٍّ كبيرٍ في حماية الأصول المهمة في المنظمة، وبالتالي يمكنُ القول أنّ أمنَ المعلومات هو وسيلةٌ لتحقيقِ غايات المنظمة، وليس غاية في حد ذاته.[37]
2. **إجراءاتُ أمن المعلومات إجراءاتٌ إدارية، وفنية في وقت واحد:** على الرغم من أنَّ أمنَ المعلومات الفعّال يتطلّبُ نشرَ أدواتِ أمن المعلومات مثلَ جدرانِ الحماية، وبرامج مكافحة الفيروسات، والتشفير، فإنَّ مشاركةَ الإدارة العليا ، ودعمَ أهدافِ أمن المعلومات خلالَ جميعِ مراحل دورةِ حياة أمن المعلومات أمرٌ ضروريٌّ للغايةِ لتحقيق مستوىً عالٍ لأمن المعلومات.[38]
3. **أمنُ المعلومات هو جزءٌ أساسيٌّ من عمليات الإدارة الناجحة:** نظراً لأنّه لا يمكن القضاءُ على مخاطر أمن المعلومات تماماً، فإنَّ هدفَ الإدارة الناجحة هو تحقيقُ التوازنِ الأمثل بين حماية المعلومات، واستخدام موارد المعلومات المتاحة، وبالتالي فإنّ الإدارةَ العليا هي التي تتحمّلُ مسؤوليةَ تحديدِ مستوى المخاطر المقبول للمنظمة ككلّ، ونظم المعلومات بشكلٍ خاصّ بما يحققُ التوازنَ المطلوب لحمايةِ المعلومات من جهة مع توافرها عندَ الحاجة إليها من جهةٍ أخرى.[39]
4. **تحقيقُ أمن المعلومات يتطلّبُ دراسةً واعيةً لإدارة المخاطر:** لا يمكن القضاءُ على المخاطر التي يتعرّضُ لها النظام تماماً، لذلك من المهمّ إدارةُ المخاطر من خلال تحقيقِ التوازن بين قابلية الاستخدام، وتنفيذِ ضوابطِ أمن المعلومات، فالهدفُ الأساسيّ لإدارةِ المخاطر هو تنفيذُ تدابيرِ الحماية الأمنيّة التي تتناسبُ مع المخاطر، لأنّه قد يؤدّي تطبيقُ ضوابطِ غير ضرورية إلى إهدارِ الموارد، وزيادةِ صعوبة استخدام الأنظمة وصيانتها، وعلى العكس من ذلك فإنَّ عدمَ تطبيقِ الضّوابطِ اللازمة لحمايةِ النظام قد يتركُه ومعلوماته عرضةً للانتهاكات في السرية، والسلامة، والتوافر، مما يعيقُ، أو يوقفُ أعمالَ المنظمة.[40]

---

[37] Nieles, Michael, Dempsey, Kelley, Yan Pillitteri, Victoria, 2017, **an Introduction to Information Security**, NIST, USA, p: 7.

[38] Romney, Marshall, Steinbart, Paul, Summers, Scott, Wood, David, 2021, **Accounting Information Systems**, 15th edition, Pearson, UK, p:336

[39] فيلالي، أسماء، 2019، **مرجع سبق ذكره**، ص 65.

[40] Nieles, Michael, Dempsey, Kelley, Yan Pillitteri, Victoria, 2017, **Op cit.**, p: 8.

5. **أمنُ المعلومات الفعال يستندُ إلى تفادي الخطر بالوقت المناسب:** إنَّ استخدامَ استراتيجياتٍ مناسبة لأمن المعلومات يجب أن يهدفَ إلى اكتشافِ، ومنعِ وقوع هجمات، أو انتهاكات، واتخاذِ خطواتٍ مضادة في الوقت المناسب ، لإحباط الهجوم قبلَ أن يتمَّ فَقْد المعلومات، أو تعريضها للخطر.[41]
6. **أمنُ المعلومات يجب أن ينفذَ برؤيةٍ اقتصاديةٍ فعّالة:** إنَّ الفوائدَ الأمنيّة لها تكاليفُ مباشرةٍ وغير مباشرة، تشملُ التكاليفُ المباشرة شراءَ، وتركيبَ، وإدارةَ الإجراءات الأمنية، بالإضافةِ إلى ذلك يمكن أن تؤثّرَ الإجراءات الأمنية في بعض الأحيان على أداء النظام، أو معنويات الموظفين، أو متطلبات إعادة التدريب، وبالتالي في كثيرٍ من الحالات قد تتجاوزُ هذه التكاليفُ الإضافية التكلفةَ الأوليّة لعنصر التحكم.[42]
7. **تتطلبُ برامج أمن نظم المعلومات إعادةَ تقييمٍ دوريّة:** إنَّ أمنَ المعلومات ليس عمليةً ثابتة، ويتطلبُ مراقبةً، وإدارةً مستمرة لحماية سريّة المعلومات، وسلامتها، وتوافرها، وكذلك لضمان تحديد نقاط الضعف، والتهديدات الجديدة بسرعةٍ، والاستجابة لها وفقًا لذلك.[43]
8. **دراسةُ أنظمةِ أمن المعلومات شاملة و متكاملة:** يتطلبُ توفيرُ أمن المعلومات الفعّال إلى اتباعِ نهجٍ شاملٍ يأخذ في الاعتبار مجموعةً متنوعة من المجالات داخلَ وخارجَ مجالِ أمن المعلومات، وبالتالي يتمُّ تطبيقُ هذا النهج طوالَ دورةِ حياةِ المعلوماتِ بأكملها.[44]
9. **أمنُ المعلومات يتأثّرُ بالعوامل الاجتماعية:** تؤثّرُ العواملُ المجتمعية على كيفيةِ فهم الأفراد واستخدامهم للأنظمة التي تؤثّرُ بالتالي على أمن المعلومات للنظام والمنظمة، حيثُ يتخذُ الأفرادُ قراراتٍ قائمة على المخاطر بطرقٍ مختلفة، لمعالجةِ هذا الأمر تجعلُ المنظمات وظائفَ أمن المعلومات شفافةً، وسهلةَ الاستخدام، ومفهومةً، بالإضافةِ إلى ذلك، فإنّ توفيرَ تدريبِ التوعية الأمنية بانتظام يقلّلُ أيضاً من الفروق الفردية في إدراك المخاطر.[45]

---

[41] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p:339

[42] Nieles, Michael, Dempsey, Kelley, Yan Pillitteri, Victoria, 2017, **Op cit.,** p: 8.

[43] Nieles, Michael, Dempsey, Kelley, Yan Pillitteri, Victoria, 2017, **Ibid.,** p: 9

[44] فيلالي، أسماء، 2019، **مرجع سبق ذكره**، ص 65.

[45] Nieles, Michael, Dempsey, Kelley, Yan Pillitteri, Victoria, 2017, **Op cit.,** p:9.

المبحث الثاني: أهداف ومعايير ودورة حياة أمن المعلومات:

2-2-1 أهدافُ أمن المعلومات:

يجب أن تكونَ أهداف استراتيجية أمن المعلومات متناسبةً مع قيمة المعلومة الواجبُ حمايتها، حيثُ يهدفُ أمن المعلومات إلى:[46]

1. **ضمانِ سلامة المعلومة:** تقليصُ مخاطر ضياعِ، و تشويه، و تدمير المعطيات هو واحدٌ من أهمّ الأهداف، و من أجل تحقيقه، يجبُ أولاً العملُ على وضعِ برنامج يضمنُ حمايةَ معطيات نظام المعلومات، يتمُّ اختباره و مراجعته بانتظام بالتنسيق، و بمساعدة مستعملي نظام المعلومات بالمنظمة، وعليه فإنّ سلامةَ المعلومة يعني حمايتَها من كلّ تشويهٍ، أو تدميرٍ، أو ضياعٍ بطريقة ما.
2. **ضمانِ سرية المعطيات ذات الطابع الشخصي:** على المنظمة تفعيلُ كلّ الإجراءات الضرورية من أجل ضمان خصوصية، و سرية المعلومات الخاصة، و الحدِّ من تسريب المعلومة إلا للأشخاص المخوّلين و المصرّح لهم، هذه الإجراءاتُ ليست فقط تقنيةً، بل لكي تكونَ فعالة فهي تتطلبُ تكييفَ إجراءاتٍ عمليّة، و مشاركةَ ذوي الخبرة في هذا المجال.
3. **تثبيتِ المسؤوليات:** فمن أجلِ ضمانِ جودة المعلومة، يجب أن يكونَ هناك قدرةً على تثبيت المسؤوليات في حالةِ تشويه المعطيات، و التصرّف ضدّ أيّ شخصٍ يرفضُ تحمّلَ مسؤوليته في ما يتعلقُ بوثيقةٍ، أو أيّ غرضٍ آخر.
4. **ضمانِ الاستمرارية:** تأسيسُ برنامج استمرارية النشاط من أجل ضمان أنّه في أيّ حالٍ من الأحوال الأنشطةُ الحيويةُ للمنظمة لن تتوقف، و في حالِ توقّفِ نظام المعلومات، و هناكَ أمثلةً عديدةً عن منظمات توقّفَ فيها عمل أنظمة المعلومات لعدة أيّام بسببِ انقطاع التيار الكهربائي، أو التعّرضِ لفيروسٍ خطير، لذا يجبُ الاحتياط قبلَ وقوعِ الكارثة.

2-2-2 معايير أمن المعلومات:

نظراً لأهمية أمن المعلومات، والدور الذي يلعبُه في حماية المنظمات في بيئة الأعمال الحديثة، فقد دعا ذلك العديدَ من المنظمات، والهيئات المهنية المحلية، والعلمية إلى إصدار العديدِ من المعايير، وأطر العمل المتخصّصة في مجالِ أمن المعلومات، حيثُ توفّرُ معاييرُ أمن المعلومات ضوابطاً لتنفيذِ عمليات أمنيّة شاملة تغطي كافةَ أصول المنظمة المادية، والتكنولوجية، حيثُ تشملُ معاييرُ أمن المعلومات أربعةَ أطرٍ هي:[47]

---

[46] فيلالي، أسماء، 2019، **مرجع سبق ذكره**، 2019 ص:67

[47] Otero, Angel R., 2019, **Op Cit.**, p: 324.

1. جمعيةُ ضبط ،وتدقيق نظم المعلومات (ISACA)، والتي أصدرت إطارَ أهداف الرقابة على المعلومات و التكنولوجيا ذات الصلة (COBIT).

2. المنظمةُ الدولية للمعايير (International Organization for Standardization)، والتي أصدرت المعيار (ISO / IEC 27002).

3. المعهدُ الوطني الأمريكي للمعايير والتكنولوجيا (NIST)، والذي أصدرَ المعيارَ (NIST SP 800-53).

4. أما على الصعيد الوطني فقد أصدرت الهيئةُ الوطنية لخدمات الشبكة، السياسة الوطنية لأمن المعلومات (NANS/ISC/NISP1.0).

ويقومُ الباحث بشرحِ كلّ إطارٍ على حدى وفق الآتي:

1. إطارُ أهداف الرقابة على المعلومات و التكنولوجيا ذات الصلة (COBIT):

تمَّ إصدارُ إطار COBIT منذ عام 1996 بالتعاون ما بين جمعيةِ ضبطِ وتدقيق نظم المعلومات (ISACA)، ومعهدِ حوكمة تكنولوجيا المعلومات (ITGI) والذي انتقلَ من تدقيقِ نظم المعلومات إلى الرقابة، ثمّ إدارة تكنولوجيا المعلومات، فحوكمة تكنولوجيا المعلومات، وصولاً لعام 2012 إذ ظهرَ الإصدارُ الخامس (COBIT5) والذي شكّلَ قفزةً نوعيةً، إذ قُدّمَ كإطارٍ للحوكمة المؤسسية لتكنولوجيا المعلومات، التي عُرّفت من قبل جمعية (ISACA) بأنَّها جانبٌ من الحوكمة يضمنُ أن تعملَ المعلومات والتكنولوجيا ذات الصلة على دعمِ وتمكينِ استراتيجية المنظمة وتحقيق أهدافها، كما تشملُ الحوكمة الوظيفية لتكنولوجيا المعلومات أيّ ضمانٍ لتوفير قدرات تكنولوجيا المعلومات بشكلٍ فعال، وعليه لا يُعدُّ (COBIT5) نسخةً مُصغرة مُطوّرة عن الإصدارات السابقة، فهو يتضمنُ مفاهيمَ مختلفة، وتأكيداتٍ جديدة، وترتيباتٍ جديدة، فقد صُمّمَ ليكونَ إطاراً واحداً مُتكاملاً يُمكن استخدامه لكلٍّ من الحوكمة، والإدارة معاً، إذ استفادَ من الأطر، والمعايير، وأفضل الممارسات الموجودة قبله، مما جعلَه الإطارَ الأوسعَ، والأكثرَ تنافسيةً لتطبيقِ الحوكمةِ المؤسسية لتكنولوجيا المعلومات، وإدارتها.[48]

يساعدُ (COBIT 5) المنظمات على إنشاءِ القيمة المثلى من تكنولوجيا المعلومات من خلال الحفاظِ على التوازن بين تحقيق الفوائد، وتحسينِ مستويات إدارة المخاطر، واستخدامِ الموارد، ويمكن القول أنَّ إطارَ (COBIT 5) من الممكن أن يلائمَ جميعَ أنواع المنظمات، بما في ذلك المنظماتُ التجارية، وغير الهادفة للربح، أو حتى القطاع العام، حيثُ يوفّرُ إطار (COBIT 5) مجموعةً من معايير التحكم في تكنولوجيا المعلومات، التي لا تساعدُ فقط

[48] آقبيق، نور، 2020، **دور الضوابط الرقابية وفق إطار COBIT في الحد من مخاطر أمن نظم المعلومات المحاسبية في شركات التأمين السورية- دراسة ميدانية**، رسالة ماجستير، جامعة دمشق، سورية، ص: 52.

محترفي إدارة، وحوكمة تكنولوجيا المعلومات على إدارة عمليات تكنولوجيا المعلومات الخاصّة بهم، وإنّما تمثّلُ مرجعاً لمدققي تكنولوجيا المعلومات في مهامهم لفحص هذه الأهداف.[49]

لاحقاً تمَّ تحديثُ (COBIT 5) إلى (COBIT 2019)، حيثُ يتضمنُ الإصدارُ المطوّر رؤيةً جديدةً لحوكمة تكنولوجيا المعلومات إلا أنَّه يحافظُ على الإطار العامّ الوارد في إصدار (COBIT 5)، نوضّحُ الاختلافات الرئيسية بين (COBIT 5) و (COBIT 2019) في الجدول الآتي:[50]

الجدول (2-0): جدولُ المقارنة بين إطار (COBIT 5) وإطار (COBIT 2019).

COBIT 5	COBIT 2019
يضمُّ خمسةَ مبادئ للحوكمة	يضمُّ ستةَ مبادئ للحوكمة
يناقش 37 من العمليات ، والإجراءات التي تدعمُ أهدافَ حوكمة تكنولوجيا المعلومات.	يناقش 40 من العمليات والإجراءات التي تدعمُ أهدافَ حوكمة تكنولوجيا المعلومات.
تستخدمُ مصطلحات "إدارة" لعمليات الإدارة تستخدم مصطلحات "ضمان" لعمليات الحوكمة	تستخدم المصطلحات "المدارة" لعمليات الإدارة تستخدم المصطلحات "مضمون" لعمليات الحوكمة
لا يناقش مبادئ حوكمة تكنولوجيا المعلومات	تمت إضافةُ مبادئَ حوكمة تكنولوجيا المعلومات
يستخدم لقياس الأداء مقياس 0–5 بناءً على ISO / IEC 33000	تمَّ استخدامُ مخططاً لإدارة أداء CMMI
تمَّ تضمينُ العوامل التمكينية لحوكمة تكنولوجيا المعلومات	يتمُّ إعادة تسمية العناصر التمكينية لحوكمة تكنولوجيا المعلومات
لا تتوفرُ عواملَ محدّدةَ التصميم نظام حوكمة تكنولوجيا المعلومات	تمَّ تقديمُ 11 عاملاً من عوامل التصميم التي تؤثّرُ على تصميم نظام حوكمة تكنولوجيا المعلومات

المصدر: www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison

يقدّمُ إطارُ (COBIT 2019) إطاراً شاملاً يناقشُ مجموعةً من المبادئ، والعمليات، والإجراءات التي تساعدُ المنظمات في تحقيق أهدافها في مجالات حوكمة تقانة المعلومات، وإدارتها ، وذلك بمساعدته إياها في تحديد القيمة القصوى المستفادة من هذه التقانة، بالإضافة إلى تحديد الأساليب للمحافظة على الاتّزان بين تحقيق الفوائد ، وتقليل مستوياتِ المخاطر، والاستخدام الكفء، كما يتميزُ إطارُ (COBIT 2019) بالعمومية أي إنَّه مفيدٌ لكافةِ المنظمات، والمؤسسات بغضّ النظر عن حجمها، وصناعتها، سواءً أكانت ربحية أم غير ربحية، عامةً أم خاصة حكوميةً أم غير حكومية.[51]

---

[49] Otero, Angel R., 2019, **Op Cit.**, p: 325.

[50] www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison

[51] عوكل، محمد، 2018، **إمكانية تطبيق كوبت COBIT لتحسين أداء منظمات الأعمال السورية**، أطروحة دكتوراه، جامعة دمشق، سورية، ص:28

2. المعيار (ISO / IEC 27002: 2013) الصادر عن (International Organization for Standardization) المنظمة الدولية للمعايير، تحتَ عنوان تكنولوجيا المعلومات . التقنيات الأمنية . مدونة قواعد الممارسة لإدارة أمن المعلومات:

تمَّ إصدارُ المعيار بواسطة المنظمة الدولية للمعايير (ISO) في عام 2000 تحتَ عنوان (ISO / IEC 17799) والذي جاءَ كتعديلٍ عن المعيار (BS7799) الصادر عن المعهد البريطاني للمعايير في عام 1995، و من ثمّ تمَّ تطويرُ المعيار من قبل المنظمة الدولية للمعايير ليتمَّ إعادة إصدار نسخة جديدة منه في عام 2005 إلى جانبِ منشورٍ جديدٍ تحت عنوان (ISO / IEC 27001) وذلك لاستخدامهما معاً بحيثُ يكمل أحدهما الآخر، وبالتالي أصبحُ المعيار (ISO / IEC 27002) معياراً عالمياً يوفّرُ مجموعةً من التّوصيات لأفضل الممارساتِ المتعلقة بإدارة أمن المعلومات، حيثُ يمكنُ تطبيقُ هذا المعيار من قبل المسؤولين عن بدءٍ وتنفيذ، أو صيانةِ أنظمة إدارة أمن المعلومات، ويقدّمُ المعيار المئاتَ من الضوابط، وآليات التحكم في أمن المعلومات مثلَ: تقييمِ المخاطر، السياسةِ الأمنية لإدارة الأصول، أمنِ الموارد البشرية، الأمنِ المادي والبيئي، صلاحيةِ التحكم وصلاحيةِ الدخول، اقتناء نظم المعلومات، وتطويرها وصيانتها، إدارة حوادث أمن المعلومات، إدارة استمرارية العمل والامتثال،[52] بالإضافة إلى ذلك، يساعدُ المعيار المنظمة المعتمدة على:[53]

- تحسينِ أمن المنظمة.
- إدارةٍ، وتخطيطٍ أمنيٍّ أكثر فعاليةً.
- شراكات، وتجارة إلكترونية أكثر أماناً.
- تعزيزِ ثقة العملاء.
- عمليات تدقيق أمنية أكثر دقةً، وموثوقيةً.
- انخفاض المسؤولية.

3. المعيار (NIST SP 800-53) الصادر عن المعهد الوطني الأمريكي للمعايير والتكنولوجيا (NIST) تحت عنوان ضوابط الأمان والخصوصية لأنظمة المعلومات الفيدرالية والمنظمات:

يقومُ المعهدُ الوطنيّ الأمريكيّ للمعايير، والتكنولوجيا بإصدارِ معايير وإرشادات عديدة لمعالجة أمن المعلومات الفيدرالية على مستوى الحكومة الأمريكية، حيثُ أصدرَ في عام 1974 المعيار (FIPS 31) تحتَ عنوان "إرشادات لمعالجة البيانات التلقائية للأمن المادي، وإدارة المخاطر" قدّمَ هذا المعيارُ التوجيهَ الأوّلي للمنظمات الفيدرالية لتطوير برامج الأمن المادي، وإدارة المخاطر لعناصر نظام المعلومات، وفي أذار 2006 أصدرَ المعهدُ الوطني

[52] International Organization for Standardization, October 2013, **ISO / IEC 27002: 2013**, p: VI.
[53] Otero, Angel R., 2019, **Op Cit.**, p: 326.

الأمريكيّ للمعايير والتكنولوجيا المعيار (NIST FIPS 200) تحتَ عنوان "الحدّ الأدنى لمتطلباتِ الأمن لأنظمة المعلومات، والمعلومات الفيدرالية"، لتصدر نسخة جديدة منه في آب 2011 وهي المعيارُ: (NIST SP 800-53)، حيثُ ساعدت إرشاداتُ المعهد الوطني الأمريكي للمعايير، والتكنولوجيا (NIST) الوكالات والمنظمات الفيدرالية في تحسينِ جودة أمن تكنولوجيا المعلومات بشكلٍ كبيرٍ من خلال:[54]

- توفيرِ إطارٍ معياريّ لإدارة، وتقييم مخاطر أنظمة المعلومات في المنظمات.
- السماحِ باتخاذِ قراراتٍ تستندُ إلى المخاطر، مع ضمانِ التنفيذ الفعال من حيثُ التكلفة.
- وصفِ نهجٍ أكثر مرونةً، وديناميكيةً يمكنُ استخدامه لرصد حالة أمن المعلومات لأنظمة معلومات المنظمات.

يقدّمُ هذا المعيار مرجعاً لضوابط أمن، وخصوصية أنظمة المعلومات في المنظمات لحماية العمليات، والأصول والأفراد، والمنظمات الأخرى ذات العلاقة من التهديدات والمخاطر، بما في ذلك الهجماتُ العدائية، والأخطاءُ البشرية، والكوارثُ الطبيعية، والجهاتُ الاستخباراتية الأجنبية، ومخاطرُ الخصوصية، حيثُ يعرضُ مجموعةً من الضوابط المرنة، والقابلة للتخصيص، والتنفيذ كجزءٍ من عمليات المنظمة لإدارة المخاطر، كما يستجيبُ هذا المعيار من خلال التحديث الأخير (Revision 5) لتطورات تكنولوجيا المعلومات، وإتاحة مجموعة شاملة من تدابير الحماية لقاعدةٍ واسعة من مؤسسات القطاعين العام والخاص، التي تتبنّى مجموعاتٍ متنوعة من تلك التقنيات كأنواع منصات الحوسبة، والأنظمة الفيزيائية الإلكترونية، والأنظمة القائمة على السحابة، والأجهزة المحمولة، وأجهزة إنترنت الأشياء (IoT)، وأنظمة الفضاء، وأنظمة الاتصالات، وأنظمة التحكم البيئية، وأجهزة الكمبيوتر الفائقة، وأنظمة التحكم الصناعية، بحيثُ تشملُ تدابير الحماية هذه تنفيذَ ضوابطِ الأمن، والخصوصية لحماية العمليات والأصول الهامة ، والأساسية للمنظمات، وخصوصية الأفراد، والحدّ من الأضرار الناجمة عن الهجمات عند حدوثه، وجعل الأنظمة مرنةً ، وقابلةً للبقاء على اتصال بالإنترنت.[55]

4. السياسة الوطنية لأمن المعلومات(NANS/ISC/NISP1.0)، الصادرة عن الهيئة الوطنية لخدمات الشبكة:

تمَّ إصدارُ السياسة الوطنية لأمن المعلومات من قبلِ الهيئة الوطنية لخدماتِ الشبكة التابعة لوزارة الاتصالات والتقانة في عام 2014، حيثُ وُضِعَ الإطارُ العامّ للسّياسة الوطنيّة لأمن المعلومات بحيثُ تكونُ المرجعَ الرئيسيّ لجميعِ الجهات الحكوميّة في الجمهوريّة العربيّة السوريّة أثناءَ إعداد خطّة أمن المعلومات، وتهدفُ هذه السّياسة إلى:[56]

أ. تحديدِ المتطلّبات الأساسيّة لأمن المعلومات، وما يجبُ لحماية الأصول المعلوماتيّة في الجهات الحكوميّة.

---

[54] Otero, Angel R., 2019, **Op Cit.**, p: 328.

[55] National Institute of Standards and Technology, 2020, **NIST Special Publication 800-53 (Revision 5), Security and Privacy Controls for Information Systems and Organizations**, USA, P: xiv.

[56] الهيئة الوطنية لخدمات الشبكة، 2014، **مرجع سبق ذكره**، ص: 5.

ب. توفيرِ البيئةِ الآمنة لتقديم، وتطوير الخدمات الإلكترونيّة.

ج. تحديدِ المهامّ، والمسؤوليّات لتنفيذِ هذه السّياسة في الجهات الحكوميّة.

د. توفيرِ مرجعيّةٍ وطنيّة لكافّة النّواحي المتعلّقة بأمن المعلومات.

تقدّمُ السياساتُ الوطنية لأمن المعلومات مرجعاً وطنياً لدى الجهات الحكومية بما يضمنُ حماية المعلومات، والبيانات (المخزّنة والمنقولة) والخدمات الإلكترونية، بحيثُ تشملُ البرمجيات، والتجهيزات، وشبكات الاتصال، والأفراد وأماكن وجودها، والتي تمَّ تضمينُها في أربعة عشر مجالاً: سياسات أمن المعلومات، تنظيم أمن المعلومات، أمن الموارد البشريّة، أمن المتعاقدين، التّوعية والتّأهيل، إدارة الأصول المعلوماتيّة، الأمن الفيزيائي والبيئة المحيطة، إدارة وسائل النّفاذ، تصميم وتطوير واختبار منظومات المعلوماتيّة، التّشفير، أمن عمليّات التّشغيل، إدارة الحوادث الأمنيّة، إدارة استمراريّة العمل، الامتثال.[57]

5. مقارنةٌ بين الأطر المختلفة لأمن المعلومات الصادرة عن الهيئات ذات الصلة:

يعرضُ الجدول (2-1) الآتي مقارنةً بين المعايير المختلفة لأمن المعلومات الصادرة عن الهيئات ذات الصلة:

الجدول (2-1): جدولُ المقارنة بين المعايير المختلفة لأمن المعلومات.

	COBIT 2019	ISO / IEC 27002	NIST SP 800-53	السياسات الوطنية لأمن المعلومات
الجهة المصدرة:	جمعيةُ ضبط وتدقيق نظم المعلومات (ISACA)، ومعهد حوكمة تكنولوجيا المعلومات (ITGI)	المنظمةُ الدولية للمعايير.	المعهدُ الوطني الأمريكي للمعايير والتكنولوجيا.	الهيئةُ الوطنية لخدمات الشبكة التابعة الوزارة الاتصالات والتقانة السورية.
تاريخ اخر إصدار:	2018	2013	2020	2014
المكونات أو المجالات.	يحوي المعيار (6) مبادئَ لحوكمة تكنولوجيا المعلومات، بالإضافة إلى مناقشة (40) عنصراً من العمليات والإجراءات التي تدعمُ أهدافَ حوكمة تكنولوجيا المعلومات.	يحوي المعيار المئاتَ من الضوابط وآليات التحكم في أمن المعلومات، حيثُ تمَّ تقسيم المعيار إلى (12) فصلاً، تناولت: تقييمَ المخاطر ومعالجتها، السياسات الأمنية، تنظيمَ أمن المعلومات، إدارة الأصول، أمنَ الموارد البشرية، الأمنَ المادي	يقدّمُ هذا المعيارُ مرجعاً لضوابط أمن وخصوصية أنظمة المعلومات في المنظمات لحماية العمليات والأصول والأفراد والمنظمات الأخرى ذات العلاقة من التهديدات والمخاطر، كما يراعي معاييرَ أمن المعلومات للتقنيات الحديثة، والمتطورة.	تمّ تضمينه في أربعة عشر مجالاً: سياسات أمن المعلومات، تنظيم أمن المعلومات، أمن الموارد البشريّة، أمن المتعاقدين، التّوعية والتّأهيل، إدارة الأصول المعلوماتيّة، الأمن الفيزيائي والبيئة المحيطة، إدارة وسائل النّفاذ، تصميم وتطوير

[57] الهيئة الوطنية لخدمات الشبكة، 2014، **مرجع سبق ذكره**، ص:6.

		والبيئي، إدارةَ العمليات والاتصالات، التحكمَ في الوصول، حيازةَ وتطوير وصيانةَ أنظمة المعلومات، إدارةَ حوادث أمن المعلومات، إدارةَ استمرار العمل، الامتثالَ والتوافق.		واختبار منظومات المعلوماتيّة، التّشفير، أمن عمليّات التّشغيل، إدارة الحوادث الأمنيّة، إدارة استمراريّة العمل، الامتثال.
الجهات المعنية بالتطبيق	مفيدٌ لكافة المنظمات بغض النظر عن حجمها وصناعتها سواءً أكانت ربحيةً أم غير ربحية، عامةً أم خاصة، حكوميةً أم غير حكومية.	كافة المنظمات الحاصلة على شهادة التطبيق من المنظمة الدولية للمعايير.	لمعالجة أمن المعلومات الفيدرالية على مستوى الحكومة الأمريكية، كما يمكنُ للقطاع الخاص الاسترشاد به، في سبيل تدعيم أمن المعلومات لديها.	الجهات الحكوميّة في الجمهوريّة العربيّة السوريّة.

المصدر: من إعداد الباحث.

ويمكنُ أن نلاحظَ أنَّه على الرغم من اختلافِ الأطر السابقة من حيثُ المفاهيم الاساسية التي تمَّ بناءُ كلٍّ منها على أساسها، إلا أنَّها تتشابهُ جميعها في سعيها إلى تحقيقِ هدفٍ واضحٍ تركّزُ عليه كلّ واحدةٍ من الأطر، والمعايير السابقة وهو ضمانُ أمن المعلومات في المنظمة، وبالتالي يمكنُ القول إنّه على الإدارة العليا، ومديري أمن المعلومات في المنظمات الاطلاع بشكلٍ كافٍ وعميق على مبادئ و سياسات وإجراءات لكلّ واحدٍ من الأطر السابقة، والمزج بينها بما يحقّقُ أقصى عائداً للمنظمة بأقلّ تكاليفَ ممكنةٍ، لأنّه حتى ولو لاحظَ مسؤولو أمن المعلومات أنَّ أحدَ الأطرِ غير مناسبٍ بالمجمل ليتمَّ تبنّيه في المنظمة، إلا أنّه قد يحوي في طيّاته بعضَ الضوابطِ والإجراءات التي تتمثل في تفاصيلها الحلّ الملائم للمشاكل الأمنيّة في المنظمة.

2-2-3 دورة حياة أمن المعلومات:

على الرغمِ من أنّ أمنَ المعلومات الفعّال يتطلبُ نشرَ الأدواتِ التكنولوجية مثلَ جدرانِ الحماية، ومكافحةِ الفيروسات والتشفير، فإنَّ مشاركةَ الإدارة العليا والدعم خلالَ جميعِ مراحل دورةِ حياة الأمن أمرٌ ضروريٌّ للغاية، فتحقيقُ متطلبات أمن المعلومات في المنظمة يتطلّبُ القيامَ بخطواتٍ محدّدة و لكنّها مستمرةٌ، لأنَّ التطورات التكنولوجية في الوقت الحالي تعدُّ تطوراتٍ ديناميكية، فما إن تحقق المنظمة مستوىً معين لأمن المعلومات تجدُ نفسها أمامَ تحدياتٍ جديدةٍ تفرضُ عليها إعادةَ النظر في متطلبات أمن المعلومات، ونظراً لأنَّ تحقيقَ أمنِ المعلومات يتطلبُ دوماً اتخاذَ قراراتٍ سريعةٍ وعاجلة كانَ لا بُدَّ من مشاركةِ الإدارة العليا في صنعِ القرارات المتعلقة بأمن المعلومات، فمسألة أمن المعلومات لم تعد مسألةً تقنيةً فقط، وإنما هي واحدةٌ من وظائف وعمليات الإدارة لتتماشى مع

استراتيجيتها في الاستجابة للمخاطر، ويمكنُ عرض مراحل دورةِ حياة أمن المعلومات في مجموعةٍ من الخطوات على الشكل الآتي:

الشكل (2-1): دورة حياة أمن المعلومات.



المصدر: من إعداد الباحث.

ويمكنُ عرض الخطوات والمراحل التي تمرُّ بها دورة حياة أمن المعلومات وفق الآتي: [58]

الخطوةُ الأولى: تتمثّلُ في **تقييمِ التهديدات المتعلّقة بأمن المعلومات التي تواجهها المنظمة، وتحديد الاستجابة المناسبة:**

يمتلكُ متخصصو أمن المعلومات الخبرةَ اللازمة لتحديدِ التهديدات، وتقدير احتمالِها وتأثيرِها، ومع ذلك يجبُ على الإدارة العليا اختيار أيّ من الاستجابات الأربعة للمخاطر (تقليل، أو قبول، أو مشاركة، أو تجنب) مناسبة لاعتمادها بحيثُ تعكسُ الموارِدُ المستثمرة في أمن المعلومات نزعةَ المنظمة للمخاطر.

الخطوةُ الثانية: تتضمنُ **وضعَ سياساتٍ لأمن المعلومات وإبلاغها لجميع الموظفين:**

يجبُ أن تشاركَ الإدارةُ العليا في تطوير السياسات لأنَّ عليهم تقريرَ العقوبات التي يرغبونَ في فرضِها بسبب عدم الامتثال، بالإضافة إلى ذلك يعدُّ الدّعمُ الفعّال ومشاركةُ الإدارة العليا ضرورياً لضمان أخذِ التدريب، والتواصل في مجال أمن المعلومات على محمل الجدّ لكي تكونَ فعالة، كما يجبُ أن يتضمنَ هذا الاتصالُ أكثر من مجرد تسليمِ الأشخاص وثيقة مكتوبة، أو إرسالِ رسالةِ بريدٍ إلكتروني إليهم، ومطالبتِهم بالتّوقيع على إقرارٍ بأنَّهم تلقّوا قراءة الإشعار، بل يجبُ أن يتلقّى الموظفون رسائلَ تذكيرٍ دوريّة حولَ السياساتِ الأمنيّة، والتدريب على كيفية الالتزام بها.

[58] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David,2021, **Op cit.,** p: 337.

الخطوةُ الثالثة: من دورةِ حياةِ الأمان تتضمنُ **اقتناءَ أو إنشاءَ أدواتٍ، وحلولِ تكنولوجيا المعلومات:**
يجب أن تسمحَ الإدارة العليا باستثمارِ الموارِدِ اللازمة للتخفيفِ من التّهديدات المحدّدة، وتحقيقِ المستوى المطلوب من الأمن.

الخطوةُ الرابعة: في دورةِ حياة الأمن **مراقبة الأداء بانتظام لتقييمِ فعالية برنامج أمن معلومات المنظمة:**
يخلقُ التقدّم في تكنولوجيا المعلومات تهديداتٍ جديدة، ويغيرُ المخاطر المرتبطة بالتهديدات القديمة، لذلك يجبُ على الإدارة إعادةَ تقييمِ الاستجابة للمخاطر في المنظمة بشكلٍ دوريّ، وعندَ الضرورةِ يجبُ إجراءُ تغييراتٍ على سياسات أمن المعلومات، والاستثمار في حلولٍ جديدة لضمانِ دعمِ جهود أمن المعلومات الخاصّة بالمنظمة لاستراتيجية أعمالها بطريقةٍ تتّسق مع إدارة المخاطر.

وبنظرةٍ تحليليّةٍ للخطوات الأربعة لدورة حياة أمن المعلومات، نلاحظُ الآتي:

1. تمثّلُ الخطوةُ الأولى، والمتعلّقة بتقييمِ التهديدات، والاستجابة لها، عمليةً مستمرةً، نتيجة لتبدل المخاطر مع مرور الزمن، وبالتالي على المنظمة تحديد التهديدات في الوقت المناسب، والاستجابة لها مع أخذ عامل التكلفة بعين الاعتبار.
2. تعدُّ أفعالُ وممارسات الإدارة العليا أفضلَ دليلاً للموظفين في تبنّي إجراءاتٍ سليمة لضمان أمن المعلومات في المنظمة.
3. يجب أن تقتني أو تنشئ المنظمة معداتٍ، ومنظومات كأجهزة جدران الحماية، وأنظمة كشف التسلل، وغيرها من العتاد الفنّي والتقني التي تمثّلُ الأصولَ الهامة لحماية باقي أصول المنظمة، وضمانِ استمرارية أعمالها.
4. إنَّ أمنَ المعلومات عمليةٌ مستمرةٌ، لا تتوقف عن التجديد، والتطور لمواكبة التطورات التكنولوجية، بل يجبُ تقييم مدى كفايةِ، والتزام المستويات الإدارية والتنفيذية بالإجراءات والسياسات الموضوعة مسبقاً، وتبنّي الحلولَ الحديثة لمشكلات، وتهديدات أمن المعلومات.

المبحث الثالث: تهديداتُ أمن المعلومات، والمخاطر المرتبطة بها:

2-3-1 تعريف تهديدات أمن المعلومات:

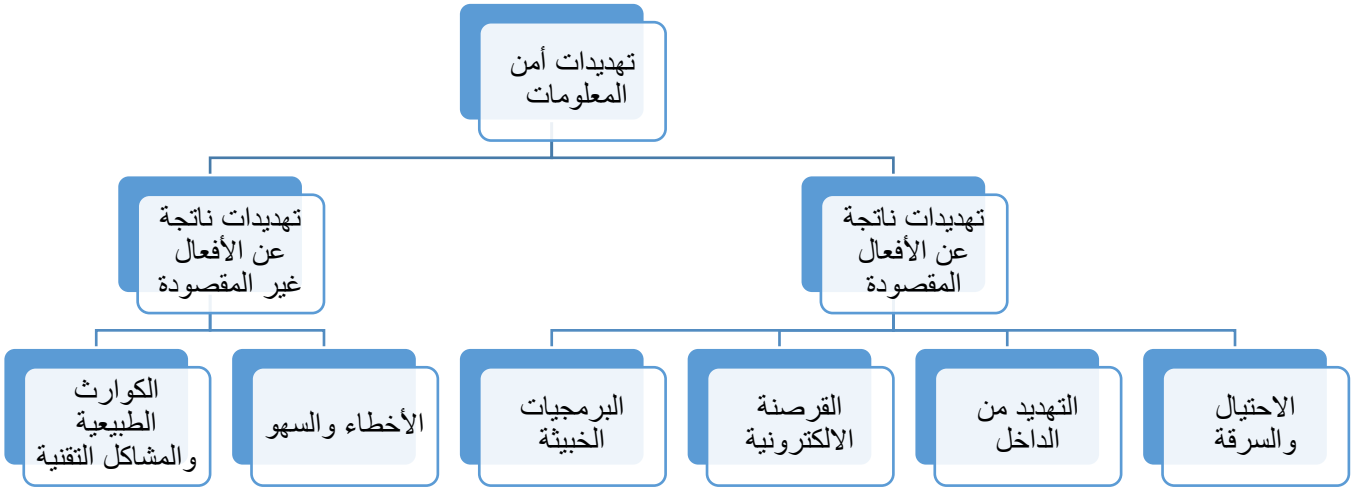
يمكنُ تعريفُ التهديدات على أنَّها: "أيّ طرفٍ، أو حدثٍ، أو فعلٍ يمكن أن يسبّبَ ضرراً على المعلومات من خلال تدمير، أو كشف، و تعديلٍ أو رفضِ خدمات، أو أجزاء الأنظمة المعلوماتية".[59]

يتمُّ استخدامُ مصطلحَ (التهديد) للتركيز على تحديد السيناريوهات غير المتوقعة، أو غير المرغوب فيها، وتحليلها، والتي في حال حدوثها فمن شأنِها أن تسبّبَ ضرراً للمنظمة، مما يعني أنَّه إذا كانَ هناك سيناريو محتمل للتهديد،

[59] الهيئة الوطنية لخدمات الشبكة، 2014، **اللوائح التنظيمية الخاصة بالسياسة الوطنية لأمن المعلومات**، وزارة الاتصالات ، سوريا، ص: 5.

فنحن بحاجة إلى إجراء تحليل للمخاطر وتقييمها وعلاجها، وقد يكونُ التهديدُ ناتجاً عن أفعالٍ مقصودةٍ، أو غير مقصودة، وأحداثٍ لا يمكن التحكم بها كالكوارث الطبيعية،[60] والتي يمكنُ عرضها في الشكل الآتي:

الشكل (2-2): تهديدات أمن المعلومات.



المصدر: من إعداد الباحث.

ويمكنُ عرض أنواع التهديدات بشيءٍ من التفصيل وفق الآتي:

1. **التهديدات الناتجة عن الأفعال المقصودة:**

أ. الاحتيالُ، والسرقة: يمكنُ استغلال الأنظمة في عمليات الاحتيال، والسرقة عن طريق "أتمتة" الطرقِ التقليدية للاحتيال، أو باستخدامِ طرقٍ جديدةٍ، وقد يرتكبُ الاحتيالُ، والسرقة من قبل المطلعين (أي المستخدمين المصرّح لهم بالدخول إلى النظام) ،أو أطرافٍ خارجية، فمن الممكن أن يكونَ مسؤولي النظام المعتمدين، والمستخدمين الذين لديهم إمكانية الوصول إلى النظام والإلمام به هم المسؤولون عن عمليات الاحتيال، كما يشكّلُ الموظفون السابقون في المنظمة أيضاً تهديداً نظراً لمعرفتهم بعمليات المنظمة، خاصةً إذا لم يتم إنهاء وصولهم على الفور[61]، هناك العديد من التقنيات التي يمكن استخدامها للقيام بعمليات الاحتيال، بعض هذه التقنيات تشمل:

- **وسائل التواصل الاجتماعي:** سمحَ الانتشارُ الواسع لوسائل التواصل الاجتماعي لمجرمي الإنترنت باستغلال المنصة لشنّ هجماتٍ باستخدام حساباتِ وسائط اجتماعية سهلة الصنع، ومزيفة وغير مؤكدة، حيثُ يمكنُ لمجرمي الإنترنت انتحالَ صفة زملاء العمل، أو ممثلي خدمة العملاء أو غيرهم من الأفراد الموثوق بهم لإرسال

[60] Chopra, Abhishek, Chaudhary, Mukund, 2020, **Op cit.**, p: 79.
[61] Chopra, Abhishek, Chaudhary, Mukund, 2020, **Op cit.**, p: 80.

