الجمهورية العربية السورية
وزارة التعليم العالي
جامعة دمشق
كلية الاقتصاد
قسم المحاسبة

تقييم كفاءة أنظمة المعلومات المحاسبية في حماية البيانات والمعلومات في المصارف السورية

(دراسة مقارنة)

بحث مقدم لنيل درجة الدكتوراه في المحاسبة

إعداد

سهى شفيق سنكري

إشراف

أ.د. حسين القاضي

د.م. مادلين عبود

٢٠١٣

Damascus University
Faculty of Economic
The Department of Accounting

Assessing The Efficiency of Accounting Information Systems in Protecting The Data And Information in Syrian Banks.

(AComparative Study)

(THESIS PRESENTED FOR THE PH.D IN ACCOUNTING)

Prepared by

Souha chafik sankari

Supervised by

Dr. Madlen aboud **Dr.housen Al kadi**

2013

قائمة المحتويات

قائمة الجداول

قائمة الأشكال

تقييم كفاءة أنظمة المعلومات المحاسبية في حماية البيانات والمعلومات في المصارف السورية
(دراسة مقارنة)

الملخص

هدف البحث الى التعرف على المخاطر والمشاكل الناتجة عن استخدام البنوك والمصارف للتقنيات الحديثة وما هي إجراءات الحماية المتبعة متمثلة بالسياسات والاجراءات الادارية والفنية والرقابية المطبقة في المصارف والتي تعزز من كفاءة نظم المعلومات .ومن ثم تقييم كفاءة نظم المعلومات المحاسبية للمصارف السورية في حماية البيانات والمعلومات المحاسبية وتحديد العوامل المؤثرة في كفاءة نظام المعلومات المحاسبي على ضمان امن بياناته ومعلوماته. لتقدم بعد ذلك المساهمة العلمية في وضع حلول للمشكلات التي يتوقع ان تجابها البنوك في سوريا من جراء استخدام تطبيقات التقنية الحديثة.

تم بلوغ هدف البحث من خلال عرض مفهوم كفاءة نظم المعلومات والعوامل المؤثرة في هذه الكفاءة وواقع بيئة العمل الالكتروني بالمصارف السورية والخدمات التي تقدمها المصارف لعملائها، كما قامت الباحثة أيضاً ، ببيان المخاطر والمهددات التي تجابه إستخدامات التقنية بصورة عامة وبالبنوك بصفة خاصة وذلك في ظل إستخدام الشبكات العالمية – الإنترنت – فتفتح بذلك نافذة على مخاطر لا يمكن التغلب عليها الا باتخاذ اجراءات وسياسات وتطبيق معايير حيث ركزت الباحثة هنا على معيار الكوبيت والآيزو(٢٧٠٠١) و(٢٧٠٠٢) .

إتخذت الباحثة المصرف العقاري ومصرف عودة عينة لدراستها لمعرفة مدى تأثرها بإستخدامات تقنية المعلومات والمخاطر التي تتعرض لها، ولمعرفة الاجراءات الادارية والأمنية والفنية المتخذة للحد من مخاطر إستخدامات التقنية . وذلك من خلال تحليل و تقييم واقع حماية المعلومات والبيانات عبر مقارنة معطيات الواقع العملي لها بمعايير الأمان المحددة من المرجعيات المناسبة.

تم جمع البيانات والمعلومات اللازمة عن أنظمة المعلومات المحاسبية المستخدمة في المصارف عينة الدراسة من خلال التقارير الإدارية والإحصائيات، والمقابلات الشخصية مع

العاملين ذوي العلاقة بأمن المعلومات. كما أجريت بعض الاختبارات التجريبية كأختبار **Acunetix Website Audit** لمعرفة عدد الاختراقات والثغات التي يمكن حدوثها والتي يمكن من خلالها تحديد مستوى الحماية في بعض العمليات المصرفية الإلكترونية.

و خلص البحث إلى أن كفاءة نظم المعلومات المحاسبية في تحقيق الأمان للمصرفين محدودة نسبيا، وكان من الممكن أن تكون أفضل. فهي لم تتمكن من بلوغ مستوى متقدم من أهداف الأمان من خلال سياساتها وإجراءاتها الأمنية التي كانت رسمتها.

الإطار العام للدراسة

المقدمة:

مع بداية القرن العشرين، بدأت مرحلة جديدة في صناعة المصارف، وذلك بالتوسع في استخدام شبكات المعلومات، واعتمادها في جميع المعاملات المصرفية ، هذا بالإضافة إلى ظهور الشبكة العالمية للمعلوماتInternet ، واعتماد المصارف والشركات عليها، في تنفيذ الأعمال التجارية فيما يعرف بالتجارة الإلكترونية .e-commerce وهذا النظام يعتمد على وسائل الدفع الإلكترونية المختلفة والمتمثل في:

- العمل المصرفي من خلال الشبكة العالمية Internet Banking
- النظم المصرفية الإلكترونية(Electronic Banking System (EBS
- وسائل أخرى

مثل(Credit cards , Debit cards , E-cash, E-fund, Cyber-cash)

وكما نعلم فإن العمل المصرفي يعتمد أساساً على الثقة، سواء كان ذلك من المودعين أو المساهمين أو غيرهم من العملاء. وأن هذه الثقة تنبع أساساً من السرية والأمانة التي تتعامل بها المصارف والبنوك مع حسابات ومعلومات العملاء ودقتها وسلامتها .

وقد صاحب اعتماد المصارف والبنوك على النظم الإلكترونية، وشبكات المعلومات، تخوف من قدرة المصارف في الحفاظ على سرية المعلومات المخزنة بأجهزتها ودقتها وسلامتها، وعدم تسريبها أو تغييرها أو حذفها نتيجة للأخطار التي تتعرض لها هذه الأجهزة والنظم من قبل المتسللين عبر الشبكات، والعابثين من داخل المؤسسات المصرفية.

وفي المقابل أيضاً نشأت مشكلة أخرى متمثلة في عمليات توثيق الحركات المالية، المتعلقة بالعملاء، لنكران بعضهم ورفضهم لبعض العمليات والحركات المالية التي تنشأ منهم عبر الشبكات

كل هذه المشاكل جعلت حماية النظم والمعلومات يتصدر قائمة الإهتمامات في مجال العمل المصرفي والتجارة الإلكترونية. وهذا ما يجعل الباحثة تسعى لتغطية المخاطر والمهددات التي تتعرض لها المصارف واقتراح الإجراءات الوقائية والرقابية التي ينبغي اتخاذها لحماية البيانات والمعلومات بالمصارف وهذه الحماية تحتاج إلى توفر العديد من الإجراءات والسياسات والمعايير التي تعتمدها الإدارة لضمان تطبيقها ، ومن أهم المعايير المطبقة في المصارف هي الآيزو والكوبيت والخدمات الائتمانية لأنها من أهم المعايير التي تهتم بأمن المعلومات وسلامتها

وعليه إن تطبيق المصارف لهذه المعايير يجعل نظم المعلومات المحاسبية المطبقة لديها تتمتع بموثوقية عالية وقدرة وكفاءة على حماية بياناتها ومعلوماتها.

مشكلة الدراسة:

تتوفر الحماية البيانات والمعلومات في المصارف من خلال مجموعة من الإجراءات والقواعد والسياسات والمعايير التي ترسم بهدف الحد من المخاطر التي يمكن أن يواجهها النظام وضمان أمن البيانات. هذه المخاطر تزداد وتتنوع في ظل التبادل الإلكتروني للبيانات .

تتمثل مشكلة البحث في الإجابة عن الأسئلة التالية:

- هل يعتبر نظام المعلومات المحاسبي المصرفي كفؤاً في حماية بياناته ومعلوماته؟ وما هي العوامل المؤثرة في كفاءته؟
- هل اجراءات الحماية المطبقة في المصارف السورية تعزز من كفاءة نظم المعلومات ؟

هدف الدراسة:

يهدف البحث إلى:

١-التعرف على المخاطر والمشاكل الناتجة عن استخدام البنوك والمصارف للتقنيات الحديثة .

٢- التعرف على السياسات والاجراءات المطبقة في المصارف والتي تعزز من كفاءة نظم المعلومات .

٣- تقييم كفاءة نظم المعلومات المحاسبية للمصارف السورية في حماية البيانات والمعلومات المحاسبيةوتحديد العوامل المؤثرة في كفاءة نظام المعلومات المحاسبي على ضمان امن بياناته ومعلوماته.

٤- وضع الحلول والتوصيات الكفيلة بتوفير الأمن والحماية للمصارف .

٥- المساهمة في وضع حلول للمشكلات التي يتوقع ان تجابها البنوك في سوريا من جراء استخدام تطبيقات التقنية الحديثة.

أهمية الدراسة:

أدى إستخدام تقنيات المعلومات والاتصالات المتطورة في تشغيل نظم المعلومات إلى تزايد المخاطر والتهديدات التي تتعرض لها المصارف ، فوصل الشبكات والإنترنت من أجل بناء

تطبيقات التبادل الالكتروني للبيانات والتحويل الالكتروني للأموال، سمح للمستخدمين الخارجين النفاذ إلى نظم المعلومات الداخلية للمصرف ، وأصبح لزاماً على المصارف والمطورين لهذه النظم التفكير بالآليات التي تضمن حماية المصارف من هذه المخاطر والتهديدات أو التقليل من الأثار السلبية لها وتوفير السبل الكفيلة بحفظ هذا الكم الهائل من البيانات والمعلومات والمحافظة عليها من التراكم والضياع والاستخدام غير المشروع وبما يؤثر سلباً في أعمال المصارف واستمراريتها ، مما دعا لضرورة تبني أساليب مناسبة للعناية بها ، وحمايتها .

يستدعي وجود مثل هذه البيئة لنظم المعلومات وضع الأسس والمعايير التي تحكم ظهور هذه المعوقات ومعالجتها ، ورسم السياسات والاستراتيجيات المناسبة لضمان أمن هذه النظم ، والاستفادة من التقنيات المتجددة التي تسهل وتسرع وتزيد من دقة المعلومات المنتجة عند الاستخدام الآمن والصحيح لمدخلات النظم ومخرجاتها في بيئة تقانة المعلومات . من هذا المنطلق تنبع أهمية الدراسة على المصارف السورية ومن كونها تناولت مشكلة معاصرة تعانيها المصارف عموما والمصارف السورية كما أنها حددت جوانب الخلل في أنظمة الحماية وقدمت اقتراحاتها لتجنبها.

الدراسات السابقة:

لم تتناول الدراسات السابقة مسألة حماية بيانات نظم المعلومات المحاسبية ومعلوماتها في المصارف السورية، وخاصة في بيئة المنافسة الواسعة والتبادل الإلكتروني للبيانات. غير أن بعض الدراسات كانت أعدت حول مشكلات هذه النظم في البيئة التكنولوجية المعاصرة، وكان بعضها أعد في بيئات أخرى. وقد تم اختيار أهم الدراسات الأكثر قربا من مشكلة البحث، فيما يلي أهمها:

١- دراسة شاهين[١] ٢٠١٢"العوامل المؤثرة في كفاءة وفاعلية نظم المعلومات المحاسبية المحوسبة في المصارف التجارية العاملة في فلسطين"

تهدف هذه الدراسة إلى تحليل ومناقشة العوامل المؤثرة في مستوى كفاءة وفاعلية نظم المعلومات المحاسبية المحوسبه، وتقييم تأثيرها على تطبيقات تلك النظم في المصارف التجارية الفلسطينية، وقد تم جمع البيانات اللازمة للدراسة من خلال قائمة استقصاء وتوزيعها على عينة من العاملين في كل من دوائر المحاسبة والتدقيق ونظم المعلومات والحاسوب في المصارف بواقع (١٠) استبانات لكل

[١] شاهين، علي عبدالله، "العوامل المؤثرة في كفاءة وفاعلية نظم المعلومات المحاسبية المحوسبة في المصارف التجارية العاملة في فلسطين "،الجامعة الأسلامية غزة، ٢٠١٢

مصرف وبعدد ١٢٠ استبانة واسترد منها ١٠٣ استبانة، وقد أظهرت الدراسة وجود تأثيرات عالية لكل من العوامل المتعلقة بالبيئة القانونية والأنظمة والضوابط المهنية التنظيمية والتقنية، والثقافية والاجتماعية، والعوامل الاقتصادية على مستوى كفاءة نظم المعلومات المحاسبية وفاعليتها، غير أن تأثير تلك المتغيرات تتفاوت أحياناً بدرجات مختلفة وفقاً لمستوى الاهتمام والدعم الذي تلقاه من الإدارة المصرفية.

واختتمت الدراسة ببعض التوصيات التي من شأنها الرفع من مستوى كفاءة أداء تلك النظم وفاعليتها وتطويرها في القطاع المصرفي الفلسطيني.

٢-**دراسة قرم**[٢]، ٢٠١٢، بعنوان ""**أنظمة الدفع الإلكتروني وتطبيقها في سورية**":

هدفت الدراسة إلى معرفة الأسباب التي تحول دون التوسع في استخدام أنظمة الدفع الإلكتروني لما لها من فوائد تعود على العميل من إدارة للوقت, وتخفيض التكاليف على المصرف والحدّ من الأخطاء التي تنتج عن العمل بالأساليب التقليدية. وذلك مع الأخذ بالحسبان خصوصية المجتمع السوري. وإلى إلقاء الضوء على الوعي المصرفي لدى المجتمع والاطلاع على مراحل نقل التقانة في المصارف. كما هدفت إلى إلقاء نظرة عامة على الصيرفة الإلكترونية وأنظمة الدفع الإلكتروني من حيث الأساليب والطرق والمزايا والمخاطر, ودراسة الواقع المصرفي السوري.

قامت الدراسة باختبار المؤثرات التي تساعد أو تعيق انتشار أنظمة الدفع الإلكتروني وأثر تزايد الوعي المصرفي للعملاء، وقدرة المصرف على تقديم الخدمات الإلكترونية على انتشار هذه الأنظمة, وذلك بالاعتماد على أسلوب البحث الوصفي الاستدلالي, والاعتماد على استبيانات وُزِّعت على عملاء وموظفي المصارف الذين يشكلون عينة البحث, مع تحليل شامل للإجابات.

أهم النتائج التي خلصت إليها الرسالة:

- هناك تحول كبير في أنظمة الدفع التقليدية باتجاه أنظمة الدفع الإلكترونية. والسبب الرئيس لذلك هو خفض التكاليف وضمان خدمة العملاء (٢٤/٢٤) ساعة يومياً وعلى مدار أيام الأسبوع, ويمثل هذا التطور الربح للجميع (win-win), حيث العميل يحفظ وقته وجهده والمصرف يخفض الكلفة.
- ظهور أشكال جديدة من المعاملات والخدمات المرتبطة بالمصارف, وهي عبارة عن تنفيذ كل أو معظم ما يتعلق بالعمليات المصرفية عبر شبكة الإنترنت, أو الهاتف الثابت والجوال, أو التلفاز أو غيره, وبشكل عابر للحدود الزمانية والمكانية، ذلك لأن العملاء يفضلون الخدمة الذاتية لإدارة

[٢] قرم، عباس، "أنظمة الدفع الالكتروني وتطبيقها في سورية"، الجامعة الافتراضية السورية، رسالة ماجستير، ٢٠١٢.

أنشطتهم المالية, وبالتالي فإن المصارف التي لا تتوفر لديها التقانة المتطورة والكافية, ستواجه بلا شك نتائج سلبية تنعكس على استمرارها في السوق المصرفية, أو أقله تناقص حصتها السوقية.

٣- دراسةAbolfazl Azizi Sharif & Bagher Shamszadeh ٢٠١٢ بعنوان "مواجهة نظم المعلومات المحاسبية المحوسبة للتهديدات الامنية[٣]"

هدفت هذه الدراسة الى تحديد التهديدات الأمنية الكبيرة التي تواجه النظم المحاسبية المحوسبة والعلاقة بين أمن هذه الأنظمة و مستوى التعليم والخبرة في لمستخدمي النظام، وجودة تصميم النظام ونوع الصناعة في شركات مختلفة. وقامت هذه الدراسة باجراء . دراسة مسحية وصفية. وتحديد العلاقة بين المتغيرات أماطريقة جمع البيانات فقد تم استخدام (الاستبيانات) ، على أنظمة المحاسبة المحوسبة ل Hamadan للأوراق المالية في الفترة الزمنية من ٢٠٠٦ حتي ٢٠١١ .. وتشير النتائج إلى أن التهديدات الأمنية في شركات مختلفة في كثير من الأحيان تعود لأسباب مختلفة حسب طبيعة ونوعية التصميم لها تأثير يذكر على أمن النظام لأن معظم التهديدات لها أصل الإنسان وهناك علاقة إيجابية بين مستوى الخبرة في العمل والتعليم من المستخدمين مع نظام الضمان.

وتشير النتائج إلى أن التهديدات الأمنية في شركات مختلفة غالباً ما تكون مختلفة المنشأ وطبيعة ونوعية تصميم له تأثير ضئيل على نظام أمن لأن معظم التهديدات التي واجهت النظم تنشأ عن العنصر البشري وهناك علاقة إيجابية بين مستوى خبرة المستخدمين مع نظام الأمن.

٤-دراسة الساكني وعواودة[٤]، ٢٠١١، بعنوان " مخاطر استخدام تكنولوجيا المعلومات وأثرها على أداء نظم المعلومات المحاسبية:"

---

[3] Abolfazl Azizi Sharif and Bagher Shamszadeh: Computerized Accounting Information Systems (Cais) Versus Security Threats، Journal of Academic Research in Economics Spiru Haret University, Faculty of Accounting and Financial Management ،4 (2012)

[٤] الساكني، عبد الكريم، سعد والعواودة، علي، حنان "مخاطر استخدام تكنولوجيا المعلومات وأثرها على أداء نظم المعلومات المحاسبية" جامعة الاسراء, ٢٠١١.

هدفت الدراسة إلى قياس أثر مخاطر استخدام تكنولوجيا المعلومات على أداء نظم المعلومات المحاسبية وقد أجريت هذه الدراسة التطبيقية لعينة من الشركات المساهمة المدرجة في بورصة عمان للأوراق المالية.

تم اختيار عينة عشوائية بلغت ١٠٠ موظف من العاملين في الشركات المساهمة المدرجة في بورصة عمان للأوراق المالية. ولهذا الغرض تم توزيع الاستبانات لقياس اتجاهات العاملين حول متغيرات البحث وأثر مخاطر استخدام تكنولوجيا المعلومات على أداء نظم المعلومات المحاسبية،حيث تم اتباع المنهج الوصفي التحليلي.

أظهرت الدراسة أن هناك علاقة تأثير بين مخاطر استخدام تكنولوجيا المعلومات وأداء نظم المعلومات المحاسبية وبالتحديد مخاطر التشغيل ومخاطر عدم تحديد الصلاحيات

٥- دراسة القاسم [٥]، عبد الرزاق و ردايده مراد ، ٢٠١٠ بعنوان " أمن البيانات ونظم المعلومات المحاسبية في بيئة تكنولوجيا المعلومات في البنوك الأردنية " دراسة ميدانية

يهدف هذا البحث إلى معرفة مدى اهتمام البنوك الأردنية بتطبيق إجراءات أمن البيانات ونظم المعلومات المحاسبية، وذلك من خلال محاولة التعرف على مدى الاهتمام بالأمن المادي لوسائط التخزين، وبأمن الأفراد مستخدمي النظم الآلية والبيانات، والنظم والتطبيقات والبرمجيات، و الأجهزة والمعدات، وعمليات تبادل وحفظ وتخزين المعلومات، باستخدام استبانة مكونة من ثلاثين فقرة، وزعت على موظفي البنوك من مستوى مدير في المجال التقني أو المجال المحاسبي في البنوك المشمولة .

وتبين من النتائج أن نسبة الاهتمام بالأمن المادي للمعلومات المحاسبية ولوسائط التخزين عالٍ؛ حيث بلغت (٨٧.٣٣٪)، كما بلغت نسبة الاهتمام بأمن الأفراد (٩١.٧٣٪)، ونسبة الاهتمام بأمن النظم والتطبيقات والبرمجيات (٩٠.٦٨%)، ونسبة الاهتمام بأمن الأجهزة والمعدات (٩٠.٩٤٪)، ونسبة الاهتمام بأمن طرق الحفظ السليمة وتبادل المعلومات وتخزينها (٩٢.٥٣٪)، وهذا يدل على أن الإجراءات المتبعة لحماية البيانات والمعلومات المحاسبية كافية وشاملة.

وتم اختتام البحث بمجموعة توصيات تؤكد على ضرورة الاستمرار بتطوير وتحديث وسائل حماية البيانات ونظم المعلومات المحاسبية في بيئة تكنولوجيا المعلومات، وأماكن ووسائل حفظ وسائط

---

[٥] القاسم ، عبد الرزاق و ردايده ، مراد " أمن نظم المعلومات المحاسبية في البنوك الأردنية"– دراسة ميدانية، المجلة العربية للعلوم الادارية والاقتصادية ، لبنان ، ٢٠١٠

التخزين الآلية، وضرورة المحافظة على الوضع المرتفع لأسلوب تطوير كافة الإجراءات الكفيلة بأمن وحماية البيانات ونظم المعلومات المحاسبية ووسائط التخزين الآلية في البنوك الأردنية.

6- دراسة حمادة[٦] ،٢٠١٠" أثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية في زيادة موثوقية المعلومات المحاسبية "

تناولت هذه الدراسة الضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية وأثرها في زيادة موثوقية المعلومات المحاسبية. ولتحقيق أهداف الدراسة طورت استبانة وزعت على مكاتب مراجعة الحسابات في مدينة دمشق، وقد تضمنت الاستبانة الضوابط الرقابية العامة الأربعة لنظم المعلومات المحاسبية الإلكترونية المتمثلة في الضوابط التنظيمية –وضوابط الرقابة على الوصول– وضوابط أمن الملفات وحمايتها – وضوابط تطوير النظام وتوثيقها؛ وذلك من حيث أثرها في زيادة موثوقية المعلومات المحاسبية في الشركات وخلصت الدراسة إلى أن هناك تأثيراً كبيراً للضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية في زيادة موثوقية المعلومات المحاسبية في الشركات.

٧- دراسة زيدان و حمو، ٢٠١٠،" متطلبات أمن المعلومات المصرفية في بيئة الإنترنت "

هدفت الدراسة إلى إبراز متطلبات تحقيق الأمن المعلوماتي للبنوك في بيئة الإنترنت وسبل مواجهة عمليات الاحتيال المصرفي، مع تسليط الضوء على جهود البنوك العاملة في المملكة العربية السعودية في مواجهة قراصنة المعلومات.

توصلت الدراسة إلى وجود بنى تقنية تحتية عالمية تستخدمها المؤسسات المالية والمصارف من شأنها أن تكفل أمن وسلامة عمل هذه المؤسسات، وأن هناك تطور في مجال تقنية أمن المعلومات للتعامل مع التهديدات الأمنية ذات العلاقة بشبكة الإنترنيت، كما يوجد نقص في التشريعات والقوانين المنظمة للعمل المصرفي في بيئة الإنترنيت، وغياب معايير ومبادئ للتحري والاستعلام، وهو ما يؤدي إلى حدوث حالات احتيال مالي ومصرفي.

[٦] حمادة، رشا, "أثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الالكترونية في زيادة موثوقية المعلومات المحاسبية(دراسة ميدانية). ٢٠١٠

٨- دراسة ليدا بركات ،٢٠١٠ بعنوان "ادارة المخاطر التشغيلية في بيئة الأعمال المصرفية الالكترونية في المصارف السورية [٧]"

هدفت الدراسة الى تحديد الإجراءات الأمنية المتبعة لدى المصارف العاملة في سورية لتغطية المخاطر الأمنية في بيئة الاعمال المصرفية الالكترونية والمتعلقة بسرية وسلامة وإتاحة المعلومات كما هدفت الى تحديد الاجراءات المتبعة لضمان استمرار عمل النظام وتقييم إدراك العاملين لدى المصارف لاهمية الاجراءات الأمنية والإدارية المتبعة لتحقيق أمن النظام .

وقد استخدم الباحث الاسلوب الميداني والتجريبي في جمع البيانات من خلال إجراء المقابلات الشخصية وتوزيع الاستبانة وخلص البحث الى مجموعتين من النتائج :

١- للتعرف على الاجراءات المتبعة لدى المصارف العاملة في سوريا لمواجهة المخاطر الأمنية المتعلقة بضمان سرية وسلامة المعلومات والتحكم في الدخول الى الأنظمة والشبكات والتأكد من هوية وسماحيات المستخدمين وتخفيض خطر توقف النظام .

٢- للتعرف على آراء العاملين داخل المصارف حول الاجراءات الاساسية اللازمة لإحكام السيطرة على المخاطر الأمنية وتحقيق أمن النظام المعلوماتي للمصرف .

٩-دراسة معهد الرقابة على نظم المعلومات،٢٠٠٩،"بعنوان الضوابط الرقابية وفق معاييرالكوبيت(COBIT) "دراسة حالة شركة تشارلز سكوب للائتمان[٨]

تستخدم شركة سكوب بيئة معلومات معقدة ومتنوعة .وأصبحت هذه الشركة في السنوات الأخيرة من أكبر الشركات المالية القابضة في الولايات المتحدة لذا كان لا بد من تطوير نظامها الرقابي بما يتماشى مع هذا التطور.

شمل البحث دراسة الضوابط الرقابية المستخدمة من قبل الشركة التي منها على سبيل المثال : ضوابط الدخول – أشكال أمان النظام – الإدارة والتحكم بأمان النظام.

---

[٧] بركات ، ليدا ، "ادارة المخاطر التشغيلية في بيئة الأعمال المصرفية الالكترونية في المصارف السورية"، رسالة ماجستير ،جامعة دمشق ،٢٠١٠ .

[٨] ISACA**, COBIT Case study : Charles Schwab** .
http://www.isaca.org/Template.cfm?Section=Case_Studies3&
CONTENTID=8036&TEMPLATE=/ContentManagement/ContentDisplay.cfm), 2009, USA.

انتهى البحث إلى ضرورة تطوير الضوابط الرقابية المستخدمة بما يتماشى والتطور التكنولوجي الذي حدث في نظام المعلومات .فمع بيئة تقنية معقدة ومتنوعة يجب استخدام مستوى أعلى من الأساليب الرقابية، كما أن بيئة المعلومات تسهل تطبيق هذه الأساليب الرقابية عالية المستوى وتجعل العمل أكثر مرونة.

١٠-دراسة Sunday and Arnold ،٢٠٠٨ بعنوان "الوصول إلى الخدمات الإلكترونية اعتماداً على المعاملات الاحتيالية[9]

هدفت هذه الدراسة الى بيان أثر الصيرفة الإلكترونية على ربحية المصارف وكفاءة أعمالها وتحليل الإجراءات الأمنية المطبقة عملياً واقتراح الحل المناسب للتخفيض من الاحتيال في عمليات الصيرفة الالكترونية ، ولتحقيق أهداف الدراسة اعتمد الباحثان في النتائج التي توصلا إليها على عينة مؤلفة من ١٠٥ مدراء من مصرف Zenith Bank في نيجيريا و Nordea Bank و Skandinevisk Enskilde Bank في السويد وقد توصلت الدراسة إالى ما يلي :

- ساعد ظهور الأعمال المصرفية الإلكترونية على تحسين كفاءة وفاعلية العمل المصرفي بمعنى زيادة قدرة المصارف على تقديم خدمات أفضل لعملائها والاستجابة لمتطلباتهم في الوقت المناسب مما قلل من تذمر العملاء ولكنها لم تساعد على ربحية المصارف .
- لم تساعد بيئة الأعمال المصرفية الإلكترونية على تخفيض الاحتيال من المصارف .

وقد اقترح الباحثان أنه للحصول على بيئة صيرفة إلكترونية أكثر أمناً فإنه لابد من الإعتماد على ثلاثة عوامل على الأقل للتأكد من الهوية هي :

- كلمة المرور للتأكد مما يعرفه العميل .
- والبطاقة الذكية للتأكد مما يملكه .
- والخصائص البيولوجية للتأكد من هويته البيولوجية .

[9] O.Sunday and E.arnold “Accessing E- banking Best on resilint transaction “Blekinge,Insitute of Tecnology Master Thesis , 2008

١١-دراسة عبد الله وقطناني[١٠]، ٢٠٠٧، بعنوان " البيئة المصرفية وأثرها على كفاءة وفاعلية نظم المعلومات المحاسبية: دراسة تحليلية على المصارف التجارية في الأردن

هدفت الدراسة إلى التعرف على الخصائص والمتغيرات والعوامل التي تشكل بمجموعها البيئة المصرفية وقياس مدى تأثيرها على مستوى كفاءة نظم المعلومات المحاسبية وفاعليتها في المصارف التجارية في الأردن.