روابطَ برامج ضارةٍ تسرقُ معلوماتٍ مؤسسية شخصية، أو حسّاسة، وبالتالي تعملُ وسائلُ التواصل الاجتماعي على تفاقمِ مشكلة الاحتيال، ويجبُ على المنظمات أن ترى أنّها مصدرُ قلقٍ خطيرٍ عندَ تنفيذِ الأنظمة. [62]

- **هندسة اجتماعية:** الهندسةُ الاجتماعية هي تقنيةٌ تعتمدُ بشكلٍ كبيرٍ على التفاعلِ البشري للتأثير على الفرد لخرق بروتوكول الأمن العادي الخاص به، وتشجعُ الفرد على إفشاء المعلومات السرية، عادةً ما يتمُّ ارتكابَ هذه الأنواع من الهجمات عبر الهاتف، إلا أنَّ الهجمات التي تُرتكب عبر الهاتف هي أبسطُ هجمات الهندسة الاجتماعية التي يتم ارتكابها، كما يمكن أيضًا تنفيذَ هجمات الهندسة الاجتماعية عبر الإنترنت.[63]

ب. تهديد الاضطراب والأذى: يمكن أن يمثّلَ الموظفون تهديداً داخلياً لمنظمةٍ ما نظراً لمعرفتهم بأنظمة صاحب العمل، وتطبيقاته، بالإضافة إلى الإجراءات التي قد تسبّبُ الضررَ، أو الأذى، أو الاضطراب، حيثُ يُعدُّ تخريب الموظف – الذي يتمّ تحريضه غالباً عن طريق التهديد بالفصل مثلاً – قضيةً مهمةً للمنظمات وأنظمتها، في محاولةٍ للتخفيفِ من الضّرر المحتمل النّاجم عن تخريب الموظف، يجبُ تعطيلَ وصول الموظف المفصول حديثاً إلى البنية التحتية لتكنولوجيا المعلومات على الفور، ويجبُ مرافقةَ الفرد خارجَ مباني الشركة، تتضمنُ أمثلةُ تخريب الموظف المرتبط بالنظام ما يلي:[64]

- إتلافَ الأجهزة، أو المرافق.
- زرعَ القنابل المنطقية التي تدمّر البرامج أو البيانات.
- إدخالَ البيانات بشكلٍ غير صحيح، أو الاحتفاظ بها، أو حذفها.
- تعطيلَ النظام.

ج. القرصنة الالكترونية: المتسلّلُ الضّار هو مصطلحٌ يستخدم لوصفِ فردٍ، أو مجموعة ممن يستخدمونَ فهماً متقدماً للأنظمة، والشبكات، والبرمجة للوصول إلى الأنظمةِ بطريقةٍ غير مشروعة، أو التسبّب في تلفِ، أو سرقةِ المعلومات، يمكن أن يساعدَ فهمُ الدافع الذي يدفعُ المتسلّل الضّار المنظمة على تنفيذِ ضوابط الأمن المناسبة لمنعِ احتمالية اختراقِ النظام، يمثّلُ المتسلّلُ الضّار فئةً واسعةً من التهديدات المقصودة التي يمكنُ تقسيمها إلى فئاتٍ أصغر اعتماداً على الإجراءاتِ المحدّدة، أو نيّة المتسلّل الضار وفقاً لما يلي: [65]

- **المهاجمون:** يقتحمُ المهاجمون الشبكات من أجلِ الإثارة، والتّحدي أو من أجلِ المفاخرة في مجتمع المهاجمين، إنَّ القرصنةَ عن بُعد كانت تتطلّبُ في السابق مهاراتٍ كبيرة، أو معرفة بالكمبيوتر، إلا أنّه يمكنُ للمهاجمين الآن تنزيلَ البرامج النّصية، والبروتوكولات للهجوم من الإنترنت، وإطلاقِها ضدَّ مواقع الضحايا، حيثُ أصبحت أدوات الهجوم هذه أكثرَ تعقيداً، وأسهل في الاستخدام، وبالتالي لا يمتلكُ العديدُ من المهاجمين الخبرةَ المطلوبة

---

[62] Nieles, Michael, Dempsey, Kelley, Yan Pillitteri, Victoria, 2017, **Op cit.,** p: 21.

[63] الشوابكة، عدنان، 2019، **مرجع سبق ذكره**، ص: 170.

[64] Chopra, Abhishek, Chaudhary, Mukund, 2020, **Op cit.**, p: 117.

[65] Nieles, Michael, Dempsey, Kelley, Yan Pillitteri, Victoria, 2017, **Op cit.,** p: 23.

لتحديدِ الأهداف الصعبة مثل الشبكاتِ الحكومية الحساسة، ومع ذلك فإنَّ عددَ المهاجمين في جميعِ أنحاء العالم يشكّلون تهديداً مرتفعًا نسبيًا بحدوثِ اضطراباتٍ يمكن أن تسبّبَ أضراراً جسيمة للأعمال التجارية، أو البنية التحتية.

- **الجماعات الإجرامية:** تسعى الجماعاتُ الإجرامية إلى مهاجمة الأنظمة لتحقيق مكاسب مالية، حيثُ تستخدم مجموعات الجريمة المنظمة البريدَ العشوائي والتصيدَ الاحتيالي، وبرامجَ التجسس، و البرامجَ الضّارة لارتكاب سرقة الهوية والاحتيال عبر الإنترنت، وقد تحاولُ بعض الجماعات الإجرامية ابتزازَ الأموال من منظمة عن طريقِ التهديد بشنِّ هجومٍ إلكتروني.[66]

د. البرمجيات الخبيثة: تشيرُ البرمجيات الخبيثة إلى الفيروسات، والديدان، وأحصنة طروادة، والقنابل المنطقية، وأيّ برامج أخرى يمكنُ استخدامها لمهاجمة أحد الأنظمة الأساسية، وهي الآتي:

- **الفيروسات:** هي عبارةٌ عن جزء من التعليمات البرمجية القابلة للتنفيذ ذاتياً، والتي تربطُ نفسها بملفٍ، أو برنامج ما، وخلالَ عملية تنصيب البرنامج على الحاسب، ينتقلُ الفيروس إلى الحاسب حيثُ تقومُ الفيروسات بتدمير البيانات، أو البرامج، أو تغييرِها، أو التحكم في الحاسب، أو إعادةِ تسمية الملفات، أو الدلائل، أو إعادة تهيئة القرص الصلب، أو تغيير محتوى الملفات، أو منع المستخدمين من تشغيل النظام، أو الوصولِ إلى البيانات على القرص الصلب، كما يمكنُ للفيروس اعتراضَ عمليات الإرسال، وتغييرها، أو عرض الصور، أو الرسائل المُعَطّلة، أو التسبّب في تغيير لون الشاشة، أو اختفائها، كما تقومُ العديدُ من الفيروسات تلقائيًا بإرسال رسائلَ البريد الإلكتروني، أو الفاكسات، أو الرسائل النصية مع اسم الضحية كمصدرٍ لإرسال تلك الرسائل.[67]
- **الديدان:** وهي عبارةٌ عن برامج مستقلة تنتقلُ من حاسب لآخر داخلَ الشبكة دونَ الحاجة لتدخلاتٍ بشرية، وتنتشرُ بسرعةٍ أكبر من الفيروسات، ويمكنُ للديدان أن تخفي بعضَ المعلومات، أو البرامج، وإتلافها، وعلى عكسِ الفيروسات، فهي قادرةٌ على نسخِ نفسها بدون تدخلاتٍ داخلية، أو خارجية، إذ إنَّها لا تحتاجُ إلى تحميل ملفٍ، أو إرسال بريدٍ الكتروني من أجل نشرها، فهي قادرةٌ على العيش منفصلةً عن أصلها، وتبقى على اتصال معه.[68]

وبالتالي يمكنُ التمييز بين الفيروسات، والديدان من خلال مجموعةٍ من الصفات منها:[69]

- الفيروسُ عبارةٌ عن جزءٍ من الشفرة مخبأة في برنامج مضيف، أو ملفٍ قابلٍ للتنفيذ، أو مرفقٍ به، في حين أنَّ الدودةَ عبارةٌ عن برنامجٍ مستقلّ.

---

[66] Chopra, Abhishek, Chaudhary, Mukund, 2020, **Op cit.**, p: 117.

[67] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p: 275.

[68] فيلالي، أسماء، 2019، **مرجع سبق ذكره**، ص: 92

[69] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p: 275.

- تطلبُ الفيروس من الإنسان فعلَ شيءٍ (تشغيل برنامج، فتح ملف، وما إلى ذلك) لتكرارِ نفسه، في حين أنَّ الدودةَ لا تحتاجُ إلى فعل شيءٍ خارجيّ حتى يتمّ تنفيذها، وتسعى بنشاطٍ إلى إرسال نسخٍ من نفسها إلى أجهزة الشبكة الأخرى.
- وعادةً لا تعيشُ الدودةُ لفترةٍ طويلة، لكنّها مدمرةٌ أثناءَ وجودِها، يستغرقُ القليلَ من المعرفةِ التقنية لإنشاءِ دودة ، أو فيروس، وتوفّر العديدُ من مواقع الويب تطبيقات تمكّن المستخدمين من إنشاء ديدان.

- **حصان طروادة:** برنامجٌ حاسوبيّ ظاهرُه بريءٌ، ومفيد، لكنه يضمر جزءاً ماكراً يتمثّلُ في أعمالٍ خبيثةٍ، ومضرّة، ينشطُ هذا الجزء بمجردِ تشغيل البرنامج، فيقوم بالسيطرة على الجهاز أو إتلافه، أو التجسس عليه، وجمع ما يمكن من معلوماتٍ سرية، أو شنّ هجماتٍ على حواسيب أخرى من خلال الحاسب المسيطر عليه. [70]

2. التهديدات الناتجة عن الأفعال غير المقصودة:

أ. الأخطاء والسهو: يمكن أن تحدثَ الأخطاء والسهو عن غير قصدٍ بسببِ مشغلي النّظام الذين يعالجونَ مئات المعاملات يومياً أو عن طريق المستخدمين الذين يقومون بإنشاءِ وتحريرِ البيانات على الأنظمة الفرعية، حيثُ يمكن أن تؤدّي هذه الأخطاء، والسّهو إلى تدهورِ البيانات، وتكامل النظام، بغضّ النّظر عن مستوى الخطأ، فإنّه يقعُ على عاتقِ المنظمة مسؤوليةَ إنشاءِ برنامج توعيةٍ، وتدريبٍ سليم، لتقليلِ عدد الأخطاء والسهو.[71]

ب. فقدان الدعم المادي والبنية التحتية نتيجة الكوارث الطبيعية والمشاكل التقنية: تشملُ خسارةُ البنية التحتية الداعمة انقطاعَ التيار الكهربائي، وفقدانَ الاتصالات، وانقطاعَ المياه والتسربات، وأعطالَ الصرف الصحي، وتعطّل خدمات النقل، والحرائق، والفيضانات، والاضطرابات المدنية، وغالبًا ما يؤدّي فقدان البنية التحتية إلى تعطّلِ النّظام بطرقٍ غير متوقعة.[72]

2-3-2 المخاطر المرتبطة بتهديدات أمن المعلومات:

تعدُّ مخاطرُ أمنِ المعلومات أحدَ مكوناتِ المخاطرِ الشاملة للمنظمة، وعليه فإنَّ مخاطرَ أمن المعلومات حسبَ جمعيةِ ضبطِ، وتدقيق نظم المعلومات (ISACA) هي مخاطرُ استخدام، وتملّك، وتشغيل، وتبنّي تكنولوجيا المعلومات، فهي احتماليةُ وقوعِ حدثٍ ما نتيجة خطأ أمنيّ، يمكن أن يؤثّرَ سلباً في السّلامة، والسّرية، والإتاحة للمعلومات أو النظام، أو يسبّب خسارةً للمالك، أو مستخدم المعلومات، أو النظام.[73]

ويعتمدُ تقييمُ المخاطر المرتبطة بأمن المعلومات على تحديدِ التهديدات التي تتعلّقُ بأمنِ المعلومات في منظمة، ممّا يعني أنَّه إذا كانَ هناك سيناريوهات محتملة للتهديدات، فإنّنا بحاجةٍ إلى إجراءِ تحليلٍ للمخاطرِ، وتقييمها

---

[70] الشوابكة، عدنان، 2019، **مرجع سبق ذكره**، ص: 170.

[71] Chopra, Abhishek, Chaudhary, Mukund, 2020, **Op cit.**, p: 80.

[72] فيلالي، أسماء، 2019، **مرجع سبق ذكره**، ص: 77

[73] آقبيق، نور، 2020، **مرجع سبق ذكره**، ص: 40.

وعلاجها، حيثُ يؤدّي كلّ نوعٍ من التهديدات إلى حدوثِ خطرٍ معينٍ، ومشاكل خاصّةٍ ترتبكُ بذلك التهديد، ومن الأمثلةِ على تلك المخاطر المرتبطة بتهديدات أمن المعلومات:[74]

- تعطّلُ الأصول التكنولوجية أو اتلافها.
- إحداثُ تغييراتٍ غير مصرّح بها في قواعد بيانات المنظمة، والأصول التكنولوجية المرتبطة بها.
- سرقةُ الأصول التكنولوجية، أو السيطرة عليها.
- الكشفُ عن الأصولِ التكنولوجية لأشخاصٍ غير مصرّح لهم بالوصول إليها.
- انقطاعُ خدماتِ تكنولوجية المعلومات.

كما يمكنُ للباحث إضافةَ مجموعةٍ أخرى من المخاطرِ في ضوء التهديدات التي تمَّ عرضها:

- تعرّضُ المنظمةِ للابتزازِ نتيجة سرقةِ معلوماتٍ هامة، وسرّية.
- تخريبُ البنية التحتيّة لنظام المعلومات من قبل الموظفين الساخطين.
- فقدانُ موثوقية البياناتِ نتيجة التغييرِ غير المصرّح به من قبل بعضِ الأطراف الداخلية، أو الخارجية.
- توقّفُ المنظمة عن العمل بشكلٍ جزئيّ، أو مؤقت للتعافي من الهجمات الحقيقية، وحوادث أمن المعلومات.
- الملاحقةُ القضائية للمنظمة من الأفراد المتضررين نتيجة سرقةِ، أو كشفِ معلوماتٍ سريّةٍ لدى المنظمة.

مما سبقَ، يمكنُ تلخيص التهديدات المختلفة لأمن المعلومات، والمخاطر المرتبطة بها، وسبل تجنبها من خلال الجدول (2–2) الآتي:

[74] Chopra, Abhishek, Chaudhary, Mukund, 2020, **Op cit.**, p: 79.

الجدول (2-2): تهديدات أمن المعلومات والمخاطر المرتبطة بها وطرق تجنبها.

التهديدات:	أنواع التهديدات:	الخطر المرتبط بها:	كيفية تجنبها:
التهديدات الناتجة عن الأفعال مقصودة:	الاحتيالُ والسرقة.	كشفُ معلومات سرية، وحساسة.	. وضعُ ضوابط تضمن التحكم بالنفاذ إلى النظام.
	التهديدُ من الداخل.	تخريبُ البنية التحتية لتكنولوجيا المعلومات.	. وضعُ ضوابط للتحكم بصلاحيات المستخدمين، وتحديد الاشخاص المخولين بالنفاذ إلى الأنظمة
	القرصنةُ الالكترونية.	تلفُ، أو سرقة المعلومات، وتعرّضُ المنظمة للابتزاز.	. يجبُ أن تكونَ التطبيقات وقواعد البيانات محميةً بشكلٍ كبيرٍ، وأن تكونَ مفصولة بأكثرِ من مستوى حماية عن شبكة الانترنت.
	البرمجياتُ الخبيثة.	تدميرٌ، أو تغييرٌ في البنية التحتية لتكنولوجيا المعلومات	. الفحصُ اليومي للخدمات ضدَّ جميعِ أنواعِ البرمجيات الخبيثة، والتأكّد من إزالتِها بالكاملِ في حال وجودها.
التهديدات الناتجة عن الأفعال غير المقصودة:	الأخطاء، والسهو.	تدهورُ البيانات، وتكاملُ النظام.	. إنشاءُ برامجَ توعويّة، وتدريبٌ مستمر للعنصر البشري، لضمان الامتثال لقواعد، ومتطلبات أمن المعلومات.
	الكوارثُ الطبيعية ، والمشاكل التقنية	فقدانُ البنية التحتية لتكنولوجيا المعلومات، وتعطّل النظام.	. استخدامُ وحدات عدمِ انقطاع التيار الكهربائي للحواسب، وتجهيزات الشبكة. . توفيرُ تجهيزاتٍ خاصّة بالنسخ الاحتياطي، ومساحاتٍ تخزينية كبيرة ، وبرمجياتٍ خاصة، واستعادة النسخ في حالِ الحاجة.

المصدر: من إعداد الباحث.

المبحث الرابع: مفهوم وأنواع ضوابط أمن المعلومات:

إنَّ التهديدات التي تحيطُ بالمنظمة، ونظامِها المعلوماتي تحتّم على المنظمة تبنّي مجموعةً من المعاييرِ، والضوابط والسياسات التي تكفلُ حمايةَ أمن المعلومات، حيثُ يمكنُ أن تصنّفَ الضوابطُ المختلفة لأمنِ المعلومات على ثلاث مراحل مختلفة، ومتكاملة، أولها الضوابطُ الوقائية، والتي تكفلُ حمايةَ المعلومات من أن تكونَ عرضةً للمخاطر، والتهديدات في بيئةِ عملِ المنظّمة، أما في حال وقوعِ نظام المعلومات تحتَ تأثيرِ تهديدٍ فعليّ، فيجب أن تكفلَ الضوابطُ الاستكشافية تحديدَ ذلك التهديد، والتصدي له في الوقت المناسب، أما الضوابطُ التصحيحيّة فتمثّلُ الخيارَ الأخيرَ لاستعادةِ الوضع الطبيعي في حال التأكّدِ من وقوعِ ضررٍ نتيجة تهديدٍ ما، يمكنُ توضيح الأصناف الثلاث لضوابطِ أمن المعلومات، وفقاً للآتي:

2-4-1 الضوابط الوقائية لأمن المعلومات:

إنَّ الوقايةَ هي خطُّ الدفاع الأول في الهيكلية الرقابية، فهي الإجراءاتُ المُصمّمة للحدّ من تكرار وقوع الأحداث غير المرغوب فيها، حيثُ تفرضُ الضوابطُ الوقائية الامتثالَ للإجراءات المحدّدة، أو المطلوبة لمنع الغشّ، والأخطاء لأنَّ ذلكَ من الممكن أن يكونَ أكثرَ فعاليةً من حيثُ التكلفة من كشفِ، وتصحيحِ المشاكل بعدَ وقوعها، ولكن مع ذلك تبقى بعضُ الأحداث لا يمكن منعُها أو الوقاية منها والتي تخترقُ هذا المستوى من الضوابط.[75]

تجدرُ الإشارةُ إلى أنَّ الضوابطَ الوقائيّة يجب أن تراعي المكونات الأساسيّة لنظام المعلومات، من **الأشخاص** المشغّلين لنظام المعلومات، ثمَّ **العمليات** التي تحكم إجراءات عمل نظام المعلومات، وصولاً **للتكنولوجيا المعلومات** التي يتبنّاها نظامُ المعلومات ويدارُ من خلالها.

1. **الأشخاص:** إنَّ إدارةَ المنظمة مسؤولةٌ عن التأكّد من أنَّ المديرين والمستخدمين لنظام المعلومات على درايةٍ بالمخاطر الأمنية المرتبطة بأنشطتهم، وأنَّ الموظفينَ مدربون تدريباً كافياً لتنفيذِ واجباتهم، ومسؤولياتهم المتعلقة بأمن المعلومات، وبالتالي يمكن أن تتفرعَ الضوابطُ المتعلقة بالأفراد العاملين في المنظمة إلى ضابطينِ أساسيين:[76]

أ. **خلقُ ثقافةٍ واعية بأمن المعلومات:** يجبُ على المنظمةِ التخطيطَ لنشرِ الوعي الأمني، وإجرائِه على كافة المستوى التنظيمي، ذلك لأنَّه عندما يتمّ تنفيذ ضوابط أمنيةٍ محدّدة، فإنَّه سيساعدُ الموظفينَ على فهمِ ما يتمّ تنفيذه من ضوابط، بالإضافة إلى سبب تنفيذِها وما هي الفوائدُ المرتبطةُ بها.

---

[75] آقبيق، نور، 2020، **مرجع سبق ذكره**، ص: 36.

[76] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p: 338.

غالباً ما تقومُ معظمُ المنظمات بتثقيفِ أعضاء فريق أمن المعلومات حولَ تطبيقِ الأمن فقط، ولا تصلُ أبداً إلى جميع الموظفين، ولكن من المهمّ أن ندركَ أنَّ كافةَ الموظفين يجب أن يكونوا على درايةٍ بأهميةِ حمايةِ المعلومات، وأنّهم أحياناً هم الذين يتسببونَ عن غير قصدٍ في حدوث انتهاكاتٍ أمنية.[77]

لإنشاءِ ثقافةٍ واعيةٍ بأمن المعلومات يلتزمُ فيها الموظفون بالسياسات التنظيمية، يجب ألا تقومَ الإدارةُ العليا بإبلاغ سياساتِ أمن المعلومات فحسب، بل يجبُ أيضاً أن تكونَ مثالاً يحتذى به، فمن الأرجح أن يمتثلَ الموظفون لسياسات أمن المعلومات، فعندما يرونَ أنَّ مديريهم يقومون بذلك، وعلى العكس إذا لاحظَ الموظفون أنَّ المديرين ينتهكونَ سياسة أمن المعلومات، على سبيل المثال عن طريقِ كتابة كلمة مرور، ولصقِها على الجهاز، فمن المحتمل أن يقلّدوا هذا السلوك.[78]

ب. التدريب: يتمّ التعرّف على مجتمع المستخدمين على أنّه الحلقةُ الأضعفُ في تأمين الأنظمة، وبالتالي يساعدُ توعية مستخدمي النظام بمسؤولياتهم الأمنية، وتعليمهم الممارسات الصحيحة على تغيير سلوكهم، كما أنّه يدعمُ المساءلةَ الفردية، والتي تعدُّ من أهمّ الطرقِ لتحسينِ أمن المعلومات، فبدون معرفةِ التدابير الأمنية اللازمة، أو كيفية استخدامها، لا يمكن للمستخدمين أن يكونوا مسؤولين حقاً عن أفعالهم.

الغرضُ من الوعي، والتدريب، والتعليم بأمن المعلومات هو تعزيزُ الأمن من خلال:[79]

- زيادة الوعي بالحاجة إلى حماية موارد النظام.
- تطوير المهارات، والمعرفة حتى يتمكّن مستخدمو النظام من أداءِ وظائفهم بشكلٍ أكثر أمناً.
- بناء معرفةٍ متعمقة حسبَ الحاجةِ لتصميمِ برامج أمنية، أو تنفيذها ،أو تشغيلها للمنظمات، والأنظمة.

يجبُ الإشارة إلى أنَّ التدريبَ على الوعي الأمنيّ مهمٌّ لكافةِ المستوياتِ الإدارية، والتنظيمية، من الإدارة العليا إلى المتوسطة، والدنيا، كما أنَّ تدريبَ مهنيي أمنِ المعلومات مهمٌّ أيضاً، فالتطوراتُ الجديدةُ في التكنولوجيا تخلقُ باستمرار تهديداتٍ أمنيةٍ جديدةٍ، وتجعلُ الحلولَ القديمة غير مناسبةٍ، لذلك من المهمّ للمنظمات دعم التعليم المهنيّ المستمرّ للمتخصّصين في مجالِ الأمن.

2. العمليات والإجراءات: تعدُّ العمليات، والإجراءات التي تحكمُ عملَ نظام المعلومات من أهمّ الضوابط التي تضمنُ مستوىً عالٍ لأمن المعلومات، وتتمثّلُ هذه العمليات في:

أ. ضوابط وصول المستخدم: تختلفُ متطلبات الاستخدام في الأنظمة متعدّدة المستخدمين، فعلى سبيلِ المثال يجب أن تكونَ بعض المعلومات في متناولِ جميعِ المستخدمين، وقد تكونُ بعض الأقسام فقط هي من يحتاجُ معلوماتٍ أخرى، وبالتالي يجبُ أن يكونَ لدى المستخدمين حقَّ الوصولِ إلى معلوماتٍ محدّدةٍ مطلوبة لأداء

---

[77] Chopra, Abhishek, Chaudhary, Mukund, 2020, **Op cit.**, p: 103.
[78] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p: 339.
[79] Nieles, Michael, Dempsey, Kelley, Yan Pillitteri, Victoria, 2017, **Op cit.,** p: 59.

وظائفهم، كما أنَّه من المهمّ أيضاً التحكّم في نوعِ الوصولِ المسموح به (على سبيل المثال: قدرةُ المستخدم العادي على تنفيذِ برامج النظام، وليسَ تغييرها)، تعملُ هذه الأنواع من قيود الوصول على فرض السياسة وتساعدُ على ضمانِ عدمِ اتّخاذ إجراءاتٍ غير مصرّحٍ بها.[80]

وتنطوي ضوابط وصول المستخدمين على استخدام نوعينِ متّصلين، ولكن متميّزين من عناصر التحكم في وصول المستخدم، وهي الآتية:

- **ضوابط المصادقة:** تعرف المصادقة على أنّها إجراءٌ تقنيٌّ يمنعُ الأفرادَ أو الاجهزة غير المصرّح لهم من دخول النظام[81]، الهدفُ الأساسيُّ لعملياتِ المصادقة هو التأكّدُ من أنّ المستخدمين الشرعيين فقط يمكنُهم الوصول إلى النظام، ويمكنُ استخدام ثلاثة أنواع من بياناتِ الاعتماد للتحقّق من هوية الشخص:
  - شيءٌ يعرفه الشخص، مثل كلماتِ المرور، أو أرقامِ التعريف الشخصية.
  - شيءٌ لدى الشخص، مثل البطاقاتِ الذكية، أو شارات الهوية.
  - بعضُ الخصائص الفيزيائية، أو السلوكية (يشارُ إليها باسم **المعرف الحيوي**) للشخص، مثل بصماتِ الأصابع، أو أنماط الكتابة.

على الرغم من أنَّ بيانات اعتماد المصادقة الأساسيةّ الثلاثة بحد ذاتها غير مضمونةٍ، فإنَّ استخدامَ نوعين أو ثلاثة أنواع معاً (وهي عمليةٌ يشارُ إليها باسم المصادقة متعدّدة العوامل) تعتبرُ فعالةً للغاية.

تجدرُ الإشارةُ إلى أنَّ عمليةَ المصادقةِ مهمةٌ ليسَ فقط للتعرّف على الأشخاص، ولكن أيضاً كلّ جهازٍ يحاولُ الاتّصال بالشبكة، حيثُ تحتاجُ كلّ محطةِ عملٍ، أو طابعة، أو أيّ جهاز كمبيوتر آخر إلى بطاقة دخول الشبكة (NIC) للاتّصال بالشبكة الداخلية للمنظمة، حيثُ يتميزُ كلّ جهازٍ بمعرّف فريد، يشارُ إليه باسم عنوان التحكم بالوصولِ الى الوسائط (MAC)، لذلكَ يمكنُ للمنظّمة تقييد الوصول إلى الشّبكة على الأجهزةِ المملوكة للشركة فقط من خلال مقارنة MAC للجهاز بقائمةٍ من عناوين MAC المعترّف بها، ومع ذلك يوجدُ برنامجٍ يمكنُ استخدامه لتغييرِ عنوان MAC الخاصّ بجهازٍ ما، ممّا يتيحُ للمستخدمين الخبثاء من "انتحال" هويةِ الجهاز، لذلك تتضمنُ الطريقة الأقوى لمصادقةِ الأجهزة استخدام الشهاداتِ الرقمية التي تستخدمُ تقنياتِ التشفير، لتعيين معرّفات فريدة لكلّ جهاز.[82]

- **ضوابط التفويض:** يعرّف التفويضُ على أنّه عمليةُ تقييدِ، ووصولِ المستخدمين المصادق عليهم إلى أجزاءٍ محدّدةٍ من النظام، والحدّ من الإجراءاتِ المسموح لهم بتنفيذها.[83]

---

[80] Nieles, Michael, Dempsey, Kelley, Yan Pillitteri, Victoria, 2017, **Ibid.,** p: 59.
[81] Nieles, Michael, Dempsey, Kelley, Yan Pillitteri, Victoria, 2017, **Ibid.,** p: 62.
[82] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p: 345.
[83] Nieles, Michael, Dempsey, Kelley, Yan Pillitteri, Victoria, 2017, **Op cit.,** p: 38.

غالباً ما يتمّ تطبيق عناصر التحكم في التفويض عن طريقِ إنشاءِ مصفوفة تحكم في الوصول، فعندما يحاولُ الموظفُ المصادق عليه الوصولَ إلى موردِ أنظمة معلوماتٍ معيّن، يقومُ النظامُ بإجراءِ اختبار توافق يطابقُ بيانات اعتماد المصادقة للمستخدم مع مصفوفةِ التحكم في الوصول، لتحديد ما إذا كانَ ينبغي السماحُ لذلك الموظف بالوصولِ إلى هذا المورد، وتنفيذُ الإجراء المطلوب، كما أنَّه من المهمّ تحديث مصفوفة التحكم في الوصول بانتظام لتعكس التغييرات في واجباتِ الوظيفة بسبب الترقيات، أو عمليات النقل، وإلا فمع مرورِ الوقت قد يجمعُ الموظفُ مجموعةً من الحقوقِ، والامتيازات التي تتعارضُ مع الفصلِ الصحيحِ بين الواجبات، ولا تنطبقُ ضوابطُ التفويض على الأشخاصِ فقط، ولكن من المهمّ جداً أن يتمَّ تطبيقها أيضاً على الأجهزة المختلفة، والمرتبطة بنظام المعلومات، على سبيلِ المثال يتيحُ تضمين عناوين MAC ، أو الشهادات الرقمية في مصفوفةِ التّحكم في الوصول، تقييدَ الوصولِ إلى نظامِ كشوف المرتبات، والملّفات الرئيسية لكشوف المرتبات لموظّفي قسمِ كشوف المرتبات فقط عندَ تسجيلِ الدخول من سطح المكتب، أو الكمبيوتر المحمولِ المخصّص لهم، فمثلاً لماذا يحتاجُ كاتب كشوف المرتبات إلى تسجيلِ الدخولِ من محطةِ عملٍ موجودة في المستودع، أو محاولةِ إنشاءِ اتصالٍ هاتفيّ من بلدٍ آخر.[84]

ب. اختبارات الاختراق: يمكن أن يستخدمَ اختبارُ الاختراق العديدَ من الطّرق لمحاولةِ اختراقِ النّظام، يدويّاً ، أو آليّاً، يتضمنُ النوع الأكثر فائدةً من اختبار الاختراق استخدامَ الطّرقِ التي من المتوقّع استخدامها بالفعل ضدَّ النظام المدروس، بالنّسبة للعديدِ من الأنظمة تعدُّ الإجراءات المتساهلة، أو الافتقار إلى الضوابط الداخلية على التطبيقات من نقاطِ الضّعف الشائعة التي يمكنُ أن يستهدفَها اختبارُ الاختراق.[85]

يوفّرُ اختبارُ الاختراق طريقةً صارمةً لاختبارِ فعاليةِ أمن معلومات المنظمة، حيثُ يعدُّ اختبارُ الاختراق محاولةً معتمدةً من قبل فريقِ التدقيق الداخلي، أو شركةٍ استشاريةٍ أمنيّةٍ خارجيّة لاقتحامِ نظام معلومات المنظمة، تحاولُ هذه الفرق بذلَ كلّ جهدٍ ممكنٍ لاختراقِ نظام المنظمة، ونظراً لوجودِ العديدِ من موجهي الهجوم المحتملين، تنجحُ اختبارات الاختراق دائماً تقريباً، وهكذا فإنَّ قيمتَها لا تكمن في إظهارِ أنَّه يمكنُ اختراق النظام، ولكن في تحديدِ الأماكن التي تكونُ هناك حاجة فيها إلى المزيدِ من الحماية لزيادةِ الوقتِ، والجهد اللازمينِ لعرقلةِ النظام.[86]

ج. تغيير الضوابط وإدارة التغيير: تقومُ المنظمات بتعديلِ أنظمة المعلومات الخاصة بها باستمرارٍ لتعكسَ الممارسات التجارية الجديدة، والاستفادة من التطورات في تكنولوجيا المعلومات.

يشيرُ تغييرُ الضوابطِ، و إدارة التغيير إلى العمليةِ الرسمية المستخدمة للتأكّد من أنَّ التعديلات على الأجهزة، أو البرامج، أو العمليات، لا تقلّل من موثوقية الأنظمة، فغالباً ما يؤدّي التّحكم الجيد في التغيير إلى تحسينِ أداءِ التشغيل نظراً لوجودِ عددٍ أقلّ من المشكلات التي يجبُ إصلاحها، وبالتالي المنظمات التي لديها إدارة جيدة للتغييرات ، وعمليات التحكم في التغيير تواجهُ أيضاً تكاليفَ أقلّ عندَ وقوعِ حوادثَ أمنيّة، حيثُ تعدُّ القدرةُ على تحديدِ

---

[84] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p: 345.
[85] Nieles, Michael, Dempsey, Kelley, Yan Pillitteri, Victoria, 2017, **Op cit.,** p: 43.
[86] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p: 356

التغييرات غير المصرّح بها بسرعة، ومعاقبة المسؤولين عن التحايلِ المتعمّد على عملية التحكّم في التغييرِ، وإدارةِ التغيير واحدةً من أهمّ الخصائصِ التي تميّزُ المنظمات ذات الأداءِ الجيد عن غيرها، وتشملُ خصائص عملية التحكم في التغيير، وإدارة التغيير المصممة بشكلٍ جيّدٍ ما يلي:[87]

- توثيقَ جميعِ طلبات التغيير، وتحديد طبيعة التغيير، وأساسه المنطقي، وتاريخ الطلب، ونتائج الطلب.
- موافقةً موثّقةً على جميعِ طلباتِ التغيير بمستوياتٍ مناسبة من الإدارة، فمن المهمّ بشكلٍ خاصّ أن تقومَ الإدارةُ العليا بمراجعةِ، واعتمادِ التغييراتِ الرئيسية في العمليات، والأنظمة لضمانِ توافقِ التغيير المقترح مع الخطط الاستراتيجية طويلة الأجل للمنظمة.
- اختبارَ جميعِ التغييرات في نظامٍ منفصلٍ، وليسَ النظام المستخدم في العمليات التجارية اليومية، لأنَّ هذا يقلّلُ من خطرِ أنَّ "الأخطاء" في التعديلات قد تعطّلُ الأعمال العادية.
- ضبطَ التحويل لضمانِ نقل البيانات بدقةٍ، و بشكلٍ كاملٍ من النظام القديم إلى النظام الجديد. يجبُ على المدققين مراجعة عملية التحويل.
- تحديثَ جميعِ الوثائق (تعليمات البرنامج، أوصاف النظام، كتيبات الإجراءات، إلخ)
- تطوير، وتوثيق خطط "back out" لتسهيلِ العودة إلى التكوينات السابقة إذا كانَ التغييرُ الجديد يخلقُ مشاكلَ غير متوقعةٍ.
- رصداً دقيقاً، ومراجعة حقوق المستخدم، والامتيازات أثناءَ عمليةِ التغييرِ لضمان الحفاظ على الفصل الصحيح بين الواجبات.

3. **حلول تكنولوجيا المعلومات:** يمكنُ الاستفادة من بعضِ مميزاتِ تكنولوجيا المعلومات في الحدِّ من إمكانيةِ وقوعِ انتهاكاتٍ، أو تهديداتٍ لنظامِ المعلومات في المنظمة، حيثُ إنَّ المنظمات التي تخصّص جزءً من استثماراتها في اقتناءِ البرمجيات المتخصّصة في أمن المعلومات قد يساعدُها ذلك على تجنّب الأضرارِ المختلفة التي قد تحدث نتيجةَ المشاكل التي قد تصيبُ تكنولوجيا المعلومات غير المحميّة، وتتمثّلُ حلولُ تكنولوجيا المعلومات من خلالِ مجموعةٍ من الضّوابط هي الآتي:

أ. **ضوابط مكافحة البرامج الضارة:** البرامجُ الضّارة (مثل الفيروساتِ، والديدان، وبرامج تسجيل ضغط المفاتيح، وما إلى ذلك) تشكّلُ تهديداً كبيراً لأمن المعلومات، حيثُ يمكن أن تتسبّبَ البرامجُ الضارة في إتلافِ المعلومات، أو تدميرها، أو توفيرِ وسيلةٍ للوصول غير المصرّح به، لذلك يعرض COBIT 2019 الحماية من البرمجيات الخبيثة كأحدِ مفاتيح الحماية الفعّالة، وعلى وجهِ التّحديد التوصية بما يلي:[88]

- التوعيةُ بالبرامج الخبيثة.

[87] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Ibid.,** p: 356
[88] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p: 346.

- تثبيتُ أدوات الحماية من البرامج الضارة على جميع الأجهزة.
- الإدارةُ المركزية للتصحيحات، والتحديثات لبرامج مكافحة البرامج الضّارة.
- مراجعةٌ منتظمة لتهديدات البرامج الضّارة الجديدة.
- تصفيةُ حركة المرور الواردة لمنع المصادر المحتملة للبرامج الضّارة.
- تدريبُ الموظّفين على عدمِ تثبيتِ البرامج المشتركة، أو غيرِ الموافق عليها.

ب. **ضوابط الوصول إلى الشبكة:** توفّرُ معظمُ المنظمات للموظفين، والعملاء والموردين إمكانيةَ الوصول عن بُعد إلى أنظمةِ المعلومات الخاصّة بهم، وعادةً ما يحدثُ هذا الوصولُ عبرَ الإنترنت، كما توفرُ العديدَ من المنظمات أيضاً إمكانيةَ الوصول اللاسلكي إلى أنظمتها، وبالتالي يجبُ تأمين المعلومات المتنقلة عبر الشبكة من خلال مجموعةٍ من الوسائل، كجدران الحماية، وأنظمة منع التطفل، والتي نشرحها في الآتي: [89]

- **جدران الحماية:** يمكنُ تعريف جدار الحماية بأنَّه كلّ آلةٍ موضوعةٍ في شبكةٍ معلوماتية، وقادرة على تحقيق غربلة على التواصلات الداخلة والخارجة، حيثُ يعدُّ استخدامُ أجهزةٍ متعددةٍ لتصفيةِ البيئة الخاص بشبكة الاتصال في المنظمة أكثرَ كفاءةً وفعاليةً من الاعتمادِ على جهازٍ واحد فقط، وبالتالي تستخدمُ معظم المنظمات أجهزةً متعددةً لتصفيةِ الحزم البرمجية السيئة أو الضارة بشكلٍ واضح، وتمرير الباقي إلى جدار الحماية الرئيسي، حيثُ يقومُ جدارُ الحماية الرئيسي بفحصٍ أكثر تفصيلاً، ثمَّ تقومُ جدرانُ الحماية الأخرى بفحصٍ متعمّق، لحماية أجهزةٍ معيّنة بشكلٍ كامل مثل خادمِ الويب الخاص بالمنظمة، وخادم البريد الإلكتروني.[90]
- **أنظمة منع التطفل (IPS):** تقومُ بمراقبةِ حركة المرور التي تمرُّ عبرَ جدرانِ الحماية، لتحديدِ أنماطِ حركة مرور الشبكة المشبوهة، وحظرها ، والتي قد تشيرُ إلى حدوثِ هجومٍ، كما تجدرُ الإشارةُ إلى أنَّه من السّهل، وغير المكلف للموظفين إعدادُ نقاط وصولٍ لاسلكية غير مصرّح بها في مكاتبهم، لذلك يجبُ على موظفي أمن المعلومات، أو التدقيق الداخلي إجراءَ اختباراتٍ دورية لوجودِ نقاط الوصول الدخيلة، وتعطيل أيّ نقاط يتمّ اكتشافها، وتأديب الموظفين المسؤولين عن تثبيتها بشكلٍ مناسب.

ج. **ضوابط تقوية الأجهزة والبرمجيات:** يمكنُ للمنظمة تعزيزَ أمنِ المعلومات من خلال استكمالِ عناصرِ التحكم الوقائية في بيئة الشبكة من جدرانِ حماية، وأنظمة منع التطفل (IPS)، وذلك باستخدام عناصرَ تحكّمٍ وقائية إضافية على أجهزة الحاسب، والخوادم، والطابعات، والأجهزة الأخرى التي يشارُ إليها عادةً بنقاطِ النهاية، حيثُ تشملُ عناصرُ التحكّم الإضافية المتعلقة بأمن نقاط النهاية كلاً من: [91]

- **إعدادات نقطة النهاية:** يمكنُ جعلُ نقاط النهاية (اجهزة الحواسيب، والخوادم، والطابعات، والأجهزة الأخرى) أكثرَ أماناً عن طريق تعديلِ الإعدادات الافتراضية لها، فعادةً ما تقومُ الإعدادات الافتراضية لمعظمِ الأجهزة

---

[89] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Ibid.,** p: 347

[90] فيلالي، أسماء، 2019، **مرجع سبق ذكره**، ص: 106

[91] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p: 351.

بتشغيل عددٍ كبيرٍ من الإعدادات الاختيارية التي نادراً ما يتمّ استخدامها، وبالمثل تقومُ عمليات التثبيت الافتراضية للعديدِ من أنظمةِ التّشغيل بتشغيلِ العديدِ من البرامجِ ذات الأغراض الخاصّة، والتي تسمّى الخدمات، وبالتالي يؤدّي تشغيلُ ميزاتٍ غير ضروريةٍ، وخدماتٍ إضافية إلى زيادةِ احتمالِ خلقِ نقاط ضعفٍ لأمن المعلومات. [92]

يمثّلُ كلّ برنامجٍ يتمّ تشغيله نقطةً محتملةً للهجوم لأنّه قد يحتوي على عيوبٍ، تسمى **الثغرات الأمنية**، والتي يمكنُ استغلالها إما لتحطيمِ النظام، أو السيطرةِ عليه، وبالتالي يجبُ تعطيل أيّ برامج، وميزاتٍ اختيارية غير مستخدمةٍ، حيثُ يمكن استخدامُ الأدوات التي تسمى **ماسحات الثغرات الأمنية** للتعرّف على البرامجِ غير المستخدمة، وبالتالي البرامج غير الضرورية التي تمثّلُ تهديداتٍ أمنية محتملة. [93]

- **إدارة حساب المستخدم:** يشدّدُ COBIT 2019 على الحاجةِ إلى إدارة جميع حسابات المستخدمين بعناية، خاصةً تلك الحسابات التي لها حقوقٌ إداريةٌ غير محدودةٍ على الحاسب، ذلك لأنّ الإمكانيات القوية لتعديلِ معظمِ إعدادات البرامج تجعلُ الحسابات ذات الحقوقِ الإدارية الواسعة أهدافاً للمهاجمين، لذلك يجبُ تعيينُ حسابين للموظفين الذين يحتاجون إلى صلاحياتٍ إدارية على حاسبٍ معيّن: واحدٌ له حقوقٌ إدارية، والآخرُ لديه امتيازات محدودة فقط، كما يجبُ تدريب هؤلاء الموظفين على تسجيلِ الدخول ضمنَ حساباتهم المحدودة لأداءِ الواجبات اليومية الروتينية، وتسجيلِ الدخول إلى حسابهم الإداري فقط عندما يحتاجونَ إلى القيامِ ببعضِ الإجراءات، مثلَ تثبيتِ برنامجٍ جديد، ومن المهمّ بشكلٍ خاصّ أن يستخدمَ الموظّفُ حسابَ مستخدمٍ عاديّ محدود عندَ تصفّح الويب، وبهذه الطريقة إذا زارَ الموظفُ موقعَ ويب مخترق أو فتحَ بريداً إلكترونياً مصاباً، فإنَّ المهاجمَ سيحصل على حقوقٍ محدودةٍ فقط على الجهاز، وعلى الرغم من أنَّ المهاجمَ يمكنه استخدامَ أدواتٍ أخرى للحصولِ على حقوقٍ إداريةعلى هذا الجهاز، إلا أنَّ عناصرَ تحكّمٍ أمنيةٍ أخرى قد تكتشفُ وتحبطُ مثل هذه المحاولات، وعلى النقيضِ من ذلك، إذا كانَ الموظفُ يستخدمُ حساباً له حقوقٌ إداريةٌ، فإنَّ البرامجَ الضّارة ستضرّ بالجهاز تماماً قبلَ أن تتمكّنَ أيّ عناصر تحكّمٍ أخرى من اكتشافِ وجود مشكلة، كما أنَّه من المهمّ تغيير كلماتِ المرور الافتراضية على جميع الحسابات الإدارية التي يتمُّ إنشاؤها أثناءَ التثبيت الأوليّ لأيّ برنامجٍ، أو جهازٍ لأنَّ أسماءَ الحسابات، وكلمات المرور الافتراضية الخاصة بها تكونُ متاحةً للجمهور على الإنترنت، وبالتالي تزويدُ المهاجمين بطريقةٍ سهلة للاحتيال على النظام.[94]

---

[92] فيلالي، أسماء، 2019، **مرجع سبق ذكره**، ص: 101

[93] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p: 352.