وقد تم جمع بيانات الدراسة من خلال قائمة الاستقصاء التي تم تصميمها لهذا الغرض حيث تم توزيع وأحد وخمسين استبياناً على عينة من العاملين في إدارة نظم المعلومات في المصارف التجارية في الأردن بواقع ثلاث استبيانات لكل مصرف.

بينت نتائج الدراسة درجة تأثير عالية جداً العوامل القانونية والتشريعات المهنية، والعوامل التقنية وتكنولوجيا المعلومات، على مستوى كفاءة نظم المعلومات المحاسبية وفاعليتها في المصارف التجارية في الأردن .

كما بينت نتائج التحليل الإحصائي للبيانات المتعلقة بمجتمع الدراسة أن درجة كفاءة وفاعلية نظم المعلومات المحاسبية في المصارف التجارية في الأردن تختلف باختلاف مستوى الاهتمام المبذول من قبل الإدارة المصرفية بهذه العوامل عند بناء نظم المعلومات المحاسبية وتصميمها وتطويرها.

١٢-دراسة نورالدين محمد حامد[١١]،٢٠٠٧، "بعنوان أمن نظم ومعلومات المصارف وحمايتها بإشارة خاصة للواقع السوداني"

هدفت الدراسة إلى معرفة المخاطر والمشاكل الناتجة عن استخدام البنوك والمصارف للتقنيات الحديثة، وهدف أيضاً إلى وضع الحلول والتوصيات الكفيلة بتوفير الأمن والحماية للمصارف

وخلصت الدراسة إلى وضع توصيات لحماية نظم المعلومات، ونظم المعلومات المصرفية بصورة خاصة، وذلك من واقع تجارب الآخرين، وشملت التوصيات الأهداف الأمنية الأساسية وهي سرية معلومات العملاء، وتكاملها وتوفر الخدمة وجاهزيتها، بدءاً بتوصيات لسد الثغرات بالبنوك

---

[١٠] عبد الله، خالد أمين, وقطناني، خالد بعنوان "البيئة المصرفية وأثرها على كفاءة وفاعلية نظم المعلومات المحاسبية: دراسة تحليلية على المصارف التجارية في الأردن"، الأكاديمية العربية للعلوم المالية والمصرفية، جامعة عمان الأهلية ,٢٠٠٧.

[١١] محمد حامد، نورالدين[١١]، " أمن نظم ومعلومات المصارف وحمايتها بإشارة خاصة للواقع السوداني" ، رسالة ماجستير ،جامعة النيلين ،٢٠٠٧

السودانية لتفادي أسباب السرقات وللأخذ بأسباب الحماية لمنع جرائم الحاسوب بصورة شاملة، وتمثلت التوصيات في طرق الوقاية من المهددات والمخاطر الأمنية, وسائل اكتشاف الاختراقات، وطريقة إيقافها ثم معالجة آثارها عند حدوثها.

وحثت الدراسة على أهمية تطوير سياسات أمن نظم المعلومات وحمايتها ووضع معايير ومواصفات قياسية لاستخدامات نظم المعلومات وتطبيقها بصورة فاعلة، كما حثت على أهمية وجود إدارات مؤهلة ومختصة لأمن نظم المعلومات مراجعتها وتدقيقها، بالإضافة إلى ضرورة رفع الوعي الأمني الموظفين جميعهم بشتى مستوياتهم، كما أشارت الدراسة إلى أهمية سن القوانين الرادعة لجرائم الحاسوب ودور الحكومات في ذلك وتطرق لقانون مكافحة جرائم المعلوماتية بالسودان والدول العربية وباقي دول العالم.

١٣-دراسة البحيصي وشعبان[١٢]، ٢٠٠٧، "مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المصارف العاملة في غزة":

هدفت الدراسة إلى التعرف إلى المخاطر التي تواجه نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة، والتعرف إلى أهم الأسباب التي تؤدي إلى حدوث تلك المخاطر والإجراءات التي تحول دون وقوع تلك المخاطر.

قام الباحثان بالاطلاع على الدراسات السابقة والأبحاث التي اهتمت بهذا المجال، ثم أعدا استبياناً خاصاً تم توزيعه على البنوك العاملة في محافظات قطاع غزة، ومن ثم تم تحليل البيانات التي تم جمعها ،وخلصت الدراسة إلى النتائج التالية:

١- أن مخاطر نظم المعلومات وإن كانت تحدث لدى البنوك العاملة في قطاع غزة إلا أنها تتكرر.
٢- قلة عدد موظفي تكنولوجيا المعلومات في المصارف العاملة في قطاع غزة.
٣- حدوث المخاطر يرجع إلى أسباب تتعلق بموظفي البنك نتيجة قلة الخبرة، والوعي والتدريب إضافة إلى أسباب تتعلق بإدارة المصرف نتيجة لعدم وجود سياسات واضحة ومكتوبة وضعف الإجراءات والأدوات الرقابية المطبقة لدى المصرف.
٤- المصارف العاملة في قطاع غزة تتبع إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية .

[١٢] البحيصي، محمد عصام وشعبان،حرية "مخاطر نظم المعلومات المحاسبية الألكترونية: دراسة تطبيقية على المصارف العاملة في غزة", ٢٠٠٧.

١٤-دراسة**Deborah and H.JosephWen ، 2007"بعنوان تقليل مستويات التهديد لنظم المعلومات المحاسبية، وتحدياتها لكل من الإدارة والمحاسبين والمراجعين والأكاديمين**[١٣] ".

هدفت هذه الدراسة إلى تعريف التهديدات التي تواجه نظم المعلومات المحاسبية الإلكترونية وأمن المعلومات، وتحديد العلاقة بين مستويات التهديد المختلفة، ودرجة قوة إدارة الشركة فضلاً عن درجة أمن المعلومات فيها.

وقد حددت الدراسة أنه عند مستوى التهديد الحذر يمكن اتخاذ مجموعة من القرارات المالية والإدارية والاستثمارية الرشيدة لأنها تستند إلى معلومات ملائمة وشفافة وموثوق بها، وقد توصلت الدراسة إلى مجموعة من النتائج أهمها:

– إن تطبيق مستوى ملائم من الضوابط الرقابية يضمن إنتاج معلومات مالية يمكن الاعتماد عليها إنما يقع على عاتق الإدارة في الشركة.

–إن إدراك خطر التهديد الذي تواجهه الشركات إنما يقع على عاتق المحاسبين والإدارة ومحللو النظم وعليهم أن الإبلاغ عن الأخطار الناجمة عن التهديدات التي تواجهها أنظمة المعلومات في الشركة.

١٥–دراسة [١٤]Abu–Musa، 2004، بعنوان:

"Import Threats to Compuerized Accounting Information Systems :An Empirical Study on Saudi Organizations :"

هدفت الدراسة إلى التعرف إلى المخاطر المهمة التي تهدد أمن المعلومات المحاسبية الإلكترونية في المنشآت السعودية، ولقد أظهرت نتائج الدراسة أن نسبة عالية من المنشآت التي شاركت في الاستقصاء قد عانت من وجود خسائر مالية كبيرة نتيجة بعض التهديدات على أمن نظم المعلومات المحاسبية فيها سواء من قبل أطراف داخلية أم أطراف خارجية، كما أوضحت الدراسة أن كثيراً من تلك التلاعبات والاختلاسات والتهديدات على أمن نظم المعلومات المحاسبية قد تم اكتشافها عن طريق الصدفة نتيجة لعدم كفاية وفاعلية الأدوات والضوابط الرقابية المطبقة، وأن معظم الاختلاسات

[١٣] Deborah and H. Joseph Wen: Reducing the threat levels for Accounting Information Systems Challenges for Management , Accountants, Auditors, and Academicians, The CPA Journal Publication of the New York state society of CPA, online , May (2007).

[14] Abu-Musa "Import Threats to Comptuerized Accounting Information Systems ":An Empirical Study on Saudi Organizations،2004

والتلاعبات التي تم اكتشافها قد تمت تسويتها داخلياً ولم يتم الإفصاح أو التقرير عنها للجمهور حفاظاً على سمعة الشركة وتحسين صورتها في السوق.

وخلصت الدراسة إلى أن أهم المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في المنشآت السعودية هي:

١- الإدخال المتعمد وغير المتعمد لبيانات غير صحيحة بواسطة موظفي المنشآت.

٢- إدخال فيروسات الكمبيوتر إلى النظام المحاسبي.

٣- مشاركة الموظفين في استخدام نفس كلمات السر.

٤- الكشف غير المرخص به للبيانات والمعلومات عن طريق عرضها على شاشات العرض أو طبعها على الأوراق .

٥- توجيه المطبوعات والمعلومات إلى أشخاص غير مخول لهم الاطلاع على تلك المعلومات.

١٦-دراسة Whitman [١٥]،2003

بعنوان"Enemy at the Gate : Threats to Information Security"

سعت الدراسة للإجابة على ثلاث فقرات، الأولى تتعلق بحصر التهديدات التي تواجه أمن المعلومات، والثانية تتعلق بدرجة خطورة هذه التهديدات، والثالثة تتعلق بعدد مرات حدوثها شهرياً.

قام الباحث بتقييم لعدد من الأبحاث والمقالات في مجال أمن المعلومات، وحصر التهديدات التي تواجه أمن المعلومات، ثم أعد دراسة مسحية شملت ألف موظف أغلبهم من مديري نظم المعلومات، والمديرين والمشرفين.كما أوضحت الدراسة أن التهديدات حقيقية، وخطورتها عالية، وأن الأنظمة المعرضة للتهديد يصعب حمايتها.

١٧-دراسة Skillen، ٢٠٠٣، بعنوان: Desktop Data Security

أشارت الدراسة إلى أن استخدام نظم التشغيل الموزعة، وإن كان قد أدى إلى زيادة إنتاجية نظم الحاسبات، إلا أنه قد سهل من انتهاك أمن البيانات. فعلى الرغم من أن شبكات الحاسبات مزودة بوسائل لزيادة أمنها، من خلال اتباع كلمات السر، إلا أن هذه الوسائل يمكن للمستخدمين ذوي الخبرة اختراقها. لذا ينبغي أن يتضافر التقدم في الوحدات الآلية لشبكات الحاسبات مع نظم التشغيل، بغرض زيادة أمن الحاسبات والحد من الوصول غير المصرح به لشبكات الحاسب ومن

[15] Whitman "Enemy at the Gate: Threats to Information Security" 2003

بين هذه الآليات المتطورة محلل الشبكة الإلكتروني المتقدم والذي يعمل على مراقبة المرور من خلال ارتباطه بالنظام السلكي للشبكة ومن ثم يعمل على الوقاية من التنصت الإلكتروني بغرض معرفة كلمات السر.

بالإضافة إلى الرقابة على شبكات الحاسبات من خلال الوحدات الآلية، قدمت الدراسة بعض إجراءات الرقابة على أمن الشبكات والتي تهدف إلى الحماية من الغش وفيروسات الحاسبات. ومن أهم هذه الإجراءات استخدام بطاقة الأمن تحت الحمراء حيث لا يمكن الدخول إلا بموجب هذه البطاقة وكلمة السر الصحيحة. ولمزيد من الأمن يمكن استخدام نظام الترميز الرقمي للبيانات، والذي يعمل على الوقاية من عدوى الفيروسات وسرقة البيانات .

تقييم الدراسات السابقة:

لقد كانت الدراسات السابقة مهمة جداً في طرح العديد من الموضوعات حول نظم المعلومات المحاسبية وكيفية ضمان موثوقية هذه النظم وأمن معلوماتها من خلال ضوابطها الرقابية. يلاحظ من الدراسات المعروضة أنها لم تتناول مسألة كفاءة أنظمة المعلومات المحاسبية المصرفية التي تعتمد على التبادل الإلكتروني للبيانات في حماية البيانات والمعلومات. فقد ركزت على بعض الجوانب كتوفير الأمن أو على تقييم أنظمة محلية في بيئات مختلفة.

وعليه فإن هذه الدراسة تتميز عن غيرها من الدراسات في أنها تتناول تقييم قدرة أنظمة معلومات المصارف السورية على حماية بياناتها ومعلوماتها وتحديد كفاءتها من خلال سياساتها وإجراءاتها المتبعة.

فرضيات الدراسة:

يمكن صياغة الفرضية الرئيسة التالية:

تعتبر كفاءة نظم المعلومات المحاسبي للمصارف في سورية، في البيئة التكنولوجية المعاصرة، غير قادرة على بلوغ أهدافها في ضمان أمن البيانات والمعلومات بالشكل المطلوب

تتوزع هذه الفرضية إلى فرضيات ثلاث فرعية وهي :

- الفرضية الفرعية الأولى : السياسات والاجراءات الادارية المتبعة في المصارف تعزز كفاءة نظم المعلومات.
- الفرضية الفرعية الثانية : السياسات والاجراءات الامنية المتبعة في المصارف تعزز كفاءة نظم المعلومات .

- الفرضية الفرعية الثالثة : السياسات والاجراءات الرقابية المتبعة في المصارف تعزز كفاءة نظم المعلومات .

منهجية الدراسة

تعتبر الدراسة دراسة وصفية تحليلية مقارنة

- دراسة وصفية كونها توصف واقع انظمة الأمان كما هي في الواقع،
- ودراسة تحليلية من حيث مضمونها كونها تحلل واقع أهداف الأمان وسياساته واجراءاته، لتكشف جوانب الضعف والخلل فيه،
- ودراسة مقارنة من حيث أدواتها كونها تستند في عمليات التحليل على المقارنة المرجعية مع المعايير العالمية الرائدة في مجال رقابة العمليات الالكترونية

الفصل الأول:كفاءة نظم المعلومات المحاسبية في المصارف الإلكترونية وضرورات تقييمها

المبحث الأول : كفاءة نظم المعلومات

المبحث الثاني : العمل المصرفي الإلكتروني ومخاطره

الفصل الأول :كفاءة نظم المعلومات المحاسبية في المصارف الإلكترونية

1-المبحث الأول : كفاءة نظام المعلومات

١ - 1مفهوم الكفاءة

ثمة فارق بسيط، لا بد في البداية من إظهاره، بين الحكم على كفاءة النظام المحاسبي في تحقيق الحماية للبيانات والمعلومات في المصرف، من جهة، وبين الحكم على قدرة النظام في توفير الأمان للبيانات والمعلومات لهذا المصرف. فقدرة النظام ترتبط بعوامل مختلفة كتوافر الموارد والبيئة المناسبة ووجود أهداف وسياسات وإجراءات ترتبط بأمن البيانات. وهذا ما سيكشفه البحث عند اختبار الفرضيات. وعندما يكون النظام غير قادر على توفير الأمان لبياناته ومعلوماته، فإنه دون شك سيكون أقل كفاءة مما هو مطلوب في تحقيق هدف الأمان. غير أن الكفاءة لا تقف عند هذا الحد. فهي مقياس كمي، وليس نوعياً، يعبر عن مدى بلوغ الأهداف المحددة مسبقا. وبما أن البحث يتمحور حول كفاءة نظام المعلومات المحاسبي في تحقيق الأمان للبيانات والمعلومات، فإن الهدف الذي يسعى البحث لتقييم كفاءة النظام في الوصول إليه هو أمن البيانات التي يعالجها ويخزنها النظام، والمعلومات التي ينتجها للمستخدمين. أي إن أمن البيانات والمعلومات هو هدف يسعى النظام المحاسبي إلى بلوغه.