[94] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p: 341.

4. **الأمن المادي والبيئي:** يشيرُ مصطلحُ الأمن الماديّ، والبيئيّ إلى التدابيرِ المتّخذة لحمايةِ الأنظمة، والمباني، والبنية التحتية الدّاعمة ذات الصلة من التّهديداتِ المرتبطة ببيئتها المادية، تغطي الضوابطُ الماديةُ، والبيئية ثلاثةَ مجالاتٍ واسعةٍ:[95]

أ. **طبيعة أماكن تواجد النظام:** عادةً ما يكونُ المرفقُ المادي هو المبنى، أو السيارةُ التي تحتوي على مكوناتِ النظام، والشبكة، وبالتالي يمكنُ تمييزُ الأنظمة بناءً على موقعِ التشغيل الخاص بها على أنَّها ثابتةٌ، أو متحركةٌ، أو محمولةٌ، أي الخصائص الفيزيائية لهذه المباني، والمركبات هي التي تحدّدُ مستوى التهديدات المادية مثل الحريق، أو التلف، أو الوصول غير المصرّح به.

ب. **الموقع الجغرافي للنظام:** يحدّدُ موقعُ التشغيل الجغرافي العام للمنشأة خصائصَ التهديداتِ الطبيعية، والتي تشملُ الزلازلَ، والفيضانات، والتهديدات التي من صنعِ الإنسان مثل السطو، أو اعتراض الإرسال، وإتلاف موارد النظام، بما في ذلك الانسكابات الكيميائية السامة، والانفجارات، والحرائق، والتداخل الكهرومغناطيسي.

ج. **المرافق الأخرى الداعمة لعمليات تشغيل النظام:** المرافقُ المساندة هي تلك الخدماتُ (الفنية والبشرية) التي تحافظُ على تشغيلِ النظام. يعتمدُ تشغيل النظام عادةً على المرافقِ الداعمة مثل الطاقةِ الكهربائية، والتدفئة، وتكييف الهواء، والاتصالات. قد يؤدّي الفشلُ، أو الأداءُ المتدني لهذه المرافق إلى قطعِ تشغيل النظام/ والتسبّب في تلفٍ ماديّ لأجهزة النظام، أو البياناتِ المخزنة.

وبالتالي يمكنُ تحقيقُ متطلباتِ الأمن المادي من خلال جملةٍ من الضوابط وهي:

- تحديدُ الوصول المادي إلى الأنظمة، والمعدّات، وبيئات التشغيل على الأفراد المصرّح لهم.
- حمايةُ المنشأة المادية، والبنية التحتية الداعمة للأنظمة.
- توفيرُ المرافق الداعمة للأنظمة.
- حمايةُ الأنظمة من الأخطار البيئية.
- توفيرُ ضوابطٍ بيئيةٍ مناسبة في المرافقِ التي تحتوي على أنظمة.

2-4-2 الضوابط الاستكشافية لأمن المعلومات:

من الواضح أنَّه من غير الممكن أن تكونَ الضوابطُ الوقائية في المنظمة فعالةً بنسبة 100% في منعِ كافةِ التهديدات المختلفة، والمخاطر المحيطة بأمن معلومات المنظمة، لذلك تُشكّلُ الضوابطُ الاستكشافية خطَّ الدفاع الثاني، حيثُ تضمُّ الإجراءات التي تهدفُ إلى تحديدِ، وكشفِ الأحداث غير المرغوب فيها، والتي تستعصي على الضوابط الوقائية، فالضوابطُ الاستكشافية تهدفُ إلى تحديدِ الخروقات الأمنية في الوقتِ المناسب، كما تهدفُ إلى

[95] Nieles, Michael, Dempsey, Kelley, Yan Pillitteri, Victoria, 2017, **Op cit.,** p: 65.

الكشفِ عن التهديداتِ، والمحاولاتِ الفعلية للإضرار بأمن المعلومات في المنظمة، ومنعِها من إحداثِ ضررٍ حقيقيّ في الأصول المادية، والمعلوماتية للمنظمة، ويمكنُ تصنيفُ هذه الضوابط في مجموعةٍ من العناصر:

1. **تحليل السجل:** يعرفُ تحليل السجل على أنَّه عمليةُ فحصِ السجلات لتحديدِ أدلةِ الهجمات المحتملة، تأتي معظمُ الأنظمة مع إمكاناتٍ واسعة لتسجيل الدخول إلى النظام، والإجراءات المحدّدة التي يقومُ بها كلّ مستخدمٍ، وبالتالي يجبُ تحليلُ السجلات بانتظام للكشفِ عن المشكلات في الوقت المناسب، إلا أنَّ هذا ليسَ بالأمر السّهل، لأنَّ السجلات يمكن أن تنمو في الحجمِ بسرعة، كما أنَّه يوجدُ مشكلةً أخرى هي أنَّ العديدَ من الأجهزة تنتجُ سجلاتٍ بتنسيقاتٍ خاصّة، ممّا يجعلُ من الصعبِ ربط السجلات، وتلخيصِها من أجهزة مختلفة، تحاولُ أدوات البرامج مثل أنظمةِ إدارة السجلات، وأنظمةِ إدارة أمن المعلومات، معالجةَ هذه المشكلات عن طريق تحويلِ تنسيقات السّجل الخاصّة بالمورد إلى عروضٍ مشتركةٍ، وإنتاج تقاريرٍ تربطُ وتلخصُّ المعلومات من مصادرَ متعددةٍ. [96]
2. **أنظمة كشف التسلل:** تعرفُ أنظمة كشف التسلل بأنّها الأنظمةُ التي تقومُ بعمليةِ مراقبةِ الأحداث التي تحدثُ في نظام الكمبيوتر، أو الشبكةِ لاكتشاف علامات الوصول غير المصرّح به، أو الهجوم، حيثُ تتكوّنُ أنظمة كشف التسلّل إلى الشبكة (IDS) من مجموعةٍ من المستشعرات، ووحدة مراقبة مركزية تنشئُ سجلاتٍ لحركة مرورِ الشبكة التي سُمحَ لها بالمرور خلالَ جدارِ الحماية، ثم تحلل هذه السجلات بحثاً عن علامات لمحاولات أو اقتحام ناجح.[97]
3. **المراقبة المستمرة:** تشدّد الممارسة الإدارية لـ COBIT 2019 على أهميةِ المتابعة المستمرةّ لكلّ من امتثال الموظف لسياسات أمن معلومات المنظمة، والأداء العام للعمليات التجارية، هذا الرصدُ هو عنصرُ تحكم استكشاف مهم يمكّن من تحديدِ المشكلات المحتملة في الوقت المناسب، وتحديدِ الفرص المتاحة لتحسين الضوابطِ الحالية، ومع أنَّ قياسَ الامتثال للسياسات واضحٌ، ومباشر، ولكن يتطلّبُ رصد الأداءِ بشكلٍ فعّال اجتهاداً ومهارة، يمكن للمحاسبين توفيرُ إسهام إضافي من خلال الاعتماد على COBIT 2019 لتقييم أمن المعلومات للمساعدة في تصميم تقارير فعالة تبرزُ المجالات الأكثر احتياجاً إلى الاهتمام.[98]
4. **تقنية (honeypots) مصائد الاختراق:** يُطلقُ مصطلح (honeypots) على أداةٍ دفاعيةٍ مهمّة تستخدمها العديد من المنظمات، تشملُ تقنية (honeypots) نظاماً خادعاً يستخدم لتوفيرِ تحذير مبكر بأنَّ طرفاً داخلياً أو خارجياً يحاولُ الحصولَ على معلوماتٍ سريّة، حيثُ يبدو (honeypots) وكأنَّه جزءٌ أساسيّ من الشبكة الداخلية للمنظمة فعلى سبيل المثال: قد يتمّ تكوين نموذجٍ (honeypots) لمحاكاة خادم البحث، والتطوير أو

---

[96] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p: 353.
[97] ISACA, 2015, **Glossary of Terms English-Arabic 3rd Edition**, p: 39.
[98] ISACA, 2018, **COBIT 2019 FRAMEWORK: INTRODUCTION & METHODOLOGY**, P: 52.

بعض الأهداف الأخرى التي يحتملُ أن تكونَ هدفاً مغرياً لعمليات الاختراق، وبالتالي فإنَّ محاولات الوصول إلى (honeypots) توفر تحذيراً مبكراً بأنَّ شخصاً ما (سواءً كان موظفاً أو طرفاً خارجياً) يبحثُ عن معلومات سرية، مما يمكّن فريق أمن المعلومات من مراقبةِ محاولة الاختراق، والتدخل بشكلٍ فوري.[99]

2-4-3 الضوابط التصحيحية لأمن المعلومات:

لا يكفي اكتشافُ المشكلات في الوقت المناسب، رغمَ أهمية ذلك فإنَّ المنظمات تحتاجُ إلى إجراءاتٍ للقيام بالأنشطة التصحيحيّة في الوقت المناسب أيضاً، إنَّ العديدَ من الضوابط التصحيحية تعتمدُ على الحكم البشري، وبالتالي تعتمدُ فعاليتها إلى حدٍّ كبيرٍ على التخطيطِ، والإعدادِ المناسبين، يكمن أهمّ عنصرين من الضوابط التصحيحية لأمن المعلومات في الهيكل التنظيمي للمنظمة حيثُ يتمّ ذلك من خلال:

1. **فريق الاستجابة لحوادث الحاسوب (CIRT):** إن إنشاء فريقٍ للاستجابة لحوادث الكمبيوتر (CIRT) يتمثَّلُ أحدَ العناصر الرئيسية في القدرة على الاستجابة للحوادث الأمنية بشكلٍ سريعٍ، وفعّال، حيثُ يجبُ ألّا يشملُ CIRT الاختصاصيين التقنيين فحسب، بل يشملُ أيضاً الإدارةَ العليا للعمليات، لأنَّ بعضَ الاستجابات المحتملة للحوادث الأمنية لها عواقبُ اقتصادية كبيرة، على سبيل المثال: قد يكونُ من الضروري إيقاف خادم التجارة الإلكترونية مؤقتاً، قرارُ القيام بذلك هو أمرٌ مهمٌّ للغاية بحيث لا يمكن تركه لتقدير موظفي أمن تكنولوجيا المعلومات، إدارة العمليات هي التي تمتلكُ المعرفةَ الواسعة لتقييم التكاليف، والفوائد المترتبة على مثل هذا الإجراءِ بشكلٍ صحيح، ويجب أن يكونَ لها فقط سلطةُ اتخاذ هذا القرار، وبالتالي يجب أن تقودَ CIRT بعملية الاستجابة لحوادث المنظمة من خلال الخطوات الأربع التالية:[100]
   أ. الاعتراف بوجود مشكلة.
   ب. احتواء المشكلة: بمجرد اكتشاف التسلل، يلزم اتخاذ إجراءً عاجلاً لوقفه واحتواء الضرر.
   ج. التعافي: يجب إصلاح الأضرار الناجمة عن الهجوم، قد يتضمن ذلك القضاء على أي برامج ضارة، واستعادة البيانات من النسخ الاحتياطي، وإعادة تثبيت البرامج التالفة.
   د. المتابعة: بمجرد الانتهاء من عملية الاسترداد، يجب أن تقود CIRT تحليل كيفية وقوع الحادث، فقد يلزم اتخاذ خطوات لتعديل سياسة، وإجراءات الأمن الحالية لتقليل احتمال وقوع حادث مماثل في المستقبل.

من المهم أيضاً تجربة خطة الاستجابة للحوادث، وذلك حتى تكون المنظمة على استعدادٍ لتنفيذ الخطة الموضوعة في حال حدوث أي تهديد، فمن الأفضل بكثير اكتشاف ثغرةً في الخطة أثناءَ التنفيذ التدريبي مقارنةً بوقوع تهديد حقيقي، كما تساعد التدريبات المنتظمة على تحديد الحاجة إلى استجابة للتغيرات التكنولوجية، على سبيل المثال: تقومُ العديد من المنظمات بالتبديل من نظام الهاتف التقليدي إلى نظام قائم على نقل الصوت عبرَ الإنترنت

[99] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p: 354.
[100] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p: 355.

(VoIP)، هذا يمكن أن يوفّرَ الكثيرَ من المال، لكن هذا يعني أيضاً أنه إذا تعطّلت شبكةُ الكمبيوتر، فإنَّ نظامَ الهاتف سينهار أيضاً، وقد لا يتمّ ملاحظة هذا التأثير الجانبي حتى يتمّ تطبيق خطة الاستجابة للحوادث.[101]

2. **مدير أمن المعلومات (CISO):** يعتبرُ هذا الشخص الرئيس الإداري للأمن، ويعدُّ مسؤولاً عن الوعي الأمني ويعمل كنقطة محورية للبتّ في جميع القضايا الأمنية، يمكن تلخيص بعض المسؤوليات الرئيسية لـ CISO في النقاط الآتية:[102]

- قيادة عمليات أمن المعلومات والأنشطة المتعلقة بأمن المعلومات.
- إعداد إرشادات أمنية لفريق إدارة أمن المعلومات.
- الحفاظ على نظام إدارة أمن المعلومات، ومراجعة تقارير تقييم المخاطر.
- مراقبة الامتثال المستمر للمعايير الأمنية في المنظمة.
- إعداد الخطط، والإجراءات المتعلقة بالإدارة والمعلومات.
- التأكد من أنَّ أعضاءَ الفريق مدربون تدريباً كافياً على مجال الأمن من أجل تلبية متطلبات أمن المعلومات.
- تحليل التقارير التي أعدّتها إدارات الدعم المختلفة واتخاذ الإجراءات التصحيحية عند الاقتضاء.
- تخطيط، وإجراء عمليات التدقيق الداخلي لأمن المعلومات ومراجعات الإدارة.
- التأكد من اتخاذ الإجراءات التصحيحية ضد القضايا المثارة أثناءَ عمليات التدقيق الداخلية أو الخارجية.
- تقرير عن أداء إدارة أمن نظم المعلومات للإدارة العليا.

---

[101] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Ibid.,** p: 356

[102] Chopra, Abhishek, Chaudhary, Mukund, 2020, **Op cit.**, p: 53.

مما سبق نلاحظُ أنَّ الضوابطَ المختلفة لأمن المعلومات تتضمنُ مجموعات من العناصر، نلخصها في الجدول (2-3) الآتي:

الجدول (2-3): ضوابط أمن المعلومات وعناصرها:

الضوابط:	العناصر:
الوقائية:	**_الأشخاص: . خلق ثقافة واعية بالأمن.** **. التدريب.** **_العمليات: . ضبط وصول المستخدم (المصادقة والتفويض).** **. اختبار الاختراق.** **. تغيير الضوابط و إدارة التغيير.** **_حلول تكنولوجيا المعلومات: . مكافحة البرامج الضارة.** **. أدوات التحكم في الوصول إلى الشبكة.** **. تقوية الأجهزة والبرامج.** **_الأمن المادي والبيئي.**
الاستكشافية:	**_تحليل السجل** **_أنظمة كشف التسلل** **_المراقبة المستمرة** **_تقنية (honeypots) مصائد الاختراق**
التصحيحية:	**_فرق الاستجابة لحوادث الحاسوب(CIRT)** **_مدير أمن المعلومات(CISO)**

المصدر: من إعداد الباحث

تمثّلُ الضوابطُ السابقة إطارَ عملٍ متكاملٍ لتحقيقِ فعالية أمن المعلومات في المنظمة، حيثُ تشملُ مجموعةَ خطوط دفاعية تحمي نظامَ المعلومات عندَ كافةِ المستويات الإدارة والتنظيمية، وتوفّر بيئةَ عمل تأخذ مخاطر، وتهديدات أمن نظم المعلومات كواحدةٍ من الأهداف الاستراتيجية التي تتبنّاها الإدارة العليا، وتجدر الإشارة إلى أنَّ هذه الضوابط يجب أن تكونَ مرنةً، وديناميكية تتلائمُ مع المستجدات، والظروف، والتطورات في بيئة تكنولوجيا المعلومات، كما نجدُ أنَّ الأنواعَ الثلاث لضوابط أمن المعلومات لا تمثّل بدائلَ يمكنُ تبنّي بعضَها دون الآخر، وإنما تمثّلُ مجتمعة إطاراً متكاملاً لتحقيق مستوى عالٍ لأمن المعلومات، حيثُ تتناولُ بمجملها كافةَ الاحتمالات المتوقّعة للإخلال بأمن المعلومات، وتهدفُ هذه الضوابط إلى تشكيلِ خطوطٍ دفاعية متعاقبة لخلقِ بيئةٍ نظيفةٍ محميّة من التهديدات المختلفة، تضمنُ للمنظمة مستوياتٍ منخفضة من الخطر.

الفصل الثالث: نظام الرقابة الداخلية في بيئة تكنولوجيا المعلومات.

تمهيد:

تعتبرُ الرقابة الداخلية من أهمّ العناصر التي يعتمدُ عليها المدقق الداخلي، والخارجي عندَ قيامِه بعملية التدقيق، فالخطوةُ الأولى لعمل المدقق الداخلي هي دراسةُ وتقييمُ إجراءاتِ الرقابة الداخلية، بهدفِ التأكّدِ من مطابقة الأداء الفعلي للنظم التي صمّمتها ووضعتها الإدارة، ومن التزام المستويات الإدارية بالسياسات واللوائح والقوانين الموضوعة ومن ثمّ العمل على تحسينها باستمرار، وذلك بتقديمِ الاقتراحات والتوصيات والحلولِ المناسبة لما قد يظهرُ من مشاكل، إذ إنَّ نظامَ الرقابة الداخلية يعتبرُ بمثابةِ خطّ الدفاع الأول الذي يحمي مصالحَ المساهمين بصفةٍ خاصةٍ، وكافة الأطراف ذات الصلة بصفةٍ عامة، لأنّه النظام الذي يوفّرُ الحمايةَ لعملية إنتاج المعلومات المالية التي يمكنُ الاعتماد عليها في اتخاذ قرارات الاستثمار، والائتمان الرشيدة.[103]

إلا أنَّ مفهومَ الرقابةِ الداخلية شهدَ تطوراً كبيراً نتيجة لتطور حجم المشروعات الاقتصادية، وزيادة اعتمادها على تكنولوجيا المعلومات مما جعل المنظمات في محيط مليء بالتغيرات والتحديات، حيثُ انعكسَ هذا التطورُ التكنولوجي على البيئة الرقابية، مما زادَ حرصَ المنظمات على أهميةِ مواكبةِ نظام الرقابة الداخلية لمتطلبات تكنولوجيا المعلومات وللتطورات المرتبطة به، من خلال وضع نظام رقابة داخلية يمتازُ بالكفاءة والفاعلية، يعملُ على حمايةِ المنظمة من المخاطر التي تواجهها في بيئة تكنولوجيا المعلومات، كما وأصبحَ نظام الرقابة الداخلية من أهمّ الأقسام التي تتطلّب استخدامَ تكنولوجيا المعلومات وذلك لما لها من أهميةٍ في تزويد الإدارة بالمعلومات التي تحتاجها في اتخاذ القرارات في الوقت المناسب، الأمر الذي أدى إلى دفعِ العديدِ من المنظمات إلى إنشاءِ إداراتٍ مستقلة للرقابة الداخلية ودعمها بالكفاءات البشرية المؤهلة التي تمكّنها من تحقيق أهدافها بفعالية.[104]

من هنا برزت أهمية نظام الرقابة الداخلية مع ظهور بيئةٍ رقابية جديدة تختلفُ عن البيئة الرقابية التقليدية، فالمشاكل التي تواجهُ المدققين بالطرق التقليدية خصوصاً في المنظمات الكبيرة جعلَ عمليةَ الرقابة صعبةً، وشاقةً، ومكلفةً في آنٍ واحدٍ، ولكن مع بدء استخدام تكنولوجيا المعلومات في مجالات الرقابة الداخلية الذي يعني توظيفَ وسائل تكنولوجيا المعلومات لممارسة الأعمال الرقابية، أدّى ذلك إلى تغييرٍ في المعايير الرقابية التي سمحت للمدققين بإجراء رقابة أكثر دقةً، وشموليةً في المنظمة.

يتناولُ الباحثُ في هذا الفصل الإطارَ المفاهيمي لنظامِ الرّقابة الداخلية بما فيه من تعريفٍ وأهداف وأهمية ومكونات، ومبادئ نظام الرقابة الداخلية، والتركيز على مقومات نظام الرقابة الداخلية الفعّال والأساليب والإجراءات والمعايير، والأطر المرتبطة به، كما يتناولُ آليات مواجهة مخاطر تكنولوجيا المعلومات في ظلّ نظام الرقابة الداخلية.

---

[103] خرخاش، جميلة، 2018، **اثر تطبيق حوكمة الشركات في تفعيل أنظمة الرقابة الداخلية لدى البنوك التجارية الجزائرية**، أطروحة دكتوراه، جامعة محمد بوضياف بالمسيلة، الجزائر، ص: 85

[104] غزال، مصباح، سعيد، عمر، مهاوه، صدام حسين، 2018، **اثر تكنولوجيا المعلومات على فاعلية نظام الرقابة الداخلية**، رسالة ماجستير، جامعة الوادي، الجزائر، ص: 2

المبحث الأول: الإطار المفاهيمي لنظام الرقابة الداخلية:

3-1-1 تعريف الرقابة الداخلية:

يعرّفُ معيارُ التدقيق الدولي (315) "تحديدُ مخاطر التحريف الجوهري وتقييمها من خلال فهم المنشأة وبيئتها" الرقابة الداخلية بأنّها: آليةٌ يصمّمها، ويطبّقها، ويصونها المكلفون بالحوكمة، والإدارة وغيرهم من العاملين، لتوفير تأكيداً معقولاً عن تحقيق أهداف المنظمة، فيما يتعلّقُ بإمكانيةِ الاعتماد على التقرير المالي، وكفاءة، وفاعلية العمليات، والالتزام بالأنظمة، واللوائح المطبقة.[105]

وتعرفُ لجنة المنظمات الراعية (COSO) الرقابة الداخلية على أنّها: عمليةٌ تتأثّرُ بمجلس إدارة المنظمة والإدارة العليا والموظفين الآخرين، وهي مصمّمةٌ لتقديمِ تأكيدٍ معقول فيما يتعلقُ بتحقيقِ الأهداف في الفئات التالية: فعالية وكفاءة العمليات، موثوقية التقارير المالية، الامتثال للقوانين، واللوائح المعمول بها.[106]

أما الرقابةُ الداخلية من وجهة نظر المعهد الكندي للمحاسبين المعتمدين فهي: الخطةُ التنظيميةُ، وكلّ الطرقِ، والمقاييس المعتمدة داخل المنظمة من أجل حماية الأصول، وضمانِ دقة، وصدق البيانات المحاسبية، والتي تساعدُ على التحكّم في جميع نواحي المنظمة من أجلِ تحقيق الأهداف، والسير وفقاً للسياسات المرسومة.[107]

كما عرفه المعيار الدولي لممارسة أعمال التدقيق، والتأكيد وقواعد أخلاقيات المهنة رقم (400)"تقييم المخاطر والرقابة الداخلية"، الصادر عن الاتحاد الدولي للمحاسبين (IFAC) على أنّها: كافةُ السياساتِ والإجراءاتِ التي تتبنّاها المنظمة لمساعدتها قدرَ الإمكان في الوصولِ إلى أهدافها، مع ضمانِ إدارةٍ منتظمة وكفاءة عملٍ عالية، بالإضافة إلى الالتزام بسياسات حماية الأصول، ومنعِ الغش، واكتشافِ الأخطاء، والتحقّق من دقةِ، واكتمالِ السجلات المحاسبية، و تهيئةِ معلومات مالية موثّقة في الوقت المناسب.[108]

عرّفت لجنة بازل أيضاً الرقابةُ الداخلية بأنّها: عمليةٌ تتأثّر بدعمِ الإدارة العليا، ومجلس الإدارة، والأفراد في جميع المستويات الوظيفية، وهي ليست مجردَ مجموعة من الإجراءات، أو السياسات التي تنفذ في وقتٍ محدد، بل هي عمليةٌ مستمرة في جميع المستويات الوظيفية داخل المنظمة، ويعد مجلس الإدارة والإدارة العليا مسؤولين عن إنشاء الثقافة المناسبة لتنفيذ الرقابة، والمراقبة المستمرة لتقييم مدى كفاءتها، كما يجبُ أيضاً مشاركة جميع الأفراد في عملية الرقابة.[109]

---

[105] الهيئة السعودية للمحاسبين القانونيين، 2020، **المعايير الدولية للمراجعة والفحص والتأكيدات الأخرى والخدمات ذات العلاقة**، المملكة العربية السعودية، ص: 219.

[106] Kegerreis, Mike, Schiller, Mike, Davis, Chris, 2020, **IT Auditing Using Controls to Protect Information Assets**, third edition, USA, P: 937.

[107] حاج قويدر، قورين، 2019، **دور نظام الرقابة الداخلية في الحد من المخاطر البنكية**، جامعة حسيبة بن بوعلي الشلف، المجلة الأكاديمية للدراسات الاجتماعية والإنسانية، العدد الأول، الجزائر، ص: 37.

[108] بن عزيزة، محمد، 2019، **دور المراجعة الداخلية في تفعيل نظام الرقابة الداخلية في المؤسسة**، رسالة ماجستير، جامعة الجيلالي بونعامة خميس مليانة، الجزائر، ص: 11.

[109] حاج قويدر، قورين، 2019، **مرجع سبق ذكره**، ص: 38.

في حين تناولَ آخرون تعريفَ نظام الرقابة الداخلية بصورةٍ أكثر شموليةً على أنّه: كلّ ما تضعه، أو تتبعه المنظمة من قوانين، وأنظمة، ولوائح، وضوابط، وإجراءات، وأساليب، والتي يجبُ ان تشملَ كافةَ الخطة التنظيمية، والطرق ، والمقاييس التي تتّبعها المنظمة بقصدِ حماية أصولها، ومنع الغش والخطأ، وضمان صحة، واكتمال، ودقة، وسلامة السجلات المحاسبية، وضمان دقة المعلومات المالية والإدارية، والتشغيلية، وزيادة الثقة في الاعتماد عليها وضمان تحقيق كفاءة العمليات، والعمل على التشجيع، والالتزام بالسياسات المقررة، وتنفيذ الخطط الموضوعة، وتحقيق الأهداف الكلية، والفرعية.[110]

في ضوء التعريفات السابقة يمكن القول إنّ الرقابةَ الداخلية: عمليةٌ مستمرةٌ تهدفُ لتحقيق أهداف المنظمة، وحماية أصولها ، وممتلكاتها من كافة المخاطر، من خلال أساليب وإجراءات تتبنّاها الإدارة العليا، وتشرفُ على ضمان امتثال كافةِ المستويات الإدارية بها، مما يحقّق كفاءةً في أداء العاملين، ودقة في البيانات، والتقارير التي تنتجها أنظمة المعلومات المختلفة في المنظمة، وتخفيض المخاطر إلى المستوى المقبول.

3-1-2 أهداف نظام الرقابة الداخلية:

تلعبُ الرقابة الداخلية دوراً هاماً في مساعدة الإدارة على تحقيق أهدافها، حيثُ تناولت الأدبيات العلمية عدةَ أهداف لرقابة الداخلية من بينها:[111]

1. حماية أصول المشروع من السرقة والاحتيال: يقصد بحماية الأصول هو الوقايةُ من الأخطاء المعتمدة، أو غير المعتمدة في معالجة العمليات، وذلك بقصد إخفاء غش أو اختلاس، أو نتيجة أخطاء في تطبيق المبادئ المحاسبية.
2. التأكد من دقة البيانات المحاسبية: في الواقع إنَّ كلاً من إدارة المنظمة، والأطراف الخارجية تعتمدُ على البيانات المحاسبية إلى حدٍّ كبير في اتخاذ مختلف القرارات الإدارية الداخلية، أو الاستثمارية الخارجية، وهنا يبرزُ دورَ الرقابة الداخلية في ضمانِ دقة إثبات العمليات المالية التي حدثت في المنظمة.
3. الارتقاء بالكفاءة الإنتاجية: أحدَ أهداف إدارة المنظمة هو العملُ على تجنّب نواحي الإسراف في استخدام الموارد المتاحة في المنظمة أي الاستخدام الأمثل للموارد داخل المنظمة، وهذا ما يحققه نظام الرقابة الداخلة الفعال.
4. تشجيع الالتزام بالسياسات والقرارات الإدارية: إنَّ الرقابةَ الداخلية تساعدُ إدارة المنظمة في التحقق من الالتزام بالسياسات، والقرارات من قبل الجهات التنفيذية.

كما يمكن عرض أهداف نظام الرقابة الداخلية في ثلاث فئات مختلفة من الأهداف تسمح للمنظمة بالتركيز على كافة الجوانب المختلفة للرقابة الداخلية: [112]

1. **أهداف العمليات:** والتي تشمل:

---

[110] الوردات، خلف، 2017، **دليل لتدقيق لداخلي وفق المعايير الدولية الصادرة عن IIA**، الطبعة الأولى، دار الوراق للنشر والتوزيع، الأردن، ص: 279.

[111] بوعبد الله، فريدة، منومس، شيماء، 2020، **دور نظام المعلومات المالي في تحقيق فعالية الرقابة لداخلية**، رسالة ماجستير، معهد العلوم الاقتصادية والتجارية وعلم التسيير، الجزائر، ص: 59.

[112] خرخاش، جميلة، 2018، **مرجع سبق ذكره**، ص: 83.

- الفصلَ الملائم بين الواجبات والاختصاصات.
- توضيحَ خطوط السلطة في المنظمة.
- التركيزَ على الكفاءة والفعالية لكافة عمليات المنظمة، بما في ذلك أهداف الأداء التشغيلي، والمالي.
- حمايةَ الأصول من المخاطر المتعلقة بها.

2. أهداف إعداد التقارير:

- والتي تتعلّق بإعداد التقارير المالية، وغير المالية الداخلية والخارجية حيث تركّز على الموثوقية والتوفر، والتوقيت، والشفافية وغيرها من البنود المنصوص عليها من قبل المنظمين، أو واضعي المعايير أو السياسات في المنظمة.

3. أهداف الامتثال:

- والتي تتعلّق بتحديد مدى التزام الأفراد في المنظمة بالقوانين، واللوائح التي تخضعُ لها المنظمة، والتأكّد من تطبيق قرارات، وأوامر، وخطط الإدارة العليا للوصول إلى الأهداف المرسومة، والمخططة بكفاءةٍ، وفعالية.

3-1-3 أهمية نظام الرقابة الداخلية:

نظراً لأنَّ كلّ فردٍ في المنظّمة يتحمّلُ جزءً من المسؤولية عن الرقابة الداخلية، فمن الطبيعي أن تكونَ هناك وجهات نظر مختلفة حولَ أهميةِ نظام الرقابة الداخلية، حيثُ يعدُّ نظام الرقابة ذو قيمةٍ، وأهميةٍ لعدد من الأطراف المرتبطة بالمنظمة، نوضح ذلك فيما يلي:

1. **من وجهة نظر الإدارة:** تعدُّ الإدارة مسؤولةً عن تحديد الأهداف في المنظمة، فإنَّ أهميةَ نظام الرقابة الداخلية من وجهةِ نظر الإدارة تتمثّلُ باحتواءِ نظام الرقابة الداخلية على عددٍ من الأنشطة المصمّمة للتخفيف من المخاطر، أو تحقيق الفرص التي تؤثّرُ على تحقيق أهداف المنظمة، وبالتالي فإنَّ مشاركةَ الإدارة في تصميم نظام رقابة داخلية فعّال يسمحُ لها بالتفاعل مع كافة جوانب المنظمة، و تحديد مدى التزام العاملين، وامتثالهم للقوانين، واللوائح، والخطط الموضوعة من قبل الإدارة، كما يضمنُ للإدارة إنتاج معلومات تساعدُ على اتخاذ القرار، وتقليل المخاطر المحيطة بالمنظمة.[113]
2. **من وجهة نظر المدققين الداخليين:** ينظرُ المدقّقين الداخليين إلى نظام الرقابة الداخلية من حيثُ دورها في التحقق من مدى تحقيق الأهداف التنظيمية، حيث إنّ الإدارةَ هي المسؤولةُ عن وضع نظام الرقابة الداخلية، فإنَّ المدققين الداخليين يتمّ تكليفهم بالتحقّق بشكلٍ مستقلٍ من أنَّ ضوابطَ المنظمة مصمّمةٌ بشكل مناسب، وتعملُ بشكلٍ فعّال كما تنوي الإدارة، أي إنّ هذا التحقق المستقل يأخذُ في الاعتبار جميع الأنظمة، والعمليات والوظائف، والأنشطة الخاصة بالمنظمة، وبالتالي يزيدُ من احتمالية تحقيق أهداف المنظمة، حيثُ يقومُ المدققين

[113] بوعبد الله، فريدة، منومس، شيماء، 2020، **مرجع سبق ذكره**، ص: 61.

الداخليين بتقديمِ وجهة نظرهم حولَ التكلفة، والعائد من أنشطة الرقابة التي تتبنّاها المنظمة، بالإضافة إلى تحديد مدى فاعلية الضّوابط الموضوعة، وامتثال مستويات الإدارة المتخلفة بتلك الضوابط.[114]

3. **من وجهة نظر المدققين الخارجيين:** تتمثّلُ المسؤولية الأساسية لمدققين الخارجيين في إبداء الرأي حولَ عدالة البيانات المالية، إلا أنَّ بعضَ الجهات التنظيمية طلبت من المدققين الخارجيين إبداءَ رأي حولَ فعالية الرقابة الداخلية على التقارير المالية، لذلك يركّزُ المدققين الخارجيين عندَ قيامهم بعملية التدقيق على دراسة نظام الرقابة الداخلية في المنظمة، وذلك لإبداء الرأي حولَ فعالية نظام الرقابة الداخلية فيها من جهة، ولتحديد حجم إجراءات التدقيق المتبعة من جهة أخرى، وذلك لأنَّ التدقيقَ لم يعد شاملاً، وإنما يعتمدُ بشكلٍ أساسيّ على تدقيق العينة، والتي تتناسبُ مع مدى فعالية نظام الرقابة الداخلية في المنظمة، أي إنّ نظامَ الرقابة الداخلية الفعّال يعني عينةَ تدقيقٍ أصغر، وإجراءات تدقيق أقل، والعكس بالعكس.[115]

وبناءً على ما سبق نجدُ أنَّ نظامَ الرقابة الداخلية في المنظمة لم يعد أمراً داخلياً تعنى به الأطراف الداخلية في المنظمة من أجل تحقيق الأهداف، والإشراف على أداء العمل بكفاءةٍ، وفعالية، وإنما يعدُّ نظام الرقابة الداخلية الفعّال وسيلةً لإظهار المنظمة بصورةٍ جديدة أمامَ الأطراف الخارجية ذات العلاقة بالمنظمة من هيئاتٍ إشرافية أو تشريعية، أو من مستثمرين حاليين ومحتملين، كما يمثّلُ نظام الرقابة الداخلية الفعّال دليلاً على نزاهة العمل الإداري في المنظمة، وضماناً معقولاً للدائنين والمقرضين، على أنَّ المنظمةَ قادرةٌ على تحقيق أهدافها، والمحافظة على مركزها المالي والائتماني، والوفاء بالالتزامات الحالية، والمستقبلية.

3-1-4 مكونات نظام الرقابة الداخلية:

تشيرُ لجنة (COSO) ومعيار التدقيق (315) إلى أنَّ الرقابةَ الداخلية تتكون من خمسة مكونات هي الآتية:

1. **<u>بيئة الرقابة:</u>** تحدّد بيئة الرقابة الموقفَ العمومي للمديرين، وفلسفة الإدارة تجاه نظام الرقابة الداخلية، وأهميته في المنظمة، حيث إنَّ موقفَ الإدارة هو الذي سيحدّدُ جوهرَ الرقابة الفعالة، فإذا كانت الإدارة العليا تعتقد أنَّ الرقابةَ هامة سيشعر العاملون بذلك، وسيستجيبون لمتطلبات الرقابة الداخلية، وتشملُ عوامل البيئة الرقابية النزاهةَ، والقيم الأخلاقية، وكفاءة أفراد المنظمة، فلسفة الإدارة وأسلوب التشغيل، الطريقة التي تحدّد بها الإدارة السلطة ، والمسؤولية ، وتنظّم وتطوّر موظفيها، والاهتمام، والتوجيه المقدمين من مجلس الإدارة. [116]

وبالتالي يمكنُ تحديد مكونات بيئة الرقابة بالعناصر الآتية:[117]

---

[114] دهيليس، أيوب، بوطريفة، أيوب، 2018، **<u>دور المراجع الداخلي في تحسين نظام الرقابة الداخلية في المؤسسات الاقتصادية</u>**، رسالة ماجستير، جامعة أكلي محند أولحاج، الجزائر، ص: 52.

[115] بوعبد الله، فريدة، منومس، شيماء، 2020، **<u>مرجع سبق ذكره</u>**، ص: 61.

[116] Kegerreis, Mike, Schiller, Mike, Davis, Chris, 2020, **<u>Op cit.,</u>** P: 938.

[117] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **<u>Op cit.,</u>** p:304

أ. فلسفة الإدارة، وأسلوب عملها، ومدى تقبلها للمخاطرة.

ب. الالتزام بالنزاهة، والقيم الأخلاقية، والكفاءة.

ج. متابعة تنفيذ إجراءات الرقابة الداخلية من قبل مجلس الإدارة والمكلفين بالحوكمة.

د. الهيكل التنظيمي.

هـ. طرق تحديد السلطة والمسؤولية.

و. معايير الموارد البشرية التي تجذب الأفراد الأكّفاء، وتنميهم وتحتفظ بهم.

ز. التأثيرات الخارجية وتوصيات الجهات الإشرافية.

2. **تقييم المخاطر :** تواجهُ كلّ منظمة مجموعةً متنوعةً من المخاطر من المصادر الخارجية والداخلية، حيثُ ينبغي على الإدارة تقييم تلك المخاطر والسعي لإبقاء تلك المخاطر ضمنَ الحدِّ المقبول، حيثُ يقومُ تقييم المخاطر على تحديد، وتحليل المخاطر ذات الصلة بعمل المنظمة، ونظراً لأنَّ الظروفَ الاقتصادية، والصناعية، والتنظيمية، والتشغيلية ستستمرّ في التغيير، وبالتالي هناك حاجةً إلى آلياتٍ لتحديد المخاطر الخاصّة المرتبطة بالتغيير، والتعامل معها في الوقت المناسب.[118]

كما يجبُ أن تأخذَ الإدارة نظرةً شاملةً للمخاطر على مستوى المنظمة ، وتقييم احتمالية المخاطر، وتأثيرها بالإضافة إلى تكاليف، وفوائد الاستجابات المطلوبة لتلك المخاطر، حيث يمكن للإدارة أن تستجيبَ للمخاطر بإحدى الطرق الأربع[119]:

- تقليلُ المخاطر: أي تقليل احتمالية، وتأثير المخاطر من خلال تطبيق نظام فعال للرقابة الداخلية .
- قبولُ المخاطر: تقبّل احتمالية، وتأثير المخاطر، وذلك لضعفِ تأثيرها، وارتفاع تكلفة الاستجابة لها مقارنةً بالمنفعة الناجمة عن التصدي لتلك المخاطر.
- مشاركةُ المخاطر: مشاركة المخاطر، أو تحويلها إلى شخص آخر عن طريق التأمين، أو الاستعانة بمصادر خارجية، أو الدخول في معاملات تحوط .
- تجنبُ المخاطر: تجنب المخاطر من خلال عدمِ الانخراط في النشاط الذي ينتج عنه، حيثُ يتطلب ذلك من المنظمة بيعَ قسم أو، الخروج من خط الإنتاج، أو عدم التوسع كما هو متوقّعٌ.

3. **أنشطة الرقابة:** تضمُّ أنشطة الرقابة السياسات والإجراءات التي تساعد على ضمان تنفيذ توجيهات الإدارة، فيما يتعلقُ الإجراءات اللازمة لمعالجة المخاطر وبالتالي تحقيق أهداف المنظمة، حيثُ تدخل أنشطة الرقابة في جميع أنحاء المنظمة وعلى جميع المستويات، وفي جميع الوظائف، وتشملُ مجموعةً من الأنشطة المتنوعة

[118] Kegerreis, Mike, Schiller, Mike, Davis, Chris, 2020, **Op cit.,** P: 938.
[119] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p:309

مثل ترخيصِ العمليات، والتفويضات، والتحقق، والتسويات، ومراجعات الأداء التشغيلي، وأمن الأصول، وفصل المهام.[120]

حيثُ تشملُ أنشطة الرقابة مجموعةً من الإجراءات تشمل:

أ. التفويض المناسب للمعاملات والأنشطة.

ب. الفصل بين الواجبات.

ج. تطوير المشروع، وضوابط الاستحواذ.

د. تغيير ضوابط الإدارة.

هـ. تصميم، واستخدام الوثائق والسجلات.

و. حماية الأصول، والسجلات، والبيانات.

ز. ضوابط مستقلة على الأداء.