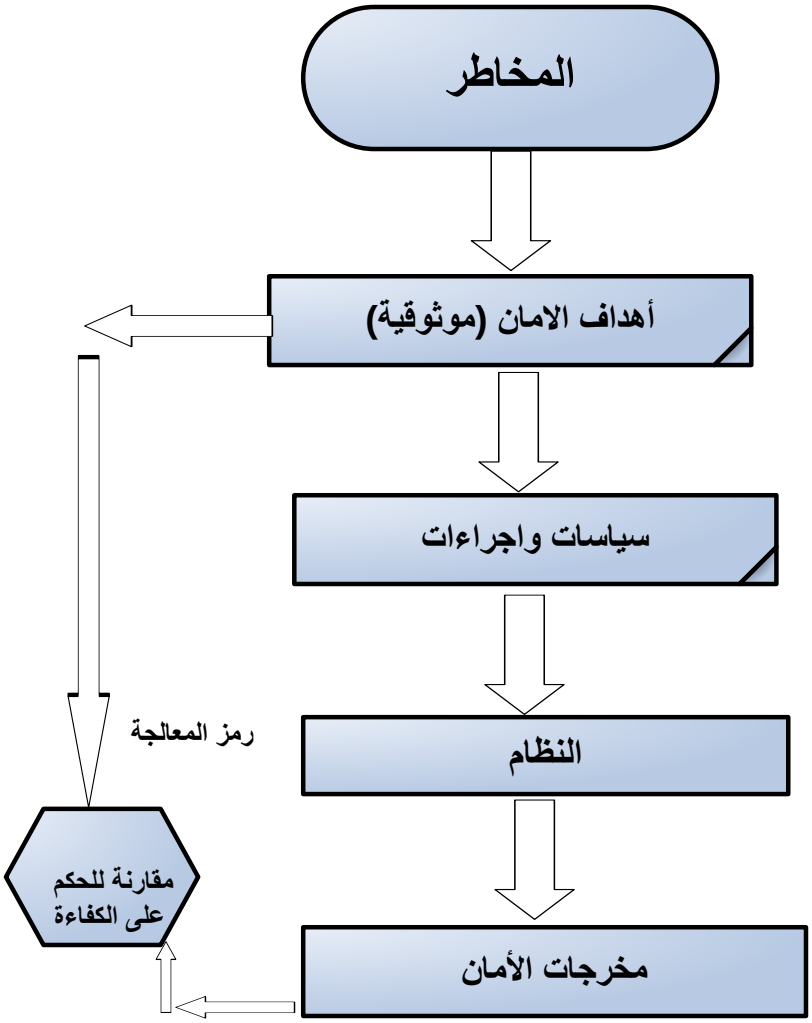
معرفة كفاءة النظام في تحقيق هدف الأمان يستوجب كشف العلاقة بين مدخلات العمليات اللازمة لبلوغ الهدف ومخرجاتها.

المدخلات في المصارف عينة الدراسة هي الموارد المخصصة لضمان أمن البيانات والمعلومات: موارد مادية، تقنية، بشرية مؤهلة ومدربة، الخ، بالإضافة إلى السياسات والإجراءات التي تضمن أمن البيانات، باعتبارها موارد تنظيمية تسهم في بلوغ هدف الأمان. وهذا ما تناوله البحث فيما سبق.

أما المخرجات فهي البيانات والمعلومات التي تتمتع بخصائص: الموثوقية والموضوعية والتي توافرها إجراءات الأمان المستخدمة من قبل نظام المعلومات. وبالتالي فإن الحكم على كفاءة النظام في تحقيق هذا الهدف يستوجب التوقف عند مثل هذه المدخلات في الواقع العملي للمصارف عينة البحث، وعند تلك المخرجات التي وفرها النظام فعليا.

غير أن الحكم على العلاقة بين المدخلات والمخرجات يجب أن يأخذ بالاعتبار وجود مدخلين مختلفين عند رسم أهداف الأمان وسياساته وإجراءاته:

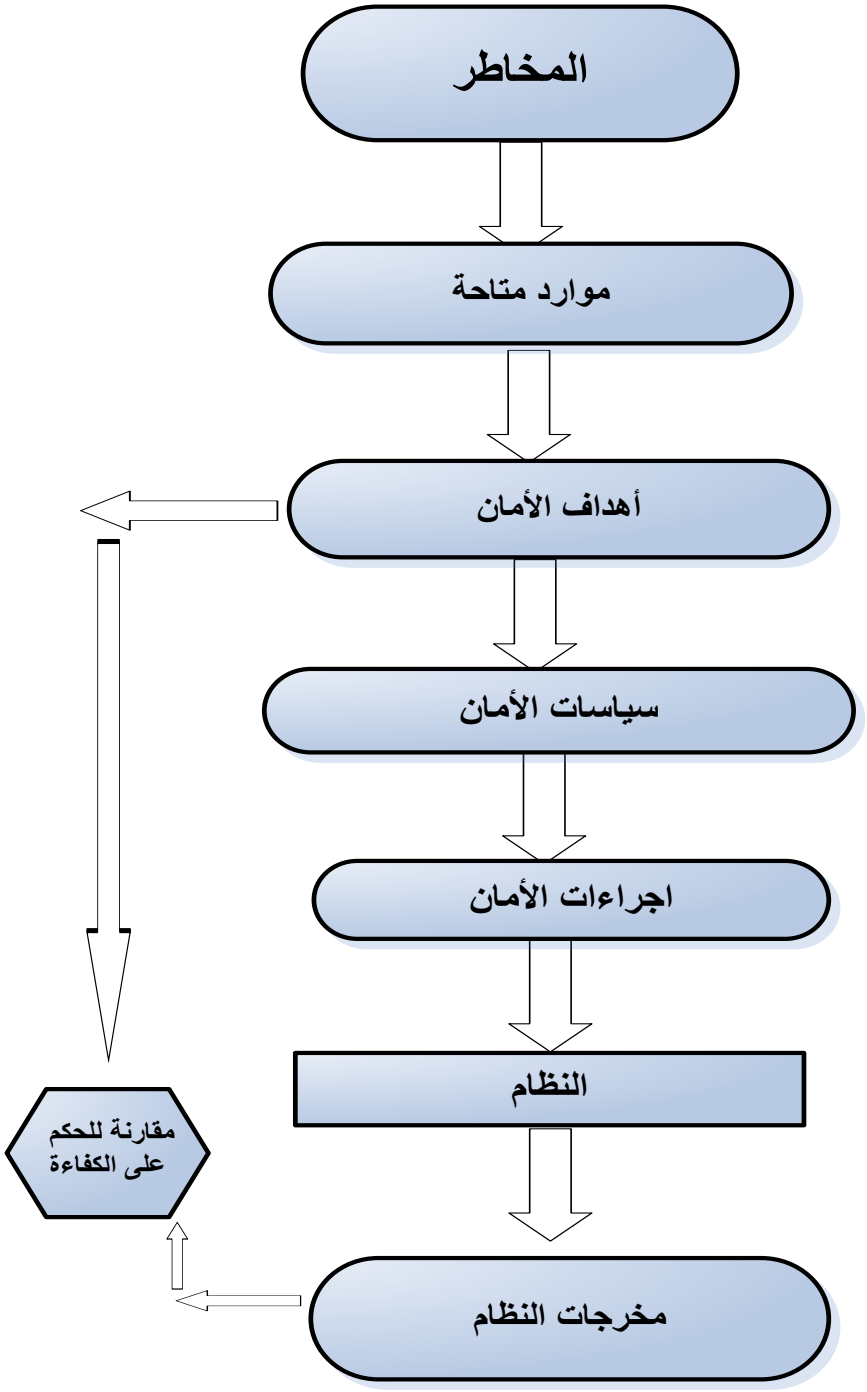
١. الأول ينطلق مخرجات مستهدفة باستخدام مدخلات وموارد غير محددة مسبقا (بغض النظر عن الموارد المتاحة). بمعنى أنه يتم الانطلاق من أهداف محددة مسبقا ترتبط بمخرجات النظام كالموثوقية وغيرها، ثم ترسم في ضوئها السياسات والإجراءات . ليتم بعدها توفير الموارد اللازمة وهكذا . عند تقييم كفاءة النظام في تحقيق الأهداف المرسومة طبقا لهذا المدخل يتم تحديد حجم الموارد المستخدمة فعليا(موارد فعلية). ثم تتم عملية المقارنة بين حجم الموارد اللازم (المخطط) والحجم المستخدم فعليا (أي مقارنة بين الموارد المخططة والموارد الفعلية). انظر الشكل التالي:



الشكل رقم (1) مقارنة بين الموارد المخططة والموارد الفعلية

المصدر: الشكل من إعداد الباحثة

٢. **الثاني** ينطلق من الموارد المتاحة للوصول إلى أفضل مستوى من الأهداف، أي استخدام أمثل للموارد. فيتم حصر الموارد المتاحة للاستخدام أولاً، ثم يتم رسم الأهداف بعدها السياسات ثم الإجراءات التي يمكن أن تساعد في الوصول إلى الأهداف،. وعند تقييم كفاءة النظام في تحقيق أهدافه طبقا لهذا المدخل، يتم تحديد الأهداف التي تم بلوغها أي الأهداف المحققة، ليتم مقابلتها مع الأهداف المرسومة مسبقا لتحديد الانحرافات، كما في الشكل التالي:



الشكل رقم (2) مقارنة أهداف محققة مع أهداف مرسومة

المصدر : الشكل من إعداد الباحثة

في بيئة العمل المصرفي في سورية، خاصة التنظيمية وكذلك المادية والتقنية، حيث الموارد المتاحة لتوفير الأمان للبيانات والمعلومات محدودة نسبياً، يسعى المصرف، عادة، إلى بلوغ أفضل مستوى من الأمان باستخدام الموارد المتاحة. ولا شك أن تحسن وتطور موارد المصرف يدفع نحو

تطوير سياسات وإجراءات الأمان. وعليه تكون مستويات الأمان متغيرة تبعا لتطور الموارد المتاحة والبيئة المحيطة بالعمل المصرفي. وتبعا لذلك يتم رسم أهداف وإجراءات أمان لتكون هدفا وموجها للممارسة العملية.

من هنا فإن السعي نحو تقييم كفاءة نظم المعلومات المحاسبية في توفير الأمان للبيانات والمعلومات، يوجب أولاً معرفة أهداف الأمان وسياساته وإجراءاته المحددة مسبقا، ثم التعرف على الأهداف التي تم بلوغها والإجراءات التي تم الالتزام بها. بعدها يتم مقارنة معطيات الواقع مع تلك المخططة للوقوف على كفاءة نظم المعلومات المحاسبية للمصارف في توفير الأمان للبيانات والمعلومات (كما في الشكل السابق).

تشكل كفاءة نظام المعلومات معيارا أساسيا للحكم على قدرة النظام على تحقيق أهدافه في توفير المعلومات المرغوب توافرها فيها بالخصائص المطلوبة. وهي ترتبط بالأداء الجيد لوظائفه.

يمكن تعريف كفاءة نظام المعلومات المحاسبي في المصارف بأنه تحقيق أكبر قدر ممكن من المخرجات (المعلومات المفيدة) ذات الجودة الملائمة وتوصيلها إلى كافة الأطراف المستفيدة في الوقت المناسب وذلك باستخدام كمية مناسبة من الموارد، مع مقارنة الناتج المحقق بالمستوى والمعايير المحددة مقدماً لأداء نظم المعلومات المحاسبية في الوحدات المصرفية[١٦].

تتجسد أهمية نظم المعلومات المحاسبية بوصفها إحدى عوامل مراقبة ومواكبة تنفيذ عمليات الخطط والسياسات، والعمل على عدم حدوث الأخطاء ومحاولة تجنبها والعمل على تصحيح مسار التنفيذ من خلال معالجة الانحرافات وتنمية الإيجابيات بأسلوب يدفع العاملين إلى تحسين الأداء وتطويره وتحقيق التعاون فيما بينهم من أجل تحقيق الأهداف المرجوة.

١-٢ العوامل المؤثرة في كفاءة نظم المعلومات المحاسبية في المصارف

في ضوء التطورات المستمرة والمتسارعة التي تحدث في نظم المعلومات وتأثيراتها الإيجابية على الأداء المالي لمنشآت الأعمال فقد أصبحت كفاءة وفاعلية تلك النظم من الأمور التي تستوجب الاهتمام وأن يكون استخدامها معاً فقد تكون المنظمة فعالة ولكنها ليست كفؤة أي إنها تحقق أهدافها بخسارة، وإن عدم كفاءة المنظمة يؤثر سلباً على فعاليتها مما يوجب أخذ كليهما في الاعتبار ضمن مقاييس نجاح نظم المعلومات، كما أن المقياس النهائي لهذه الفعالية والكفاءة يستوجب الأخذ في الاعتبار العوامل التي تؤثر فيهما خاصة في مجال العمل المصرفي، والذي تحيط به مجموعة من

١. عبد الحميد ،عبد اللطيف،" البنوك الشاملة عملياتها وإدارتها ", الدار الجامعية، مصر، ٢٠١٠ ، ص٤٤-٥٠

المتغيرات البيئية والاقتصادية والاجتماعية والتقنية وغيرها وذلك لتحقيق الأمان، كما يتضح مما يلي[١٧]:

١-٢-١ البيئة التنظيمية والإدارية الداعمة للنظام مثل الموارد البشرية الكفؤة والفعالة وكذلك المستلزمات البرمجية المستخدمة في تشغيل وإدارة الأجهزة وتطبيقاتها والتي تلعب دوراً كبيراً في تشغيل واستغلال الحاسب والشبكات وتنظيم عمل وحداته، بالإضافة إلى توفر الأجهزة والشبكات وما يرتبط بها من وسائل إدخال وإخراج ومعالجة وتخزين، هذا فضلاً عن توفر الإطار التنظيمي الذي يشتمل على تحديد المستويات الإدارية والهياكل الوظيفية التابعة لها، ويتم قياس فاعلية وكفاءة هذا الإطار من خلال المؤشرات التالية :

- درجة توفر القواعد والمعايير التي تحكم أداء العمل المصرفي.
- درجة تفويض الصلاحيات والسلطات إلى المستويات الإدارية في المصرف.
- وجود وصف وظيفي مكتوب يحدد المهام والصلاحيات والإجراءات الواجب تطبيقها.
- مدى تطبيق نظام محاسبة المسؤولية على جميع المستويات الإدارية المختلفة في المصرف.
- درجة تحقيق التكامل بين الإدارات والأقسام وتجنب التعارض بين الأنشطة في الأقسام المختلفة[١٨].

١-٢-٢ الأوضاع الاقتصادية السائدة وانعكاساتها على الأداء المصرفي وأنشطته المعلوماتية والتي يتم قياسها من خلال المؤشرات التالية:

- مؤشرات الاستقرار والنمو الاقتصادي.
- درجة تباين الأسواق التي يتعامل معها القطاع المصرفي.
- درجة المنافسة القطاعية والقدرة على التنبؤ بتصرفات المنافسين.

١-٢-٣ البيئة القانونية والضوابط المهنية المطبقة

وتتمثل في القوانين والأنظمة الحاكمة للعمل كالنظام الأساسي للمصرف وقانون السلطة النقدية والقانون المصرفي والضوابط والتعاميم المنظمة للعمل المصرفي والتي تؤثر على نظم

---

[١٧] عجمي ، منصور ،"قياس كفاءة وفاعلية النظم المحاسبية في شركات النفط الكويتية (دراسة مقارنة)"، رسالة ماجستير غير منشورة ، جامعة عمان العربية ، عمان ، الأردن ،٢٠١١،ص٦٥

[١٨] عاني،مزهر شعبان ،وشوقي، ناجي جواد،" العملية الإدارية وتكنولوجيا المعلومات"،إثراء للنشر والتوزيع الطبعة الأولى، عمان:الأردن،٢٠٠٨، ص١١٢

المعلومات المحاسبة، وبطبيعة الحال فإن البيئة القانونية والأنظمة والضوابط المتعلقة بها تعتبر من المتغيرات الهامة التي تؤثرعلى سير العمل ونظم المعلومات المحاسبة المتعلقة بها، الأمر الذي يستلزم تصميم نظم المعلومات المحاسبية بما يحقق الاعتبارات المذكورة، هذا ويتم قياس أثر هذه المتطلبات من خلال:

- تحديد أثر تطبيق الأنظمة والتشريعات القانونية ذات العلاقة بالمصارف التجارية على نظم المعلومات المحاسبية سواء كان ذلك بصورة مباشرة كقانون المصارف أو قانون السلطة النقدية أم بصورة غير مباشرة كالأنظمة والتعليمات المنظمة للأداء المالي والمصرفي.
- قياس أثر تطبيق المعايير المحاسبية الدولية والمبادئ المحاسبية المتعارف عليها وغيرها من القواعد والمعايير المهنية ذات العلاقة والأعمال المصرفية على نظم المعلومات المحاسبية[١٩].

١-٢-٤ البيئة التقنية:

ويقصد بها توفر البيئة التقنية الداعمة وتتضمن الأجهزة ومكوناتها المادية والعناصر القادرة على جمع وتخزين البيانات ومعالجتها وتوصيل المعلومات اللازمة إلى مستخدميها ومن الجدير بالذكر أن القطاع المصرفي هو القطاع الأكثر استفادة من التطورات المتسارعة وذلك نتيجة لارتفاع حدة المنافسة بين مفردات ومكونات الجهاز المصرفي والتي تستدعي مسايرة هذا التطور والتوسع في استخدام أدوات العصر[٢٠].

هذا ويمكن قياس تأثير تلك الوسائل على الجهاز المصرفي من خلال:

- مدى توفر الوسائل التقنية التي يرتكز عليها نظام المعلومات المحاسبية واللازمة لتحقيق الرقابة على مكوناته المادية والبرمجية ومخرجاته المعلوماتية.
- مدى مساهمة الوسائل التقنية المستخدمة في تحقيق الترابط والتنسيق والتكامل اللازم بين أقسام البنك المختلفة التي تدعم أنشطة وتوفر نظام فعال من المعلومات.
- مدى مساهمة الوسائل التقنية على تطوير وظائف الإدارة من تخطيط ورقابة واتخاذ القرارات وتوفر خصائص جودة المعلومات المحاسبية التي يتعين توافرها في نظام المعلومات الفعال.

---

[١٩] المجمع العربي للمحاسبين القانونين ،"المعايير الدولية لإعداد التقارير المالية "عمان ،الأردن،٢٠١٠.

[٢٠] قطناني ، خالد محمود ،" أثر خصائص البيئة التقنية وتكنولوجيا المعلومات في مخاطر الرقابة التشغيلية "دراسة تحليلية في المصارف الأردنية ، مجلة المنارة ، المجلد ١٣،العدد ٢،جامعة آل البيت ، الاردن ،٢٠٠٧،ص٩-٣٨

١-٢-٥ العوامل الاجتماعية والثقافية:

تؤثر العوامل الاجتماعية والثقافية المحيطة بالمصارف على نظم المعلومات المحاسبية وتشمل الأنماط السلوكية والرضا الوظيفي للعاملين داخل المصارف والرضا من قبل مستخدمي مخرجات النظام، مما يستوجب مراعاة العديد من تلك العوامل مثل القيم الاجتماعية والأخلاقية والفنية السائدة في المجتمع، بالإضافة إلى الإطار الثقافي والاتجاه الفكري نحو التعامل مع المنتجات المصرفية وتقنياتها المتطورة، وبالتالي فإن هذه العوامل سيكون لها تأثيراً مباشراً على الأداء المصرفي ومن ثم على نظم المعلومات المحاسبية كمخرجات لهذا الأداء.

ويمكن قياس مستوى تأثير تلك العوامل على نظم المعلومات المحاسبية من خلال درجة رضا المستخدم لهذه المعلومات والمنفعة التي تعود عليه وتلبية مطالبه، وسهولة استخدام النظام وقدرته على التعامل مع تطبيقاته والاستفادة منها.

وحول العوامل السابقة يتبين دورها المؤثر على كفاءة وفاعلية نظم المعلومات المحاسبية في القطاع المصرفي، فالقوانين والتشريعات والأنظمة والمعايير الناظمة للأداء المصرفي تشكل أساساً لضبط العمل والذي تؤدي إلى توفير معلومات دقيقة ووافية عن الأنشطة المرتبطة به والمساعدة في إنجاز المعاملات ودقتها، كما أن العوامل الإدارية والتنظيمية وما يرتبط بها من سياسات وإجراءات تشكل دوراً فاعلاً في تحقيق عناصر التناسق والترابط بين مكونات النظام مما ينعكس إيجاباً على مخرجاته، كما أن العوامل التقنية تساهم في تطوير مخرجات النظام وتعمل على زيادة قيمته الفنية المضافة والتي تؤدي إلى تحسين مستوى كفاءة وفاعلية نظام المعلومات المحاسبية ورفع مستوى جودة مخرجاتها المصرفية وبالتالي تحقيق الأمان للنظم المحاسبية من خلال تحقيق تتمثل في سرية المعلومات، سلامة المعلومة، وتوافر المعلومة .من خلال تأمين المعلومات بشكل يمكن فقط الأشخاص المصرح لهم الوصول إليها دون غيرهم (أصحاب الصلاحية أو المخول لهم). وضمان سلامة مصادر المعلومات، بحيث لا يمكن تغييرها أو تحديثها إلا من قبل الأشخاص المصرح لهم فقط أي منع اختراق النظام من اي طرف داخلي أم خارجي غير مخول له الدخول وأيضاً إمكانية وسهولة توفير المعلومات وقت الحاجة إليها .

تقلل محددات الأمان، عموما، فعالية نظام المعلومات دون شك. ولكن ليس لها بالضرورة تأثيرٌ في كفاءته. فالكفاءة ترتبط بدرجة بلوغ النظام لأهدافه. عند تحديد الأهداف يتم مراعاة هذه المحددات بالقدر الذي يتناسب مع قدرات المصرف التقنية والمادية والبشرية. ثم ترسم السياسات وتتحدّد الإجراءات التي من شأنها المساهمة في بلوغ الأهداف. وفي حال عدم بلوغ الأهداف تكون

الكفاءة ضعيفة. عدم بلوغ هدف تطوير أنظمة الحماية في الوقت المحدد، على سبيل المثال، قد تعود إلى التأخر في تنفيذ برامج التطوير المرسومة، أو إلى تأخر أو سوء تنفيذ إجراءات تأهيل وتدريب العاملين ما يؤدي إلى ضعف الكفاءات البشرية اللازمة، من ناحية التأهيل العلمي والخبرة العملية الضرورية لتشغيل أنظمة أمان متطورة تم حيازتها. أو قد تعود إلى تعذر توافر الموارد المالية الضرورية في الوقت المناسب، الخ... لتحديد كفاءة النظام في بلوغ أهداف الأمان يتم قياس المدى الذي بلغه النظام باتجاه تحقيق أهدافه، دون النظر إلى فعالية النظام. علما أن ضعف كفاءة النظام تضعف فعاليته. قد تسهم مجموعة محددات في تعذر بلوغ النظام لأهدافه منها تغيرات في الظروف المحيطة (في سوق الأجهزة الإلكترونية مثلا، مما يتسبب في عدم توافر التجهيزات التقنية الضرورية)، ضعف ثقافة أمن المعلومات لدى الإدارة والعاملين، الخ... هذه العوامل تؤخذ بالحسبان عند رسم الأهداف، وهذا يعني تحييد تأثيرات هذه العوامل التي تكون خارج سيطرة الإدارة، على عمليات تنفيذ السياسات والإجراءات. وعند تنفيذ السياسات والأهداف يبقى التأثير للعوامل الداخلية الخاصة بالمصرف مثل: مستوى التنظيم، سلامة السياسات الأمنية وإجراءات الحماية المتخذة وغيرها.

١-٣ معايير تقييم الكفاءة

1-3-1 معيار تلبية حاجات مستخدمي المعلومات وإشباعها:

انّ الهدف الأساسي لنظم المعلومات المحاسبية في أي وحدة اقتصادية هو انتاج وتوصيل المعلومات للأطراف المستفيدة سواء كانت داخلية ام خارجية، وبالتالي يجب إعداد هذه النظم بما يلائم حاجات ومتطلبات متتبعي المؤسسات المالية من المعلومات المحاسبية وبحيث تعبر مخرجات هذه النظم عن أفضل هذه المعلومات منها معلومات داخلية عن النشاط الحالي للمنظمة، معلومات داخلية عن الخطط والموازنات السابق إعدادها، معلومات خارجية عن ظروف المنافسة، الظروف التكنولوجية، المؤشرات الاقتصادية، مستجدات البيئة المصرفية[٢١]، وغيرها من المعلومات التي تمثل الاحتياجات الأساسية لاتخاذ القرارات الاستراتيجية، ونشير إلى أن هذه المعلومات (المخرجات) يجب أن تحقق الخصائص النوعية للمعلومات(الملاءمة والثقة...) التي حددها مجلس معايير المحاسبة الدولية[٢٢] **IASB**.

---

[٢١] عبد الصادق، أسامة سعيد ," التقييم المحاسبي لكفاءة وفعالية نظم المعلومات الاستراتيجية في ظل عولمة النشاط الاقتصادي بالتطبيق على البيئة المصرية"، مجلة الدرسات المالية والتجارية، جامعة القاهرة، كلية تجارة بني سويف، السنة الثانية عشر، العدد الثاني، يوليو، ٢٠٠٢، ص ٤٠٦

[٢٢] قاسم الشحادة ,عبد الرزاق, والعاصي, سعد محمد,"إطار متكامل لتقييم كفاءة نظم المعلومات المحاسبية في المؤسسات المصرفية في ظل الأزمة المالية العالمية"، المؤتمر العلمي الثاني، مرجع سابق، ص ص٧-١٢.

1-3-2 معيار تفعيل أنشطة المصرف وفعالياتها:

إنّ تفعيل نشاطات المصرف وتحقيق أهدافه بكفاءة يحتاج دوما إلى تدفق البيانات والمعلومات بين الأقسام المختلفة للمصرف، إذ أن توفير البيانات يعتبر الركيزة لأداء الأعمال في قسم من أقسام المصرف في إطار خلق التكامل والترابط المطلوب لهذه الأقسام فيما بينها، وبذلك يؤدي تكامل هذه النظم إلى تفعيل أنشطة هذه الأقسام وتزيد هذه النظم من فعالية المصرف وذلك بوجود قاعدة بيانات واسعة موحدة ومركزية تؤدي إلى تنسيق وتكامل كافة وظائف الوحدة المصرفية[٢٣]، وبالتالي فإن تكامل أنشطة وفعاليات العمل المصرفي تبقى مرهونة بوجود نظم معلومات محاسبية كفؤة تحقق للمصرف التدفق السليم للبيانات والمعلومات في الوقت والشكل السليمين[٢٤]. وكلما زادت أنشطة المصرف وتقدمت تكون هناك حاجة أكبر لتأمين حماية لهذه البيانات المعلومات.

1-3-3 المساعدة على تحقيق ميزة تنافسية:

يمكن لنظم المعلومات المحاسبية الكفؤة والمتكاملة أن تقدم المعلومات الملائمة والموثوقة بدقة وفي الوقت المناسب وبذلك تحقق تخفيضا في تكاليف الحصول على المعلومات وتحليلها، وبالتالي تسمح للمصرف بالحصول على ميزات تنافسية على منافسيها في الصناعة المصرفية سيما في ظل استخدام النظم الآلية للمعلومات.