4. **المعلومات والتوصيل:** إنَّ الغرضَ الأساسي من نظام معلومات المحاسبية هو جمعُ، وتسجيل، ومعالجة، وتخزين، وتلخيص ، ونقل المعلومات، ويتضمنُ ذلك فهمَ كيفية بدء المعاملات، والتقاط البيانات، والوصول إلى الملفات وتحديثها، ومعالجة البيانات، والإبلاغ عن المعلومات، إذ توفّر هذه العناصر مساراً تدقيقاً، مما يسمحُ بتتبع الإجراءات بين نشأت المعاملات، والبيانات المالية الناتجة عنها، كما يجبُ تصنيف المعاملات بشكلٍ صحيحٍ، وتسجيل المعاملات بقيمتها النقدية المناسبة، وفترة الجرد المناسبة، وتقديم المعاملات والإفصاحات ذات الصلة بشكلٍ صحيح في البيانات المالية.[121]

وبالتالي يجبُ تحديد المعلومات الهامة، والتقاطها، والإبلاغ عنها في شكلٍ، وإطارٍ زمنيّ مناسب يسمح للأطراف ذات العلاقة القيام بمسؤولياتهم، حيث تنتجُ أنظمة المعلومات تقاريرَ تحتوي على معلومات تشغيلية، ومالية تمكّن من إدارة العمل، والتحكّم به بشكلٍ فعّال، كما أنَّ بعضَ هذه الأنظمة لا تتعاملُ مع البيانات التي تمَّ إنشاؤها داخلياً فحسب، بل تتعاملُ أيضاً مع المعلومات المتعلقة بالأحداث، والأنشطة الخارجية، والظروف اللازمة لاتخاذ قرارات العمل التنبؤية، وإعداد التقارير الخارجية، ومن ثمّ يجبُ أن يحدثَ الاتصال الفعّال بمعنى أن تتدفقَ المعلومات عبرَ المستوياتِ المختلفة في المنظمة حتى يتلّقى جميع الموظفين رسالةً واضحةً من الإدارة العليا بأنَّ مسؤوليات الرقابة يجب أن تؤخذ على محمل الجد، كما يجب أن يفهمَ كلاً منهم دوره الخاص في نظام الرقابة الداخلية، وكذلك كيفية ارتباط الأنشطة الفردية بعمل الآخرين، وأن يكونَ لديهم وسيلةً لتوصيل المعلومات المهمة للمستويات الإدارية

[120]Kegerreis, Mike, Schiller, Mike, Davis, Chris, 2020, **Op cit.,** P: 938

[121] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p:318

المناسبة، كما يجب أن يكونَ هناك اتصالاً فعالاً مع الأطراف الخارجية، مثل العملاء والموردين، والمساهمين والجهات التشريعية، والتنظيمية المختصة.[122]

5. **أنشطة المراقبة:** تحتاج أنظمة الرقابة الداخلية إلى المراقبة، والتي تقوم بها الإدارة بهدف تحديد فيما إذا كانت الضوابط تؤدي الغرض من وضعها، وتتمثّل الرقابة بتقييم جودة أداء النظام بمرور الوقت، ويتم تحقيق ذلك من خلال أنشطة المراقبة المستمرة، أو التقييمات الدورية، أو مزيج منهما، حيث تحدث المراقبة المستمرة في سياق العمليات، وتشمل الأنشطة الإدارية، والإشرافية، والإجراءات الأخرى التي يقوم من خلالها الموظفون بأداء واجباتهم، أما التقييمات الدورية سيعتمد نطاقها بشكلٍ أساسي على تقييم المخاطر، وفعالية إجراءات المراقبة المستمرة، حيث يجب الإبلاغ عن أوجه القصور في الرقابة الداخلية في المراحل الأولية إلى الإدارة العليا، ومجلس الإدارة.[123]

3-1-5 مبادئ الرقابة الداخلية:

تمثّل مبادئُ الرقابة الداخلية التي نصّ عليها إطار عمل (COSO)، شرحاً أكثر تفصيلاً لمكونات نظام الرقابة الداخلية في المنظمة، والتي تحقق رقابةً داخلية فعالة تنطبقُ على جميع أهداف الرقابة الداخلية المختلفة، حيث تتكون هذه المبادئ من (17) مبدأً تفصيلياً ترتبط بالمكونات المختلفة للرقابة الداخلية: [124]

1. **المبادئ المتعلقة ببيئة الرقابة:** تعدُّ بيئة الرقابة العنصرَ الأساسي لجميع المكونات الأخرى، حيثُ يمثل الأفراد جوهرَ عمل المنظمة، و يمثل اتّصافهم بالنزاهة، والانضباط، والقيم الأخلاقية، والكفاءة الأساسَ الذي يقوم عليه نظام الرقابة الداخلية الفعّال، وبالتالي تتمثل المبادئ المتعلقة ببيئة الرقابة في الآتي:
   أ. الالتزام بالنزاهة، والقيم الأخلاقية في المنظمة.
   ب. استقلالية مجلس الإدارة لممارسة دورة الرقابة وتطوير الرقابة الداخلية في المنظمة.
   ج. تحدد الإدارة العليا مع إشراف مجلس الإدارة الهياكل والتسلسل الإداري والسلطات والمسؤوليات المناسبة من أجل تحقيق الأهداف.
   د. التزام المنظمة بجذب الأفراد الأكّفاء، وتنميتهم، والاحتفاظ بهم بما يتماشى مع الأهداف.
   هـ. تحميل الأفراد مسؤوليات الرقابة الداخلية في سبيل السعي لتحقيق الأهداف.
2. **المبادئ المتعلقة بتقييم المخاطر:** يجب على المنظمة تحديد، وتحليل، وإدارة المخاطر المحيطة بها، حيث تعدُّ عملية إدارة المخاطر عمليةً ديناميكية نظراً للتغييرات في البيئة الخارجية والداخلية، والتي قد تؤثر على تحقيق الأهداف، وبالتالي تتمثّل المبادئ المتعلقة بتقييم المخاطر في الآتي:

---

[122] Kegerreis, Mike, Schiller, Mike, Davis, Chris, 2020, **Op cit.,** P: 938
[123] Kegerreis, Mike, Schiller, Mike, Davis, Chris, 2020, **Ibid.,** P: 938
[124] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p: 304.

أ. تحدّد المنظمة الأهدافَ بوضوح حتى تتمكّن من تحديد، وتقييم المخاطر المتعلقة بالأهداف.

ب. تحدّد المنظمة المخاطرَ التي تهدّد تحقيق أهدافها، وتحلّل المخاطر كأساس لتحديد كيفية إدارة المخاطر.

ج. تأخذ المنظمة بعين الاعتبار إمكانيةَ الاحتيال عند تقييم المخاطر التي تهدّد تحقيق الأهداف.

د. تحدّد المنظمة، وتقيّم التغييرات التي يمكن أن تؤثّر بشكلٍ كبير على نظام الرقابة الداخلية.

3. **المبادئ المتعلقة بأنشطة الرقابة:** يتمّ تنفيذ أنشطة الرقابة على جميع المستويات، وفي كافةِ المراحل المختلفة لمعالجة العمليات في المنظمة، حيث تساعدُ سياسات، وإجراءات، وأنشطة الرقابة على ضمانِ تنفيذ الخطط التي حدّدتها الإدارة لمعالجة المخاطر، وتحقيق أهداف المنظمة بشكلٍ فعّال، وبالتالي تتمثّلُ المبادئ المتعلقة بأنشطة الرقابة في الآتي:

أ. تختار المنظمة، وتطوّر أنشطة الرقابة التي تساهمُ في التخفيفِ من المخاطر لتحقيق الأهداف إلى مستوياتٍ مقبولة.

ب. تختارُ المنظمة، وتطور أنشطة الرقابة على تكنولوجيا المعلومات لدعم تحقيق الأهداف.

ج. تنشر المنظمة أنشطة الرقابة من خلال السياسات التي تحدّد ما هو متوقعٌ، والإجراءات التي تضع السياسات موضعَ التنفيذ.

4. **المبادئ المتعلقة بالمعلومات والاتصالات:** يجبُ أن يتمّ الاتصال داخلياً وخارجياً لتوفير المعلومات اللازمة لتنفيذ أنشطة الرقابة الداخلية في المنظمة، حيثُ تقومُ أنظمة المعلومات والاتصالات بالتقاط، وتبادل المعلومات اللازمة لإجراء عمليات المنظمة، وإدارتها والتحكم فيها، وتتمثّل المبادئ المتعلقة بهذا العنصر في الآتي:

أ. تحصلُ المنظمة على معلوماتٍ عالية الجودة، أو تنتجها، وتستخدمها لدعم عمل المكونات الأخرى للرقابة الداخلية.

ب. تنقلُ المنظمة المعلومات داخلياً، بما في ذلك أهداف، ومسؤوليات الرقابة الداخلية، اللازمة لدعم عمل المكونات الأخرى للرقابة الداخلية.

ج. تتواصلُ المنظمة مع الأطراف الخارجية فيما يتعلق بالأمور التي تؤثّر على عمل الرقابة الداخلية.

5. **المبادئ المتعلقة بأنشطة المراقبة:** يجب مراقبة العملية بأكملها، وإجراء التعديلات حسبَ الحاجة، حيث تؤكّد التقييمات الدورية ما إذا كانَ كلّ عنصر من عناصر الرقابة الداخلية موجوداً، ويعملُ كما هو مخططٌ، وبالتالي يتم الإبلاغ عن أوجه القصور في الوقت المناسب إلى الإدارة العليا، ومجلس الإدارة، ويتفرّعُ عن هذا العنصر المبدأين الآتيين:

أ. تختارُ المنظمة، وتطوّر، وتنفّذ تقييمات مستمرة للتأكّد مما إذا كانت مكوناتُ الرقابة الداخلية موجودةً، وتعمل بالشكل الأمثل.

ب. تقوم المنظمة بتقييم أوجه القصور في الرقابة الداخلية وإبلاغها في الوقت المناسب لتلك الأطراف المسؤولة عن اتخاذ الإجراءات التصحيحية، بما في ذلك الإدارة العليا، ومجلس الإدارة، حسب الحاجة.

يلاحظُ الباحثُ أنَّ المبادئَ التي قدّمتها لجنة (COSO)، ماهي إلا شرحٌ مفصّلٌ لما يجب على الإدارة العليا مراعاته في كلّ عنصرٍ من عناصر نظام الرقابة الداخلية، من أجل تصميم، وبناء نظام رقابة داخلية فعال، يحقق متطلبات المنظمة ، ويدعم أهدافها واستراتيجياتها، ويتّصف بالمرونةِ، والقابلية للتطوير، والوضوح في التطبيق والإشراف، كما نلاحظُ أنَّ المبادئَ التي قدمتها لجنة (COSO) قد تطرقت بشكلٍ، أو بأخر إلى ضرورة ارتباط نظام الرقابة الداخلية بمتطلبات تكنولوجيا المعلومات، وأهمية وجود ضوابط، وأنشطة رقابية عليه لتحقيق أهدافه.

المبحث الثاني: مقومات نظام الرقابة الداخلية الفعال، والأساليب، والإجراءات، والمعايير المرتبطة به:

3-2-1 مقومات نظام الرقابة الداخلية في بيئة تكنولوجيا المعلومات:

يقومُ نظام الرقابة الداخلية على مجموعةٍ من المقومات، والركائز، والتي من خلالها يستطيعُ تحقيقَ أهدافه، تشمل هذه المقومات الآتي:

1. **هيكل تنظيمي كفء:** تختلفُ الخطة التنظيمية من منظمة إلى أخرى، فكلّ منظمةٍ يجب أن يكونَ لها هيكلٌ تنظيمي يتناسب مع الأهداف التي تتبناها، كما يجب على هذه لأهداف أن تتميزَ بالبساطةِ، والوضوح حتى يسهل فهمها، حيث يشير الهيكلُ التنظيمي المعقد، أو غير الواضح إلى مشاكلَ خطيرة، كصعوبةِ تعقب الهيكل التنظيمي متعدّد الطبقات، وبالتالي تسعى المنظمات اليوم إلى استبدال الهياكل الهرمية بهياكلَ تنظيمية مسطّحة، تضمّ فرقاً ذاتية القيادة يتم تزويدها بالأهداف النهائية والتوجه العام للمنظمة، وتتخذُ القرارات دونَ الحاجة إلى طبقاتٍ متعددة من الموافقات، وبالتالي فإنَّ هذا التغيير في الهياكل التنظيمية يؤثّر حتماً على طبيعة، ونوع نظام الرقابة الداخلية المستخدم.[125]
2. **نظام محاسبي سليم:** لتحقيق فاعلية الرقابة الداخلية، يجب أن يتّسمَ النظام المحاسبي بما يلي:[126]

- أن يقومَ النظام المحاسبي على المفاهيم، ومبادئ المحاسبية السليمة والتي تتّسم بالوضوح، والثبات.
- يتضمنُ النظام المحاسبي طرقاً، وأساليبَ، وإجراءات فنية لتحقق من جدّية العمليات المحاسبية، والتأكّد من دقتها وسلامة التبويب لها.
- اتباع مبدأ تقييم العمل، لتحقيق الفصل الملائم بين الواجبات والمسؤوليات.
- يجب أن يعتمدَ النظام المحاسبي على مجموعةٍ مناسبة من التقارير، والقوائم المالية.

---

[125] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p:306

[126] بوعبد الله، فريدة، منومس، شيماء، 2020، **مرجع سبق ذكره**، ص: 62.

3. **كفاءة الأفراد وتنميتهم والاحتفاظ بهم:** إنَّ فعاليةَ نظام الرقابة الداخلية في تحقيق أهدافها لا يقتصرُ فقط على تنظيمٍ محاسبي سليم ،وتنظيم إداري ملائم، لكن يجب أن توفّرَ المنظمة مجموعةً من الموظفين ورؤساء الإدارات العاملين بالمنظمة من ذوي الدرجات العالية في الكفاءة.[127]

وبالتالي يجبُ تعيين الموظفين على أساسِ الخلفية التعليمية، والخبرة، والإنجازات، والصدق، والنزاهة، وتلبية متطلبات العمل، كما يجبُ أن يخضعَ جميع موظفي المنظمة، بما في ذلك طاقم التنظيف، والموظفين المؤقتين لسياسات التوظيف، حيث من الممكن أن يتظاهرَ بعض المحتالين بكونهم عمالَ نظافةٍ، أو موظفين مؤقتين للوصول المادي إلى أجهزة كمبيوتر المنظمة، كما ويجب أن توضّح برامج تدريب الموظفين الجدد مسؤولياتهم، وسياسات المنظمة وإجراءاتها، وثقافتها، وأسلوب عملها، حيث يمكنُ تدريب الموظفين من خلال إجراء مناقشاتٍ غير رسميةٍ، واجتماعات رسمية، وإصدار مذكرات دورية، وتوزيع مبادئ توجيهية مكتوبة، ومدونات لأخلاقيات المهنة، ونشر تقارير عن السلوك غير الأخلاقي، وعواقبه، وتعزيز برامج التدريب على ضوابط الأمن، مما يساعدُ الموظفين على مواجهة التحديات الجديدة، والتكيّف مع التقنيات المتغيرة، والتعامل بفعالية مع البيئة المتطورة.[128]

4. **مستويات ومعايير أداء سليمة:** تؤثّر سلامةُ الواجبات، والوظائف في كلّ قسمٍ بدرجة كبيرة على فعالية الرقابة الداخلية، وعلى كفاءة العمليات المنجزة في المنظمة، حيث يجبُ أن تشملَ الإجراءات الموضوعة الخطوات التي يتم بمقتضاها اعتماد العمليات، وتسجيلها والمحافظة على الأصول، كما يجب أن تمدَّ مستويات الأداء بالوسائل التي تضمنُ دقةَ اتخاذ القرارات، والتسجيل، كما أنَّ كفاءةَ العاملين الذين تمَّ توظيفهم بالمنظمة لا يعني التخلي عن توافر معايير لقياس أداء العاملين، وذلك لمحاولة المقارنةِ بين الأداء المخطّط مع الأداء الفعلي، وتحديد الانحرافات، والإجراءات الواجب اتخاذها لتصحيح الانحرافات.[129]
5. **تحديد الصلاحيات والمسؤولية بدقة ووضوح:** يجب أن تتأكّدَ الإدارة من فهم الموظفين لأهداف المنظمة وغاياتها، وتحديدِ السلطات والمسؤوليات الممنوحة للإدارات والأفراد، ومحاسبةِ الأفراد على تحقيقها، وتشجيع استخدام المبادرة لحل المشكلات، حيث يتمّ تعيين السلطات، والمسؤوليات المتصلة بها باستخدامِ التوصيفات الرسمية للوظائف، وتدريبِ الموظفين، وجداول التشغيل، ومجموعة السياسات، والإجراءات المكتوبة، والتي تمثّلُ مرجعاً أساسياً، ومفيداً أثناءَ العمل للموظفين الحاليين، وأداةً مفيدةً لتدريب الموظفين الجدد.[130]
6. **إسناد مهام الرقابة الداخلية لمجلس الإدارة والمسؤولين عن الحوكمة مباشرةً:** يجبُ أن يضمَّ مجلس الإدارة أعضاءً يتمتعون بالمهارات، والخبرة اللازمة، لطرح أسئلةٍ استقصائيةٍ، ومساءلة مستمرة للإدارة العليا، كما يجب أن يضمّ مجلس الإدارة عدداً كافياً من الأعضاء المستقلين عن الإدارة العليا حتى يتمكّن مجلس الإدارة من

---

[127] حاج قويدر، قورين، 2019، **مرجع سبق ذكره**، ص: 37.

[128] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** (2021), p:307

[129] غزال، مصباح، سعيد، عمر، مهاوه، صدام حسين، 2018، **مرجع سبق ذكره**، ص: 15.

[130] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p:306

تقييم الأداء بموضوعية، ويمكن لأعضاء مجلس الإدارة استكمالَ خبراتهم من خلال تعيين مستشارين خارجيين على سبيل المثال: قد يحتاجونَ إلى مساعدةٍ في تقييم مستوى أمن المعلومات، وسلامة المعالجة، والتوافر، والسرية، والخصوصية لأنظمة معلومات المنظمة، وذلك حتى يكون مجلس الإدارة مستعداً، وقادراً على اتخاذ أي إجراءاتٍ ضرورية لحماية مصالح المساهمين، والأطراف ذات العلاقة.[131]

يرى الباحث أنَّ مقومات نظام الرقابة الداخلية، تشملُ المنظمة بجميع أبعادها التنظيمية، والتنفيذية، ابتداءً من الإطار الذي يحدّد التنظيم الإداري في المنظمة، ومن ثمّ استقطاب، وتوظيف الكفاءات، والخبرات المناسبة، ودور الإدارة في عملية التخطيط، وتحديد إجراءاتٍ تضمنُ تنفيذَ الخططِ بوضوح، ليتمّ بعد ذلك الإشراف على كافة المستويات الإدارية وفقَ ما تمَّ إعطاءه من صلاحياتٍ، ومسؤوليات لكلِّ فردٍ، ولا تتحقق أهداف نظام الرقابة الداخلية في المنظمة إلا بإسنادِ وظائف الرقابة الداخلية إلى مجلس إدارة مستقل يسمحُ بوجودِ حوكمةٍ فعّالة في المنظمة.

3-2-2 أساليب وإجراءات الرقابة الداخلية في بيئة تكنولوجيا المعلومات:

3-2-2-1 أساليب الرقابة الداخلية الملائمة في بيئة تكنولوجيا المعلومات:

تتعدّدُ أساليبُ الرقابة الداخلية غير التقليدية التي تمَّ تصميمها خصيصاً لمواجهة التحديات التي تفرضها بيئة تقنية المعلومات على المنظمة، وقد حدّدت معايير التدقيق مجموعتين رئيستين من أساليب الرقابة في ظلّ بيئة تكنولوجيا المعلومات وهي **أساليبُ الرقابة على التطبيقات**، و**أساليب الرقابة العامة**، ونتيجةً لذلك يتوجبُ أن يكونَ المبرمج على علمٍ بالأمور المالية، والمحاسبية، أو أن يعملَ ضمن فريق عمل يضمّ مختصين في مجال المحاسبة المالية ليتمكّن من وضع نظام، أو برمجة النظام بشكلٍ يمنعُ اختراقه.

1. **<u>أساليب الرقابة على التطبيقات:</u>** تعملُ ضوابطُ التطبيقات على منعِ، وكشفِ، وتصحيح أخطاء المعاملات والاحتيال في البرامج، والتطبيقات الالكترونية، وهي معنيّةٌ بدقة، واكتمال، وصلاحية، وتفويض البيانات التي تمَّ التقاطها، وإدخالها ، ومعالجتها، وتخزينها، ونقلها إلى أنظمةٍ أخرى، والتقرير عنها.[132]

تشتملُ أساليب الرقابة على التطبيقات على ثلاث عناصر هي الآتي:

أ. **أساليب الرقابة على المدخلات:** يتمّ تصميم الرقابة على المدخلات للتأكّد من كافةِ المعلومات التي تمّ تشغيلها بواسطة نظام المعلومات، وأن تتسمَ بالصحةِ، والاكتمال، والدقة، وتعدُّ هذه الرقابةُ مهمة جداً، لأنّ الجزءَ الأكبرَ من الخطأ في نظم المعلمات الالكتروني ينتجُ عن أخطاء المدخلات، وتهدفُ إلى توفير درجة معقولة من صحةِ اعتماد البيانات، ومن سلامةِ تحويلها بصورةٍ تمكّن نظام المعلومات من التعرّف عليها، ومن عدمِ فقدانها، أو الإضافة إليها، أو حذف جزء منها، أو طبع صورة منها، أو عمل أي تعديلات غير مشروعة في البيانات

---

[131] غزال، مصباح، سعيد، عمر، مهاوه، صدام حسين، 2018، **<u>مرجع سبق ذكره</u>**، ص: 15.

[132] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **<u>Op cit.</u>**, p:298

المرسلة، وتتعلّقُ أساليب الرقابة على المدخلات برفضِ تصحيح، وإعادةِ إدخال البيانات السابق رفضها، ويفضل اختبار مدخلات البيانات في مرحلةٍ مبكرةٍ من مراحل معالجتها، وتتضمنُ أساليب الرقابة على المدخلات:[133]

- **الفحص بالعين:** وهو التدقيقُ الذي يقوم به الموظفُ المعني على البيانات الداخلة فمثلاً: عادةً ما يقول الكاتب في قسمِ أوامر البيع بفحصِ الأمر الذي يصل إليه من العميل، ويدقق في كلّ مفردات البيانات المطلوبة، والتأكّد من صحة رقم صنف المنتج، أو البضاعة.
- **تصميم جيد للمستندات:** يشجّع على تسجيلِ بياناتٍ كاملة، وصحيحة عن العمليات المطلوبة تسجيلها، حيث يفترضُ أن توجدَ في المستندات تعليماتٍ واضحة، ومسافات مناسبة، وواضحة لكتابة البيانات المستندة؛
- **سجل المستندات:** حيث تسجل فيه المستندات الواردة قبل عملية التشغيل والخارجة بعد عملية التشغيل، بذلك يمكن تتبع حركة المستندات، والرقابة عليها، ومن أمثلة سجل المستندات (دفتر اليومية، المتحصلات النقدية، سجل الأجور والمرتبات).
- **ترميز الحسابات:** وهو نظامٌ لإعطاءِ رموز معينة (حروف وأرقام) لكلّ الحسابات التي تتضمنها خريطة الحسابات في الوحدة الاقتصادية، ويساعدها على تسجيل العمليات، وتتّبع البيانات والتأكّد من استخدام إجراء التشغيل المناسب.

ب. **أساليب الرقابة على معالجة البيانات:** بعدَ إتمامِ خطوة إدخال البيانات إلى نظام المعلومات، والتأكّد من صحتها، تبدأُ عملية التشغيل داخلَ نظام المعلومات بواسطة البرمجية التي تمثّلُ الصندوقَ الأسود بالنسبة لمشغل النظام، حيثُ لا يمكن رؤية ما يحدث داخل الحاسب الآلي، وإنما تقتصرُ قدرته الرقابية على تدقيق الناتج بعد عملية التشغيل، ولذلك فإنَّ معظمَ الوسائل الرقابية التي يمكن استخدامها خلالَ مرحلةِ التشغيل عادةً تكون مجهزةً داخل البرمجية ذاتها، وهذا يقعُ على عاتق المبرمج الذي يحاولُ تصميم البرمجية المعينة بقدراتٍ معينة لمنع، وتصحيح الأخطاء تلقائياً، وبصورةٍ ذاتية، ونتيجة لذلك من الضروري أن يكون المبرمج على علم بالأمور المالية، و المحاسبية ليتمكّن من وضع نظامٍ، أو برمجية نظام بشكلٍ يمنعُ اختراقه من الناحية المحاسبية (الفنية).[134]

ج. **أساليب الرقابة على المخرجات:** تركّزُ أساليب الرقابة على المخرجات على إبراز أي خطأ بعدَ إتمام عملية التشغيل، وليس على منع الخطأ كما هو الحال في الرقابة على المدخلات، وعلى عمليات التشغيل، ولذلك تتمثّل أهمّ طرق الرقابة على المخرجات في التدقيق ببيانات الناتج النهائي، وتحديد مدى معقوليتها بواسطة أحد

---

[133] بوعبد الله، فريدة، منومس، شيماء، 2020، **مرجع سبق ذكره**، ص: 74.

[134] موسى بن عيسى، بومدين، مكي، 2019، **دور نظام المعلومات المحاسبي في تعزيز الرقابة الداخلية**، رسالة ماجستير، جامعة محمد بوضياف، الجزائر، ص: 33.

أعضاء فريق العمل، أي الخبرة، والدراية، و المعرفة الكافية بالمعلومات التي يتضمنّها ناتج عمليات التشغيل ويتمّ ذلك عن طريق إجراءِ عدد من الاختبارات للبيانات في ناتج المخرجات أهمها:[135]

- **اختبار الدقة الحسابية:** وهو اختبارٌ صغيرٌ بواسطة إجراء بعض العمليات الحسابية البسيطة للتأكّد من دقةِ، وصحة التشغيل، مثال على ذلك التأكّد من أنّ صافي دخل كلّ موظفٍ، ومجموع الاقتطاعات من مرتبه مساوي لإجماليّ دخله، وأيضاً أنَّ مجموعَ صافي دخول جميع العاملين بالإضافةِ إلى إجمالي الاقتطاعات مساوي لإجمالي المرتبات التي يتمّ صرفها للعاملين.
- **اختبار المعقولية:** من خلال هذا الاختبار يمكن التأكّد من دقة العمليات إذا أظهرَ المخرج النهائي لنظام المعلومات بعض البيانات غير المتسقة، مثال ذلك أن يظهرَ الناتج عددَ ساعات العمل لأحد الموظفين يتعدى الحد الأقصى المسموح به دونَ احتساب هذه الساعات الزائدة باستخدام معدّل الأجر الصافي، كما أنّه يمكن تحديدُ الخطأ إذا تعدّى مثلاً قيمة الراتب الحد المتعارف عليها لفئةٍ معينة من العاملين.
- **اختبار الشمولية والاكتمال:** ويتضمنُ هذا الاختبار إبراز أي أخطاء تتعلقُ بنقصٍ في أحد مجالات البيانات المطلوبة، مثال ذلك كشف الرواتب يجب التأكد من ظهور جميع البيانات الضرورية عن كلّ عامل، أو موظف مثل الاسم، العنوان، عدد ساعات العمل العادية، عدد ساعات العمل الإضافية، اسم القسم الذي يعمل فيه، عدد سنوات الخبرة، وما إلى ذلك من البيانات المطلوبة بواسطة المنظمة.

2. **<u>الأساليب الرقابة العامة:</u>** يتمّ تطبيق أساليب الرقابة العامة للتأكّد من أنَّ بيئةَ الرقابة في المنظمة مستقرةٌ، وتضمن حسنَ إدارة الموارد، و أمن البنية التحتية لتكنولوجيا المعلومات، وضوابط اقتناء البرامج، وتطويرها وصيانتها، تتمثّل هذه الأساليب فيما يلي:[136]

أ. **أساليب الرقابة على العاملين:** يعتمدُ تشغيل نظام المعلومات إلى حدٍّ كبيرٍ على الأفراد في إدارة عمليات النظام نفسه، عندَ إدخال البيانات، والإشراف على معالجة هذه البيانات في أجهزة الكمبيوتر، ومن ثم توزيعُ المخرجات على المختصين المصرّح لهم بتسليم هذه التقارير، ويتمّ استخدام أساليب الوقاية المعتمدة للتأكّد من سلامة أداءِ كافة هذه الوظائف، تتمثّل أساليب الرقابة المتعلقة بالعاملين في الآتي:

- **الفصل بين الواجبات:** تتطلب الرقابة الداخلية الجيدة عدمَ إعطاء موظفٍ واحد الكثيرَ من الصلاحيات والمسؤوليات عن المعاملات، أو العمليات التجارية، أي إنه يجب ألا يكونَ الموظف في وضعٍ يسمحُ له بارتكابِ الاحتيال، وإخفائه، يتمّ تحقيق الفصل الفعّال لواجبات المحاسبة عند فصل الوظائف التالية :[137]

– التفويضُ: اعتماد المعاملات، والقرارات.

---

[135] بوعبد الله، فريدة، منومس، شيماء، 2020، **<u>مرجع سبق ذكره</u>**، ص: 75.

[136] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **<u>Op cit.</u>**, p:298

[137] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **<u>Ibid.</u>**, p:312

- التسجيلُ: إعداد وثائق العمليات، وإدخال البيانات في أنظمة الكمبيوتر، والحفاظ على المجلات، أو دفاتر الأستاذ أو الملفات، أو قواعد البيانات.
- الجيازة: التعامل مع النقد، أو الأدوات، أو المخزون، أو الأصول الثابتة، واستلام شيكات العملاء الواردة، أو كتابة الشيكات.

كما يجبُ أن تقومَ المنظمة بالفصل بين الواجبات المتعلقة بالأنظمة، حيث يشملُ الفصل بين واجبات الأنظمة 7 وظائفَ هي الآتية:

- التفويضُ: اعتماد المعاملات، والقرارات المتعلقة بالتعديل على عناصر نظام المعلومات.
- إدخال البيانات: وظيفةُ إدخال البيانات مسؤولةٌ عن إدخال البيانات لجميع المعاملات التجارية، وإنشاءِ جميع حسابات المستخدمين الجدد، وجميع علاقات العمل الجديدة بعد الموافقة على إنشائها من قبل المسؤول عن التفويض.
- البرمجة: مسؤولون عن تطوير، وترميز، واختبار جميع تطبيقات البرامج الجديدة، كما أنّهم مسؤولون عن تعديل جميع التطبيقات الموجودة، ولكن يحتاجونَ بالضرورة إلى موافقةٍ لبدءِ أنشطة تطوير البرنامج، أو تعديله، كما يجبُ الموافقة على منتجاتهم النهائية من قبل المخولين بتفويض مثل تلك العمليات.
- العمليات: يقومُ مشغلو الكمبيوتر بتشغيل البرنامج على أجهزة الكمبيوتر، والتأكّد من إدخال البيانات بشكلٍ صحيح، ومعالجتها بشكلٍ صحيح، وتخزينها بشكل صحيح، وإنتاج المخرجات المطلوبة، كما قد تكونُ وظيفة العمليات مسؤولةً أيضاً عن معالجة التحديثات المعتمدة للحسابات الرئيسية مثل تغييرات العنوان للعملاء والموردين وغيره.
- تخزين البيانات: وظيفةُ تخزين البيانات هي المسؤولةُ عن التخزين المادي، والحفاظ على قواعد بيانات المنظمة ، والملفات، وبرامج الكمبيوتر، كما أنَّهم مسؤولون عن الاحتفاظ بنسخٍ احتياطية للبيانات الأساسية خارجَ موقع العمل في مكان آمن، أي إنّهم يحتفظون بالعهدة المادية لعناصر أجهزة تكنولوجيا المعلومات اللازمة للعمليات ومعالجته، بالإضافة إلى أنَّهم مسؤولون أيضاً عن حفظِ مخرجات نظام المعلومات.
- المستخدمون: يقومُ المستخدمون بتسجيلِ المعاملات، وتفويضِ البيانات لمعالجتها، والوصولِ المادي إلى بيانات المنظمة، وإنتاج مخرجات النظام، كما أنَّهم مسؤولون عن حفظ أي بياناتٍ يمكنهم الوصول إليها، أو توزيعها كمخرجات للنظام.
- مديرو قواعد البيانات: مسؤولون عن تنسيقِ قاعدة البيانات، والتحكم فيها، وإدارتها.

وبالتالي فإنَّ السماحَ لشخصٍ ما بأداء وظيفتين، أو أكثر من الوظائف السبع الموضّحة قد يعرّضُ المنظمة للاحتيال.

- **منح الموظفين إجازاتهم السنوية:** من أفضلِ أساليب الرقابة الوقائية هو الإصرارُ على أن يأخذَ الموظف إجازتَه السنوية، مما يحرم هذا الموظف من فرصةِ محاولة إخفاء التلاعب.

ب. **أساليب الرقابة على نظام المعلومات المحاسبية من قبل مدققي النظم:** إنَّ عمليةَ تدقيق النظام ماهي إلا وسيلةٌ رقابيةٌ في حدِّ ذاتها فإنَّ معظمَ وسائلِ الرقابة على نظام المعلومات المحاسبية ما هو إلا إجراءٌ لا جدوى له ما لم تنفذ بشكلٍ صحيحٍ، وسليم، ولذلك تقعُ مسؤولية التأكد من سلامةِ تنفيذ هذه الإجراءات على المدقق ، ويساهمُ التدقيق في اكتشافِ مواطن القوة لنظام المعلومات، ومواطن الضعف فيه، والتي تتمثّل في وجودِ وسائل رقابية على التطبيقات المحاسبية، وقد تكون عملية تدقيق النظم فجائيةً، أو مخططةً.[138]

ج. **الاستعانة بفريق المراقبة:** يتكوّنُ فريق المراقبة من شخصٍ، أو أكثر يكون مسؤولاً عن إنشاءِ، واستخدام وسائل الرقابة على التطبيقات، والحثّ على اتباعها، ويختلفُ حجم وتكوين هذا الفريق من منظمةٍ إلى أخرى، وقد يقوم الفريق بأداء وظائف تماثلُ تلك التي يقوم بها قسمُ التدقيق الداخلي مثل أداءِ اختبارات صحّة تشغيل كلّ من الأجهزة، وبرامج الكمبيوتر. [139]

يرى الباحثُ أنَّ الأساليبَ السابقة تمثّلُ نموذجاً توضيحياً لما يمكن لإدارة المنظمة أن تتبنّاه عندَ بناءِ وتصميم نظام الرقابة الداخلية في بيئة تكنولوجيا المعلومات، أي إنّ الأساليبَ السابقة لا تعدُّ إطاراً متكاملاً، وإنَّما يمكن القول إنَّ هذه الأساليب تمثّلُ صورةً عامةً عن عمليات الرقابة الداخلية يمكن شرحها بشكلٍ أكثر تفصيلاً من خلال جملة من الإجراءات نوضّحها في فقرة إجراءات الرقابة الداخلية.

3-2-2-2 إجراءات الرقابة الداخلية:

حتى تتحقق الأهداف المرجوّة من الرقابة الداخلية في المنظمة يتوجّب على الإدارة العليا اتخاذَ إجراءات محاسبية وإدارية، تضمنُ من خلالها تحقيقَ فعالية الرقابة الداخلية، حيث تتضمّنُ هذه الإجراءات:[140]

1. **<u>الإجراءات التنظيمية، والادارية:</u>** وتتمثّلُ تلك الإجراءات بالآتي:

أ. تحديدُ الاختصاصات بقصد تجنب التداخل بين المسؤوليات مما يقلّل من احتمال وقوع حالات الغش، والأخطاء.

ب. توزيعُ الواجبات بين الموظفين بحيث لا ينفردُ أحدهم بعملٍ ما من بدايته إلى نهايته.

ج. توزيع المسؤوليات بشكلٍ واضح يساعدُ على تحديد الخطأ، أو الإهمال.

د. تقسيمُ العمل بين الموظفين بحيثُ يتم الفصل بين الوظائف.

هـ. تنظيمُ الأقسام بحيث يجتمعُ الموظفون الذي يقومون بعملٍ واحدٍ في مكان واحد.

---

[138] غزال، مصباح، سعيد، عمر، مهاوه، صدام حسين، 2018، **<u>مرجع سبق ذكره</u>**، ص: 24

[139] شريف، اسماعيل، 2020، **<u>تكنولوجيا المعلومات ودورها في تطوير نظام الرقابة الداخلية</u>**، جامعة الجفلة، مجلة الباحث للعلوم الرياضية والاجتماعية، المجلد 4 العدد 7، ص: 73.

[140] بوعبد الله، فريدة، منومس، شيماء، 2020، **<u>مرجع سبق ذكره</u>**، ص: 63.

و. إيجادُ خطة عمل معينة تتضمنُ خطوات كلّ عمليةٍ بالتفصيل بحيث لا يترك فرصةً لأي موظفٍ للتصرف الشخصي إلا بموافقةِ شخص آخر مسؤول.

ز. إجراءُ حركة تنقلات بين الموظفين من حين لآخر، بحيث لا يتعارضُ ذلك مع حسن سيرِ العمل.

ح. ضرورةُ قيام كلّ موظفٍ بإجازته السنوية دفعةً واحدة، وذلك لإيجاد الفرصة لمن يقوم بعمله أثناءَ غيابه لاكتشاف أي تلاعبٍ في ذلك العمل.

2. **<u>الإجراءات المحاسبية:</u>** وتتمثّلُ تلك الإجراءات بالآتي:

أ. إثباتُ العمليات المحاسبية على النظام المحاسبي فورَ حدوثها، للتقليلِ من فرص الغش، والتلاعب، ولإبقاء المعلومات التي ينتجها النظام محدثةً، وتعكس الواقع كما هو.

ب. عدمُ إثبات أي عمليةٍ في النظام المحاسبي قبلَ اكتمال كافة الوثائق المؤيّدة لها.

ج. عدمُ إشراك موظف في تدقيق عملٍ قام به، بل يجب أن يتم تدقيقه من قبل شخصٍ آخر.

د. استعمالُ إجراءات آلية للضبط الحسابي للآلات المحاسبية مما يقلّلُ من احتمالات الخطأ، ويقودُ إلى السرعة في الإنجاز.

هـ. إجراءُ مطابقاتٍ دورية بين الكشوف الواردة من الخارج، وبين التقارير التي يقدّمها النظام المحاسبي.

و. القيامُ بجردٍ مفاجئ دورياً للنقدية، والبضاعة والاستثمارات، ومطابقة ذلك مع الأرصدة الدفترية.

3-2-3 المعايير، والأطر المرتبطة بنظام الرقابة الداخلية:

1. أطر عمل COSO (Committee of Sponsoring Organizations) للرقابة الداخلية وإدارة المخاطر:

تعدُّ لجنة المنظمات الراعية (committee of sponsoring organizations) مبادرةً مستقلة ترعاها المنظمات التالية: جمعيةُ المحاسبة الأمريكية (AAA)، والمعهدُ الأمريكي للمحاسبين القانونيين (AICPA)، ومعهدُ المديرين الماليين (FEI)، ومعهدُ المدققين الداخليين (IIA)، ومعهدُ المحاسبين الإداريين (IMA)، تأسّست هذه اللجنة عام 1985، لا تملك COSO سلطةَ وضع المعايير، ولكنها توفّر توجيهاتٍ، وإرشاداتٍ بشأنِ الرقابة الداخلية، وإدارة مخاطر المنظمة، حيثُ أصدرت أولَّ إطار عمل لها، والخاص بالرقابة الداخلية، وإدارة المخاطر في عام 1992 والذي تمَّ اعتمادُه من قبل العديدِ من المنظّمات لتقييم فعالية الرقابة الداخلية، لكن نتيجةً للتغيرات في بيئة العمل منذ إنشاء إطار عام 1992 والتقدم التكنولوجي الكبير، وتعقد بيئة الأعمال، أصدرت COSO إطارًا محدثًا للرقابة الداخلية في عام 2013، حيث يحتفظُ إطار عمل 2013 بالعديد من العناصر الأساسية لإطار عام 1992، بما في ذلك المكونات الخمسة للرقابة الداخلية (بيئة الرقابة، وتقييم المخاطر، وأنشطة الرقابة، والمعلومات والاتصالات، وأنشطة المراقبة)، إلا أنَّ إطارَ عمل 2013 يحوي مبادئَ تفصيلية (17 مبدأً) يقوم عليها كلّ مكونٍ من هذه المكونات، تمثّلُ هذه المبادئ المفاهيمَ الأساسية المتعلقة بأنظمة الرقابة الداخلية الفعّالة، كما تشملُ التغييرات

الإضافية "نقاط التركيز"، والتي تسلّط الضوء على الخصائص المهمة المتعلقة بكلّ من المبادئ السبعة عشر، كما يؤكّد إطار عمل 2013 على أهميةِ تطبيق ضوابط الرقابة الداخلية، ويوسّع أهداف التقارير عن نظام الرقابة الداخلية ليشملَ أهدافاً داخلية، وغير المالية،[141]

2. تقرير SAC (Systems Auditability and Control):

تقريرُ رقابة، وتدقيقِ الأنظمة الخاص بقسم الأبحاث التابعة لمعهد المدققين الداخليين الأمريكي، حيثُ عرف تقرير (SAC) الرقابة الداخلية، ووصف مكوناته، وقدّم عدة تصنيفاتٍ للضوابط الرقابية، كما وصفَ أهداف الرقابة والمخاطر، وعرّف دور المدقق الداخلي، وقد قدّم التقرير إرشاداتٍ بالنسبة للاستخدام، والمعالجة، وحماية مصادر تكنولوجيا المعلومات، حيث عرّف التقرير نظام الرقابة الداخلية على "أنّه مجموعةٌ من العمليات، والوظائف، والأنشطة، والنظم الفرعية، والأشخاص يعملون معاً من أجل ضمانِ تحقيق الأغراض، والأهداف"، وقد ركّزَ التقريرُ على دور، وأثر نظم المعلومات المحوسبة على نظام الرقابية الداخلية، كما ركّز على الحاجةِ إلى تقييم المخاطر، والأخذ بعين الاعتبار التكاليف، والمنافع، وبناء ضوابط رقابية في النظم بدلاً من إضافتها بعد التطبيق، وبموجبِ التقرير تمَّ تحديد مكونات نظام الرقابة الداخلية في ثلاثة عناصر:[142] بيئة الرقابة، النظم اليدوية والمؤتمنة، الإجراءات الرقابية، وتشملُ **بيئة الرقابة** على الهيكلِ التنظيمي، وإطار الرقابة، والسياسات والإجراءات، والتأثيرات الخارجية، وتتكون **النظم المؤتمتة** من نظم، وتطبيقات البرمجيات (Software) ، وقد قدّمَ التقرير خمسَ خططٍ تصنيفية **للضوابط الرقابية الداخلية** في نظم المعلومات: (1) المانعة، والكاشفة، والمصححة (2) الاختيارية، وغير الاختيارية (3) التطوعية، والاجبارية (4) اليدوية، والمؤتمتة و (5) التطبيق، والضوابط الرقابية العامة. تركّز هذه الخطط على متى تطبّق الرقابة، وما إذا كان بالإمكان تخطي الرقابة في البرمجيات. أما بالنسبة لأهداف الرقابة، والمخاطر، فإنَّ المخاطرَ تشتمل على الاحتيال، والأخطاء، والاختلالات في الأعمال، والاستخدام غير الكفء، والفاعل للموارد. فالأهدافُ الرقابية تخفّض من هذه المخاطر، وتضمنُ، وتؤكّد تمامَ، وسلامة المعلومات، والتزامها بالقوانين الرقابية بالنسبة للمدخلات، والعمليات التشغيلية، والمخرجات والبرمجيات. أمّا مقاييسُ الأمان، فتشملُ الضوابط الرقابية للبيانات، والأمور المتعلقة بالالتزام، والتطابق، والتوافق مع القوانين والتشريعات، والمعايير المحاسبية، ومعايير التدقيق، والسياسات، والإجراءات الداخلية.