1-3-4 معيار الرقابة والتحكم الاداري:

إن وجود نظم معلومات محاسبية كفؤة في البنوك يجب أن تؤدي إلى تحقيق نوع من الرقابة على كافة أنشطة المصرف من خلال التأكد بأن المنظمة تعمل وفقا للأسلوب المخطط وأنّ الخطة تنفذ وأنّها تتحرك نحو بلوغ أهداف المصرف المرجوة، وعليه فإن نظم معلومات محاسبية في البنوك، فضلا على أنّها تقدم معلومات عن أرصدة الحسابات في شكل قوائم مالية، فهي تقدم رقابة إدارية ومعلومات عن العمليات التشغيلية.

وتزداد أهمية الرقابة المصرفية من أجل تخفيض أثر التهديدات المالية المتعددة التي يتعرض لها المصرف. وبالتالي لكي تتمتع نظم المعلومات المحاسبية في المصارف بالكفاءة اللازمة فإن على هذه النظم تأمين الحماية الكافية لأصول وسجلات المصرف من هذه التهديدات، والمساهمة في استخدام موارد المصرف المتاحة بكفاءة، ويتم ذلك من خلال توفير كافة الإجراءات المتبعة لمواجهة

---

[23] Moscove. S.A,Simkin,MG.,Bagranoff,N.A,: Core Concepts of Accounting Information System,7th ed ,John&Sons Ltd,England, UK, 2002,p233

[٢٤] الشحادة , عبد الرزاق ,"دراسة العوامل المؤثرة في كفاءة نظم المعلومات المحاسبية في المصارف التجارية السورية", مجلة بحوث جامعة حلب، العدد ٣٤، ٢٠٠٣ ,ص٢٦

التهديدات والتحديات المحيطة بالمصرف وتشمل كلاً من الأنشطة الرقابية التقليدية والأنشطة الرقابية الآلية المؤتمتة والتي تؤكد تنفيذ عمليات الوحدة المصرفية بكفاءة وفاعلية. Garrison[٢٥],عرفت هذه الإجراءات على أنها: "عملية تنفيذ الوظائف الرقابية، حيث يسعى المدراء بأن الخطة تنفذ وعندئذ نحصل على التغذية العكسية لضمان أن كل أجزاء المنظمة تعمل بفعالية وتتحرك نحو أهداف المصرف العامة، حيث تشكل التغذية العكسية مفتاح الرقابة الفعالة" . تشكل مخرجات هذه النظم أداة رقابية فعالة. فقد بّين Bodner [٢٦] أن "نظم المعلومات المحاسبية لم تصمم من أجل توفير معلومات عن أرصدة الحسابات فحسب، بل صممت لتقدم رقابة إدارية ومعلومات عن العمليات.

وبالتالي فإنه لتحقيق الكفاءة المطلوبة في أنشطة المصرف وعملياته لا بد من وجود نظام رقابة، وهذا الأمر لن يتوافر إلا بوجود نظم معلومات محاسبية قادرة على المساعدة في إيجاد نظام رقابة متين فعال وكفء، قادر على متابعة العمليات أول بأول والتقرير عن كفاءتها وفعاليتها. حيث إن نظم المعلومات المحاسبية في المصارف والرقابة على العمليات مرتبطان يبعضهما ارتباطاً وثيقاً بالإضافة لتأمين نظام الرقابة لدرجة الثقة المطلوبة في التقارير المالية المعدة والتي تمثل مخرجات هذه النظم، وكذلك توفير المعلومات المطلوبة عن مدى الالتزام بالقوانين والتعليمات النافذة مما يمكن الإدارة من الوقوف على حقيقة الوضع واتخاذ الإجراءات والتدابير المناسبة من أجل تحقيق أعلى درجات الكفاءة الإنتاجية في المصرف[٢٧].

1-3-5 تقليل المخاطرة والمساهمة في إدارتها:

مع تنوع وتطور وتعدد الأنشطة والخدمات المصرفية أصبحت المخاطر جزءا لا يتجزأ من بيئة العمل المصرفية، حتى باتت السمة الأساسية التي تحكم نشاط البنوك هي كيفية إدارة المخاطر وليس تجنبها، وبالتالي فإنّ المخاطر هي حالة تنحرف فيها النتائج المحققة عن النتائج المتوقعة سواء كان الانحراف إيجابيا أم سلبيا، وعليه فإن تقييم المخاطر عملية مستمرة تعتمد على شبكة معلومات بعيدة المدى تولد تدفقا مستمرا من المعلومات حول أنشطة المصرف.

ونستطيع القول هنا إنه عند توافر المعايير السابقة في البيئة المصرفية تستطيع الحكم على نظم المعلومات المحاسبية بأنها كفوءة وبالتالي قادرة على تأمين الحماية اللازمة لبياناتها ومعلوماتها.

---

[25] Garrison Ray H&Noreen, Eric E& Brewer, Peter C :" Managerial accounting ", 11 th ed, Mc Graw – Hill Inc, New York, USA 2006 ,P 28

[26] Bondner George H&William S.Hopwood, Optic " Accounting Information Systems " Prentice Hall International INC,New Jersey, USA, 2000,P 182

[٢٧] سيسي ،صلاح الدين حسن ،"التسهيلات المصرفية للمؤسسات والأفراد "،دار الوسام للطباعة ، ٢٠٠٨، ص٤٤-٥٠

١- ٤ ضرورات تقييم الكفاءة في بيئة عمل المصارف المعاصرة

لقد أحدثت تكنولوجيا المعلومات تغيرات جذرية في مختلف جوانب الحياة المعاصرة. ويعتبر الجهاز المصرفي هو الأكثر استفادة من هذه التغيرات والتطورات المتسارعة، وذلك نتيجة لارتفاع حدة المنافسة بين مفردات ومكونات الجهاز المصرفي، والتي تستدعي مسايرة هذا التطور والتوسع في استخدام أدوات العصر، وزيادة حجم توظيفاتها (استثماراتها) في تقنيات النظم وتكنولوجيا المعلومات والاتصالات. توظيف هذه الاستثمارات لخدمة عملياتها وتحسين قدرتها التنافسية حيث أسهمت التطورات التكنولوجية الحديثة في مجال الأجهزة والبرمجيات ونظم الاتصالات المصارف في إعادة هندسة عملياتها وتنويع خدماتها المصرفية [٢٨].

وقد واكب التطور الاقتصادي في السنوات الأخيرة تطوراً في قطاع المصارف وفي الخدمات المصرفية للمصارف السورية وتأثر عمل المصارف بشكل كبير ايضاً بالتطور التقني خاصة في مجال معالجة البيانات ونقلها ، فظهرت تغيرات جوهرية في بيئة نظم المعلومات المحاسبية فاستخدمت الشبكات لربط جميع اقسام وادارات وفروع المصارف وللتواصل مع العملاء،وحدثت تغيرات جذرية في تكنولوجيا معالجة البيانات.

ومع تنوع وتطور الأعمال المصرفية في ظل تكنولوجيا الإتصالات والمعلومات وظهور الخدمات الإلكترونية ،إزدادت مخاطر العمل المصرفي التي يتوجب على الرقابة الداخلية تداركها وتجنب آثارها ،وازدادت اهمية الرقابة الداخلية ،خصوصا مايتعلق بأمن البيانات والمعلومات . لهذا بات على المصارف تحديد أهداف الأمان لبيانات أنظمتها ومعلوماتها ،ورسم سياساتها التي يجب أن تسهم في بلوغ تلك الأهداف ,وترجمة تلك السياسات إلى جملة من التعليمات والإجراءات واجبة التطبيق .

لم تتمكن العديد من المصارف السورية من تقديم الخدمات المصرفية المتطورة , وبقيت على خدماتها التقليدية التي لا تتمتع بمعدل عائد مرتفع لأسباب كثيرة منها :

[٢٨] الشيخ، عاصم، "الاستخدامات الإلكترونية في القطاع المصرفي، مجلة الدراسات المالية والمصرفية"، المجلد ١٠، العدد ٢، يونيو ٢٠٠٢، ص٤ - ٧.

- تخوف الإدارة من مخاطر التبادل الالكتروني للبيانات .
- عدم توفر الإمكانات المادية والبشرية للتعامل مع التكنولوجيا المعاصرة.

لهذا انحصر عدد المصارف التي قدمت خدماتها الالكترونية وكان في مقدمتها المصرف العقاري ومصرف عودة ،وقد أخذت نظم المعلومات المحاسبية على عاتقها مهمة حماية البيانات والمعلومات ، فالمستوى الجيد للحماية في النظام المحاسبية :

- تزيد من ثقة المتعاملين مع المصرف والعاملين فيه .
- تزيد موثوقية المستثمرين والمستخدمين الآخرين لمعلومات النظام المحاسبي.
- تسهم في تطور الخدمات المصرفية واتساعها وتنوعها.

أما ضعف الحماية للبيانات والمعلومات فإنه يتسبب في :

- ضعف الموثوقية بمخرجات النظام،وبالتالي ضعف موثوقية المتعاملين بالبيانات ومستخدمين معلوماته .
- تخلف العمل المصرفي وخدمات المصرف بسبب :
  - عدم القدرة على تقديم الخدمات المتطورة .
  - ضعف القرارات الإدارية لإعتمادها معلومات لا تصور حقائق .
  - تخوف المتعاملين من مخاطر تحيط بأموالهم .

ولتوفير الحماية ظهرت معايير عديدة تهتم بأمن وسلامة المعلومات أبرزها : معايير الآيزو والكوبيت والخدمات الائتمانية .

إن تطبيق المصارف لهذه المعايير يجعل نظم المعلومات المحاسبية المطبقة لديها تتمتع بقدرة وكفاءة على حماية بياناتها ومعلوماتها ، كما تشكل هذه المعايير مرجعية أساسية للحكم على كفاءة نظم المعلومات في حماية البيانات والمعلومات . وقد وضعت المصارف السورية التي تقدم خدماتها الإلكترونية نظمها لحماية وضمان أمن بياناتها ومعلوماتها وحددت أهداف الأمان لها ورسمت سياساتها التي تسهم في بلوغ تلك الأهداف وترجمت السياسات إلى تعليمات وإجراءات [٢٩].

[29] Whelpton, D., *Medical devices-measurements, quality assurance and standards: CA Caceres, HT Yolken, RJ Jones and HR Piehler American Technical Publishers Ltd, 1983, pp 306£ 32.* Journal of Biomedical Engineering, ٢٠٠٤. 6(3): p. 244

كل ما سبق جعل هناك ضرورة ملحة لتقييم كفاءة أنظمة نظم المعلومات في حماية بياناتها ومعلوماتها وذلك للوقوف على مدى تحقيق المصارف السورية للأهداف الموضوعة من خلال السياسات والإجراءات التي اتبعتها لتحقيق ذلك بالاعتماد على أهم معايير أمن المعلومات العالمية التي تساعد على تحقيق الحد الأدنى لأمن المعلومات هي: معايير الآيزو ISO والكوبيت COBIT وكذلك بعض القوانين المرتبطة بأمن المعلومات وسيتم شرح هذه المعايير لاحقاً. [٣٠]

٢- المبحث الثاني : المصارف الإلكترونية

٢-١ طبيعة العمل المصرفي الإلكتروني:

يشهد العالم منذ سنوات توسعا وتطورا في سوق المعلومات والإتصالات، حيث ارتبطت تقنيات المعلوماتية والإتصال بالعديد من الأنشطة الإقتصادية على تنوعها واختلافها, وأصبحت هذه التقنيات

[٣٠]. اتحاد المصارف العربية، المبادئ العشرة للممارسات السليمة في مجال الرقابة على، وإدارة، مخاطر التشغيل، مديرية البحوث، مجلة اتحاد المصارف العربية، إبريل ٢٠٠٣، ص٥٧ - ٦٠.

ركيزة وعنصرا هاما للتقدم والتطور وتحقيق الميزة التنافسية في تلك الأنشطة, ولعل القطاع المصرفي من ابرز القطاعات التي تأثرت بتلك التحولات, وأصبح العمل المصرفي الإلكتروني السمة الجديدة للبنوك الرائدة والمتطورة.

يضم العمل المصرفي الإلكتروني كل العمليات والنشاطات التي يتم عقدها أو تنفيذها أو الترويج لها بواسطة الوسائل الإلكترونية (مثل الهاتف والحاسوب والصراف الآلي والأنترنت وغيرها), وكذلك العمليات التي يجريها مصدروا بطاقات الدفع أو الإئتمان الإلكترونية وأيضا المؤسسات التي تتعاطى التحويلات النقدية إلكترونيا ولها مواقع للعرض والشراء والبيع[٣١].

تجري المعاملات المصرفية منذ مدة إلكترونيا في شكل آلات الصرف الأوتوماتيكية والمعاملات التليفونية. ثم إنتقلت هذه العمليات إلى شبكة الأنترنت كقناة جديدة لتقديم الخدمات المصرفية التي تحقق مزايا لكل من العملاء والبنوك, إضافة إلى كونها سريعة ومريحة ومتاحة على مدار الأربع والعشرين ساعة أيا كان مكان العميل.وعلى سبيل المثال في الولايات المتحدة الأمريكية وهي البلد السبّاق إلى استخدام تقانة المصارف الإلكترونية يزداد عدد الذين يقرؤون أو يدفعون فواتيرهم عن طريق الإنترنت باستمرار، بغض النظر عن مدى سرية هذه العمليات، فقد نشر مركز جوبيتر للأبحاث (Jupiter Research)[٣٢] تقريراً عن هذا الموضوع، بيّن فيه أن نحو ٢٩ مليون شخص استفادوا من خدمات المصارف الإلكترونية عن طريق الإنترنت خلال عام ٢٠٠٥ وأن ٥٠٪ من هؤلاء قاموا فعلاً بدفع فواتيرهم عن طريق الإنترنت. وتنبأ أن يتضاعف هذا الرقم تقريباً بحلول عام ٢٠١٠ وأن نسبة الذين سيدفعون فواتيرهم إلكترونياً تزداد ازدياداً ملحوظاً.. وتوقع أن تصل إلى ٨٥٪ من مجموع المتعاملين بحلول عام ٢٠١٠.