3. نموذج بازل (BASEL) للرقابة الداخلية البنكية:

وتشكّلت لجنة بازل تحت مسمّى لجنة التنظيمات، والإشراف والرقابة البنكية بهدف تقوية استقرار، وسلامة الأنظمة البنكية، وتكونت من مجموعة العشرة، وهي كل من: بلجيكا، كندا، فرنسا، ألمانيا، إيطاليا، اليابان، الولايات المتحدة

---

[141] Lawson, Bradley, Muriel, Leah, Sanders, Paula, 2017, **A survey on firms' implementation of COSO's 2013 Internal Control–Integrated Framework**, Research in Accounting Regulation, USA, p: 2

[142] غزال، مصباح، سعيد، عمر، مهاوه، صدام حسين، 2018، **مرجع سبق ذكره**، ص: 28

الأمريكية، المملكة المتحدة، السويد، هولندا، قامت هذه اللجنة بتقديم تقريرها الأوّل عام 1988 تحت مسمّى متطلبات بازل(1)، إذ ركّزت على قياس نسبة كفاية رأس المال، من خلال قسمة إجمالي رأس المال على الموجودات المرجّحة لمواجهة نوعاً محدداً من المخاطر يدعى المخاطر الائتمانية، وفي عام 1999 تمَّ تعديل اللجنة من أجل قياس مخاطر السوق، وفي عام 2004 أصدرت تقريرها الثاني الذي يدعى متطلبات بازل (2) والذي قدّم مناهجَ جديدة لقياس مخاطر الائتمان، وكذلك معالجة نوع جديد من المخاطر يدعى مخاطر التشغيل، وفي عام 2010 قدّمت اللجنة تقريرها الثالث تحت مسمّى لجنة بازل (3) وذلك بسبب الأزمة الاقتصادية في سنة 2008 التي عصفت بالبنوك حيثُ أعلنت إفلاسها على إثرها ممّا جعل اللجنة تعيد النظر في الاتفاقية (2) إذ إنّه لا بدَّ للبنوك أن تكونَ أكثرَ صلابةً أمامَ الأزمات، والنكبات الاقتصادية.[143]

يتكوّن نظام الرقابة الداخلية حسبَ لجنة بازل من مجموعةٍ من المكونات، والمتمثّلة في الآتي:[144]

أ. **الإشراف الإداري وثقافة الرقابة:** يضمُّ هذا المكوّن ثلاثةَ مبادئ والمتمثلة في:

المبدأ الأول: ينصُّ على:

- يجب أن يكونَ مجلسُ الإدارة مسؤولاً عن المتابعة بصورة دورية لاستراتيجيات الأعمال والسياسات الهامة للبنك.
- يجب أن يكونَ مجلسُ الإدارة مسؤولاً عن فهم المخاطر الأساسية، وتحديد المستويات المقبولة لهذه المخاطر، وضمان أن تتخذَ الإدارة العليا الخطوات اللازمة لتحديد، وقياس، ومتابعة الرقابة على هذه المخاطر.
- يجب أن يكونَ مجلسُ الإدارة مسؤولاً عن الموافقة على الهيكل التنظيمي.
- يجب أن يكونَ مجلسُ الإدارة مسؤولاً عن ضمان بأنَّ الإدارةَ العليا تقوم بمتابعة فعالية نظام الرقابة الداخلية.
- يتحمّلُ مجلسُ الإدارة المسؤوليةَ الكاملةَ عن ضمانِ وضع نظام كافٍ وفعّال للرقابة الداخلية، والحفاظ عليه.

المبدأ الثاني: ينصُّ على:

- يجب أن تكونَ الإدارةُ العليا مسؤولةً عن تنفيذ الاستراتيجيات التي تمَّ الموافقة عليها من طرف مجلس الإدارة.
- يجب أن تكونَ الإدارة العليا مسؤولةً عن تطوير العمليات التي تقيس، وتراقب المخاطر التي يتعرّض لها البنك.
- يجب أن تكونَ الإدارة العليا مسؤولةً عن المحافظة على الهيكل التنظيمي الذي يحدّد بوضوح السلطات، والمسؤوليات وعلاقات الإبلاغ.
- يجب أن تكونَ الإدارة العليا مسؤولةً عن ضمان تنفيذ المسؤوليات تنفيذاً فعالاً.
- يجب أن تكونَ الإدارة العليا مسؤولةً عن وضع سياسات الرقابة الداخلية المناسبة.

---

[143] بن جودي، هجيرة، 2020، **إدارة المخاطر في البنوك التجارية وفق بازل (3)**، رسالة ماجستير، جامعة محمد بوضياف، الجزائر، ص: 28.

[144] حاج قويدر، قورين، 2019، **مرجع سبق ذكره**، ص: 38.

- يجب أن تكونَ الإدارة العليا مسؤولةً عن متابعة مدى كفاية، وفعالية نظام الرقابة الداخلية.

المبدأ الثالث: ينصُّ على:

- يتحمّل مجلسُ الإدارة والإدارة العليا مسؤوليةَ تعزيزِ معايير الأخلاق والنزاهة، وإرساء ثقافة داخل البنك التي تؤكّد، وتبرهن لجميع مستويات الموظفين على أهميةِ نظام الرقابة الداخلية.
- يجب على جميع الموظفين في البنك أن يفهموا دورَهم في عملية الرقابة الداخلية، وأن يشاركوا مشاركةً كاملةً في هذه العملية.

ب. **الاعتراف بالمخاطر، وتقييمها:** يضمُّ هذا المكوّن المبدأ التالي:

المبدأ الرابع: ينصُّ على:

- يتطلّبُ نظام الرقابة الداخلية الفعال تحديدَ المخاطر المادية التي تؤثّر سلباً على تحقيق أهداف البنك، بحيث يجب الاعتراف بها، وتقييمها بصورةٍ مستمرة.
- يجب أن يشملَ التقييم جميعَ المخاطر التي يواجهها البنك.

ج. يحتاجُ نظام الرقابة الداخلية إلى تعديلٍ بشكل مناسب لمعالجة أيّ مخاطر جديدة، أو غير مضبوطة سابقاً.

د. **أنشطة الرقابة وفصل المسؤوليات:** يضمُّ هذا المكوّن المبدئين التاليين:

المبدأ الخامس: ينصُّ على:

- يتطلّبُ نظام الرقابة الداخلية الفعال وجودَ هيكل رقابة مناسب.
- يجب أن تكونَ أنشطة الرقابة جزءاً لا يتجزأ من الأنشطة اليومية للبنك.

المبدأ السادس: ينص على:

- يتطلّبُ نظام الرقابة الداخلية الفعال وجودَ فصل مناسب للمسؤوليات.
- يجبُ تحديد مجالات التداخل بين المسؤوليات، والعمل على التقليل منها، وإجراء متابعة مستقلة لها.

هـ. **الاتصالات والمعلومات:** يضمُّ هذا المكون ثلاثةَ مبادئ، والمتمثلة فيما يلي:

المبدأ السابع: ينصُّ على:

- يتطلّبُ نظام الرقابة الداخلية الفعال وجودَ ما يكفي من البيانات الداخلية المتعلقة بالجانب المالي، والتشغيلي والامتثال للوائح، والقوانين، وكذلك معلومات السوق الخارجية حولَ الأحداث، والشروط ذات الصلة باتخاذ القرار.

- يجب أن تكونَ المعلومات موثوقةً وفي الوقت المناسب، وأن تقدّمَ بشكلٍ متّسق.

المبدأ الثامن:

- ينصُّ على أنَّ نظام الرقابة الداخلية الفعال يتطّلبُ وجودَ أنظمة معلومات موثوقة تغطي جميعَ الأنشطةِ الهامة.

المبدأ التاسع:

- ينصُّ على أنَّ نظامَ الرقابة الداخلية الفعّال يتطلّب وجودَ قنوات اتصال فعّالة للتأكّد من أنَّ جميعَ الموظفين لديهم الفهمَ الكافي حولَ السياسات، والإجراءات، والالتزام بها، وأنَّ المعلومات الأخرى ذات الصلة تصلُ إلى الموظفين المناسبين.

و. **متابعة الأنشطة وتصحيح نقاط الضعف:** يضمُّ هذا المكون ثلاثةَ مبادئ، والمتمثلة فيما يلي:

المبدأ العاشر: ينصُّ على:

- يجب متابعة فعالية الرقابة الداخلية للبنك بشكلٍ مستمرّ.
- يجب أن تكونَ عملية متابعة المخاطر الرئيسية جزءاً من الأنشطة اليومية التي يقوم بها البنك، فضلاً عن عملياتِ التقييم الدورية التي تجريها دوائر الأعمال، والتدقيق الداخلي.

المبدأ الحادي عشر: ينصُّ على:

- يجب أن يكونَ التدقيق الداخلي فعّالاً، وشاملاً لنظام الرقابة الداخلية، والذي يقوم به موظفون مستقلون من الناحية التشغيلية ومدربون تدريباً مناسباً.
- التدقيق الداخلي يعتبرُ جزءاً من عملية متابعة نظام الرقابة الداخلية، ويجب أن تقدّمَ تقاريره مباشرة إلى مجلس الإدارة، أو إلى لجنة التدقيق التابعة له، بالإضافة إلى تقديم التقارير للإدارة العليا.

المبدأ الثاني عشر:

- ينصُّ على أنَّ نقاط الضعف يتمّ تحديدها من طرف دوائر الأعمال، التدقيق الداخلي، أو موظفي الرقابة الآخرين، بحيث يجب الإبلاغ عنها في الوقت المناسب إلى المستويات الإدارية المناسبة، ومعالجتها فوراً.

ز. **تقييم نظام الرقابة الداخلية من قبل السلطات الإشرافية:** ينصُّ هذا المكوّن على المبدأ التالي:

المبدأ الثالث عشر: ينصُّ على:

يتعيّن على السلطات الإشرافية أن يطلبوا من جميع البنوك بغضّ النظر عن حجمها، أن يكونَ لديها نظاماً فعّالاً للرقابة الداخلية يتناسبُ مع طبيعة تعقيد المخاطر الملازمة في أنشطته داخلَ، وخارج الميزانية، والتي تستجيب للتغييرات في بيئة البنك، وظروفه.

–في حال ملاحظة السلطات الإشرافية بأنَّ نظامَ الرقابة الداخلية غير كافٍ، أو غير فعّال بالنسبة للمخاطر التي تواجه البنك (لا يغطي جميعَ المبادئ المذكورة سابقاً) ، يجب على السلطات الإشرافية أن تتخذَ الإجراءات المناسبة.

4. مقارنة بين الأطر المختلفة لنظام الرقابة الداخلي الصادرة عن الهيئات ذات الصلة:

يعرضُ الجدول (3-1) الآتي مقارنةً بين المعايير المختلفة لنظام الرقابة الداخلي الصادرة عن الهيئات ذات الصلة:

الجدول (3-1): جدول المقارنة بين المعايير المختلفة للرقابة الداخلية.

	COSO	SAC	BASEL
أصحاب العلاقة الأساسيين	الإدارة	المدققون الداخليون	المسؤولين عن الحوكمة في المصارف.
اعتبار الرقابة الداخلية على أنها:	عملية	مجموعة من العمليات، والنظم الفرعية والناس	مجموعة من العمليات
أهداف الرقابة الداخلية مؤسسياً	عمليات تشغيلية كفؤة وفاعلة، وإبلاغ مالي موثوق به، والالتزام بالقوانين والتشريعات	عمليات تشغيلية كفؤة وفاعلة، وإبلاغ مالي موثوق به، والالتزام بالقوانين والتشريعات	عمليات تشغيلية بنكية كفؤة وفاعلة، وإبلاغ مالي موثوق به، والالتزام بالقوانين والتشريعات
المكونات أو المجال	المكونات : الرقابة، والبيئة، والمخاطر، الإدارة، والأنشطة، المعلومات والاتصالات، والمراقبة	المكونات : الرقابة، والبيئة، والنظم اليدوية، والإجراءات الرقابية	المكونات: الإشراف الإداري وثقافة الرقابة، الاعتراف بالمخاطر وتقييمها، أنشطة الرقابة، وفصل المسؤوليات، الاتصالات، والمعلومات، متابعة الأنشطة، وتصحيح نقاط الضعف، تقييم نظام الرقابة الداخلية من قبل السلطات الإشرافية
التركيز	المنشأة بشكل كامل	تكنولوجيا المعلومات	القطاع المصرفي
فاعلية الرقابة الداخلية المقيمة	الإدارة	الإدارة	الإدارة

المصدر: من إعداد الباحث.

المبحث الثالث: مواجهة مخاطر تكنولوجيا المعلومات في ظل نظام الرقابة الداخلية:

3-3-1 أثر تكنولوجيا المعلومات على نظام الرقابة الداخلية:

كان لبيئة الأعمال الحديثة والتي انتقلت فيها المنظمات من العمل اليدوية التقليدية إلى بيئة نظم المعلومات الالكترونية منعكسات إيجابية، وأخرى سلبية على بيئة الرقابة الداخلية في المنظمة، حيثُ نعرض فوائدَ، ومخاطر تكنولوجيا المعلومات على نظام الرقابة الداخلية وفقاً للآتي:[145] [146]

بشكلٍ عام تعود تكنولوجيا المعلومات بالفائدة على الرقابة الداخلية للمنظمة حيثُ تمكّن المنظمة من القيام بما يلي:

- تحقيقُ الاتساق في تطبيق قواعد العمل المحددة مسبقاً، وأداء العمليات الحسابية المعقّدة مع معالجة أحجام كبيرة من المعاملات أو البيانات.
- تحسينُ توقيت إصدار المعلومات ، وإتاحتها ودقتها.
- تسهيلُ التحليل الإضافي للمعلومات.
- تعزيزُ القدرة على متابعة أداء أنشطة المنظمة، وسياساتها، وإجراءاتها.
- الحدُّ من خطر التحايل على أدوات الرقابة.
- تعزيزُ القدرة على تحقيق الفصل الفعال به الواجبات عن طريق تطبيق أدوات رقابة أمنية في التطبيقات، وقواعد البيانات، ونظم التشغيل.
- إمكانية استفادة الحاسب الآلي في تحقيق الرقابة الذاتية على كلّ عمليات التشغيل اليومية.
- الإمكانيات الضخمة لتخزين البيانات في صورة ملفات إلكترونية تغني عن الكثيرِ من الملفات، والسجلات اليدوية.

في المقابل، تتسبّب تكنولوجيا المعلومات في مخاطر معينة للرقابة الداخلية الخاصة بالمنظمة، من بينها على سبيل المثال ما يلي:

- الاعتمادُ على النظم، أو البرامج التي تعالج البيانات بشكل غير دقيق، أو تنتج بيانات غير دقيقة، أو تقوم بكلا الأمرين.
- الوصولُ غير المصرّح به للبيانات، مما قد يؤدّي إلى إتلاف هذه البيانات، أو إلى حدوث تغييراتٍ غير سليمة فيها، بما في ذلك تسجيل معاملات غير مصرّح بها، أو غير موجودة، أو تسجيل غير دقيق للمعاملات، وقد تنجمُ مخاطر معينة عندما يتمكّن عدّة مستخدمين من الوصولِ إلى قاعدةِ بياناتٍ مشتركة.

---

[145] دهيليس، أيوب، بوطريفة، أيوب، 2018، **مرجع سبق ذكره**.

[146] الهيئة السعودية للمحاسبين القانونيين، 2020، **المعايير الدولية للمراجعة والفحص والتأكيدات الأخرى والخدمات ذات العلاقة**، المملكة العربية السعودية، ص: 235

- إمكانيةُ حصول موظفي تقنية المعلومات على امتيازاتِ وصول تتعدى تلك اللازمة لأداء المهام الموكّلة إليهم مما يترتّب عليه تعطّل الفصل بين الواجبات.
- التغييرات غير المصرّح بها في بيانات الملفات الرئيسية.
- التغييرات غير المصرّح بها في النظم، أو البرامج.
- احتماليةُ فقدان البيانات، أو عدم القدرة على الوصول إلى البيانات عند الحاجة.
- الحاسبُ غير قادر على التفكير، أو الحكم الشخصي وبالتالي يمكن حدوث أخطاء، ما لم توجد إجراءات للرقابة على البرامج.
- تتطلّب بيئة تكنولوجيا المعلومات ضرورةَ توفّر خبراتٍ، ومؤهلاتٍ معينة مع ضرورة التدريب المستمر للأفراد لمواكبة التطورات الحديثة في مجال تكنولوجيا المعلومات.

3-3-2 تطور نظام الرقابة الداخلية لمواجهة مخاطر تكنولوجيا المعلومات:

أصبحَ تطوير نظام الرقابة الداخلية يتطلب فهماً شاملاً لقدرات تكنولوجيا المعلومات و مخاطرها، حيثُ من الممكن أن يساعدَ المحاسبون، ومطورو الأنظمة الإدارة في تحقيق أهدافهم الرقابية من خلال:[147]

1. تصميم أنظمة رقابة فعالة تتخذ نهجاً استباقياً للقضاء على تهديدات النظا،م أو تكتشف التهديدات، وتصحيحها عند حدوثها
2. تسهيل بناء عناصر التحكم في النظام في مرحلة التصميم الأولية بدلاً من إضافتها بعد الحدوث الفعلي للتهديد.

كما تشيرُ الأبحاث إلى أنّ الإدارةَ العليا بحاجة إلى إظهار دعمها لأمن المعلومات من أجل تقليل مخاطر تكنولوجيا المعلومات إلى الحدّ المقبول مما يسمحُ بتعزيز الرقابة الداخلية في المنظمة من خلال السلوكيات الآتية:[148]

- توفيرُ الموارد الكافية لأمن المعلومات.
- الإبلاغُ بانتظام عن أهميةِ أمن المعلومات.
- أن تظهرَ الإدارة العليا من خلال أفعالها، أنَّ أمنَ المعلومات يعدُّ أمراً مهماً.
- اعتمادُ نهج استباقي للتهديدات الأمنية المحتملة، بدلاً من الرد على المشكلات بعد حدوثها.
- تضمينُ مشكلات أمن المعلومات عندَ تقييم مخاطر أيّ أنشطة جديدة في المنظمة.

حيثُ يؤدي القيام بذلك إلى إنشاءِ وعي أمنيّ، وتعزيزِ الثقافة التنظيمية بحيثُ يعتقد جميع الموظفين أنَّ أمنَ المعلومات مهمٌّ جداً، ونتيجةً لذلك، يزدادُ امتثال الموظف لسياسات، وضوابط الأمن في المنظمة، كما يعملُ دعم الإدارة العليا الواضح لأمن المعلومات على تحسين تصميم نظام الرقابة الداخلية، مما يقلّل من عددِ نقاط الضعف

---

[147] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p:298

[148] بوعبد الله، فريدة، منومس، شيماء، 2020، **مرجع سبق ذكره**، ص: 73.

المتعلقة بأمن المعلومات، كما أنَّ النتيجةَ الأكثر أهميةً لدعم الإدارة العليا لأمن المعلومات هي تحسّنُ العلاقة بين وظائف أمن المعلومات ، والتدقيق الداخلي، والحدّ من معارك النفوذ بين الوظائف، وزيادة تبادل المعلومات فيما بينها، لأنَّ وجودَ التناغم بين وظيفتي أمن المعلومات، والتدقيق الداخلي تحسّن من جودةِ أمن المعلومات، وترفعُ من فعالية نظام الرقابة الداخلية من خلال[149]:

- حمايةُ المنظمة من وقوع هجمات قد تتسبّب في ضررٍ ماديّ للمنظمة.
- الكشف في الوقت المناسب عن الهجمات قبل أن تتسبب في ضررٍ جسيم، لأنَّ حجمَ الضرر الناجم عن العديد من الانتهاكات الأمنية الكبرى في السنوات الأخيرة يرجع جزئياً إلى أنَّ المنظمات المتضررة لم تكن تعلم حتى أنّها تعرضت للهجوم منذ شهور، أو حتى سنوات.
- اتخاذ إجراءاتٍ تصحيحية فعّالة، تساعدُ على التعافي السريع في حال حدوث انتهاكاتٍ فعلية لأمن المعلومات.

3-3-3 نظام الرقابة الداخلية في ظل استخدام التقنيات الحديثة:

ظهرَ حديثاً بعض التقنيات الحديثة التي من الممكن أن تتبنّاها المنظمات في بيئة الأعمال الحديثة، كالحوسبة السحابية، والمحاكاة الافتراضية، وانترنت الأشياء، حيث تفرضُ هذه التقنيات على المنظمات العديدَ من التحديات في سبيل تأمينها، وحمايتها من التهديدات، والمخاطر المحيطة بها، ومع ذلك يرى بعضُ الباحثين أنّه إذا ما تمَّ الاستجابة لمتطلبات، وضوابط أمن تلك التقنيات فإنَّها تمثّلُ فرصةً إضافيةً للمنظمة في تدعيم فعالية نظام الرقابة الداخلية، حيثُ تناقش بعض تلك الدراسات سبلَ دعم فعالية نظام الرقابة الداخلية باستخدام الحوسبة السحابية، باعتبار أنَّ تطبيقَ الحوسبة السحابية ينطوي على العديد من المنافع واسعة النطاق بعيدة المدى، فهي ليست مجردَ حلّ تقنيّ، أو خادم تمَّ تخزينه في موقع آخر، بل هي آليةٌ هامةٌ تساعدُ على رفعِ كفاءة ، وفعالية نظام الرقابة الداخلية، وذلك في حالِ مراعاة متطلباتها، وأمن الحوسبة السحابية، حيثُ من الممكن أن تؤثّرَ الحوسبة السحابية على كافةِ عناصر نظام الرقابة الداخلية وذلك وفق للآتي:[150]

1. بيئةُ الرقابة: تطبيقُ الحوسبة السحابية يساعدُ على تحسين التنظيم الداخلي للمنظمة، وإدارة التقلبات المتزايدة بشكل استراتيجي، كما يساعدُ على تحقيق الأهداف العامة للمنظمة، ويوفّرُ بياناتٍ قياسية عالية الجودة لتوقع المواقف المؤثّرة التي قد تعوقُ تحقيق المنظمة لأهدافها الاستراتيجية، والوصول إلى نفس الفئة من التكنولوجيا الموجودة لدى المنافسين الأكبر حجماً، والأكثر قوةً.
2. أنشطةُ الرقابة: تمكّن الحوسبة السحابية الموظّفين من العمل دونَ التقيّدِ بالوقت، أو المكان، وتجنّب الخطط المعقّدة لحل الأزمات حيثُ إنَّ حلَّ المشاكل الطارئة يقعُ على عاتقِ مزوّد الخدمة، كما توفّر الحوسبة السحابية

---

[149] Romney, Marshall, Steinbart, Paul, summers, Scott, Wood, David, 2021, **Op cit.,** p:299

[150] السيد عبد العزيز، سمرة، 2019، **أثر الحوسبة السحابية على فعالية نظام الرقابة الداخلية فى الشركات الصناعية الليبية**، جامعة قناة السويس، المجلة العلمية للدراسات التجارية والبيئية، العدد الأول، المجلد العاشر، مصر، ص: 200

مزيداً من المرونة لحركة الموظفين، وتمكنّهم من الوصول إلى التطبيقات عن طريق مجموعةٍ واسعة من المواقع الالكترونية الخدمية.

3. تقييم المخاطر: تطبيقُ الحوسبة السحابية يؤكّد على أنَّ السياسات والإجراءات المستخدمة لتقييم، ومعالجة المخاطر موثّقةٌ، وجميع الموظفين على علمٍ بها، وتساعدُ على تدفق المعلومات المرتبطة بأيّة مخالفات، أو اختراقات، كما تعدُّ الحوسبة السحابية آلية ملائمةً لتحديد، وتحليل، وتقييم المخاطر المرتبطة بمدى كفاية أنظمة استرجاع المعلومات في حال فشل الأنظمة التقليدية.
4. المعلومات والاتصالات: إمكانيةُ الوصول للبيانات دونَ المخاطر المرتبطة بالتخزين المادي، حيثُ يتمُّ إدارتها وتأمينها عن طريق مزودي الخدمة، وتعدُّ آليةً فعّالة لتقديم الموظفين لاقتراحاتهم، وتوصياتهم للإدارة العليا، وتوفّر الحوسبة السحابية قنواتَ اتصال لكافةِ الموظفين محدّدة، وفعّالة.
5. المتابعة: توفّر الحوسبة السحابية إجراءاتٍ ملائمة، ووقت مناسب لمراجعة، وتقييم عمل الأنشطة الرقابية بصورة منتظمة، والوصول لمواطن الضعف بنظام الرقابة الداخلية، واتخاذ الإجراءات التصحيحية اللازمة في الوقت المناسب، وتحسّن مراقبة المستندات، حيث إنَّ كلّ ملفات المنظمة موجودة في موقع مركزيّ واحد مما يسمحُ للجميع بالعمل على نسخةٍ مركزيةٍ واحدة، كما توفّرُ الحوسبة السحابية إجراءاتٍ رقابية مستمرة، ودورية للإدارة العليا من أجلِ متابعة أداء الموظفين لمهامهم، وواجباتهم.

ممّا سبقَ نلاحظُ أنَّ التقنيات التي يخلقها تطوّر بيئة تكنولوجيا المعلومات، ما هي إلا أدوات يمكن أن تكونَ لها نتائجٌ إيجابية على عناصر نظام المعلومات بشكلٍ عامّ، ونظام الرقابة الداخلية بشكلٍ خاصّ، ذلك إذا تمَّ استخدامها على نحوٍ جيد، ومراعات آليات، وضوابط أمن المعلومات المناسبة التي ترتبطُ بها من أجلِ مواجهة المخاطر الناتجة عن مواكبة التغيرات، والتطورات في بيئة تكنولوجيا المعلومات، والاتصالات الحديثة.

الفصل الرابع: الدراسة الميدانية.

المبحث الأول: منهجية الدراسة وأدوات جمع وتحليل البيانات:

4-1-1 منهجية الدراسة:

انطلاقاً من طبيعةِ الدراسة فإنَّ المنهجَ المتّبع هو المنهجُ الوصفيُّ التحليليّ، والذي تمَّ وفقاً للخطوات الآتية:

1. تكوينُ إطارٍ معرفيّ واسع حولَ مشكلة الدراسة، ومتغيراتها بالاعتماد على المصادر الثانوية للبيانات من أدبياتٍ، ودراساتٍ سابقة عربية، وأجنبية، والتشريعات، والإصدارات المهنية ذات صلة بضوابط أمن المعلومات، ونظام الرقابة الداخلية.

2. وضعُ فرضيات الدراسة التي تتمحّور حولَ تقديمِ إجابات لمشكلة الدراسة المتمثّلة في بيان دورِ الضوابط المختلفة لأمن المعلومات في تفعيل نظام الرقابة الداخلية.

3. الاعتماد على مصادر البيانات الأولية لاختبار الفرضيات، وذلك من خلال إعداد استبيان يخدم غرض الدراسة، وتوزيعه على أفراد عينتيّ الدراسة العينة الأولى من المدققين الخارجيين المستقلين المكلّفين بالتدقيق على المصارف التقليدية المدرجة في سوق دمشق للأوراق المالية لعام 2020م، أمّا العينةُ الثانية فكانت من لجان التدقيق والموظفين في المصارف من ضمن المدققين الداخلين، ومسؤولي الرقابة الداخلية، ومسؤولي أمن المعلومات.

4. جمعُ الاستبيانات إذ وزّع استبيان الدراسة بشكلٍ ورقي، وإلكتروني على عينةِ الدراسة، وبلغَ عددُ الإجابات المستردة (224) استبياناً تم إلغاء (24) منها لعدم جدّية الإجابات، أو وجودِ تناقض في الإجابات، حيثُ كانَ عدد الاستبيانات المستردة من العينة الأولى (34) استبياناً، أمّا عددُ الاستبيانات المستردة من العينة الثانية (166) استبياناً.

5. تحليلُ بيانات الاستبيان بالاعتمادِ على برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS-25) من خلال استخدام الأدوات الإحصائية اللّازمة لاختبار الفرضيات

6. الوصولُ إلى النّتائج البحثية، وتقديم مجموعة من المقترحات.

4-1-2 مجتمع وعينة الدراسة:

مجتمع الدراسة:

مجتمعُ الدراسة يعرّف بأنّه جميعُ مفرداتِ الظاهرة التي يدرسها الباحث، فهو جميعُ الأفراد الذين يمثّلون موضوعَ مشكلة الدراسة، وبناءً على مشكلة الدراسة الحالية، وأهدافها فإنَّ المجتمعَ المدروس يتكوّن من العاملين في جميع

المصارف التقليدية المدرجة في سوق دمشق للأوراق المالية بما فيهم المدقّقين الخارجين المستقلين المكلّفين بتدقيق الحسابات لتلك المصارف.

عينة الدراسة:

عينةُ الدراسة هي مجموعةٌ جزئية من مجتمع الدراسة، تحملُ صفاته المشتركة، حيث تمَّ تحديد عينة الدراسة، ضمنَ عيّنتين الأولى من المدققين الخارجيين المستقلين المكلّفين بالتدقيقِ على المصارف التقليدية المدرجة في سوق دمشق للأوراق المالية لعام 2020م، أمّا العينةُ الثانية فكانت من أعضاءُ لجان التدقيق، ومن الموظفين في المصارف ضمن الاختصاصات الآتية:

- المدققين الداخلين.
- مسؤولي الرقابة الداخلية.
- مسؤولي أمن المعلومات.

إذ وزّع استبيان الدَراسة بشكلٍ ورقي، وإلكتروني على عينة الدراسة، وبلغَ عددُ الإجابات المستردة (224) استبياناً تمَّ إلغاء (24) منها لعدم جدّية الإجابات، أو وجود تناقض في الإجابات، حيثُ كانَ عدد الاستبيانات المستردة من العينة الأولى (34) استبياناً، أمّا عددُ الاستبيانات المستردة من العينة الثانية (166) استبياناً.

3-1-4 أداة الدراسة:

تمَّ إعدادُ استبيان كأداة لجمع البيانات من المصدر الأصلي، إذ ضمَّ الاستبيانُ مجموعةً من الأسئلة قسمت إلى قسمين:

أولاً: بيانات عامة:

اشتملت على بياناتٍ عامّة للتعرّف على المجيب: الجنس، الفئة العمرية، المؤهل العلمي، التخصص، الصفة الوظيفية الخبرة العملية.

ثانياً: محاور الدراسة:

حيثُ ضمّت مجموعةً من الأسئلة قسّمت إلى ثلاثة محاور:

المحور الأول: الضوابطُ الوقائية لأمن المعلومات، ونظام الرقابة الداخلية، إذ تكّون المحور من (21) تساؤلاً حولَ استخدام المصارف للضوابط الوقائية لأمن المعلومات، و مدى إسهام تلك الضوابط في تحقيق أهداف نظام الرقابة الداخلية.

المحور الثاني: الضوابطُ الاستكشافية لأمن المعلومات، ونظام الرقابة الداخلية، إذ تكوّن المحور من (21) تساؤلاً حولَ استخدام المصارف للضوابط الاستكشافية لأمن المعلومات، و مدى إسهام تلك الضوابط في تحقيق أهداف نظام الرقابة الداخلية.

المحور الثالث: الضوابطُ التصحيحيّة لأمن المعلومات، ونظام الرقابة الداخلية، إذ تكوّن المحور من (20) تساؤلاً حول استخدام المصارف للضوابط التصحيحية لأمن المعومات، و مدى إسهام تلك الضوابط في تحقيق أهداف نظام الرقابة الداخلية.

حيثُ تمَّ استخدام مقياس ليكرت الخماسي كمقياس للإجابة على تساؤلات الاستبيان، حيثُ يعدُّ مقياس ليكرت الخماسي مقياساً ترتيبياً، ويتمّ التعامل معه أثناءَ التحليل مع أوزان كمية تقابل كلّ حالة من حالته يتمّ حسابها من خلال قسمة عدد الخيارات (5) على عدد المسافات بين الخيارات (4) وفي حالة المقياس الخماسي يساوي (0.8):

1= موافق بشدة، 2= موافق، 3= محايد، 4= غير موافق، 5= غير موافق بشدة.

يتمّ تفسير النتائج التي نحصل عليها بمختلف أنواعها كوسط، أو وسيط، وغيره وفق الجدول التالي:

المستوى:	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
القيمة الناتجة:	1.80 – 1	2.60 – 1.80	3.40 – 2.60	4.20 – 3.40	5 – 4.20

4-1-4 الأدوات الإحصائية المستخدمة في الدراسة:

قامَ الباحثُ باستخدام الأساليب الإحصائية التالية، بالاعتماد على الحزمة الإحصائية للعلوم الاجتماعية (SPSS) النسخة 25 لتحليل البيانات:

- اختبارُ كفاية حجم العينة: عن طريق اختبار (Kaiser-Meyer-Olkin) لكاملِ مفردات العينة، و لكلّ واحدةٍ من عينتي الدراسة بشكلٍ منفصل.
- قياسُ صدق، وثبات الدراسة: وذلك عن طريق معامل ألفا كرومباخ لمعرفة ثبات أداة الدراسة (التأكّد من أنَّ قيمته فوق 60%) وجذره لمعرفة صدق أداة الدراسة لكامل مفردات العينة، و لكلّ واحدة من عينتي الدراسة بشكلٍ منفصل.

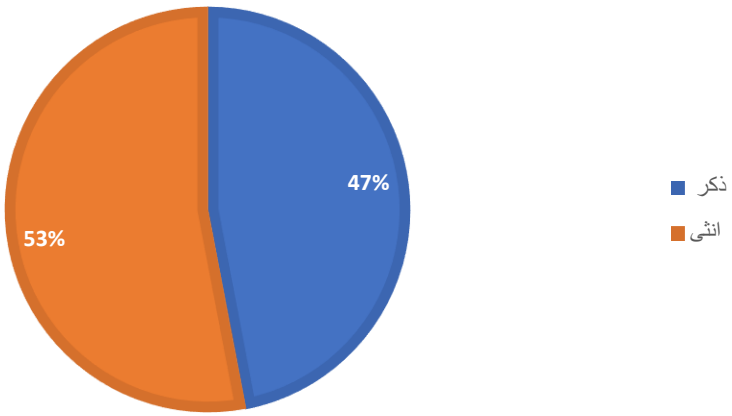
- اختبارُ التوزع الطبيعي: عن طريق اختبار (Kolmogorov–Smirnov) لكاملِ مفردات العينة، و لكلّ واحدة من عينتي الدراسة بشكلٍ منفصل.
- الإحصاءات الوصفية: لوصف العينة، ولمعرفة المتوسط الحسابي، والانحراف المعياري للمتغيرات الداخلة في الدراسة.
- اختبارُ وجود فروق ذات دلالة إحصائية بين إجابات عيّنتين الدراسة: عن طريق اختبار (Mann–Whitney) لعينتي الدراسة.
- الارتباط، والانحدار: دراسةُ علاقة الارتباط وقوتها، ونوعها عن طريق اختبار (Spearman) وذلك تمهيداً لدراسة الانحدار لمعرفة معنوية العلاقة، واختبار (Linearity Test) لاختبار خطيّة العلاقة، واختبارات (Curve Estimation) لمعرفة نوع العلاقة غير الخطيّة، بالإضافة لاختبار الانحدار الخطي البسيط.

المبحث الثاني: التحليل الإحصائي الوصفي والاختبارات الإحصائية لأراء عينتي الدراسة:

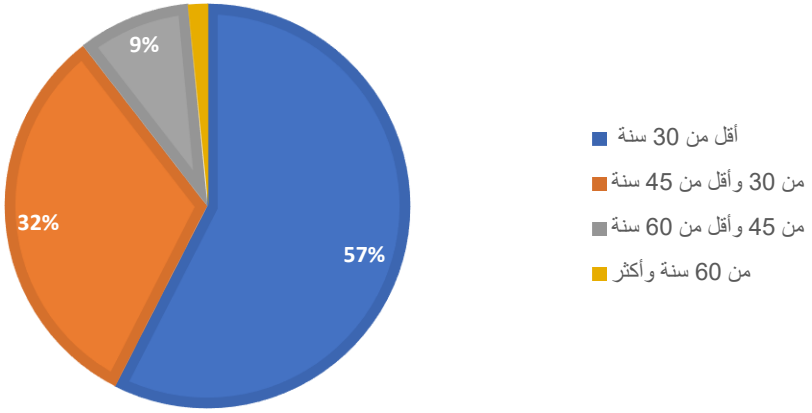
4-2-1 الوصف الإحصائي لعينة الدراسة وفق البيانات العامة:

يعرضُ الجدول (4-1) الآتي توزعَ كامل مفردات عينتي الدراسة وفقَ البيانات الديموغرافية التي تمَّ جمعها باستخدام البيانات العامة في الاستبيان، حيث يحدّد عددَ تكرار كلّ إجابةٍ، ووزنها النسبي، وذلك بحسب كلّ مجموعة من المتغيرات المحددة، للتعرّف على عناصر عينتي الدراسة وفق الآتي:

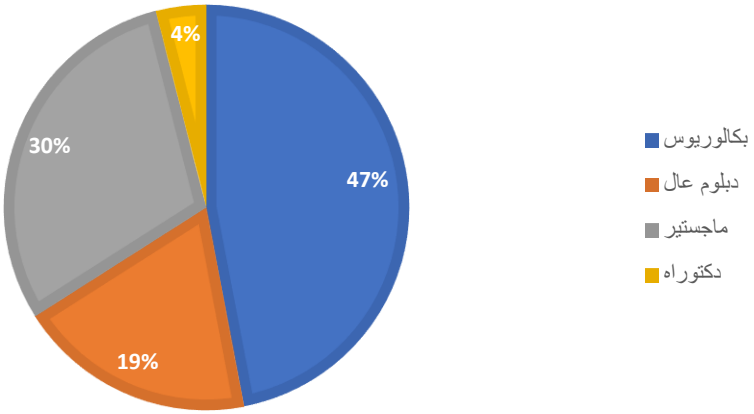
توزع عينتي الدراسة حسب الجنس:	الجنس	التكرار	النسبة المئوية
	ذكر	94	%47
	انثى	106	%53
	المجموع:	200	%100



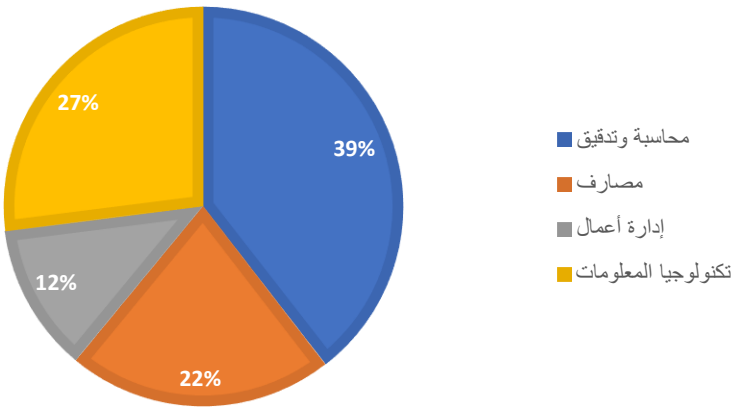
توزع عينتي الدراسة حسب الفئة العمرية:	الفئة العمرية	التكرار	النسبة المئوية
	أقل من 30 سنة	115	%57.5
	من 30 وأقل من 45 سنة	64	%32
	من 45 وأقل من 60 سنة	18	%9
	من 60 سنة وأكثر	3	%1.5
	المجموع:	200	%100



توزع عينتي الدراسة حسب المؤهل العلمي:	المؤهل العلمي	التكرار	النسبة المئوية
	بكالوريوس	94	%47
	دبلوم عالٍ	38	%19
	ماجستير	60	%30
	دكتوراه	8	%4
	المجموع:	200	%100

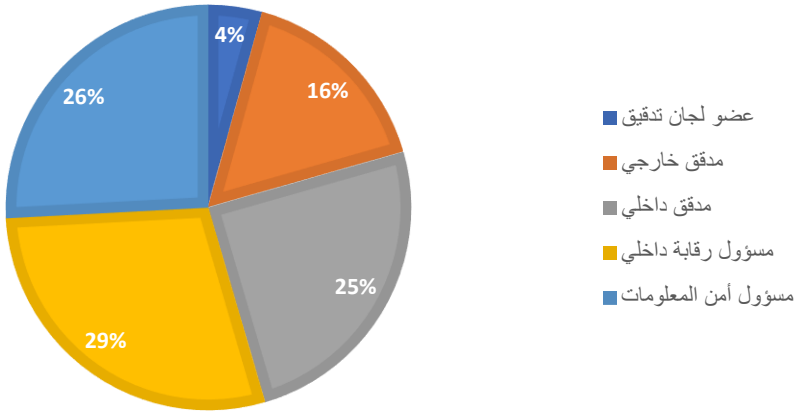


توزع عينتي الدراسة حسب التخصص:	التخصص	التكرار	النسبة المئوية
	محاسبة وتدقيق	79	%39.5
	مصارف	43	%21.5
	إدارة أعمال	24	%12
	تكنولوجيا المعلومات	54	%27
	المجموع:	200	%100

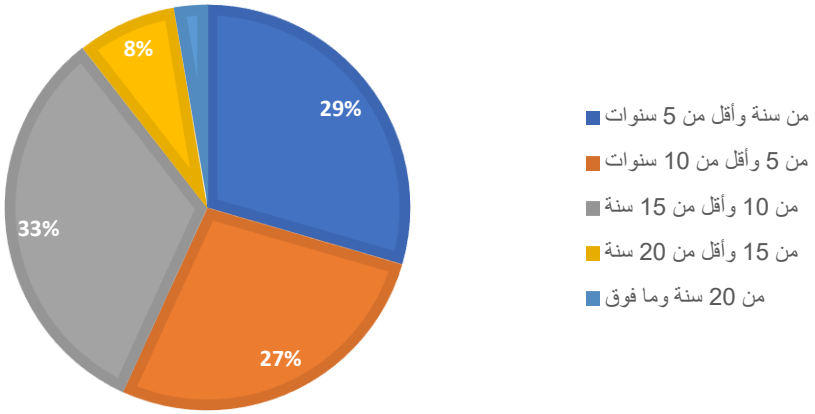


توزع عينتي الدراسة حسب الصفة الوظيفية:	الصفة الوظيفية	التكرار	النسبة المئوية
	مدقق خارجي	34	%17
	عضو لجان تدقيق	9	%4.5
	مدقق داخلي	52	%26
	مسؤول رقابة داخلية	60	%30

	مسؤول أمن المعلومات	45	%22.5
	المجموع:	200	%100



توزع عينتي الدراسة حسب الخبرة العملية:	الخبرة العملية	التكرار	النسبة المئوية
	من سنة وأقل من 5 سنوات	67	%33.5
	من 5 وأقل من 10 سنوات	62	%31
	من 10 وأقل من 15 سنة	47	%37
	من 15 وأقل من 20 سنة	18	%9
	من 20 سنة وما فوق	6	%3
	المجموع:	200	%100



الجدول (4-1) الوصف الإحصائي لكامل مفردات عينتي الدراسة وفق البيانات العامة في الاستبيان.

4-2-2 اختبار ثبات وصدق عينتي الدراسة:

اعتمدت الدراسةُ على أداةِ قياس الصدق الظاهري للتأكّد من صدقِ أداة جمع البيانات وجدواها، وفيما يتعلقُ بثبات أداة الدراسة تمّ استخدامُ معاملَ الاتساق الداخلي للتحقّق من ثبات الأداة حسبَ معامل ألفا كرونباخ، وجذر معامل الفا كرونباخ الذي يمثّلُ معامل الصدق، حيثُ تمَّ إجراء الاختبار بدايةً على كامل مفردات عينتيّ الدراسة، ومن ثمّ لكلّ واحدةٍ من عينتيّ الدراسة بشكلٍ منفصل، ويوضّحُ الجدولُ (4-2) معاملات ثبات الاتساق الداخلي إضافةً إلى معامل الصدق لكلٍّ من محاور الاستبيان، والاستبيان ككلّ، وذلك لكاملِ مفرداتِ عينتيّ الدراسة:

المحور	معامل ألفا كرونباخ	معامل الصدق
المحور الأول	0.850	0.921
المحور الثاني	0.627	0.791
المحور الثالث	0.621	0.788
كامل الاستبيان	0.850	0.921

الجدول (4-2) صدق أداة الدراسة وثباتها لكامل مفردات العينتين.