نسبة الذين يدفعون فواتيرهم إلكترونياً	عدد المتعاملين مع المصارف الإلكترونية (بالمليون)	السنة
%50	29.6	٢٠٠٥

[٣١] الحداد،وسيم،وآخرين" الخدمات المصرفية الالكترونية "، دار المسيرة للنشر والتوزيع والطباعة ٢٠١١،عمان، ص ٣٨

[٣٢] سعد، عامر ،" المصارف الإلكترونية خدمة مالية خارج حدود الزمان والمكان" مجلة المعلوماتية، العدد ٧ ، ٢٠٠٦، ص١

2006	35.3	%57
2007	40.9	%64
2008	46.2	%71
2009	51.3	%78
2010	56.0	%85

جدول رقم (١) احصائيات حول العمل المصرفي الالكتروني

٢-٢ أنواع المواقع الإلكترونية للمصارف

ليس كل موقع لبنك على شبكة الانترنت يعني مصرفاً الكترونياً. فمعيار تحديد المصرف الإلكتروني يبقى مثار تساؤل في البيئة العربية إلى أن يتم تشريعيا تحديد معيار منضبط في هذا الحقل. وفقا للدراسات العالمية، وتحديدا دراسات جهات الإشراف والرقابة الأمريكية والأوروبية، هناك ثلاثة صور أساسية للبنوك الالكترونية على الانترنت[٣٣]:

٢-٢-١ الموقع **المعلوماتي**، Informational وهو المستوى الأساسي للبنوك ، ويقوم بتمكين الزبائن من الاطلاع على المعلومات العامة عن المؤسسة المالية المعنية والخدمات التي تقدمها ومنتجاتها، إضافةً إلى إمكان السؤال عن الرصيد. ويجب أن تتحمل الشركة صاحبة الموقع المسؤولية القانونية تجاه الزبائن في حال عدم صحة أيٍّ من المعلومات المعروضة في الموقع عن منتجات الشركة وخدماتها والأسعار التي يجري التعامل بها، وأن تتحمل الشركة المسؤولية القانونية إذا قام موقعها بدورٍ ما في نشر فيروسات أو أي نوع من البرامج التخريبية إلى الحواسيب التي تتصل بالموقع.

يجب ألا يكون هناك أي احتمال للولوج إلى المعلومات المالية السرية للشركة أو لزبائنها. ويعتبر الموقع المعلوماتي للمصرف الإلكتروني شكلاً من أشكال الدعاية الإعلامية للمصرف، ولا يمكن للمصرف تقديم أي نوع من الخدمات لزبائنه من طريق الموقع المعلوماتي.

[٣٣] الحسيني خليل حسن مصطفى ، طارق ،البنوك الإلكترونية، جامعة بابل ،جامعة بابل ، ٢٠١١ ، ص١١

٢-٢-٢ الموقع **التفاعلي** Interactive أو الاتصالي Communicative بحيث يسمح الموقع بنوع ما من تبادل الاتصال بين المصرف وعملائه كالبريد الالكتروني وتعبئة طلبات أو نماذج بشكل مباشر أو تعديل معلومات.

٢-٢-٣ الموقع **التبادلي** Transactional وهذا هو المستوى الذي فيه يمارس المصرف خدماته وأنشطته في بيئة الكترونية، حيث تشمل هذه الصورة السماح للزبون بالوصول إلى حساباته وأدارتها وإجراء الدفعات النقدية والوفاء بقيمة الفواتير وإجراء كافة الخدمات الاستعلامية وإجراء الحوالات بين حساباته داخل المصرف أو مع جهات خارجية.

٢-٣ تأثير خدمات الصيرفة الالكترونية على العمل المصرفي

يتميز هذا العصر بسرعة تقادم المعلومات وضرورة التعامل بديناميكية مع المعلومات والتقارير والتكنولوجية، بالإضافة إلى الانتشار المذهل المتسارع للانترنيت ودوره في نشر المعارف والعلوم، وتوفير الإطلاع على آخر العلوم والأخبار والتقنيات, مما يجعل الإنسان مطالب بسرعة التصرف وإتخاد القرار, ودراسة هذا القرار بناء على معطيات ومعلومات صحيحة وحديثة. وهذا يطرح باستمرار قضايا إندماج دول العالم الثالث أو دول الجنوب في انتشار الفكر المعلوماتي وتكنولوجيا المعلومات، وهل ستسمح ظروفها بالتمتع برفاهية المعلومات والتجارة الإلكترونية, التي أمدت القطاع المصرفي بآليات حديثة جعلته أكثر مرونة وديناميكية وسرعة في تقديم خدماته. فقد ظهر ما يسمى بالمصارف الإلكترونية, والصيرفة الإلكترونية من خلال الصرافات الآلية, والصيرفة عبر الهاتف, وعبر الهاتف الجوال وغيرها من الآليات المتطورة.

تميز العمل المصرفي في هذا العصر بالإعتماد على تكنولوجيا المعلومات والإتصال, بغية تطوير نظم ووسائل تقديم الخدمات المصرفية, ورفع كفاءة وأداء الخدمة المصرفية بما يتماشى والتقدم المتسارع الذي مس الصناعة المصرفية في هذا القرن. وفي هذا السياق تسعى الدول المتقدمة لتكثيف إستخدام أحدث تقنيات المعلومات والإتصال, وتحقيق هدف خفض العمليات المصرفية التي تتم داخل فرع المصرف، لتصل إلى ١٠ % من إجمالي العمليات بينما تتم العمليات الأخرى بواسطة قنوات إلكترونية مثل أجهزة الصرف الآلي ونقاط البيع الإلكترونية.

ترتب على تكنولوجيا المعلومات والإتصال في العمل المصرفي تغييرات كثيرة أهمها[٣٤]:

---

[٣٤] النجار فريد ، النجار وليد وآخرون، وسائل المدفوعات الالكترونية – التجارة والأعمال الالكترونية المتكاملة – الدار الجامعية، الإسكندرية، ٢٠٠٦، ص: ١١٨

- انخفاض تكلفة التشغيل
- تزايد أهمية إستخدام وسائل الدفع الإلكترونية
- تزايد حجم المعاملات الإلكترونية عبر الحدود بين عملاء البنوك والشركات التجارية بواسطة التجارة الإلكترونية
- تحرير العملاء من قيود الزمان والمكان وظهور ما يعرف بالخدمات المنزلية المصرفية وظهور المصارف الإلكترونية،
- تقديم خدمات لم تكن معروفة من قبل كأجهزة الصراف الآلي والمصرف المحمول

ولكي تتم الإستفادة من تطبيق التكنولوجيا المصرفية وتطوير جودة الخدمات المصرفية والإرتقاء إلى مستوى التحديات التي تواجه العمل المصرفي لا بد من[٣٥]:

- إيجاد بيئة قانونية وتشريعية مناسبة .
- تنويع الخدمات المصرفية وتقليل التكاليف, خاصة في ظل المنافسة التي أصبحت تواجه البنوك, وفي ظل تحرير تجارة الخدمات المالية, وظهور نظام البنوك الشاملة.
- الإرتقاء بالعنصر البشري, بإعتباره أحد الركائز الأساسية للإرتقاء بالعمل المصرفي .
- تطوير التسويق المصرفي باعتباره أمرا ملحا في ظل احتدام المنافسة .
- مواكبة المعايير الدولية التي فرضتها الساحة المصرفية العالمية والمؤسسات الدولية, عن طريق تدعيم راس مال المصرف وتطوير السياسات الائتمانية للبنوك والاهتمام بإدارة المخاطر مع تحديث نظم الإدارة.

٢-٣-١أسباب الاتجاه نحو الصيرفة الإلكترونية

تعود هذه الأسباب إلى [٣٦]:

---

[٣٥] ٢-٩- ٢٠١١ www.bank.org/arabic/period www.Bank.Of.cd.com

[٣٦] بختي إبراهيم , " الأنترنت في الجزائر " مجلة الباحث، مجلة فصلية نصف سنوية تصدر عن كلية ا لحقوق والعلوم الإقتصادية جامعة ورقلة ،٢٠٠٢ عدد1 ص: ٣١ -33

اشتداد المنافسة في صناعة الخدمات المصرفية: حيث أن المؤسسات المصرفية وغير المصرفية تتسابق لاستحداث خدمات ومنتجات مالية كثيرة ومصرفية جديدة وتسعى دوما هذه المؤسسات إلى أن تطور نسبة زبائنها والمتعاقدين معها لتحقق أعلى ربح ممكن أو أعلى حصة سوقية ممكنة.

تسارع التطور التقني في مجال أنظمة الاتصالات والأجهزة والبرمجيات: حيث تمكننا هذه البرمجيات والأدوات من معالجة المعاملات المالية والمصرفية بسرعة كبيرة وجودة عالية وتسهل على المؤسسات الزيادة الكبيرة في حجم العمليات المصرفية فيما لو أجريت بالعمليات القليدية.

افتقاد العديد من المؤسسات المالية والمصرفية للكادر: هذا الكادر يجب أن يملك الخبرة والعلم والدراية من الناحة التقنية وإدارة المخاطر بالعمليات المصرفية الإلكترونية لكي يتمكن من معرفة وقياس حجم هذه الأخطار ورسم الخطط البديلة ووضع الحلول المناسبة لها كوننا نتعامل مع سلعة مهمة جداً وهي الأموال وإلا لفقدت المؤسسة الكثير من أرباحها وقد يؤدي ذلك بها للإفلاس.

تزايد الاعتماد على التعاقد مع جهات خارجية بتقديم هذه الخدمات: في الآونة الأخيرة بدت ظاهرة جديدة بحثت المصارف عنها كمورد إضافي وهو التعاقد مع المؤسسات الخارجية وتأمين مجموعة من الخدمات إليها وبناء تحالفات معها بغية تسهيل الإجراءات المالية فيها مما يساعد هذه المؤسسات ويقدم أرباح إضافية لقاء الخدمات المقدمة من المصرف للمؤسسات المالية.

تزايد الحاجة على المستوى الدولي: وهو نتيجة لوجود بنى تحتية عالمية مرنة وقابلة للاستخدام من قبل المؤسسات سواء لعملياتها الداخلية أو للأطراف الخارجية هذا كله يكفل لهذه المؤسسات الوقت والتكلفة ويؤمن السلامة والأمان ويوفر الملومات والخدمات بشكل آني وسريع.

تزايد امكانية حدوث احتيال مالي: تحدث هذه الأمور عندما تغيب المعايير والمبادئ الفعالة ويكون لدينا ضعف في الرقابة وبكلا الأحوال الرقابة التقليدية صعبة التطبيق رغم دقتها أما الآن يوجد ضوابط ومعايير تحدد هوية المستخدم بشكل دقيق وتممنع حدوث هذه العمليات بنسب أكبر واحتمالات أصغر[٣٧].

ظهور قضايا انتهاك الخصوصية: نتيجة لمحاولات السرقة والاختلاس التي يمكن أن تحدث لسرقة دفتر شيكات أو بطاقة ائتمان أو غيرها من العمليات الأخرى.

---

[٣٧] رحيم حسيد ،هواري معراج"الصيرفة الالكترونية كمدخل لمعرفة المصارف الجزائرية"الملتقى الوطني الأول حول المنظومة المصرفية والتحولات الاقتصادية واقع وتحديات،١٤-١٥/١٢/٢٠٠٤ جامعة شلف ص٣١٦

بشكل عام يمكن القول أن الأمور والعمليات التي يمكن أن تطبق على العمليات المصرفية التقليدية يمكن أن تطبق على العمليات المصرفية الالكترونية، وأن حجم التضخم الكبير في العمليات المصرفية التقليدية يتطلب كما هائلا من المعالجة واجراء مجموعة كبيرة من الحسابات والعمليات المصرفية التي تم اختصارها وتسهيلها في عمليات الصيرفة الإلكترونية.

٢-٣-٢أنواع خدمات الصيرفة الإلكترونية:

تتعدد خدمات الصيرفية الإلكترونية، وذلك حسب الوسيلة المستخدمة، من أهم تلك الخدمات أو الوسائل مايلي[٣٨]:

- **خدمات الصيرفية الإلكترونية من خلال الصرافات الآليةATM**

تعتبر الصرافات الآلية أول آلية لأتمتة العمل المصرفي حيث تعتمد على وجود شبكة من الإتصالات تربط فرع المصرف الواحد أو فروع كل البنوك في حالة قيامها بخدمة أي عمل من أي مصرف، وقد تطور عمل الصرافات الآلية من قيامها بالوصول إلى بيانات حسابات العملاء فوريا، إلى تقديم خدمات متقدمة في صرف المبالغ النقدية، فأصبحت تقوم بدفع الفواتير للمؤسسات الخدمية وتسديد الرسوم الحكومية,وبظهور البطاقات الذكية أصبح العميل بإمكانه شحن تلك البطاقات وإستخدامها في دفع إلتزاماته في نقاط دفع متعددة[٣٩].

- **خدمات الصيرفة الإلكترونية عبر الهاتفPHONE :**

تعتمد هذه الخدمة كذلك على وجود شبكة تربط فروع المصرف الواحد ككل وتمكن الموظف من الوصول لبيانات العميل مباشرة من أي فروع المصرف، ويقوم العميل بالاتصال برقم موحد للحصول على خدمة محددة من مصرفة, يتكفل الموظف بعد ذلك بالرد على العميل من الوصول إلى بيانات حول العميل ويبدأ بتوجيه أسئلة محددة للتأكد من هويته،كالسؤال عن آخر معاملة قام بها، أوحجم المبلغ الذي قام بإيداعه....إلخ.ولقد وصلت آخر التطورات الآن إلى إستخدام مراكز للإتصال في الإجابة على رسائل البريد الإلكتروني والذي اصبح أداة فعالة في التخاطب بين المصرف والعميل، وأصبح الإتجاه اليوم نحو الدمج وتكوين المؤسسات الكبيرة عن طريق لجوء بعض المصارف إلى المشاركة في مراكز الخدمات الهاتفية المصرفية مما أدى إلى تقليل التكلفة الكلية وتوحيد الجهد[٤٠].

---

[38] Mark Ciampa, Second Edition, Thomson Course Technology, 2005 chapter 6 , p22

[39] E-Banking, http://www.arablaw.org/Download/E-Banking.doc, consulté le 20/06/2004 ,p 6

[٤٠] عبد المنعم راضي، فرج عزت، اقتصاديات النقود والبنوك، البيان للطباعة والنشر، الاسكندرية، ٢٠٠١، ص ٣١.

- **الصيرفة عبر شبكات الإتصالات :**

ينتمي هذا النوع من الخدمات الى مجموع الخدمات التي يطلق عليها الخدمات المصرفية من المترل(home banking) الخدمات المصرفية الذاتية ،(self-serving banking) الخدمات المصرفية عبر الانترنت (online banking)، الخدمات المصرفية عن بعد (remote banking) وأسماء أخرى متعددة.