يلاحظُ أنَّ قيمَ معامل ألفا كرونباخ تراوحت بين (0.621) و (0.850) لمحاور الاستبيان، وأبعاده وكانت جميعُها أكبرَ من (0.60)، وبلغت قيمةُ المعامل للاستبيان ككل (0.850) أي إنه يمكن القول بأنَّ الاستبيانَ ذو درجةِ ثباتٍ عالية، أما بالنسبةِ لقيم معامل الصدق (الجذر التربيعي لمعامل الثبات) فنلاحظُ أنَّ القيمَ أيضاً مرتفعةٌ، و قيمته للاستبيان ككل كانت (0.921) مما يعني أنَّ الاستبيانَ صادقٌ، وممثّل للمجتمع الذي سحبت منه عينتيّ الدراسة.

أما الجدولُ (4-3) فيوضّح معاملات ثبات الاتساق الداخلي لمحاور الاستبيان إضافةً إلى معامل الصدق، وذلك لمفردات العينة الأولى (من المدققين الخارجيين):

المحور	معامل ألفا كرونباخ	معامل الصدق
المحور الأول	0.793	0.890
المحور الثاني	0.625	0.790
المحور الثالث	0.694	0.833
كامل الاستبيان	0.879	0.937

الجدول (4-3) صدق أداة الدراسة وثباتها لمفردات العينة الأولى.

يلاحظُ أنَّ قيمَ معامل ألفا كرونباخ فيما يتعلقُ بنتائج آراء العينة الأولى تراوحت بين (0.625) و (0.879) لمحاور الاستبيان وأبعاده ، وكانت جميعُها أكبرَ من (0.60)، وبلغت قيمةُ المعامل للاستبيان ككل (0.879) أي إنه يمكن

القول بأنَّ الاستبيانَ ذو درجةِ ثباتٍ عالية، أما بالنسبةِ لقيم معامل الصدق (الجذر التربيعي لمعامل الثبات) فنلاحظُ أنَّ القيمَ أيضاً مرتفعةٌ، و قيمته للاستبيان ككل كانت (0.937) مما يعني أنَّ الاستبيانَ صادقٌ، وممثّل للمجتمع الذي سحبت منه العينة الأولى.

بينما يعرضُ الجدولُ (4-4) معاملات ثبات الاتساق الداخلي إضافةً إلى معاملِ الصدق لمحاور الاستبيان والاستبيان ككل، وذلك لمفرداتِ العينة الثانية (من الموظفين في المصارف):

المحور	معامل ألفا كرونباخ	معامل الصدق
المحور الأول	0.696	0.834
المحور الثاني	0.597	0.772
المحور الثالث	0.604	0.777
كامل الاستبيان	0.843	0.918

الجدول (4-4) صدق أداة الدراسة وثباتها لمفردات العينة الثانية.

يلاحظُ أنَّ قيمَ معامل ألفا كرونباخ فيما يتعلقُ بنتائج آراء العينة الثانية تراوحت بين (0.604) و (0.843) لمحاور الاستبيان وأبعاده وكانت جميعُها أكبرَ من (0.60)، وبلغت قيمةُ المعامل للاستبيان ككل (0.843) أي إنّه يمكن القول بأنَّ الاستبيانَ ذو درجةِ ثباتٍ عالية، أما بالنسبةِ لقيم معامل الصدق (الجذر التربيعي لمعامل الثبات) فنلاحظُ أنَّ القيمَ أيضاً مرتفعةٌ، وقيمته للاستبيان ككل كانت (0.918) مما يعني أنَّ الاستبيانَ صادقٌ، وممثّل للمجتمع الذي سحبت منه العينة الثانية.

4-2-3 اختبار كفاية حجم العينة:

يستخدمُ اختبار كايزر- ماير- أولكن لحساب كفاية حجم العينة، واختبارُ ما إذا كانت الارتباطات الجزئية بين المتغيرات صغيرة، وتتراوحُ قيمة هذا الاختبار من (صفر إلى 1+) حيثُ تشيرُ القيم القريبة من (1+) إلى كفاية العينة، أو أنها مناسبةٌ، والقيمُ الأقلّ من (0.5+) تشيرُ إلى عدمِ كفاية حجم العينة، حيثُ تمَّ إجراءُ الاختبار بدايةً على كامل مفردات عينتيّ الدراسة، ومن ثمّ لكلِ واحدةٍ من عينتي الدراسة بشكلٍ منفصل، ويوضّحُ الجدول (4-5) اختبارَ كفاية حجم العينة، وذلك لكاملِ مفردات عينتيّ الدراسة:

.674	**Kaiser-Meyer-Olkin Measure of Sampling Adequacy.**
2876.012	**Bartlett's Test of Sphericity Approx. Chi-Square**
1891	**Df**
.000	**Sig.**

الجدول (4-5): اختبار كايزر- ماير- أولكن لكامل مفردات العينتين.

من الجدول السابق نجدُ أنَّ قيمةَ اختبار كايزر – ماير – أولكن لكاملِ مفردات العينتين بلغ (0.674) وهو أكبرُ من (0.5) وبالتالي حجم العينتين معاً يكون كافياً بشكلٍ معنوي.

بينما يعرضُ الجدولُ (4–6) اختبارَ كفاية حجم العينة، وذلك لمفردات العينة الأولى (من المدققين الخارجيين):

.811	Kaiser–Meyer–Olkin Measure of Sampling Adequacy.
100.528	Bartlett's Test of Sphericity Approx. Chi–Square
6	Df
.000	Sig.

الجدول (4-6): اختبار كايزر– ماير– أولكن لمفردات العينة الأولى.

من الجدول السابق نجدُ أنَّ قيمةَ اختبار كايزر – ماير – لمفردات العينة الأولى بلغَ (0.811) وهو أكبرُ من (0.5) وبالتالي حجمُ العينة الأولى يكون كافياً بشكلٍ معنوي.

فيما يعرضُ الجدولُ (4–7) اختبارَ كفاية حجم العينة، وذلك لمفردات العينة الثانية (من الموظفين في المصارف):

.830	Kaiser–Meyer–Olkin Measure of Sampling Adequacy.
419.790	Bartlett's Test of Sphericity Approx. Chi–Square
6	Df
.000	Sig.

الجدول (4-7): اختبار كايزر– ماير– أولكن لمفردات العينة الثانية.

من الجدول السابق نجدُ أنَّ قيمةَ اختبار كايزر – ماير – أولكن لمفردات العينة الثانية بلغَ (0.830) وهو أكبرُ من (0.5) وبالتالي حجم العينة الثانية يكون كافياً بشكلٍ معنوي.

4–2–4 اختبار التوزيع الطبيعي:

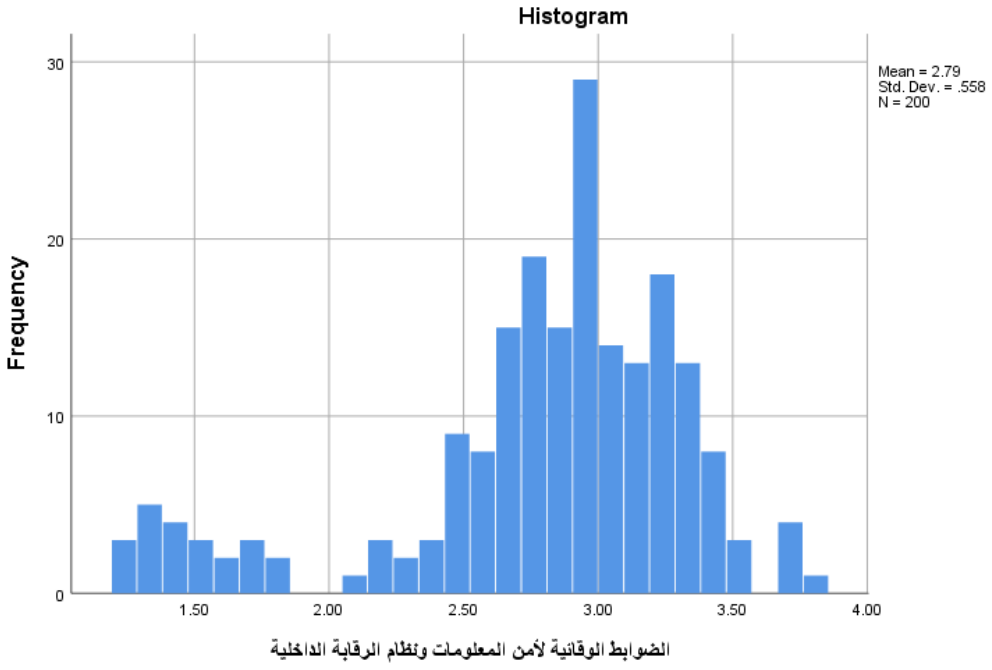
يتمُّ إجراء اختبار (Kolmogorov–Smirnov) للتوزع الطبيعي، وذلك لمعرفةِ نوعيةِ الاختبارات التي سوفَ تستخدم لاختبار الفرضيات هل هي اختباراتٌ معلمية، أم غير معلمية، حيثُ تمّ إجراءُ الاختبار بدايةً على كاملِ مفردات عينتيّ الدراسة، ومن ثمَّ لكلِ واحدةٍ من عينتي الدراسة بشكلٍ منفصل، ويوضّحُ الجدول (4–8) اختبارَ التوزيع الطبيعي للآراء لكاملِ مفردات عينتيّ الدراسة:

Tests of Normality			
	Kolmogorov–Smirnov[a]		
	Statistic	df	Sig.
الضوابط الوقائية لأمن المعلومات ونظام الرقابة الداخلية	.171	200	.000
الضوابط الاستكشافية لأمن المعلومات ونظام الرقابة الداخلية	.127	200	.000
الضوابط التصحيحية لأمن المعلومات ونظام الرقابة الداخلية	.152	200	.000
تفعيل نظام الرقابة الداخلية	.152	200	.000
a. Lilliefors Significance Correction			

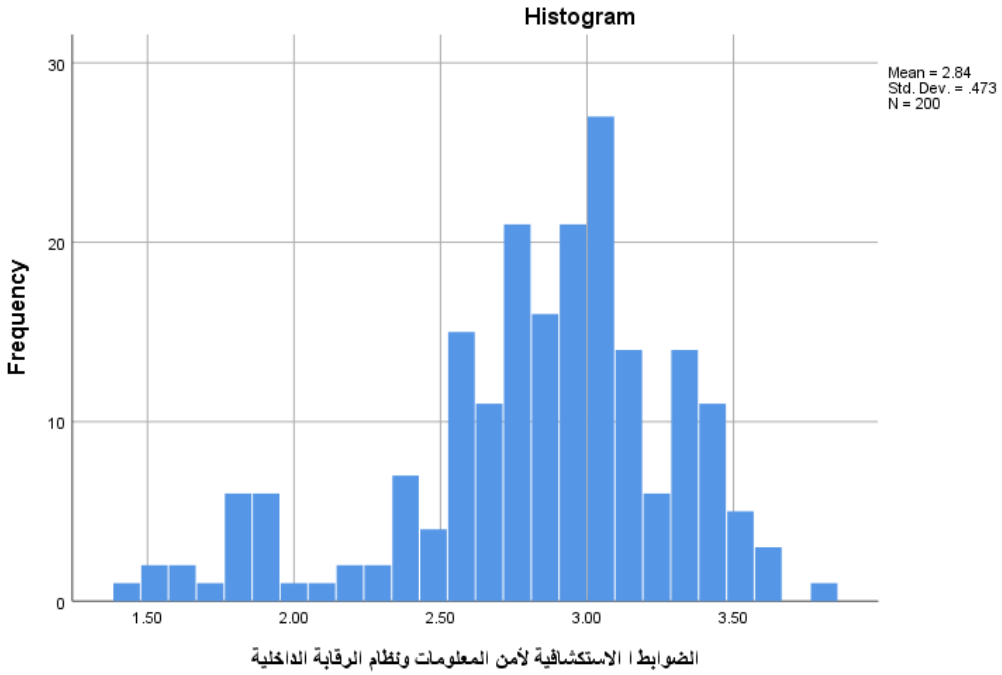
الجدول (4-8): نتائج اختبار (Kolmogorov-Smirnov) لكامل مفردات العينتين.

بقراءةِ معنوية الاختبار، ومقارنتها مع مستوى الدلالة (α=0.05) الذي تقبلُ، أو ترفضُ عنده الفرضيات يتبيّن أنَّ قيمةَ (sig) أصغرُ من (α=0.05) لجميعِ محاور الدراسة لذلك نرفضُ فرضيةَ العدم، ونقبلُ الفرضيةَ التي تنصُّ على أنَّ المتغيرات لا تتّبع التوزيع الطبيعي.

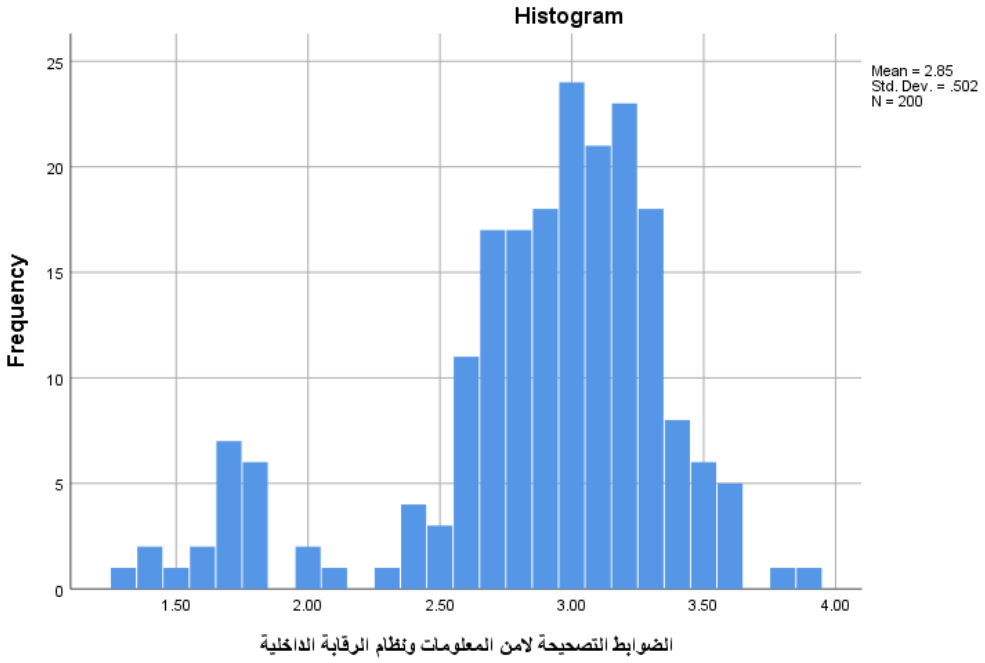
ويرافقُ مخرجات الاختبار الرسوم البيانية التي توضّحُ شكلَ التوزيع لكلِّ محورٍ من محاورِ الدراسة:



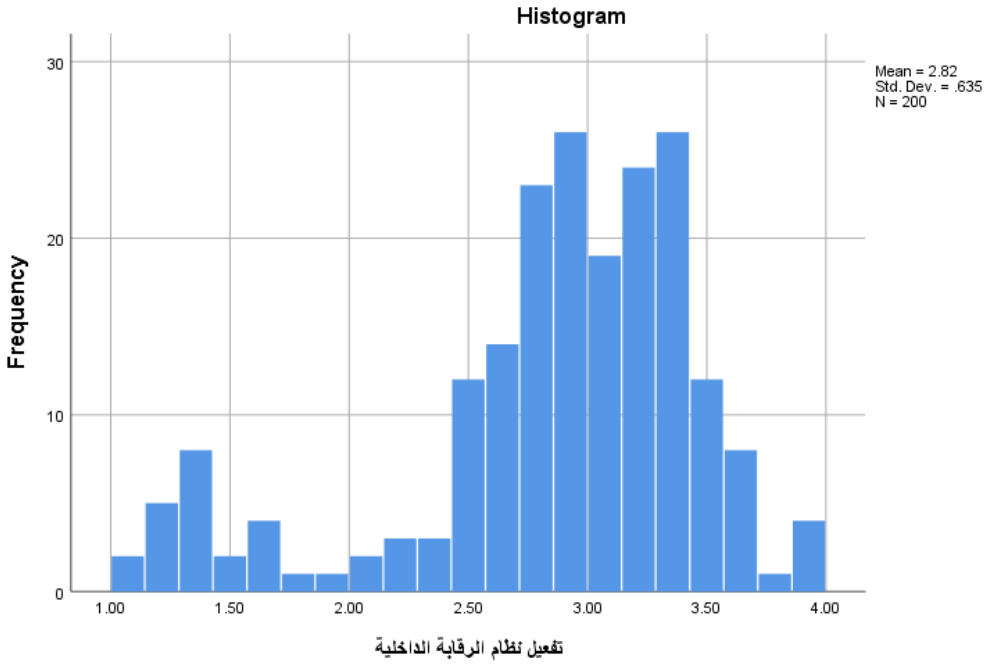
الشكل (4-1): اختبار التوزع الطبيعي لكامل مفردات عينتي الدراسة، المحور الأول.



الشكل (4-2): اختبار التوزع الطبيعي لكامل مفردات عينتي الدراسة، المحور الثاني.



الشكل (4-3): اختبار التوزع الطبيعي لكامل مفردات عينتي الدراسة، المحور الثالث.



الشكل (4-4): اختبار التوزع الطبيعي لكامل مفردات عينتي الدراسة، المحور الرابع.

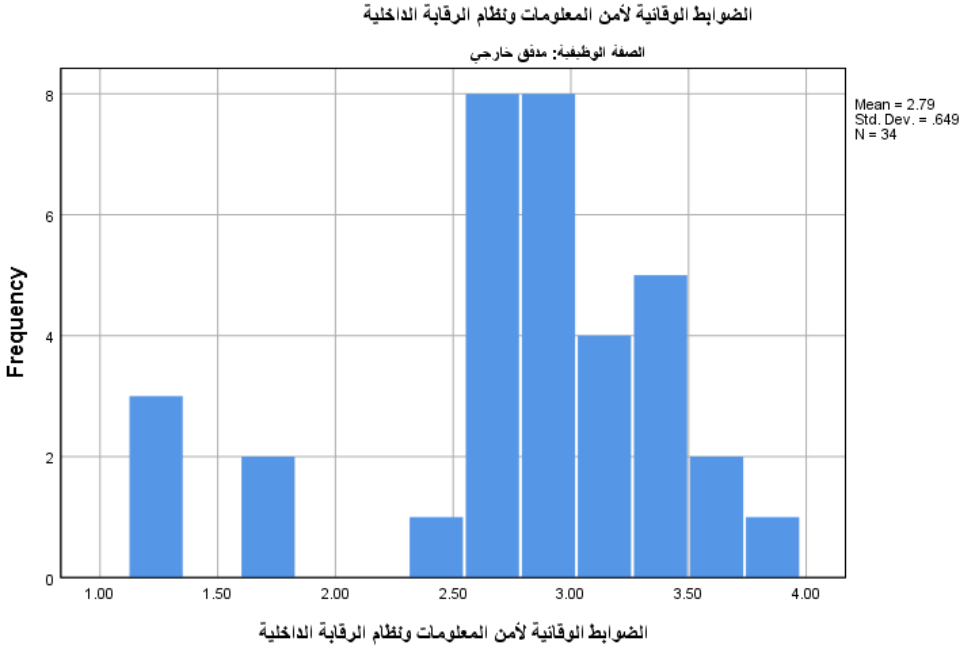
بينما يعرضُ الجدول (4–9) اختبارَ التوزّع الطبيعي، وذلك لآراء مفردات العينة الأولى (من المدققين الخارجيين):

Tests of Normality			
	Kolmogorov–Smirnov[a]		
	Statistic	df	Sig.
الضوابط الوقائية لأمن المعلومات ونظام الرقابة الداخلية	.217	34	.000
الضوابط الاستكشافية لأمن المعلومات ونظام الرقابة الداخلية	.152	34	.045
الضوابط التصحيحية لأمن المعلومات ونظام الرقابة الداخلية	.137	34	.004
تفعيل نظام الرقابة الداخلية	.167	34	.017
a. Lilliefors Significance Correction			

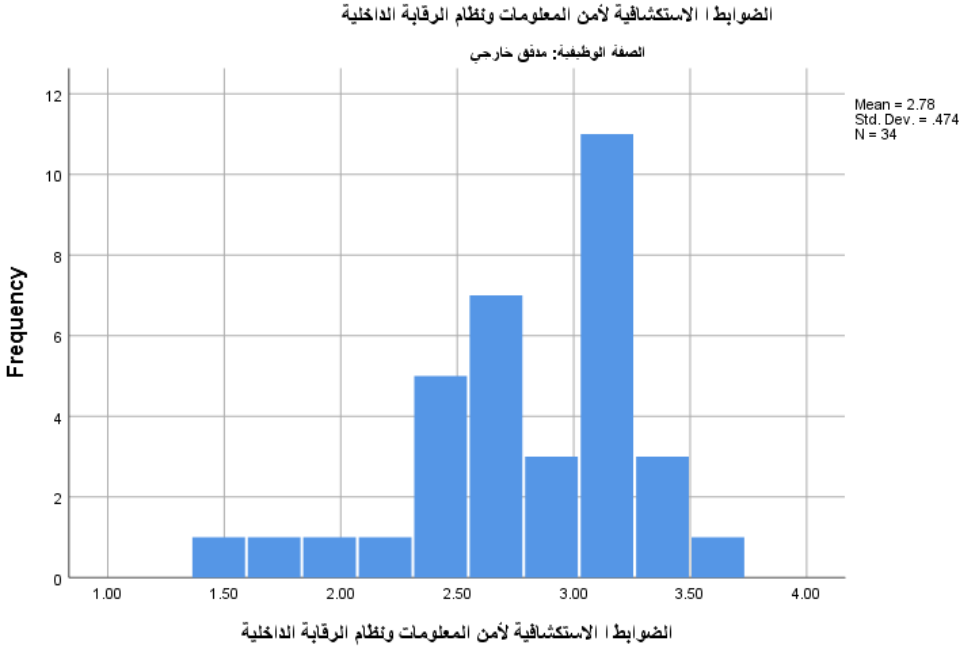
الجدول (4-9): نتائج اختبار (Kolmogorov-Smirnov) لمفردات العينة الأولى.

بقراءةِ معنوية الاختبار، ومقارنتها مع مستوى الدلالة (α=0.05) الذي تقبلُ، أو ترفضُ عنده الفرضيات يتبيّن أنَّ قيمةَ (sig) أصغرُ من (α=0.05) لجميع محاور الدراسة لذلك نرفضُ فرضيةَ العدم، ونقبلُ الفرضية التي تنصّ على أنَّ المتغيرات لا تتّبع التوزيع الطبيعي.

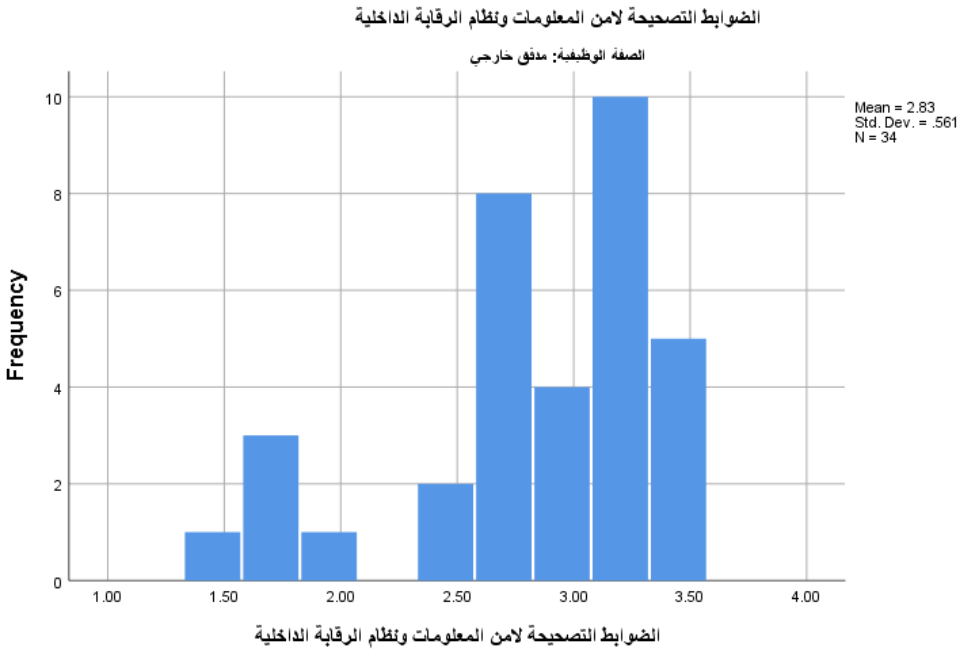
ويرافقُ مخرجات الاختبار الرسوم البيانية التي توضّح شكلَ التوزيعِ لكلِّ محورٍ من محاورِ الدراسة:



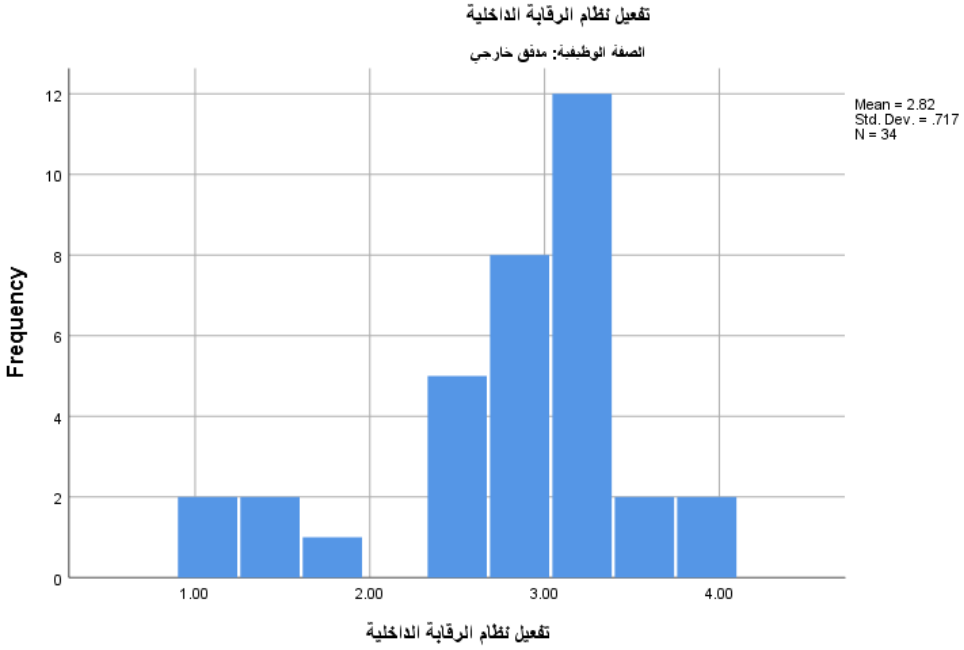
الشكل (4-5): اختبار التوزع الطبيعي لمفردات العينة الأولى، المحور الأول.



الشكل (4-6): اختبار التوزع الطبيعي لمفردات العينة الأولى، المحور الثاني.



الشكل (4-7): اختبار التوزع الطبيعي لمفردات العينة الأولى، المحور الثالث.



الشكل (4-8): اختبار التوزع الطبيعي لمفردات العينة الأولى، المحور الرابع.

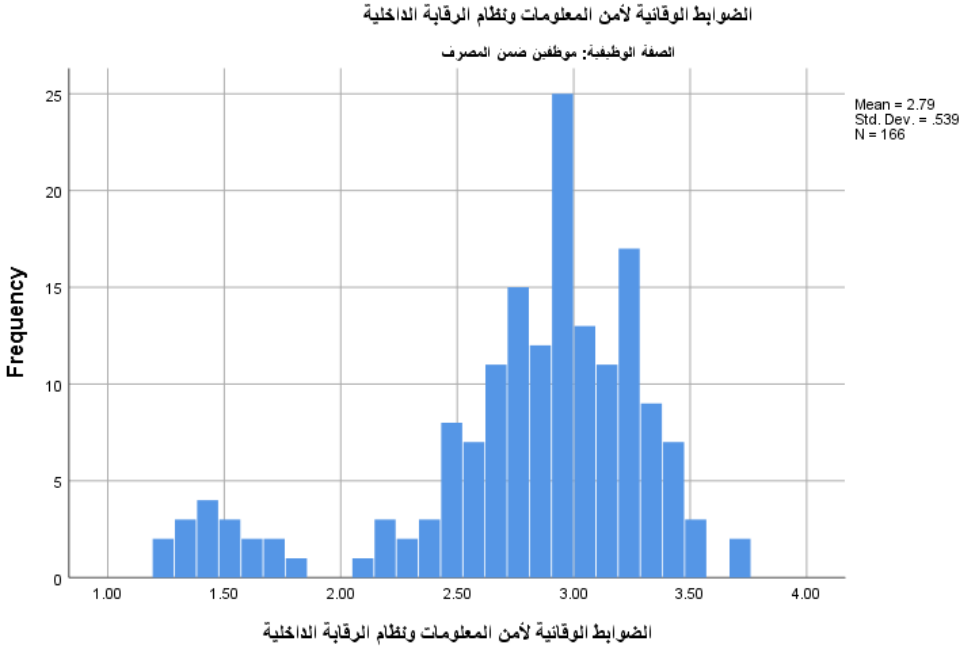
فيما يعرضُ الجدول (4–10) اختبارَ التوزّع الطبيعي، وذلك لآراء مفردات العينة الثانية (من الموظفين في المصارف):

Tests of Normality			
	Kolmogorov–Smirnov[a]		
	Statistic	df	Sig.
الضوابط الوقائية لأمن المعلومات ونظام الرقابة الداخلية	.165	166	.000
الضوابط الاستكشافية لأمن المعلومات ونظام الرقابة الداخلية	.139	166	.000
الضوابط التصحيحية لأمن المعلومات، ونظام الرقابة الداخلية	.170	166	.000
تفعيل نظام الرقابة الداخلية	.153	166	.000
a. Lilliefors Significance Correction			

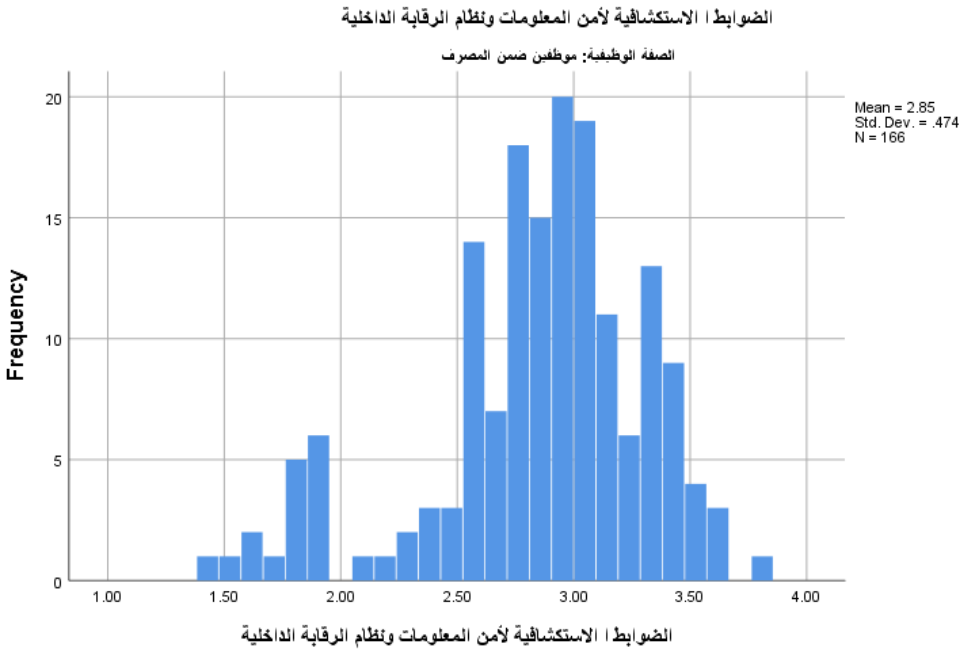
الجدول (4-10): نتائج اختبار (Kolmogorov-Smirnov) لمفردات العينة الثانية.

بقراءةِ معنوية الاختبار ومقارنتها مع مستوى الدلالة (α=0.05) الذي تقبلُ، أو ترفضُ عنده الفرضيات يتبيّن أنَّ قيمةَ (sig) أصغرُ من (α=0.05) لجميع محاور الدراسة، لذلك نرفضُ فرضيةَ العدم، ونقبلُ الفرضيةَ التي تنصُّ على أنَّ المتغيرات لا تتّبع التوزّع الطبيعي.

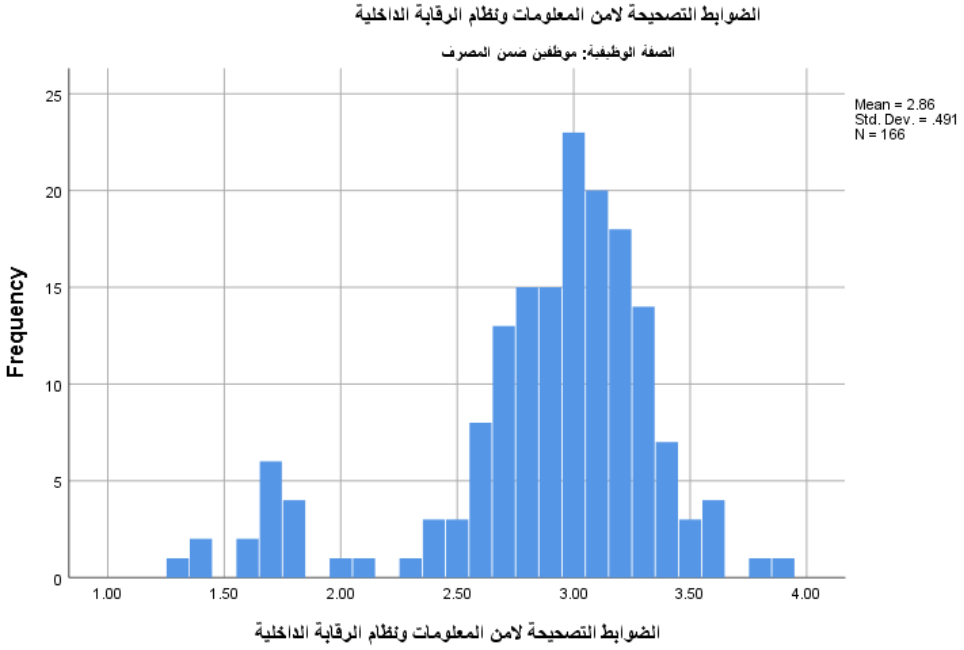
ويرافقُ مخرجات الاختبار الرسوم البيانية التي توضّح شكلَ التوزيع لكلِّ محورٍ من محاور الدراسة:



الشكل (4-9): اختبار التوزع الطبيعي لمفردات العينة الثانية، المحور الأول.



الشكل (4-10): اختبار التوزع الطبيعي لمفردات العينة الثانية، المحور الثاني.



الشكل (4-11): اختبار التوزع الطبيعي لمفردات العينة الثانية، المحور الثالث.

4-2-5 نتائج آراء عينتي الدراسة، واختبار الحياد لكل من أسئلة ومحاور الاستبيان:

تعرضُ الجداول الآتية نتائجَ آراء كلّ عينةٍ من عينتي الدراسة وفقَ أسئلة ومحاور الاستبيان، حيثُ يعرض كلَّ جدولٍ عددَ مرات تكرار كلّ إجابة، ووزنها النسبي مقابلَ باقي الإجابات، وذلك لكلّ محورٍ من محاور الاستبيان، والنتائجُ التي تمَّ التّوصّلَ إليها من خلال إجابات أفراد عينتيّ الدراسة، على الشكل الآتي:

4-2-5-1 نتائجُ آراء العينة الأولى (من المدققين الخارجيين) حول أسئلة، ومحاور الاستبيان:

الجدول (4-11): دورُ الضوابطُ الوقائيةُ لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الأولى:

المحور الأول:		موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	المتوسط الحسابي	الانحراف المعياري	sig	النتيجة
1. يسهم امتثال الإدارة العليا لضوابط أمن المعلومات في خلق بيئة رقابة فعالة.	التكرار	9	11	6	2	6	2.56	1.418	.079	محايد
	النسبة	26.5	32.4	17.6	5.9	17.6				
2. يؤثر تدريب الموظفين على متطلبات أمن المعلومات في رفع كفاءتهم التشغيلية.	التكرار	8	12	5	3	6	2.62	1.415	.125	محايد
	النسبة	23.5	35.3	14.7	8.8	17.6				
3. يتوافر دليلاً واضحاً، ومطبوعاً لضوابط أمن المعلومات.	التكرار	8	7	6	9	4	2.82	1.381	.461	محايد
	النسبة	23.5	20.6	17.6	26.5	11.8				
4. يلتزم الموظفون بدليل ضوابط أمن المعلومات.	التكرار	2	12	10	2	8	3.06	1.278	.790	محايد
	النسبة	5.9	35.3	29.4	5.9	23.5				
5. يتم تقييد الوصول إلى المعلومات ضمن النطاق المحدد لعمل الموظف.	التكرار	10	10	9	1	4	2.38	1.280	.008	موافق
	النسبة	29.4	29.4	26.5	2.9	11.8				
6. الموظفين في المصارف على دراية بمفاهيم وأنواع العمليات الاحتيالية (الهندسة الاجتماعية...الخ)	التكرار	4	8	9	10	3	3.00	1.181	1.000	محايد
	النسبة	11.8	23.5	26.5	29.4	8.8				

7. إجراء اختبارات دورية لاحتمالات اختراق نظام المعلومات.	التكرار	7	7	5	7	8	3.06	1.496	.820	محايد
	النسبة	20.6	20.6	14.7	20.6	23.5				
8. لا يسمح للموظف غير المصرح له بتنصيب البرامج على نظام المعلومات في المصرف.	التكرار	10	7	3	10	4	2.74	1.463	.299	محايد
	النسبة	29.4	20.6	8.8	29.4	11.8				
9. نظام المعلومات مصمم للتنبه بحدوث أخطاء حسابية أو غير المقصودة عند إدخال العمليات (تجاوز الحد الائتماني للعميل ...الخ)	التكرار	11	7	4	6	6	2.68	1.532	.227	محايد
	النسبة	32.4	20.6	11.8	17.6	17.6				
10. حماية أمن المعلومات على أهمية مماثلة لحماية أمن الأصول المادية.	التكرار	13	4	5	4	8	2.71	1.643	.304	محايد
	النسبة	38.2	11.8	14.7	11.8	23.5				
11. يتم استخدام برامج متطورة لحماية الأجهزة من المخاطر التكنولوجية (Anti-Virus).	التكرار	11	4	5	7	7	2.85	1.579	.591	محايد
	النسبة	32.4	11.8	14.7	20.6	20.6				
12. يتم استخدام نسخ مُرخّصة للبرامج لضمان استمرارية عمل عناصر نظام المعلومات.	التكرار	9	6	6	6	7	2.88	1.513	.653	محايد
	النسبة	26.5	17.6	17.6	17.6	20.6				
13. يتم استخدام أجهزة إنذار لضبط الوصول إلى المخدم الأساسي لنظام المعلومات.	التكرار	11	7	4	7	5	2.65	1.495	.178	محايد
	النسبة	32.4	20.6	11.8	20.6	14.7				
14. يتم استخدام المصادقات متعددة العوامل (كلمة سر، بصمة، بطاقة تعريف الكترونية...الخ) للوصول إلى مخدم نظام المعلومات.	التكرار	11	5	5	7	6	2.76	1.539	.379	محايد
	النسبة	32.4	14.7	14.7	20.6	17.6				
15. استخدام تقنية الجدران النارية لمنع الوصول إلى عناصر نظام المعلومات عبر الشبكة.	التكرار	12	8	1	5	8	2.68	1.646	.260	محايد
	النسبة	35.3	23.5	2.9	14.7	23.5				
16. لا يسمح للموظف غير المصرح له بإدخال ملحقات الكترونية على نظام المعلومات) قرص ليزي، فلاشة...الخ(	التكرار	11	2	6	8	7	2.94	1.575	.829	محايد
	النسبة	32.4	5.9	17.6	23.5	20.6				
17. يتم استخدام إجراءات مادية لمنع سرقة أحد عناصر نظام المعلومات (استخدام إقفال منع سرقة أجهزة الحاسب المحمول ...الخ)	التكرار	5	6	6	5	12	3.38	1.498	.146	محايد
	النسبة	14.7	17.6	17.6	14.7	35.3				

18. تسهم البيئة الآمنة لنظم المعلومات في ضمان دقة وموثوقية المعلومات.	التكرار	12	4	11	4	3	2.47	1.331	.027	موافق
	النسبة	35.3	11.8	32.4	11.8	8.8				
19. يحقق استخدام ضوابط الوصول التحديد الواضح للصلاحيات والمسؤوليات.	التكرار	10	8	5	1	10	2.79	1.629	.466	محايد
	النسبة	29.4	23.5	14.7	2.9	29.4				
20. تعديل الإعدادات الافتراضية للبرامج المثبتة في نظام المعلومات يزيد من الكفاءة التشغيلية.	التكرار	7	7	10	4	6	2.85	1.374	.537	محايد
	النسبة	20.6	20.6	29.4	11.8	17.6				
21. يسهم تدريب الموظفين على ضوابط أمن المعلومات في تعزيز الالتزام بإجراءات الرقابة الداخلية.	التكرار	9	9	4	5	7	2.76	1.519	.373	محايد
	النسبة	26.5	26.5	11.8	14.7	20.6				
الضوابط الوقائية لأمن المعلومات ونظام الرقابة الداخلية							2.42	.64890	.001	موافق

من الجدول السابق (4-11) نلاحظُ أنَّ آراءَ العينة الأولى حولَ دور الضوابط الوقائية لأمن المعلومات في تفعيل نظام الرقابة الداخلية تراوحُ وسطياً بين المحايد والمائل إلى الموافقة، وأنَّ المحورَ بشكلٍ كليّ يميلُ إلى الموافقة لأنَّ قيمةَ المتوسط (2.42) تدلُّ على الموافقة حسبَ مقياس ليكرت الخماسي، وقيمة (sig) أصغر من (α=0.05) مما يدلُّ على أنَّ الموافقةَ ذات دلالةٍ إحصائية، وهناك دوراً للضوابط الوقائية لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الأولى.

الجدول (4-12): دورُ الضوابطُ الاستكشافيةُ لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الأولى:

المحور الثاني:		موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	المتوسط الحسابي	الانحراف المعياري	sig	النتيجة
1. استخدام برامج لمراقبة الدخول إلى النظام للتأكد من دخول الأشخاص المصرح لهم.	التكرار	9	8	7	7	3	2.62	1.326	.102	محايد
	النسبة	26.5	23.5	20.6	20.6	8.8				
2. يسجل النظام العمليات التي قام بها المستخدم خلال الاستخدام.	التكرار	14	5	4	7	4	2.47	1.502	.048	موافق
	النسبة	41.2	14.7	11.8	20.6	11.8				
3. يتم تحليل سجلات الاستخدام بشكل دوري للتأكد من خطوط الصلاحيات و المسؤوليات للعمليات.	التكرار	9	5	5	8	7	2.97	1.527	.911	محايد
	النسبة	26.5	14.7	14.7	23.5	20.6				

4. استخدم كاميرات مراقبة وحساسات حركة في غرف المخدمات الأساسية.	التكرار	7	8	7	8	4	2.82	1.336	.447	محايد
	النسبة	20.6	23.5	20.6	23.5	11.8				
5. الاستعانة بشركات متخصصة بأمن المعلومات بشكل دوري لتحديد محاولات اختراق النظام.	التكرار	5	9	6	11	3	2.94	1.254	.786	محايد
	النسبة	14.7	26.5	17.6	32.4	8.8				
6. يعطي نظام المعلومات إشعارات لمسؤول أمن المعلومات حول إدخال عنصر جديد إلى النظام (فلاشة، ماسح ضوئي...الخ).	التكرار	8	11	5	7	3	2.59	1.305	.075	محايد
	النسبة	23.5	32.4	14.7	20.6	8.8				
7. تتعرض نظم المعلومات لمحاولات اختراق خارجية أكثر من تعرضها لمحاولات داخلية.	التكرار	4	8	7	8	7	3.18	1.336	.447	محايد
	النسبة	11.8	23.5	20.6	23.5	20.6				
8. لا يمكن الارتباط بنظام المعلومات لاسلكياً من منطقة مجاورة.	التكرار	12	9	7	5	1	2.24	1.182	.001	موافق
	النسبة	35.3	26.5	20.6	14.7	2.9				
9. لا يمكن للموظف الاتصال بشبكة الانترنت الخاصة بالمصرف من اجهزته الشخصية.	التكرار	9	8	5	4	8	2.82	1.547	.510	محايد
	النسبة	26.5	23.5	14.7	11.8	23.5				
10. نظام المعلومات مُصّمم للكشف عن محاولات الاختراق الالكترونية وتنبيه الأطراف ذات العلاقة.	التكرار	9	7	5	8	5	2.79	1.452	.414	محايد
	النسبة	26.5	20.6	14.7	23.5	14.7				
11. تُمنح الإدارة العليا صلاحيات غير محددة لتعديل وتغير البيانات.	التكرار	7	3	7	11	6	3.18	1.403	.468	محايد
	النسبة	20.6	8.8	20.6	32.4	17.6				
12. تُعتبر مراقبة أمن المعلومات عملية مستمرة وشمولية لكافة عناصر نظام المعلومات.	التكرار	13	4	3	8	6	2.71	1.605	.293	محايد
	النسبة	38.2	11.8	8.8	23.5	17.6				
13. يوفر نظام المعلومات إجراءاتٍ تلقائية للحد من محاولات التلاعب بعناصر النظام (إقفال شاشة المستخدم وطلب كلمة مرور... الخ)	التكرار	7	6	8	7	6	2.97	1.403	.903	محايد
	النسبة	20.6	17.6	23.5	20.6	17.6				
14. يتم اكتشاف محاولات التلاعب والأخطاء المتعمدة وغير المتعمدة وتنبيه الأطراف حال حدوث التهديد.	التكرار	8	10	6	4	6	2.71	1.426	.238	محايد
	النسبة	23.5	29.4	17.6	11.8	17.6				
15. يتم إجراء تدوير للموظفين في نفس القسم للكشف عن تلاعب أو أخطاء الموظفين.	التكرار	6	11	10	5	2	2.59	1.131	.041	موافق
	النسبة	17.6	32.4	29.4	14.7	5.9				

16. استخدام أنظمة محاكاة (honeypots) من أجل الكشف المبكر عن التهديدات المحتملة وتفادي الهجمات للأجزاء الهامة من النظام.	التكرار	2	9	4	10	9	3.44	1.307	.058	محايد
	النسبة	5.9	26.5	11.8	29.4	26.5				
17. المتابعة المستمرة لالتزام الموظفين بمتطلبات أمن المعلومات يضمن الالتزام بالسياسات واللوائح الخاصة بمتطلبات الرقابة الداخلية.	التكرار	11	6	6	8	3	2.59	1.395	.095	محايد
	النسبة	32.4	17.6	17.6	23.5	8.8				
18. التحليل الدوري لسجلات الاستخدام يزيد من حماية الأصول من التلاعب أو السرقة.	التكرار	8	9	6	6	5	2.74	1.399	.278	محايد
	النسبة	23.5	26.5	17.6	17.6	14.7				
19. استخدام برامج خاصة لكشف التسلل إلى نظام المعلومات يزيد من دقة وموثوقية التقارير المالية.	التكرار	6	10	9	4	5	2.76	1.304	.300	محايد
	النسبة	17.6	29.4	26.5	11.8	14.7				
20. يحقق الفصل الملائم بين الصلاحيات والمسؤوليات اكتشاف العمليات الاحتيالية.	التكرار	7	11	7	3	6	2.71	1.382	.223	محايد
	النسبة	20.6	32.4	20.6	8.8	17.6				
21. تسهم الضوابط الاستكشافية المختلفة في زيادة الكفاءة التشغيلية للموظفين.	التكرار	10	6	8	6	4	2.65	1.390	.148	محايد
	النسبة	29.4	17.6	23.5	17.6	11.8				
الضوابط الاستكشافية لأمن المعلومات ونظام الرقابة الداخلية							2.39	.64890	.012	موافق

من الجدول السابق (4-12) نلاحظُ أنَّ آراءَ العينة الأولى حولَ دور الضوابط الاستكشافية لأمن المعلومات في تفعيل نظام الرقابة الداخلية تراوحُ وسطياً بين المحايد والمائل إلى الموافقة، وأنَّ المحورَ بشكلٍ كليّ يميلُ إلى الموافقة، لأنَّ قيمةَ المتوسط (2.39) تدلُّ على الموافقة حسبَ مقياس ليكرت الخماسي، وقيمة (sig) أصغر من (α=0.05) مما يدلُّ على أنَّ الموافقةَ ذات دلالةٍ إحصائية، وهناك دورلً للضوابط الاستكشافية لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الأولى.

الجدول (4-13): دورُ الضوابطُ التصحيحيّة لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الأولى:

المحور الثالث:		موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	المتوسط الحسابي	الانحراف المعياري	sig	النتيجة
1. يتم تدريب فرق أمن المعلومات بشكل مستمر للاستجابة لحوادث أمن المعلومات.	التكرار	4	10	8	7	5	2.97	1.267	.893	محايد
	النسبة	11.8	29.4	23.5	20.6	14.7				

2. مدير أمن المعلومات يتبع للإدارة العليا مباشرةً وليس لقسم تكنولوجيا المعلومات.(IT)	التكرار	8	4	9	8	5	2.94	1.391	.807	محايد
	النسبة	23.5	11.8	26.5	23.5	14.7				
3. توفير نسخة احتياطية لكافة البرامج والملفات والبيانات المرتبطة بنظام المعلومات.	التكرار	14	5	5	9	1	2.35	1.346	.008	موافق
	النسبة	41.2	14.7	14.7	26.5	2.9				
4. حدوث انتهاكات أمن المعلومات قد يوقف عمل المصرف بشكل كامل.	التكرار	11	4	6	4	9	2.88	1.629	.676	محايد
	النسبة	32.4	11.8	17.6	11.8	26.5				
5. اكتشاف محاولة انتهاك داخلي للنظام يؤدي إلى فصل الموظف المسؤول مباشرةً.	التكرار	8	11	2	6	7	2.79	1.513	.433	محايد
	النسبة	23.5	32.4	5.9	17.6	20.6				
6. يتم اتخاذ إجراءات فورية عند اكتشاف تهديدات مباشرة لأمن المعلومات.	التكرار	9	7	5	6	7	2.85	1.520	.577	محايد
	النسبة	26.5	20.6	14.7	17.6	20.6				
7. يتم الاحتفاظ بالنسخ الاحتياطية في أماكن آمنة وبعيدة عن موقع العمل.	التكرار	10	7	8	6	3	2.56	1.330	.062	محايد
	النسبة	29.4	20.6	23.5	17.6	8.8				
8. التعافي من أضرار تهديدات الأمن يستغرق وقتاً طويلاً قبل العودة للوضع الطبيعي.	التكرار	5	6	9	9	5	3.09	1.288	.692	محايد
	النسبة	14.7	17.6	26.5	26.5	14.7				
9. يتم تزويد الموظفين بإصدارات مُحدّثة لدليل ضوابط أمن المعلومات بشكل دوري ومنتظم.	التكرار	9	8	5	7	5	2.74	1.442	.292	محايد
	النسبة	26.5	23.5	14.7	20.6	14.7				
10. يتم وضع خطط مسبقة للتهديدات المتوقعة واتخاذ الإجراءات اللازمة لتجنبها أو معالجتها.	التكرار	10	7	8	3	6	2.65	1.454	.166	محايد
	النسبة	29.4	20.6	23.5	8.8	17.6				
11. يتم اعتبار الكوارث الطبيعية ضمن التهديدات المحتملة لأمن المعلومات.	التكرار	14	4	3	7	6	2.62	1.615	.177	محايد
	النسبة	41.2	11.8	8.8	20.6	17.6				
12. اكتشاف حدوث أخطاء أو انتهاكات يوجب تصحيحها فوراً.	التكرار	10	10	5	4	5	2.53	1.419	.062	محايد
	النسبة	29.4	29.4	14.7	11.8	14.7				
13. لا يتم البحث عن حلول لتهديدات أمن المعلومات إلا عند حدوثها فعلاً.	التكرار	8	4	9	9	4	2.91	1.357	.707	محايد
	النسبة	23.5	11.8	26.5	26.5	11.8				

14. يتم اقتراح حلولاً جديدة لمشكلات أمن المعلومات التي تم حلها مسبقاً.	التكرار	11	5	8	4	6	2.68	1.492	.006	موافق
	النسبة	32.4	14.7	23.5	11.8	17.6				
15. يوجد شبكة اتصال احتياطية في حال تعطل الشبكة الرئيسية.	التكرار	9	9	3	6	7	2.79	1.533	.439	محايد
	النسبة	26.5	26.5	8.8	17.6	20.6				
16. تدريب فرق استجابة متخصصة بأمن المعلومات يزيد من الكفاءة التشغيلية.	التكرار	6	8	4	8	8	3.12	1.472	.644	محايد
	النسبة	17.6	23.5	11.8	23.5	23.5				
17. يتوفر لدى المصرف مديراً لأمن المعلومات مما يحقق فصل الصلاحيات والمسؤوليات بشكل أفضل.	التكرار	4	7	8	4	11	3.32	1.430	.196	محايد
	النسبة	11.8	20.6	23.5	11.8	32.4				
18. الفصل الملائم بين الواجبات يقدم فرص أفضل لتخفيف أضرار التهديدات الأمنية عند وقوعها.	التكرار	8	7	4	9	6	2.94	1.476	.818	محايد
	النسبة	23.5	20.6	11.8	26.5	17.6				
19. بيئة الرقابة الفعالة تضمن التزام الموظفين بالسياسات والضوابط مما يحقق مستوى عالي لأمن المعلومات.	التكرار	11	4	5	7	7	2.85	1.579	.591	محايد
	النسبة	32.4	11.8	14.7	20.6	20.6				
20. سرعة إنجاز الإجراءات التصحيحية لحوادث أمن المعلومات يزيد موثوقية، وسلامة البيانات المالية.	التكرار	10	6	4	4	10	2.94	1.650	.837	محايد
	النسبة	29.4	17.6	11.8	11.8	29.4				
الضوابط التصحيحية لأمن المعلومات ونظام الرقابة الداخلية							2.28	.56101	.008	موافق

من الجدول السابق (4-13) نلاحظُ أنَّ آراءَ العينة الأولى حولَ دور الضوابط التصحيحية لأمن المعلومات في تفعيل نظام الرقابة الداخلية تراوحُ وسطياً بين المحايد والمائل إلى الموافقة، وأنَّ المحورَ بشكلٍ كليّ يميلُ إلى الموافقةِ لأنَّ قيمةَ المتوسط (2.28) تدلُّ على الموافقةِ حسبَ مقياس ليكرت الخماسي، وقيمة (sig) أصغر من (α=0.05) مما يدلُّ على أنَّ الموافقةَ ذات دلالةٍ إحصائية، وهناك دوراً للضوابط التصحيحية لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الأولى.

4-2-5-2 نتائجُ آراء العينة الثانية (من الموظفين ضمن المصارف) حول أسئلة ومحاور الاستبيان:

الجدول (4-14): دورُ الضوابطُ الوقائية لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الثانية:

المحور الأول:		موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	المتوسط الحسابي	الانحراف المعياري	sig	النتيجة
1. يسهم امتثال الإدارة العليا لضوابط أمن المعلومات في خلق بيئة رقابية فعالة.	التكرار	46	39	27	27	27	2.70	1.442	.008	موافق
	النسبة	27.7	23.5	16.3	16.3	16.3				
2. يؤثر تدريب الموظفين على متطلبات أمن المعلومات في رفع كفاءتهم التشغيلية.	التكرار	34	27	38	31	36	3.05	1.430	.665	محايد
	النسبة	20.5	16.3	22.9	18.7	21.7				
3. يتوافر دليلاً واضحاً، ومطبوعاً لضوابط أمن المعلومات.	التكرار	33	39	31	32	31	2.93	1.406	.545	محايد
	النسبة	19.9	23.5	18.7	19.3	18.7				
4. يلتزم الموظفون بدليل ضوابط أمن المعلومات.	التكرار	34	37	37	28	30	2.90	1.391	.344	محايد
	النسبة	20.5	22.3	22.3	16.9	18.1				
5. يتم تقييد الوصول إلى المعلومات ضمن النطاق المحدد لعمل الموظف.	التكرار	50	29	26	32	29	2.77	1.493	.044	موافق
	النسبة	30.1	17.5	15.7	19.3	17.5				
6. الموظفين في المصارف على دراية بمفاهيم وأنواع العمليات الاحتيالية (الهندسة الاجتماعية...الخ)	التكرار	27	44	24	42	29	3.01	1.371	.910	محايد
	النسبة	16.3	26.5	14.5	25.3	17.5				
7. إجراء اختبارات دورية لاحتمالات اختراق نظام المعلومات.	التكرار	49	33	24	37	23	2.71	1.444	.011	موافق
	النسبة	29.5	19.9	14.5	.22	13.9				
8. لا يسمح للموظف غير المصرح له بتنصيب البرامج على نظام المعلومات في المصرف.	التكرار	48	29	38	26	25	2.70	1.420	.008	موافق
	النسبة	28.9	17.5	22.9	15.7	15.1				
9. نظام المعلومات مصمم للتنبه بحدوث أخطاء حسابية أو غير المقصودة عند إدخال العمليات (تجاوز الحد الائتماني للعميل... الخ)	التكرار	44	37	25	36	24	2.75	1.425	.027	موافق
	النسبة	26.5	22.3	15.1	21.7	14.5				
10. حماية أمن المعلومات على أهمية مماثلة لحماية أمن الأصول المادية.	التكرار	54	27	22	38	25	2.72	1.493	.016	موافق
	النسبة	32.5	16.3	13.3	22.9	15.1				

11. يتم استخدام برامج متطورة لحماية الأجهزة من المخاطر التكنولوجية (Anti-Virus).	التكرار	53	42	24	25	22	2.52	1.413	.000	موافق
	النسبة	31.9	25.3	14.5	15.1	13.3				
12. يتم استخدام نسخ مُرخّصة للبرامج لضمان استمرارية عمل عناصر نظام المعلومات.	التكرار	34	34	30	39	29	2.97	1.403	.782	محايد
	النسبة	20.5	20.5	18.1	23.5	17.5				
13. يتم استخدام أجهزة إنذار لضبط الوصول إلى المخدم الأساسي لنظام المعلومات.	التكرار	40	32	34	28	32	2.88	1.447	.285	محايد
	النسبة	24.1	19.3	20.5	16.9	19.3				
14. يتم استخدام المصادقات متعددة العوامل) كلمة سر، بصمة، بطاقة تعريف الكترونية...الخ (للوصول إلى مخدم نظام المعلومات.	التكرار	36	45	29	26	30	2.81	1.413	.090	محايد
	النسبة	21.7	27.1	17.5	15.7	18.1				
15. استخدام تقنية الجدران النارية لمنع الوصول إلى عناصر نظام المعلومات عبر الشبكة.	التكرار	55	24	31	30	26	2.69	1.481	.007	
	النسبة	33.1	14.5	18.7	18.1	15.7				
16. لا يسمح للموظف غير المصرح له بإدخال ملحقات الكترونية على نظام المعلومات) قرص ليزي، فلاشة...الخ(	التكرار	47	32	32	36	19	2.69	1.383	.004	موافق
	النسبة	28.3	19.3	19.3	21.7	11.4				
17. يتم استخدام إجراءات مادية لمنع سرقة أحد عناصر نظام المعلومات (استخدام اقفال منع سرقة أجهزة الحاسب المحمول ...الخ)	التكرار	49	39	25	27	26	2.65	1.448	.002	موافق
	النسبة	29.5	23.5	15.1	16.3	15.7				
18. تسهم البيئة الآمنة لنظم المعلومات في ضمان دقة وموثوقية المعلومات.	التكرار	52	33	31	24	26	2.63	1.449	.001	موافق
	النسبة	31.3	19.9	18.7	14.5	15.7				
19. يحقق استخدام ضوابط الوصول التحديد الواضح للصلاحيات والمسؤوليات.	التكرار	56	27	23	35	25	2.67	1.494	.006	موافق
	النسبة	33.7	16.3	13.9	21.1	15.1				
20. تعديل الإعدادات الافتراضية للبرامج المثبتة في نظام المعلومات يزيد من الكفاءة التشغيلية.	التكرار	34	33	34	35	30	2.96	1.401	.740	محايد
	النسبة	20.5	19.9	20.5	21.1	18.1				
21. يسهم تدريب الموظفين على ضوابط امن المعلومات في تعزيز الالتزام بإجراءات الرقابة الداخلية.	التكرار	40	33	30	31	32	2.89	1.457	.339	محايد
	النسبة	24.1	19.9	18.1	18.7	19.3				
الضوابط الوقائية لأمن المعلومات ونظام الرقابة الداخلية							2.36	.53917	.000	موافق

من الجدول السابق (4-14) نلاحظُ أنَّ آراءَ العيّنة الثانية حولَ دور الضوابط الوقائية لأمن المعلومات في تفعيل نظام الرقابة الداخلية تراوحُ وسطياً بين المحايد والمائل إلى الموافقة، وأنّ المحورَ بشكلٍ كليّ يميلُ إلى الموافقة لأنَّ قيمةَ المتوسط (2.36) تدلُّ على الموافقة حسبَ مقياس ليكرت الخماسي، وقيمة (sig) أصغر من (α=0.05) مما يدلُّ على أنَّ الموافقةَ ذات دلالةٍ إحصائية، وهناك دوراً للضوابط الوقائية لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الثانية.

الجدول (4-15): دورُ الضوابطُ الاستكشافية لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الثانية:

المحور الثاني:		موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	المتوسط الحسابي	الانحراف المعياري	sig	النتيجة
1. استخدام برامج لمراقبة الدخول إلى النظام للتأكد من دخول الأشخاص المصرح لهم.	التكرار	52	25	36	24	29	2.72	1.476	.015	موافق
	النسبة	31.3	15.1	21.7	14.5	17.5				
2. يسجل النظام العمليات التي قام بها المستخدم خلال الاستخدام.	التكرار	48	43	27	34	14	2.54	1.324	.000	موافق
	النسبة	28.9	25.9	16.3	20.5	8.4				
3. يتم تحليل سجلات الاستخدام بشكل دوري للتأكد من خطوط الصلاحيات و المسؤوليات للعمليات.	التكرار	31	36	33	32	34	3.01	1.410	.912	محايد
	النسبة	18.7	21.7	19.9	19.3	20.5				
4. استخدم كاميرات مراقبة وحساسات حركة في غرف المخدمات الأساسية.	التكرار	42	35	29	36	24	2.79	1.409	.056	محايد
	النسبة	25.3	21.1	17.5	21.7	14.5				
5. الاستعانة بشركات متخصصة بأمن المعلومات بشكل دوري لتحديد محاولات اختراق النظام.	التكرار	23	45	34	34	30	3.02	1.328	.861	محايد
	النسبة	13.9	27.1	20.5	20.5	18.1				
6. يعطي نظام المعلومات إشعارات لمسؤول أمن المعلومات حول إدخال عنصر جديد إلى النظام (فلاشة، ماسح ضوئي...الخ).	التكرار	39	42	26	30	29	2.81	1.431	.084	محايد
	النسبة	23.5	25.3	15.7	18.1	17.5				
7. تتعرض نظم المعلومات لمحاولات اختراق خارجية أكثر من تعرضها لمحاولات داخلية.	التكرار	32	29	40	40	25	2.98	1.342	.862	محايد
	النسبة	19.3	17.5	24.1	24.1	15.1				

8. لا يمكن الارتباط بنظام المعلومات لاسلكياً من منطقة مجاورة.	التكرار	47	35	26	24	34	2.78	1.507	.058	محايد
	النسبة	28.3	21.1	15.7	14.5	20.5				
9. لا يمكن للموظف الاتصال بشبكة الانترنت الخاصة بالمصرف من أجهزته الشخصية.	التكرار	32	41	27	41	25	2.92	1.368	.428	محايد
	النسبة	19.3	24.7	16.3	24.7	15.1				
10. نظام المعلومات مُصّمم للكشف عن محاولات الاختراق الالكترونية وتنبيه الأطراف ذات العلاقة.	التكرار	50	32	34	25	25	2.66	1.430	.002	موافق
	النسبة	30.1	19.3	20.5	15.1	15.1				
11. تُمنح الإدارة العليا صلاحيات غير محددة لتعديل وتغير البيانات.	التكرار	35	32	35	39	25	2.92	1.371	.463	محايد
	النسبة	21.1	19.3	21.1	23.5	15.1				
12. تُعتبر مراقبة أمن المعلومات عمليةً مستمرةً وشموليةً لكافة عناصر نظام المعلومات.	التكرار	43	32	33	25	33	2.84	1.470	.156	محايد
	النسبة	25.9	19.3	19.9	15.1	19.9				
13. يوفر نظام المعلومات إجراءات تلقائية للحد من محاولات التلاعب بعناصر النظام (إقفال شاشة المستخدم، وطلب كلمة مرور... الخ)	التكرار	34	27	33	36	36	3.08	1.440	.484	محايد
	النسبة	20.5	16.3	19.9	21.7	21.7				
14. يتم اكتشاف محاولات التلاعب، والأخطاء المتعمدة وغير المتعمدة وتنبيه الأطراف حال حدوث التهديد.	التكرار	38	32	30	45	21	2.87	1.371	.236	محايد
	النسبة	22.9	19.3	18.1	27.1	12.7				
15. يتم إجراء تدوير للموظفين في نفس القسم للكشف عن تلاعب أو أخطاء الموظفين.	التكرار	35	48	29	27	27	2.78	1.381	.039	موافق
	النسبة	21.1	28.9	17.5	16.3	16.3				
16. استخدام أنظمة محاكاة (honeypots) من أجل الكشف المبكر عن التهديدات المحتملة وتفادي الهجمات للأجزاء الهامة من نظام المعلومات.	التكرار	29	32	35	32	38	3.11	1.414	.325	محايد
	النسبة	17.5	19.3	21.1	19.3	22.9				
17. المتابعة المستمرة لالتزام الموظفين بمتطلبات أمن المعلومات يضمن الالتزام بالسياسات واللوائح الخاصة بمتطلبات الرقابة الداخلية.	التكرار	49	37	21	25	34	2.75	1.524	.034	موافق
	النسبة	29.5	22.3	12.7	15.1	20.5				

18. التحليل الدوري لسجلات الاستخدام يزيد من حماية الأصول من التلاعب أو السرقة.	التكرار	53	27	26	28	32	2.75	1.527	.039	موافق
	النسبة	31.9	16.3	15.7	16.9	19.3				
19. استخدام برامج خاصة لكشف التسلل إلى نظام المعلومات يزيد من دقة وموثوقية التقارير المالية.	التكرار	38	27	24	37	40	3.08	1.507	.472	محايد
	النسبة	22.9	16.3	14.5	22.3	24.1				
20. يحقق الفصل الملائم بين الصلاحيات والمسؤوليات اكتشاف العمليات الاحتيالية.	التكرار	48	31	27	30	30	2.78	1.487	.055	محايد
	النسبة	28.9	18.7	16.3	18.1	18.1				
21. تسهم الضوابط الاستكشافية المختلفة في زيادة الكفاءة التشغيلية للموظفين.	التكرار	37	47	25	30	27	2.78	1.403	.042	موافق
	النسبة	22.3	28.3	15.1	18.1	16.3				
الضوابط الاستكشافية لأمن المعلومات ونظام الرقابة الداخلية							2.32	.49061	.000	موافق

من الجدول السابق (4-15) نلاحظُ أنَّ آراءَ العينة الثانية حولَ دورِ الضوابط الاستكشافية لأمن المعلومات في تفعيل نظام الرقابة الداخلية تراوحُ وسطياً بين المحايد والمائل إلى الموافقة، وأنَّ المحورَ بشكلٍ كليّ يميلُ إلى الموافقة لأنّ قيمةَ المتوسط (2.32) تدلّ على الموافقة حسبَ مقياس ليكرت الخماسي، وقيمة (sig) أصغر من (α=0.05) مما يدلُّ على أنَّ الموافقةَ ذات دلالةٍ إحصائية، وهناك دوراً للضوابط الاستكشافية لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الثانية.

الجدول (4-16): دورُ الضوابطُ التصحيحية لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الثانية:

المحور الثالث:		موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	المتوسط الحسابي	الانحراف المعياري	sig	النتيجة
1. يتم تدريب فرق أمن المعلومات بشكل مستمر للاستجابة لحوادث أمن المعلومات.	التكرار	44	40	31	31	20	2.66	1.365	.001	موافق
	النسبة	26.5	24.1	18.7	18.7	12.0				
2. مدير أمن المعلومات يتبع للإدارة العليا مباشرةً وليس لقسم تكنولوجيا المعلومات.(IT)	التكرار	24	36	35	45	26	3.08	1.303	.440	محايد
	النسبة	14.5	21.7	21.1	27.1	15.7				
3. توفير نسخة احتياطية لكافة البرامج والملفات والبيانات المرتبطة بنظام المعلومات.	التكرار	41	39	29	32	25	2.77	1.405	.033	موافق
	النسبة	24.7	23.5	17.5	19.3	15.1				

4. حدوث انتهاكات أمن المعلومات قد يوقف عمل المصرف بشكل كامل.	التكرار	44	34	30	27	31	2.80	1.466	.082	موافق
	النسبة	26.5	20.5	18.1	16.3	18.7				
5. اكتشاف محاولة انتهاك داخلي للنظام يؤدي إلى فصل الموظف المسؤول مباشرةً.	التكرار	39	42	23	24	38	2.88	1.501	.302	محايد
	النسبة	23.5	25.3	13.9	14.5	22.9				
6. يتم اتخاذ إجراءات فورية عند اكتشاف تهديدات مباشرة لأمن المعلومات.	التكرار	44	37	25	25	35	2.82	1.503	.123	محايد
	النسبة	26.5	22.3	15.1	15.1	21.1				
7. يتم الاحتفاظ بالنسخ الاحتياطية في أماكن آمنة وبعيدة عن موقع العمل.	التكرار	31	43	22	33	37	3.01	1.452	.915	محايد
	النسبة	18.7	25.9	13.3	19.9	22.3				
8. التعافي من أضرار تهديدات الأمن يستغرق وقت طويل قبل العودة للوضع الطبيعي.	التكرار	47	28	25	35	31	2.85	1.500	.198	محايد
	النسبة	28.3	16.9	15.1	21.1	18.7				
9. يتم تزويد الموظفين بإصدارات مُحدّثة لدليل ضوابط أمن المعلومات بشكل دوري ومنتظم.	التكرار	34	34	27	34	37	3.04	1.460	.750	محايد
	النسبة	20.5	20.5	16.3	20.5	22.3				
10. يتم وضع خطط مسبقة للتهديدات المتوقعة واتخاذ الإجراءات اللازمة لتجنبها، أو معالجتها.	التكرار	34	35	43	30	24	2.85	1.333	.147	محايد
	النسبة	20.5	21.1	25.9	18.1	14.5				
11. يتم اعتبار الكوارث الطبيعية ضمن التهديدات المحتملة لأمن المعلومات.	التكرار	54	30	19	28	35	2.76	1.565	.049	موافق
	النسبة	32.5	18.1	11.4	16.9	21.1				
12. اكتشاف حدوث أخطاء أو انتهاكات يوجب تصحيحها فوراً.	التكرار	35	41	26	38	26	2.87	1.393	.244	محايد
	النسبة	21.1	24.7	15.7	22.9	15.7				
13. لا يتم البحث عن حلول لتهديدات أمن المعلومات إلا عند حدوثها فعلاً.	التكرار	33	44	32	24	33	2.88	1.413	.274	محايد
	النسبة	19.9	26.5	19.3	14.5	19.9				
14. يتم اقتراح حلولاً جديدة لمشكلات أمن المعلومات التي تمّ حلها مسبقاً.	التكرار	34	39	33	34	26	2.87	1.371	.236	محايد
	النسبة	20.5	23.5	19.9	20.5	15.7				

15. يوجد شبكة اتصال احتياطية في حال تعطل الشبكة الرئيسية.	التكرار	40	34	27	33	32	2.90	1.463	.368	محايد
	النسبة	24.1	20.5	16.3	19.9	19.3				
16. تدريب فرق استجابة متخصصة بأمن المعلومات يزيد من الكفاءة التشغيلية.	التكرار	45	24	36	30	31	2.87	1.467	.246	محايد
	النسبة	27.1	14.5	21.7	18.1	18.7				
17. يتوفر لدى المصرف مديراً لأمن المعلومات مما يحقق فصل الصلاحيات، والمسؤوليات بشكل أفضل.	التكرار	37	37	32	25	35	2.90	1.453	.394	محايد
	النسبة	22.3	22.3	19.3	15.1	21.1				
18. الفصل الملائم بين الواجبات يقدم فرصاً أفضل لتخفيف أضرار التهديدات الأمنية عند وقوعها.	التكرار	49	31	29	30	27	2.73	1.462	.018	موافق
	النسبة	29.5	18.7	17.5	18.1	16.3				
19. بيئة الرقابة الفعالة تضمن التزام الموظفين بالسياسات والضوابط مما يحقق مستوى عالٍ لأمن المعلومات.	التكرار	45	27	33	40	21	2.79	1.400	.054	محايد
	النسبة	27.1	16.3	19.9	24.1	12.7				
20. سرعة إنجاز الإجراءات التصحيحية لحوادث أمن المعلومات يزيد موثوقية، وسلامة البيانات المالية.	التكرار	36	38	38	30	24	2.81	1.353	.068	محايد
	النسبة	21.7	22.9	22.9	18.1	14.5				
الضوابط التصحيحية لأمن المعلومات، ونظام الرقابة الداخلية							2.43	.49061	.000	موافق

من الجدول السابق (4-16) نلاحظُ أنَّ آراءَ العينة الثانية حولَ دور الضوابط التصحيحية لأمن المعلومات في تفعيل نظام الرقابة الداخلية تراوحُ وسطياً بين المحايد، والمائل إلى الموافقة، وأنَّ المحورَ بشكلٍ كليّ يميلُ إلى الموافقة، لأنَّ قيمةَ المتوسط (2.43) تدلّ على الموافقة حسب مقياس ليكرت الخماسي، وقيمة (sig) أصغرُ من (α=0.05) مما يدلُّ على أنّ الموافقةَ ذات دلالةٍ إحصائية، وهناك دوراً للضوابط التصحيحية لأمن المعلومات في تفعيل نظام الرقابة الداخلية من وجهة نظر أفراد العينة الثانية.

مما سبقَ في الجدول (4-11)، (4-12)، (4-13)، (4-14)، (4-15)، (4-16)، نلاحظُ أنَّ نتائجَ آراء عينتي الدراسة كانت متقاربةً، أي إنَّ آراءَ المدققين الخارجيين المكلفين بالتدقيق على المصارف المدرجة في سوق دمشق للأوراق المالية، والموظفين في تلك المصارف ضمنَ الاختصاصات المعنية بكلّ من أمن المعلومات، ونظام الرقابة الداخلية، يوافقونَ على أنَّ الضوابطَ المختلفة لأمن المعلومات، لها دورٌ في تفعيل نظام الرقابة الداخلية، وللتأكد من أنّه لا توجد فروقاً ذات دلالةٍ احصائية بين نتائج العينتين محل الدراسة، سيتمّ إجراء اختبار مان وتني في الفقرة التالية لاختبار الفرضية البحثية والتي تقول إنّه لا يوجد فروقاتٍ ذات دلالةٍ إحصائية بين آراء كلّاً من عينتيّ الدراسة.

المبحث الثالث: اختبار فرضيات الدراسة:

4-3-1 اختبار الفرضية الرابعة: لا يوجد فروقاتٍ ذات دلالة إحصائية بين آراء كلّ من عينتي الدراسة:

يتمّ اختبار هذه الفرضية عبرَ الاختبار المسمى مان وتني: وهو الذي يعدُّ أفضلَ بديلاً لامعلمي لاختبار تي ستيودنت للعينتين المستقلة (T-test)، و نستخدمُ هذا الاختبار لأنّ البيانات لا تتّبع التوزيع الطبيعي وفقَ مخرجات اختبار (Kolmogorov-Smirnov) في الجدول (4-8) و(4-9) و(4-10)، وفيما يلي مخرجات اختبار المقارنة مان وتني:

Test Statistics[a]

	الضوابط الوقائية لأمن المعلومات ونظام الرقابة الداخلية	الضوابط الاستكشافية لأمن المعلومات ونظام الرقابة الداخلية	الضوابط التصحيحية لأمن المعلومات ونظام الرقابة الداخلية	تفعيل نظام الرقابة الداخلية
Mann-Whitney U	2787.000	2563.500	2819.000	2716.500
Wilcoxon W	16648.000	3158.500	16680.000	16577.500
Z	-.114	-.842	-.010	-.344
Asymp. Sig. (2-tailed)	.909	.400	.992	.731

a. Grouping Variable: الصفة الوظيفية

الجدول (4-17): نتائج اختبار (Mann-Whitney)

من الجدول السابق نلاحظُ أنَّ قيمَ (sig) أكبرُ من (α=0.05) أي نقبلُ فرضيةَ العدم التي تقول أنَّه لا يوجدُ فرقاً ذو دلالةٍ إحصائية بين آراء عينتي الدراسة، وبالتالي وجهات نظر أفراد العينة الأولى من المدققين الخارجيين هي نفسُها وجهة نظر أفراد العينة الثانية من الموظفين في المصارف ضمنَ الاختصاصات المعنية وفقَ ما أشارت إليه النتائج، وبناءً على ما سبق يمكنُ معاملة العينتين على أنَّهما عينةٌ واحدة في اختبار باقي الفرضيات.

4-3-2 اختبار الفرضية الأولى: لا يوجد علاقةً ذات دلالة إحصائية بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية:

يتمّ اختبارُ الفرضية من خلال دراسة الارتباط البسيط للتحقّق من وجودِ علاقة بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية، حيثُ تمّ دراسةُ الارتباط باستخدام معامل الارتباط اللامعلمي سبيرمان لمناسبته لنوع البيانات التي لا تتوزّعُ طبيعياً، إضافةً إلى أنَّ البيانات رتبية، وهو معاملُ ارتباط الرتب:

Correlations			
		الضوابط الوقائية لأمن المعلومات، ونظام الرقابة الداخلية	تفعيل نظام الرقابة الداخلية
الضوابط الوقائية لأمن المعلومات ونظام الرقابة الداخلية	Spearman's rho	1	.759**
	Sig. (2-tailed)		.000
	N	200	200
تفعيل نظام الرقابة الداخلية	Spearman's rho	.759**	1
	Sig. (2-tailed)	.000	
	N	200	200
**. Correlation is significant at the 0.01 level (2-tailed).			

الجدول (4-18): نتائج اختبار الارتباط وفق معامل سبيرمان للفرضية الأولى.

كلما اقتربت قيمةُ معامل الارتباط من (1) دلَّ على ارتباطٍ قوي بين المتغيرين، ونلاحظُ أنَّ قيمةَ معامل الارتباط بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية (0.759)، وبالتالي الارتباط طردي بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية، كما نلاحظُ أنَّ معاملَ الارتباط ذو دلالةٍ إحصائية من خلال قيمة (sig) التي هي أصغرُ من (α=0.05)، أي نرفضُ فرضيةَ العدم التي تقولُ بأنَّه لا يوجدُ علاقةً ذات دلالةٍ إحصائية بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية، ونقبلُ الفرضيةَ البديلة، أي إنّه يوجدُ علاقةً ذات دلالةٍ إحصائية بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.

Measures of Association				
	R	R Squared	Eta	Eta Squared
تفعيل نظام الرقابة الداخلية * الضوابط الوقائية لامن المعلومات ونظام الرقابة الداخلية	.759	.577	.856	.732

الجدول (4-19) جدول مقياس الارتباط (Eta) بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.

بالنظر أيضاً إلى الجدول (4-19) نجدُ أنَّ قيمةَ (Eta= 0.856) وهي مقياسٌ للاقتران (الارتباط) بين المتغير التابع (الضوابط الوقائية لأمن المعلومات)، و المتغير المستقل (تفعيل نظام الرقابة الداخلية) مما يشيرُ لوجود اقترانٍ عالٍ، أما قيمةُ (Eta-Squared=0.732) فهي تشيرُ إلى حجمِ التأثير للمتغير المستقل على المتغير التابع حيث إنَّها تمثّلُ نسبةَ التباينات الكلية للمتغير التابع التي يفسّرها المتغير المستقل، وقيمتها تدلُّ على وجود تأثيرٍ عالٍ.

بعدَ التحقّق من وجود العلاقة، و معرفة شدتها واتجاهها، ولدراسة الدور نقومُ ببناءِ نموذج الانحدار للتحقق من شكل العلاقة بين المتغيرات، وذلك من خلال اختبار العلاقة الخطية، ومجموعة الاختبارات الخاصة بتحقق شروط الانحدار:

- **اختبارُ العلاقة الخطية بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية:**

ANOVA Table							
			Sum of Squares	Df	Mean Square	F	Sig.
الضوابط الوقائية لأمن المعلومات، ونظام الرقابة الداخلية * تفعيل نظام الرقابة الداخلية	Between Groups	(Combined)	46.962	36	1.304	14.271	.000
		Linearity	35.679	1	35.679	390.315	.000
		Deviation from Linearity	11.283	35	.322	3.527	.000
	Within Groups		14.900	163	.091		
	Total		61.862	199			

الجدول (4-20): جدول (ANOVA) لدراسة العلاقة الخطية بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.

إنَّ جدول (ANOVA) يشيرُ من خلال قيمة (sig) التي هي أصغرُ من (α=0.05)، إلى وجودِ فروقٍ ذات دلالةٍ إحصائية أي إنّ العلاقةَ بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية غير خطية، وبالتالي يجبُ تحديد نوع العلاقة غير الخطية بين المتغيرين.

- **تحديد أفضل نموذج للعلاقة غير الخطية:**

من المخرجات السابقة التي تبين لنا فيها أنَّ العلاقةَ بين متغيرات الدراسة غير خطية، وبالتالي نلجأُ إلى تقدير منحنى النموذج عبر (Curve Estimation) لاختيار النموذج غير الخطي الأفضل وفقاً لمعنوية معامل التحديد الأعلى أي القوة التفسيرية لهذا النموذج، وفيما يلي مخرجات النماذج غير الخطية الأشهر ذات الدلالة المعنوية حيثُ تمَّ استبعاد كلّ النماذج غير المعنوية، والإبقاء على النماذج المعنوية فقط، والمقارنة بينها وفقَ معامل التحديد الأعلى:

Model Summary and Parameter Estimates									
Dependent Variable: الضوابط الوقائية لأمن المعلومات ونظام الرقابة الداخلية									
Equation	Model Summary					Parameter Estimates			
	R Square	F	df1	df2	Sig.	Constant	b1	b2	b3

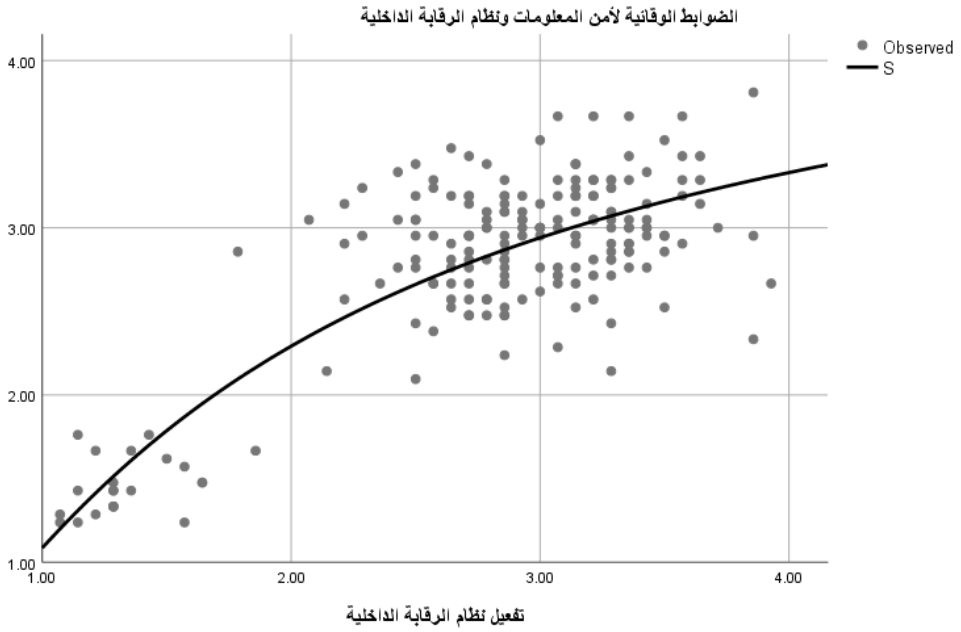
Linear	.577	269.814	1	198	.000	.915	.667		
Logarithmic	.643	356.758	1	198	.000	1.220	1.570		
Inverse	.669	399.391	1	198	.000	4.021	−3.190		
Quadratic	.680	209.390	2	197	.000	−.990	2.379	−.350	
Cubic	.681	139.397	3	196	.000	−1.601	3.245	−.719	.049
Compound	.625	329.467	1	198	.000	1.146	1.359		
Power	.709	483.486	1	198	.000	1.310	.730		
S	.750	592.762	1	198	.000	1.577	−1.495		
Growth	.625	329.467	1	198	.000	.136	.307		
Exponential	.625	329.467	1	198	.000	1.146	.307		
Logistic	.625	329.467	1	198	.000	.873	.736		
The independent variable is تفعيل نظام الرقابة الداخلية.									

الجدول (4-21) جدول تحديد أفضل نموذج للعلاقة غير الخطية بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.

من الجدول السابق نجدُ أنَّ قيمةَ (R Square) المرافقة لنموذج الانحدار غير الخطي (S) كانت (0.750) وهي الأعلى بين النماذج ذات الدلالة الإحصائية الأخرى مما يعني أنّ نموذجَ الانحدار غير الخطي (S) هو النموذجُ الأفضل لتقدير العلاقة بين المتغيرات المدروسة (الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية) وفيما يلي شكلُ معادلة النموذج، ورسمه البياني ذو الدلالةِ الإحصائية.

معادلة النموذج (S):

$$Y = e^{\left(1.577+\left(\frac{-1.495}{t}\right)\right)} \; or \; \ln(Y) = 1.577 + \left(\frac{-1.495}{t}\right)$$



الشكل (4-12): التمثيل البياني لنموذج العلاقة غير الخطية بين الضوابط الوقائية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.

4-3-3 اختبارُ الفرضية الثانية: لا يوجد علاقةً ذات دلالةٍ إحصائية بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية:

يتمّ اختبار الفرضية من خلال دراسة الارتباط البسيط للتحقّقِ من وجودِ علاقة بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية، حيثُ تمَّ دراسةُ الارتباط باستخدام معامل الارتباط اللامعلمي سبيرمان لمناسبته لنوع البيانات التي لا تتوزّعُ طبيعياً، إضافةً إلى أنَّ البيانات رتبية، وهو معاملُ ارتباط الرتب:

Correlations

		الضوابط الاستكشافية لأمن المعلومات، ونظام الرقابة الداخلية	تفعيل نظام الرقابة الداخلية
الضوابط الاستكشافية لأمن المعلومات، ونظام الرقابة الداخلية	Spearman's rho	1	.737**
	Sig. (2-tailed)		.000
	N	200	200
تفعيل نظام الرقابة الداخلية	Spearman's rho	.737**	1
	Sig. (2-tailed)	.000	
	N	200	200

**. Correlation is significant at the 0.01 level (2-tailed).

الجدول (4-22): نتائج اختبار الارتباط وفق معامل سبيرمان للفرضية الثانية.

كلما اقتربت قيمةُ معامل الارتباط من (1) دلَّ على ارتباطٍ قوي بين المتغيرين، ونلاحظُ أنَّ قيمةَ معامل الارتباط بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية (0.737)، وبالتالي الارتباط طردي بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية، كما نلاحظُ أنَّ معاملَ الارتباط ذو دلالةٍ إحصائية من خلال قيمة (sig) التي هي أصغرُ من (α=0.05)، أي نرفضُ فرضيةَ العدم التي تقول بأنَّه لا يوجدُ علاقةً ذات دلالةٍ إحصائيةٍ بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية، ونقبلُ الفرضيةَ البديلة، أي إنَّه يوجدُ علاقةً ذات دلالةٍ إحصائية بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.

Measures of Association				
	R	R Squared	Eta	Eta Squared
تفعيل نظام الرقابة الداخلية * الضوابط الاستكشافية لأمن المعلومات، ونظام الرقابة الداخلية	.737	544.	870.	757.

الجدول (4-23) جدول مقياس الارتباط (Eta) بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.

بالنظر أيضاً إلى الجدول (4-23) نجدُ أنَّ قيمةَ (Eta= 0.870) وهي مقياسٌ للاقتران (الارتباط) بين المتغير التابع (لضوابط الاستكشافية لأمن المعلومات)، و المتغير المستقل (تفعيل نظام الرقابة الداخلية) مما يشيرُ لوجود اقترانٍ عالٍ، أما قيمةُ (Eta-Squared=0.757) فهي تشيرُ إلى حجمِ التأثير للمتغير المستقل على المتغير التابع حيثُ إنّها تمثّلُ نسبةَ التباينات الكلية للمتغير التابع التي يفسّرها المتغير المستقل، وقيمتها تدلُّ على وجودِ تأثيرٍ عالٍ.

بعد التحققِ من وجودِ العلاقة، و معرفة شدتها واتجاهها، ولدراسة الدور نقومُ ببناء نموذج الانحدار للتحقّق من شكل العلاقة بين المتغيرات، وذلك من خلالِ اختبارِ العلاقة الخطية، ومجموعة الاختبارات الخاصّة بتحقق شروط الانحدار:

- **اختبارُ العلاقة الخطية بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية:**

ANOVA Table							
			Sum of Squares	df	Mean Square	F	Sig.
الضوابط الاستكشافية لأمن	Between Groups	(Combined)	30.841	36	.857	10.176	.000
		Linearity	24.234	1	24.234	287.864	.000

المعلومات ونظام الرقابة الداخلية * تفعيل نظام الرقابة الداخلية		Deviation from Linearity	6.608	35	.189	2.243	.000
	Within Groups		14.900	13.722	163	.084	
	Total		61.862	44.563	199		

الجدول (4-24): جدول (ANOVA) لدراسة العلاقة الخطية بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.

إنَّ جدول (ANOVA) يشيرُ من خلال قيمة (sig) التي هي أصغرُ من (α=0.05)، إلى وجودِ فروقٍ ذات دلالة إحصائية أي إنّ العلاقةَ بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية غير خطية، وبالتالي يجبُ تحديد نوع العلاقة غير الخطية بين المتغيرين.

- **تحديد أفضل نموذج للعلاقة غير الخطية:**

من المخرجات السابقة التي تبين لنا فيها أنَّ العلاقةَ بين متغيرات الدراسة غير خطية، وبالتالي نلجأُ إلى تقدير منحنى النموذج عبر (Curve Estimation) لاختيار النموذج غير الخطي الأفضل وفقاً لمعنوية معامل التحديد الأعلى أي القوة التفسيرية لهذا النموذج، وفيما يلي مخرجات النماذج غير الخطية الأشهر ذات الدلالة المعنوية حيثُ تمّ استبعاد كلّ النماذج غير المعنوية، والإبقاء على النماذج المعنوية فقط، والمقارنة بينها وفقَ معامل التحديد الأعلى:

Model Summary and Parameter Estimates									
Dependent Variable: الضوابط الاستكشافية لأمن المعلومات ونظام الرقابة الداخلية									
Equation	Model Summary					Parameter Estimates			
	R Square	F	df1	df2	Sig.	Constant	b1	b2	b3
Linear	.544	236.023	1	198	.000	1.296	.549		
Logarithmic	.595	291.346	1	198	.000	1.559	1.282		
Inverse	.608	307.672	1	198	.000	3.838	−2.583		
Quadratic	.619	159.874	2	197	.000	−.081	1.788	−.253	
Cubic	.619	106.084	3	196	.000	−.259	2.039	−.360	.014
Compound	.591	285.755	1	198	.000	1.462	1.259		
Power	.657	379.370	1	198	.000	1.625	.542		
S	.681	423.540	1	198	.000	1.452	−1.100		
Growth	.591	285.755	1	198	.000	.380	.230		

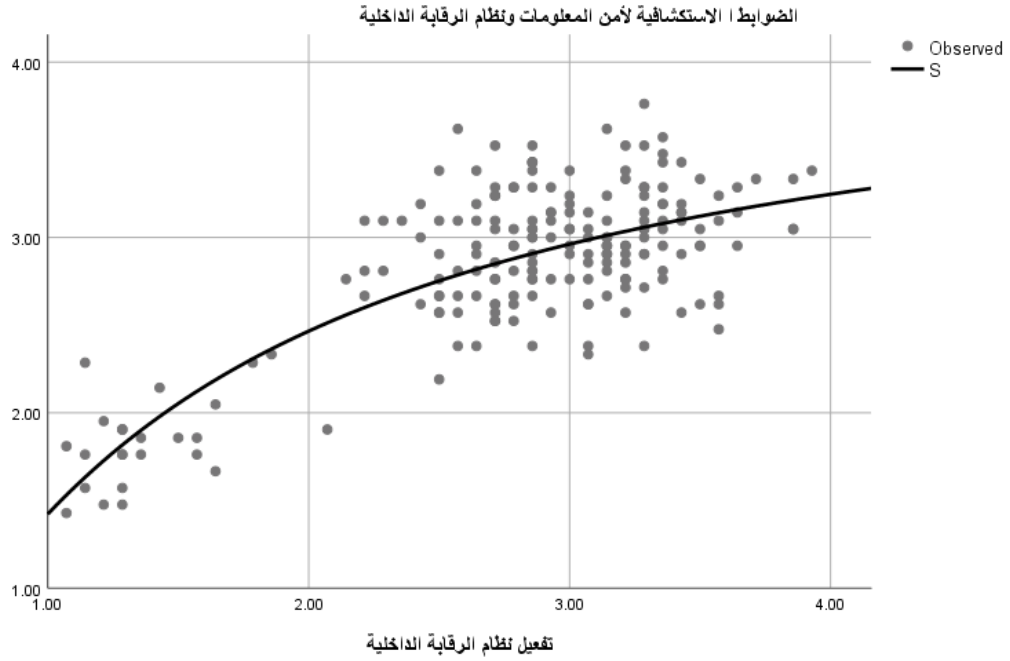
Exponential	.591	285.755	1	198	.000	1.462	.230		
Logistic	.591	285.755	1	198	.000	.684	.794		
The independent variable is تفعيل نظام الرقابة الداخلية.									

الجدول (4-25) جدول تحديد أفضل نموذج للعلاقة غير الخطية بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.

من الجدول السابق نجدُ أنَّ قيمةَ (R Square) المرافقة لنموذج الانحدار غير الخطي (S) كانت (0.681) وهي الأعلى بين النماذج ذات الدلالة الإحصائية الأخرى مما يعني أنَّ نموذج الانحدار غير الخطي (S) هو النموذجُ غير الخطي الأفضل لتقدير العلاقة بين المتغيرات المدروسة (الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية) وفيما يلي شكلُ معادلة النموذج، ورسمه البياني ذو الدلالة الإحصائية.

معادلة النموذج (s):

$$Y = e^{\left(1.452+\left(\frac{-1.100}{t}\right)\right)} \; or \; \ln(Y) = 1.452 + \left(\frac{-1.100}{t}\right)$$



الشكل (4-13): التمثيل البياني لنموذج العلاقة غير الخطية بين الضوابط الاستكشافية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.

4-3-4 اختبار الفرضية الثالثة: لا يوجد علاقةً ذات دلالة إحصائية بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية:

يتم اختبار الفرضية من خلال دراسة الارتباط البسيط للتحقق من وجود علاقةٍ بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية، حيثُ تمّ دراسةُ الارتباط باستخدام معامل الارتباط اللامعلمي سبيرمان لمناسبته لنوع البيانات التي لا تتوزع طبيعياً، إضافةً إلى أنَّ البيانات رتبية، وهو معاملُ ارتباط الرتب:

Correlations			
		الضوابط التصحيحية لأمن المعلومات ونظام الرقابة الداخلية	تفعيل نظام الرقابة الداخلية
الضوابط التصحيحية لأمن المعلومات ونظام الرقابة الداخلية	Spearman's rho	1	.764**
	Sig. (2-tailed)		.000
	N	200	200
تفعيل نظام الرقابة الداخلية	Spearman's rho	.764**	1
	Sig. (2-tailed)	.000	
	N	200	200
**. Correlation is significant at the 0.01 level (2-tailed).			

الجدول (4-26): نتائج اختبار الارتباط وفق معامل سبيرمان للفرضية الثالثة.

كلما اقتربت قيمةُ معامل الارتباط من (1) دلَّ على ارتباطٍ قوي بين المتغيرين، ونلاحظُ أنَّ قيمةَ معامل الارتباط بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية (0.764)، وبالتالي الارتباط طردي بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية، كما نلاحظُ أنَّ معاملَ الارتباط ذو دلالةٍ إحصائية من خلال قيمة (sig) التي هي أصغرُ من (α=0.05)، أي نرفضُ فرضيةَ العدم التي تقول بأنَّه لا يوجد علاقةً ذات دلالة إحصائية بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية، ونقبلُ الفرضيةَ البديلة، أي أنَّه يوجدُ علاقةً ذات دلالةٍ إحصائية بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.

Measures of Association				
	R	R Squared	Eta	Eta Squared
تفعيل نظام الرقابة الداخلية * الضوابط التصحيحية لأمن المعلومات، ونظام الرقابة الداخلية	.764	.584	.873	.761

الجدول (4-27) جدول مقياس الارتباط (Eta) بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.

بالنظر أيضاً إلى الجدول (4-27) نجدُ أنَّ قيمةَ (Eta= 0.873) وهي مقياسٌ للاقتران (الارتباط) بين المتغير التابع (الضوابط التصحيحية لأمن المعلومات)، و المتغيّر المستقل (تفعيل نظام الرقابة الداخلية) مما يشيرُ لوجودِ اقترانٍ عالٍ، أما قيمةُ (Eta-Squared=0.761) فهي تشيرُ إلى حجمِ التّأثير للمتغيّر المستقل على المتغير التابع، حيثُ إنّها تمثّل نسبةَ التباينات الكليّة للمتغيّر التابع التي يفسّرها المتغير المستقل، وقيمتها تدلّ على وجودِ تأثيرٍ عالٍ.

بعدَ التحقّقِ من وجود العلاقة، و معرفة شدّتها واتجاهها، ولدراسة الدور نقومُ ببناء نموذجِ الانحدار للتحقق من شكلِ العلاقة بين المتغيرات، وذلك من خلالِ اختبارِ العلاقة الخطية، ومجموعة الاختبارات الخاصة بتحقق شروط الانحدار:

- **اختبار العلاقة الخطية بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية:**

ANOVA Table							
			Sum of Squares	df	Mean Square	F	Sig.
الضوابط التصحيحة لامن المعلومات ونظام الرقابة الداخلية * تفعيل نظام الرقابة الداخلية	Between Groups	(Combined)	37.227	36	1.034	13.066	.000
		Linearity	29.267	1	29.267	369.808	.000
		Deviation from Linearity	7.960	35	.227	2.874	.000
	Within Groups		12.900	163	.079		
	Total		50.127	199			

الجدول (4-28): جدول (ANOVA) لدراسة العلاقة الخطية بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.

إنَّ جدول (ANOVA) يشيرُ من خلال قيمة (sig) التي هي أصغرُ من (α=0.05)، إلى وجودِ فروقٍ ذات دلالة إحصائية أي أنَّ العلاقة بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية غير خطية، وبالتالي يجبُ تحديد نوع العلاقة غير الخطية بين المتغيرين.

- **تحديد أفضل نموذج للعلاقة غير الخطية:**

من المخرجات السابقة التي تبيّن لنا فيها أنَّ العلاقةَ بين متغيّرات الدراسة غير خطيةٍ، نلجأُ إلى تقدير منحنى النموذج عبر (Curve Estimation) لاختيار النموذج غير الخطي الأفضل وفقاً لمعنوية معامل التحديد الأعلى أي القوة التفسيرية لهذا النموذج، وفيما يلي مخرجات النماذج غير الخطية الأشهر ذات الدلالة المعنوية حيثُ تمّ استبعاد كلّ النماذج غير المعنوية، والإبقاء على النماذج المعنوية فقط، والمقارنة بينها وفقَ معامل التحديد الأعلى:

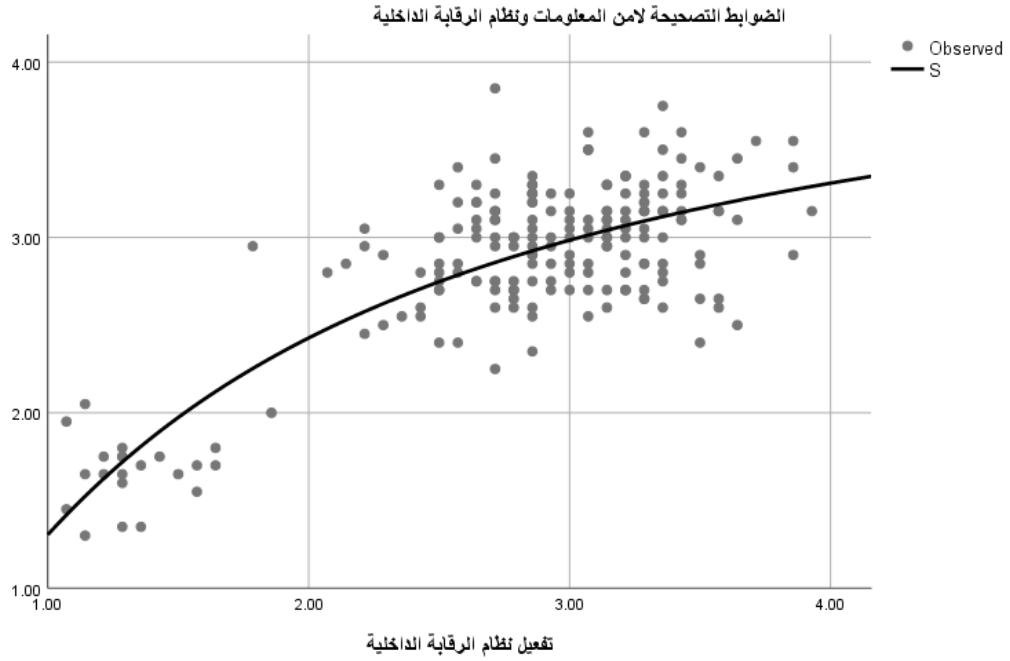
Model Summary and Parameter Estimates									
Dependent Variable: الضوابط التصحيحة لامن المعلومات ونظام الرقابة الداخلية									
Equation	Model Summary					Parameter Estimates			
	R Square	F	df1	df2	Sig.	Constant	b1	b2	b3
Linear	.584	277.794	1	198	.000	1.151	.604		
Logarithmic	.641	353.505	1	198	.000	1.439	1.411		
Inverse	.656	377.136	1	198	.000	3.948	−2.844		
Quadratic	.669	199.038	2	197	.000	−.404	2.003	−.286	
Cubic	.669	132.065	3	196	.000	−.576	2.246	−.390	.014
Compound	.623	326.606	1	198	.000	1.349	1.296		
Power	.696	452.838	1	198	.000	1.517	.611		
S	.723	516.181	1	198	.000	1.507	−1.241		
Growth	.623	326.606	1	198	.000	.299	.259		
Exponential	.623	326.606	1	198	.000	1.349	.259		
Logistic	.623	326.606	1	198	.000	.742	.772		
The independent variable is تفعيل نظام الرقابة الداخلية.									

الجدول (4-29) جدول تحديد أفضل نموذج للعلاقة غير الخطية بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.

من الجدول السابق نجدُ أنّ قيمةَ (R Square) المرافقةِ لنموذج الانحدار غير الخطي (S) كانت (0.723) وهي الأعلى بين النماذج ذاتِ الدلالة الإحصائية الأخرى، مما يعني أنَّ نموذجَ الانحدار غير الخطي (S) هو النموذجُ غير الخطي الأفضل لتقديرِ العلاقة بين المتغيرات المدروسة (الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية) وفيما يلي شكلُ معادلة النموذج، ورسمه البياني ذو الدلالة الإحصائية.

معادلة النموذج (S):

$$Y = e^{\left(1.507+\left(\frac{-1.241}{t}\right)\right)} \; or \; \ln(Y) = 1.507 + \left(\frac{-1.241}{t}\right)$$



الشكل (4-14): التمثيل البياني لنموذج العلاقة غير الخطية بين الضوابط التصحيحية لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.

4-4 النتائج والمقترحات:

4-3-1 النتائج:

توصّلت الدراسة إلى مجموعةٍ من النتائج يمكنُ عرضها وفق الآتي:

1. توجدُ علاقةً ذات دلالةٍ إحصائية بين الضوابط الوقائيّة لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.
2. توجدُ علاقةً ذات دلالةٍ إحصائية بين الضوابطِ الاستكشافيّة لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.
3. توجدُ علاقةً ذات دلالةٍ إحصائية بين الضوابطِ التصحيحيّة لأمن المعلومات، وتفعيل نظام الرقابة الداخلية.
4. لا توجدُ فروقاتٍ ذات دلالةٍ إحصائية بين آراء عينتي الدراسة.
5. يوجد دور للضوابط المختلفة لأمن المعلومات من وجهة نظر أراء عينتي الدراسة، في تحقيق الفصل بين المسؤوليات والاختصاصات ووضوح خطوط السلطة والمسؤولية.
6. يوجد دور للضوابط المختلفة لأمن المعلومات من وجهة نظر أراء عينتي الدراسة، في حماية الأصول والسجلات والتصديق على العمليات.
7. يوجد دور لتبني ضوابط أمن المعلومات المختلفة من وجهة نظر أراء عينتي الدراسة، في تحقيق الالتزام بإجراءات واساليب الرقابة الداخلية.

4-3-2 المقترحات:

1. ضرورةُ تبنّي المصارف المدرجة في سوق دمشق للأوراق المالية ضوابطَ حديثة لأمن المعلومات تواكبُ أحدثَ التطورات التكنولوجية في بيئة الأعمال بهدف تفعيل نظام الرقابة الداخلية.
2. ضرورةُ مواكبة نظم الرقابة الداخلية في المصارف التقليدية المدرجة في سوق دمشق للأوراق المالية لكافة المستجدات التكنولوجية التي تطرأُ على مكونات نظام المعلومات المختلفة.
3. ضرورةُ إجراء دوراتٍ تدريبيةٍ للعاملين في المصارف التقليدية المدرجة في سوق دمشق للأوراق المالية للوقوف على أهميّة، وكيفية تحقيق أمن المعلومات في المصارف.

مراجع الدراسة:

أولاً: المراجع العربية:

أ. الكتب:

1. اللجنة العربية للرقابة المصرفية، **سلامة وأمن المعلومات المصرفية الإلكترونية**، صندوق النقد العربي، أبو ظبي، 2017.
2. الهيئة الوطنية لخدمات الشبكة، **السياسات الوطنية لامن المعلومات**، وزارة الاتصالات والتقانة، سوريا، 2014.
3. الهيئة السعودية للمحاسبين القانونيين، **المعايير الدولية للمراجعة والفحص والتأكيدات الأخرى والخدمات ذات العلاقة**، المملكة العربية السعودية، 2020.
4. الوردات، خلف، **دليل لتدقيق لداخلي وفق المعايير الدولية الصادرة عن IIA**، الطبعة الأولى، دار الوراق للنشر والتوزيع، الأردن، 2017

ب. الأبحاث ورسائل الماجستير والدكتوراه:

1. المطيري، ناصر، **أثر استخدام تكنولوجيا المعلومات على فاعلية نظام الرقابة الداخلية في شركات النفط الكويتية**، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، 2013.
2. زهيري، ماهر، **مخاطر أمن نظم المعلومات المحاسبية الالكترونية واستراتيجيات مواجهتها**، رسالة ماجستير، جامعة تشرين، سورية، 2015.
3. النعامي، علي، سمور، حمدي، **دور تقنية المعلومات المحاسبية في تطوير نظم الرقابة الداخلية**، مجلة جامعة القدس المفتوحة للأبحاث والدراسات الإدارية والاقتصادية، المجلد الأول، العدد 2، حزيران 2015.
4. حرب، أيمن، **أثر التدقيق الداخلي في حماية أنظمة المعلومات المحاسبية في البنوك التجارية في الأردن**، Journal of Business & Management (COES&RJ-JBM), 4(4), pp. 151-171.
5. الموسوي، علي، **نظام المعلومات المحاسبي الالكتروني ودورة في تعزيز أمن المعلومات المالية**، رسالة ماجستير، جامعة القادسية، العراق، 2016.
6. الحسين، إشراقة، **أثر مخاطر نظم المعلومات المحاسبية الالكترونية على فاعلية عملية المراجعة**، رسالة ماجستير، جامعة شندي، السودان، 2017.
7. غزال، مصباح، سعيد، عمر، مهاوه، صدام، **أثر تكنولوجيا المعلومات على فاعلية نظام الرقابة الداخلية**، رسالة ماجستير، جامعة الشهيد حمه لخضر الوادي، الجزائر، 2018.
8. الجعبري، هناء، **أثر الأمن المعلوماتي على أداء شركات التأمين العاملة في فلسطين**، رسالة ماجستير، جامعة الخليل، فلسطين، 2018

9. عوكل، محمد، **إمكانية تطبيق كوبت COBIT لتحسين أداء منظمات الأعمال السورية**، أطروحة دكتوراه، جامعة دمشق، سوريا، 2018.

10. خرخاش، جميلة، **اثر تطبيق حوكمة الشركات في تفعيل أنظمة الرقابة الداخلية لدى البنوك التجارية الجزائرية**، أطروحة دكتوراه، جامعة محمد بوضياف بالمسيلة، الجزائر، 2018.

11. دهيليس، أيوب، بوطريفة، أيوب، **دور المراجع الداخلي في تحسين نظام الرقابة الداخلية في المؤسسات الاقتصادية**، رسالة ماجستير، جامعة أكلي محند أولحاج، الجزائر، 2018.

12. فيلالي، أسماء، **مستوى أمن المعلومات في المؤسسات الجزائرية ومدى تأثره بطبيعة التهديدات وطبيعة الحماية المطبقة**، أطروحة دكتوره، جامعة ابي بكر بلقايد، الجزائر، 2019.

13. حاج قويدر، قورين، **دور نظام الرقابة الداخلية في الحد من المخاطر البنكية**، جامعة حسيبة بن بوعلي الشلف، المجلة الأكاديمية للدراسات الاجتماعية والإنسانية، العدد الأول، الجزائر، 2019.

14. بن عزيزة، محمد، **دور المراجعة الداخلية في تفعيل نظام الرقابة الداخلية في المؤسسة**، رسالة ماجستير، جامعة الجيلالي بونعامة خميس مليانة، الجزائر، 2019.

15. موسى بن عيسى، بومدين، مكي، **دور نظام المعلومات المحاسبي في تعزيز الرقابة الداخلية**، رسالة ماجستير، جامعة محمد بوضياف، الجزائر، 2019.

16. السيد عبد العزيز، سمرة، **أثر الحوسبة السحابية على فعالية نظام الرقابة الداخلية في الشركات الصناعية الليبية**، جامعة قناة السويس، المجلة العلمية للدراسات التجارية والبيئية، العدد الأول، المجلد العاشر، مصر، 2019

17. آقبيق، نور، **دور الضوابط الرقابية وفق إطار COBIT في الحد من مخاطر أمن نظم المعلومات المحاسبية في شركات التأمين السورية. دراسة ميدانية**، رسالة ماجستير، جامعة دمشق، 2020.

18. بوعبد الله، فريدة، منومس، شيماء، **دور نظام المعلومات المالي في تحقيق فعالية الرقابة لداخلية**، رسالة ماجستير، معهد العلوم الاقتصادية والتجارية وعلم التسيير، الجزائر، 2020.

19. شريف، اسماعيل، **تكنولوجيا المعلومات ودورها في تطوير نظام الرقابة الداخلية**، جامعة الجفلة، مجلة الباحث للعلوم الرياضية والاجتماعية، المجلد 4 العدد 7 ، 2020

20. بن جودي، هجيرة، **إدارة المخاطر في البنوك التجارية وفق بازل (3)**، رسالة ماجستير، جامعة محمد بوضياف، الجزائر، 2020

ثانياً: المراجع الأجنبية:

أ. الكتب:

1. Romney, Marshall, Steinbart, Paul, Summers, Scott, Wood, David, **Accounting Information Systems**, 15th edition, Pearson, (2021).
2. Chopra, Abhishek, Chaudhary, Mukund, **Implementing an Information Security Management System**, APRESS, 2020.
3. Kegerreis, Mike, Schiller, Mike, Davis, Chris, **IT Auditing Using Controls to Protect Information Assets**, third edition, USA, 2020.
4. National Institute of Standards and Technology**, NIST Special Publication 800-53 (Revision 5), Security and Privacy Controls for Information Systems and Organizations**, USA, 2020.
5. Otero, Angel R., **Information Technology Control and Audit**, Fifth Edition, CRC Press Taylor & Francis Group, 2019.
6. ISACA, **COBIT 2019 FRAMEWORK: INTRODUCTION & METHODOLOGY**,2018.
7. Nieles, Michael, Dempsey, Kelley, Yan Pillitteri, Victoria, **an Introduction to Information Security**, NIST, U.S.A 2017.
8. ISACA, **Glossary of Terms English-Arabic 3rd Edition**, 2016.
9. International Organization for Standardization, **ISO / IEC 27002: 2013**, October 2013.

ب. الأبحاث:

1. Paul John Steinbart, Robyn L. Raschke, Graham Gal, William N. Dilla, **The relationship between internal audit and information security: An exploratory investigation**, International Journal of Accounting Information Systems 13 (2012).
2. Fayez Hussain Alqahtani, **Developing an Information Security Policy: A Case Study Approach**, Information Systems International Conference 2017, ISICO 2017, 6-8 November 2017, Bali, Indonesia.

3. Paul John Steinbart, Robyn L. Raschke, Graham Gal, William N. Dilla, **The influence of a good relationship between the internal audit and information security functions on information security outcomes**, Accounting, Organizations and Society (2018).
4. Thomas Stafford, George Deitz, Yaojie Li**, The role of internal audit and user training in information security policy compliance**, Managerial Auditing Journal, Volume: 33 Issue: 4, 2018.
5. Anja van Niekerk, Riaan Rudman, Risks**, controls and governance associated with internet of things technologies on accounting information**, Southern African Journal of Accountability and Auditing Research, Volume 21 Number 1, 2019.
6. Hsing-Jung Li, She-I Chang, Tawei (David) Wang and Li-Min Chang**, Information Technology Internal Control Items for the Post-Implementation Phase of Enterprise Resource Planning Systems**, Journal of Information Systems October 01, 2019.
7. Sun, PanJun, 2020, **Security and privacy protection in cloud computing: Discussions and challenges**, Journal of Network and Computer Applications 160

ت. مواقع الأنترنت:

1. www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison

الملحق (1): استبيان الدراسة.

الجمهورية العربية السورية

جامعة دمشق

كلية الاقتصاد/قسم المحاسبة

ماجستير تدقيق حسابات

السادةُ: أعضاء لجان التدقيق، المدققين الخارجيين والداخلين، مدراء الرقابة الداخلية، مسؤولي أمن المعلومات في المصارف التقليدية المدرجة في سوق دمشق للأوراق المالية.

تحيةً طيبة وبعد...

يهدفُ الاستبيان المرفق إلى استطلاع آرائكم حولَ محاور رسالة ماجستير مقدمة في جامعة دمشق كلية الاقتصاد، قسم المحاسبة، اختصاص تدقيق حسابات، حول العلاقة بين **ضوابط أمن المعلومات ونظام الرقابة الداخلية.**

يرجى التكرم بالإجابة عن الأسئلة الواردة في الاستبيان، علماً أنّ هذه البيانات لا تستخدم إلا لأغراضِ البحث العلمي فقط، ولن يتم عرضها إلا بصورةٍ إجماليةٍ رقمية ونسب مئوية.

إنَّ مشاركتَكم في هذه الدراسة ضروريٌّ جداً، حيثُ يعدُّ رأيكم، وخبرتكم في هذا المجال أحدَ مرتكزات الدراسة و، عاملاً أساسياً لاستكمالها ونجاحها، كما يمكنكم التواصل مع الباحث عبرَ البريد الالكتروني: (saria.alsawaf1@gmail.com) لتقديم أيّ إضافاتٍ، أو ملاحظات، أو استفساراتٍ، تتعلقُ بالاستبيان، والمصطلحات الواردة فيه.

كما يمكنكم تعبئةُ الاستبيان الكترونياً من خلال مسحِ علامة (QR code) الخاصة بالنموذج الالكتروني للاستبيان.

شاكرينَ تعاونكم، ومساهمتكم في هذا البحث

مع فائقِ الاحترام، والتقدير...

الباحث: سارية عبد الرحمن الصواف.

QR code

أولاً: بيانات عامة:

ـ الجنس: ذكر☐ أنثى☐

ـ الفئة العمرية: أقل من 30 سنة☐ من 30 وأقل من 45 سنة☐ من 45 وأقل من 60 سنة☐ من 60 سنة وأكثر☐

ـ المؤهل العلمي: بكالوريوس☐ دبلوم عالٍ☐ ماجستير☐ دكتوراه☐ أخرى.....

ـ التخصص: محاسبة وتدقيق☐ إدارة أعمال☐ تكنولوجيا المعلومات☐ أخرى.....

ـ الصفة الوظيفية: عضو لجان تدقيق☐ مدقق خارجي☐ مدقق داخلي☐

مسؤول رقابة داخلية☐ مسؤول أمن معلومات☐ أخرى.....

ـ الخبرة العملية: من سنة وأقل من 5 سنوات☐ من 5 سنوات وأقل من 10 سنوات☐ من 10 سنوات وأقل من 15 سنة☐ من 15 وأقل من 20 سنة☐ من 20 سنة وما فوق☐

ثانياً: محاور الدراسة:

المحور الأول: الضوابطُ الوقائيةُ لأمن المعلومات، ونظام الرقابة الداخلية:

الرقم:		موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	يسهم امتثال الإدارة العليا لضوابط أمن المعلومات في خلق بيئة رقابية فعالة.					
2	يؤثر تدريب الموظفين على متطلبات أمن المعلومات في رفع كفاءتهم التشغيلية.					
3	يتوافر دليلاً واضحاً، ومطبوعاً لضوابط أمن المعلومات.					
4	يلتزم الموظفون بدليل ضوابط أمن المعلومات.					
5	يتم تقييد الوصول إلى المعلومات ضمن النطاق المحدد لعمل الموظف.					
6	الموظفين في المصارف على دراية بمفاهيم، وأنواع العمليات الاحتيالية (الهندسة الاجتماعية...الخ).					
7	إجراء اختبارات دورية لاحتمالات اختراق نظام المعلومات.					
8	لا يسمح للموظف غير المصرح له بتنصيب البرامج على نظام المعلومات في المصرف.					
9	نظام المعلومات مصمم للتنبه بحدوث أخطاء حسابية، أو غير المقصودة عند إدخال العمليات (تجاوز الحد الائتماني للعميل ...الخ)					
10	حماية أمن المعلومات على أهمية مماثلة لحماية أمن الأصول المادية.					
11	يتم استخدام برامج متطورة لحماية الأجهزة من المخاطر التكنولوجية (Anti-Virus).					

12	يتم استخدام نسخ مُرخّصة للبرامج لضمان استمرارية عمل عناصر نظام المعلومات.					
13	يتم استخدام أجهزة انذار لضبط الوصول إلى المخدم الأساسي لنظام المعلومات.					
14	يتم استخدام المصادقات متعددة العوامل (كلمة سر، بصمة، بطاقة تعريف الكترونية...الخ) للوصول إلى مخدم نظام المعلومات.					
15	استخدام تقنية الجدران النارية لمنع الوصول إلى عناصر نظام المعلومات عبر الشبكة.					
16	لا يسمح للموظف غير المصرح له بإدخال ملحقات الكترونية على نظام المعلومات (قرص ليزي، فلاشة...الخ)					
17	يتم استخدام إجراءات مادية لمنع سرقة أحد عناصر نظام المعلومات (استخدام أقفال منع سرقة أجهزة الحاسب المحمول... الخ)					
18	تسهم البيئة الآمنة لنظم المعلومات في ضمان دقة، وموثوقية المعلومات.					
19	يحقق استخدام ضوابط الوصول التحديد الواضح للصلاحيات والمسؤوليات.					
20	تعديل الإعدادات الافتراضية للبرامج المثبتة في نظام المعلومات يزيد من الكفاءة التشغيلية.					
21	يسهم تدريب الموظفين على ضوابط امن المعلومات في تعزيز الالتزام بإجراءات الرقابة الداخلية.					

المحور الثاني: الضوابطُ الاستكشافيةُ لأمن المعلومات ، ونظام الرقابة الداخلية:

الرقم:		موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	استخدام برامج لمراقبة الدخول إلى النظام للتأكد من دخول الأشخاص المصرّح لهم.					
2	يسجل النظام العمليات التي قام بها المستخدم خلال الاستخدام.					
3	يتم تحليل سجلات الاستخدام بشكل دوري للتأكد من خطوط الصلاحيات، و المسؤوليات للعمليات.					
4	استخدم كاميرات مراقبة، وحساسات حركة في غرف المخدمات الأساسية.					
5	الاستعانة بشركات متخصصة بأمن المعلومات بشكل دوري لتحديد محاولات اختراق النظام.					
6	يعطي نظام المعلومات إشعارات لمسؤول أمن المعلومات حول إدخال عنصر جديد إلى النظام (فلاشة، ماسح ضوئي...الخ)					
7	تتعرض نظم المعلومات لمحاولات اختراق خارجية أكثر من تعرضها لمحاولات داخلية.					
8	لا يمكن الارتباط بنظام المعلومات لاسلكياً من منطقة مجاورة.					
9	لا يمكن للموظف الاتصال بشبكة الانترنت الخاصة بالمصرف من أجهزته الشخصية.					
10	نظام المعلومات مُصمّم للكشف عن محاولات الاختراق الالكترونية، وتنبيه الأطراف ذات العلاقة.					

11	تُمنح الإدارة العليا صلاحياتٍ غير محددة لتعديل، وتغير البيانات.					
12	تُعتبر مراقبة أمن المعلومات عمليةً مستمرة، وشموليةً لكافة عناصر نظام المعلومات.					
13	يوفر نظام المعلومات إجراءاتٍ تلقائية للحد من محاولات التلاعب بعناصر النظام (إقفال شاشة المستخدم، وطلب كلمة مرور ...الخ)					
14	يتم اكتشاف محاولات التلاعب، والأخطاء المتعمدة ، وغير المتعمدة ،وتنبيه الأطراف المعنية حال حدوث التهديد.					
15	يتم إجراء تدوير للموظفين في نفس القسم للكشف عن تلاعب، أو أخطاء الموظفين.					
16	استخدام أنظمة محاكاة (honeypots) والمعروفة باسم مصائد الاختراق، من أجل الكشف المبكر عن التهديدات المحتملة وتفادي الهجمات للأجزاء الهامة من نظام المعلومات.					
17	المتابعة المستمرة لالتزام الموظفين بمتطلبات أمن المعلومات يضمن الالتزامَ بالسياسات، واللوائح الخاصة بمتطلبات الرقابة الداخلية.					
18	التحليل الدوري لسجلات الاستخدام يزيدُ من حماية الأصول من التلاعب، أو السرقة.					
19	استخدام برامج خاصة لكشف التسلل إلى نظام المعلومات يزيد من دقة، وموثوقية التقارير المالية.					
20	يحقق الفصل الملائم بين الصلاحيات والمسؤوليات اكتشافَ العمليات الاحتيالية.					
21	تسهم الضوابط الاستكشافية المختلفة في زيادة الكفاءة التشغيلية للموظفين.					

المحور الثالث: الضوابط التصحيحية لأمن المعلومات، ونظام الرقابة الداخلية:

الرقم:		موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	يتمّ تدريب فرق أمن المعلومات بشكلٍ مستمرٍ للاستجابة لحوادث أمن المعلومات.					
2	مدير أمن المعلومات يتبع للإدارة العليا مباشرةً، وليس لقسم تكنولوجيا المعلومات (IT).					
3	توفير نسخة احتياطية لكافة البرامج، والملفات، والبيانات المرتبطة بنظام المعلومات.					
4	حدوث انتهاكات أمن المعلومات قد يوقف عملَ المصرف بشكلٍ كاملٍ.					
5	اكتشافُ محاولة انتهاكٍ داخلي للنظام يؤدي إلى فصلِ الموظف المسؤول مباشرةً.					
6	يتمّ اتخاذ إجراءاتٍ فورية عند اكتشاف تهديداتٍ مباشرة لأمن المعلومات.					
7	يتمّ الاحتفاظ بالنسخ الاحتياطية في أماكن آمنةٍ، وبعيدة عن موقع العمل.					
8	التعافي من أضرار تهديدات الأمن يستغرق وقتاً طويلاً قبلَ العودة للوضع الطبيعي.					

9	يتمّ تزويد الموظفين بإصدارات مُحدّثة لدليلِ ضوابط أمن المعلومات بشكلٍ دوري، ومنتظم.					
10	يتم وضع خطط مسبقة للتهديدات المتوقعة، واتخاذ الإجراءات اللازمة لتجنبها، أو معالجتها.					
11	يتم اعتبار الكوارث الطبيعية ضمنَ التهديدات المحتملة لأمن المعلومات.					
12	اكتشافُ حدوث أخطاء، أو انتهاكات يوجب تصحيحها فوراً.					
13	لا يتم البحث عن حلول لتهديدات أمن المعلومات إلا عند حدوثها فعلاً.					
14	يتم اقتراح حلولاً جديدة لمشكلات أمن المعلومات التي تمّ حلها مسبقاً.					
15	يوجد شبكةَ اتصال احتياطية في حال تعطل الشبكة الرئيسية.					
16	تدريب فرق استجابة متخصصة بأمن المعلومات يزيد من الكفاءة التشغيلية.					
17	يتوفر لدى المصرف مديراً لأمن المعلومات مما يحقق فصلَ الصلاحيات، والمسؤوليات بشكل أفضل.					
18	الفصل الملائم بين الواجبات يقدم فرصاً أفضلَ لتخفيف أضرار التهديدات الأمنية عند وقوعها.					
19	بيئة الرقابة الفعالة تضمن التزام الموظفين بالسياسات ، والضوابط مما يحقق مستوى عالٍ لأمن المعلومات.					
20	سرعة إنجاز الإجراءات التصحيحية لحوادث أمن المعلومات يزيد موثوقيةَ، وسلامة البيانات المالية.					

الملحق (2): تحكيم الاستبيان.



الجمهورية العربية السورية

جامعة دمشق

كلية الاقتصاد/قسم المحاسبة

ماجستير تدقيق حسابات

قام بتحكيم الاستبيان السادة الأساتذة الدكاترة في قسم المحاسبة، كلية الاقتصاد، جامعة دمشق:

	الأستاذ المحكم:	التوقيع:
1	د. عصام قريط	
2	د. عقبه الرضا	
3	د. سمر حبيب	

The Role of Information Security Controls in Activating the Internal Control System

(Field Study)

Prepared by: Saria Al Sawaf **Supervised by: Prof.Rasha Hamada**

Abstract

The study aimed to determine the role of information security controls in activating the internal control system, through a field study on the traditional banks listed in the Damascus Stock Exchange. The study population consisted of workers in the traditional banks listed on the Damascus Stock Exchange, as two samples were drawn from that. Society, the first sample was from independent external auditors in charge of auditing the traditional banks listed on the Damascus Stock Exchange for the year 2020 AD, and the second sample was from employees in banks within the audit committees, internal auditors, internal control officials and information security officials in those banks, and for the purposes of the study was used The descriptive and analytical approach to suit the nature and objectives of the study, in order to form a broad framework of knowledge about the variables of the study, and to prepare the field study, a questionnaire was designed to collect the necessary data from the two study samples. (224) questionnaires (24) of which were canceled due to the lack of seriousness of the answers or to the existence of a contradiction in the answers, as the number of questionnaires recovered was From the first sample (34) questionnaires, as for the number of questionnaires retrieved from the second sample (166) questionnaires, data were also analyzed using the Statistical Package for Social Sciences (SPSS - 25), and from Then testing the hypotheses, as the study reached a set of results, the most important of which are:

1. There is a statistically significant relationship between preventive controls for information security and the activation of the internal control system.

2. There is a statistically significant relationship between the exploratory controls for information security and the activation of the internal control system.

3. There is a statistically significant relationship between corrective controls for information security and the activation of the internal control system.

The Syrian Arab Republic
Damascus University
Faculty of economics
Department of Accounting

The Role of Information Security Controls in Activating the Internal Control System

(Field Study)

Prepared By:

Saria Al Sawaf

Supervised By:

Prof. Rasha Hamada

2021