بدأت المصارف تدريجيا تبني خدمات مصرفية عبر الأنترنت نظرا لقلة تكاليفها. وقد ساعد هذا التدرج في تقبل العملاء لهذه الخدمة والتأقلم معها والتدريب عليها. وكان الهدف من إستعمال الأنترنت في المصارف هو اقامة مصرف كامل يقدم خدماته للعملاء وهو ما يطلق عليه المصرف الإفتراضي [٤١](virtual bank).

تتميز الخدمة المصرفية من خلال الأنترنت برخص تكلفتها وتوفيرها لراحة للعملاء. يحتاج المصرف لتقديم هذا النوع من الخدمة داخل البلاد على الأقل إلى توفير شبكات واسعة (wide area network) وربطها بالشبكة العالمية. وتتطلب من العميل معرفة إستخدام برنامج التصفح على الشبكة (browser). يمثل عامل الأمن الهاجس الأكبر لإنتشار هذه الخدمة[٤٢].

يختلف هذا الشكل من أشكال أنظمة الصيرفة الالكتروني في عدم اعتماده على أدوات محسوسة بشكل رئيسي كونها تعمل على الشبكة العالمية، وهو ما أوجب وضع بروتوكولات أمن وسلامة البيانات مثل بروتوكول (SSL / TLS) [٤٣]. فالاتصالات الآمنة الأكثر شيوعاً تستخدم بروتوكولي: Secure Sockets Layer (SSL) و(TLS) Transport Layer Security.

---

[٤١] عرب يونس ،الملتقى السابع لمجتمع الاعمال العربي – البحرين ١٨-٢٠ اكتوبر / تشرين اول ٢٠٠٣ ورقة عمل مخاطر الانفتاح الالكتروني , ,الاردنhttp://www.arablaw.org/

[42], Kenneth C. Laudon, Carol Guercio Traver, E-Commerce , Prentice Hall,2011,p233-256

[43] Efraim Turban, PH.D., Electronic Commerce: Global Edition, Pearson Education, Limited, 2010,p412-420

بروتوكول SSL طوّر من قبل شركة Netscape لنقل المستندات بطريقة آمنة عبر الانترنت. هذا البروتوكول يستخدم مفتاح خاص لتشفير المعلومات المتبادلة على اتصال (SSL). وما يتم الآن استخدامه في الاتصالات هو النسخة الثانية من البروتوكول.

هناك بروتوكول آخر هو Personal Communication Technology ويرمز له بالرمز (PCT) وهو شبيه جداً ببروتوكول SSL، إلا أنه يستخدم خوارزميات أكثر تقدماً ومفاتيح تشفير أطول، وهو من تطوير شركة مايكروسوفت (Microsoft).

عقب ذلك صدر بروتوكول Transport Layer Security (TLS) إضافة إلى بروتوكول (SSL)، ويسمّون معاً (SSL / TLS)، ليضمنا الخصوصية (Privacy) ودقة البيانات (Data Integrity) بين كل تطبيقين متصلين عن طريق الانترنت.

بشكل عام يتكون بروتوكول (SSL/TLS) من طبقتين[٤٤]:

- **بروتوكول مصافحة الأيدي (Handshake Protocol TLS):**

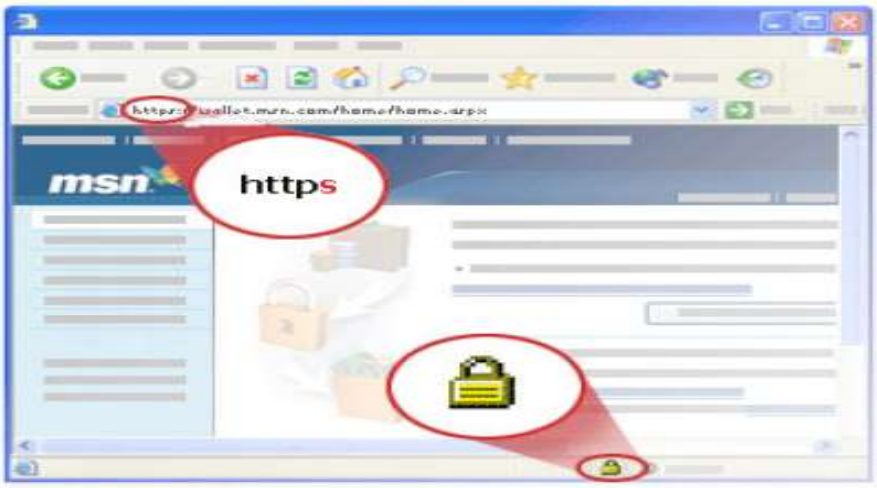
ويستخدم لاثبات شرعيـة الخادم (server) والموكّل (client) والتفاوض في خوارزمية التشفير ومفاتيحه قبل السماح للبيانات بالانتقال بين الخادم والموكل.

- **بروتوكول التسجيل (Protocol TLS Record):**

يسمح للخادم والموكّل بالاتصال فيما بينهما باستخدام نماذج خوارزميات التشفير أو بدون تشفير عند الحاجة لذلك.

إن أكثر الاستخدامات شيوعاً في الاتصالات الآمنة بين الخادم والموكّل تستخدم بروتوكول (SSL) وهي عبارة عن http بسيط محمول على SSL/TLS ويتميز نطاق المواقع التي تستخدمه بابتدائه بـ(https://) وظهور رمز قفل في نافذة المتصفح.

[44] Gary P. Schneider, Electronic Commerce, Cengage Learning, 2008,Edition 8,p 522-530



الشكل (3) بروتوكول التسجيل

- **الصيرفة عبر الهاتف الجوالMobile Banking :**

إن الإتجاه العام في العالم اليوم هو انتشار إستخدام الهاتف الجوال، حيث من المنتظر أن يصل عدد خطوط الهاتف الجوال لى ٧٥٠ مليون (fixed internet) المستخدم في نقل البيانات ١,٢ بليون جهاز بينما سيصل عدد مشتركي الأنترنت عبر الشبكة الثابتة إلى نفس الفترة. ويتيح هذا الإتجاه تطوير إستخدامات الهاتف الجوال لأغراض متعددة كإستخدامه للدخول للشبكة العالمية وإستخدامه في التطبيقات المتعلقة بها كقراء البريد الإلكتروني وتصفح المنتجات المعروضة والترويج لها, ومن ثم يمكن إستخدامه في تقديم خدمات الصيرفة[٤٥] .

- **الصيرفة عبر التلفزيون T.V**

يعتبر التلفزيون من الوسائل الناجحة في الإعلام الجماهيري. لذلك ثم تطوير نظام التلفزيون التخاطبي في الدول المتقدمة ليتيح التواصل بين المشترك ومقدمي برامج خدمة الإرسال

[45] Kerem, K.. Adoption of electronic banking : underlying consumer behavior and critical success factors. Case study of Estonia, paper presented at the 2003 conference of the technology and everyday life network, London, U.K. retrieved from(2003).p 10

http://www.lse.ac.uk/collections/EMTEL/conference/papers/kerem.pdf ,22-4-2011

(interactivetv) وهو ما اصطلح عليه بالتلفزيون التخاطبي،فقد بدأت العديد من الشركات بتقديم خدماتها بالمشاركة مع مؤسسات مالية من خلالها [٤٦].

- **التحويلات المالية الالكترونية (SWFT)**

نظام التحويلات المالية الالكترونية وهو جزء بالغ الأهمية من البنية التقنيةلأعمال البنوك الالكترونية التي تعمل عبر الانترنت والسويفت هي خدمة ارسال واستقبال الحوالات من خلال نظام سويفت ، وهو النظام المركزي العالمي لتنفيذ الحوالات المالية المتبادلة بين البنوك العالمية الكترونياً وذلك باعتماد مقاييس دولية ومن خلال رمز محدد لكل بنك يسمى SWIFT CODE يتيح هذا النظام نقل التحويلات المالية أو الدفعات المالية من حساب بنكي إلى حساب بنكي آخر بطريقة الكترونية آمنة إضافة إلى نقل المعلومات المتعلقة بهذه التحويلات. يمتاز نظام التحويلات المالية الالكترونية في حال تطبيقه بطريقة صحيحة بدرجة عالية من الأمن وسهولة الاستخدام والموثوقية.

إذن نظام التحويلات المالية الالكترونية هو عملية منح الصلاحية permission لبنك ما للقيام بحركات التحويلات المالية الدائنة والمدينة الكترونيا من حساب بنكي آخر أي أن عملية التحويل تتم الكترونيا عبر الهاتف وأجهزة الكمبيوتر وأجهزة المودم modems عوضا عن استخدام الأوراق حيث تنفذ E.F.T عن طريق دار المقاصة الآلية automated clearing house A .C.H

٢-٣-٣ تصنيف خدمات الصيرفة الإلكترونية:

زيادة على الخدمات المصرفة التقليدية التي تقدمها البنوك العادية تتيح الصيرفة الإلكترونية بقنواتها الجديدة إضافية منها هي[٤٧]:

- خدمات دفع ذات خصوصية أكثر تشخيص للشيكات للعملاء بتصميم يزيد في شعورهم بخصوصيتهم لدى المصارف، كما ورفع الالتزامات وإجراء التحويلات مباشرة لمستحقيها وبسهولة ويسر
- تكامل البيانات المالية للعميل مع البيانات الصادرة من المصرف: تتيح هذه الخدمة للعميل بيانات على حساباته مباشرة من المصرف وإجراء تسويتها، دون الحاجة إلى إعادة إدخالها مرة أخرى في نظامه الحاسوبي، كما تتيح الرجوع وطلب القيود السابقة تلقائيا

---

[46] Khalid, k. & Abdallah, R. & Elrafe, E. Elbaset, E. "customer satisfaction with internet banking web Site (Case study onthe arab Bank)". The Arab Academy for Banking and FinancialSciences, Jordan(2006)..p6-9

[٤٧] محروس حسن ، تغير الدور التقليدي للبنوك،Kotobarabia.com, 2006 ،ص١٤٥

- التصديقات المباشرة للتمويل والاستدانة من المصرف: تتيح هذه الخدمات حصول العملاء على تصديقات مباشرة من المصرف للحصول على تمويل أو استدانة، دون الحاجة للوصول بشخصه للمصرف، حيث أن المصارف يستجمع لديها كم هائل من البيانات حول تعاملات العميل والتي يتم من خلالها تقييم مركزه المالية
- تداول الأخبار بين العملاء في المصرف الواحد، حيث يتم تداول الأخبار الخاصة والتجارية عبر موقع المصرف.

٢-٣-٤ مزايا الصيرفة الالكترونية:

قدمت الصيرفة الالكترونية مزايا متعددة منها[٤٨]:

- **القيام بعمليات مصرفية في المنزل:** أصبح الآن بإمكان أي عميل أي يقوم بإجراء العمليات المصرفية وهو في بيته، متصلاً بالانترنت عن طريق موقع المصرف الخاص به. فهو قادر على الاطلاع على حسابه، إضافة رصيد أو سحب رصيد من خلال بطاقة الذكاء الالكترونية أو ما يسمى بـ (E-Card) فقد تم تسهيل الخدمات المصرفية بشكل كبير أمام الزبون مما أتاح له الفرصة في التعامل مع الخدمات بشكل أفضل وأسرع.
- **سحب وايداع الأموال في أي وقت كان (حتى وإن كان المصرف مغلقا): كما** في أيام العطل والمناسبات وعند وجود ضرورة لسحب الأموال أو لتحويل رصيد أو لإجراء ما يمكن للمستخدم أن يقوم بمجموعة العمليات هذه بشكل سلس وسهل عن طريق الانترنت فقد سهلت ويسرت المصارف هذه العمليات نتيجة لانتقالها لاستخدمات تقنيات الصيرفة الالكترونية.
- **التعامل المشفر مع البيانات:** البيانات الخاصة بالعميل تكون سرية للغاية ولا يمكن الاطلاع عليها من قبل أحد، وتقنيات تشفير البيانات تتيح هذا المستوى من السرية فأصبح الآن الأمان أكبر والحفاظ على المعلومات أفضل.
- **امكانية تحميل البيانات:** يمكن للمستخدم الالكتروني تحميل معلومات بياناته الشخصية بسهولة تامة من غير مراجعة المصرف، وسحب كشف عن حسابه والعمليات التي أجريت عليه في الوقت الذي يرغب به. وهذا شكل للمستخدم نقطة جديدة في سهولة استخدام العمليات المصرفية وتوفير في الوقت والجهد الازمين لإجراء هذه العمليات[٤٩].

---

[٤٨] قرم ،"أنظمة الدفع الإلكتروني وتطبيقها في سوريا" ، الجامعة الإفتراضية ، رسالة ماجستير ،٢٠١٢،ص٣٣-٤٠

[49] Pallab Dutta ,**Benefits of Electronic Banking**, 2011,p2

تاريخ الدخول ١-٨-٢٠١١ http://www.ehow.com/facts_5172105_benefits-electronic-banking.html

- **إدارة الحساب بسهولة:** كما سبق ذكره أن العمليات تكون على الرصيد سهلة التعامل وتوفر الوقت والجهد ولا تحتاج للكثير من الوقت والجهد ويمكنك الاطلاع وإدارة بيانات حسابك ضمن الصلاحيات الممنوحة لك.
- **تحقيق معدلات ربح عالية لبعض العمليات:** يكون ذلك نتيجة لمجموعة الخدمات الالكترونية وتوفير الجهد على موظفي المصرف وعدم الاستخدام الورقي فالزبون يقوم بخدمة نفسه بنفسه ولا يحتاج لمساعدة من أحد كي يقوم بإجراء العمليات الخاصة التي يريدها[٥٠].

٢-٣-٥ متطلبات نجاح الصيرفة الالكترونية

يتطلب نجاح الصيرفة الإلكترونية وانتشارها **عوامل** عدة، منها[٥١]:

- وجود شبكة واسعة تضم كل الجهات ذات الصلة وترتبط بالإنترنت وفقا لأسس قياسية، مع مراعاة الأمان في تصميم هذه الشبكة
- وضع خطة للبدء في إدخال خدمات الصيرفة الإلكترونية، وفقا لأولويات تحددها خطة استراتيجية على مستوى المصرف أو المصرف المركزي أو البلد أو التحالفات الدولية
- البدء في تنفيذ الخطة بتبني مشاريع استكشافية متحكم في نتائجها، حتى يتم تفاعل أطراف المجتمع ككل، مع وضع خطة تدريبية موازية للمورد البشري .
- البدء في وضع التنظيم القياسية التي تتيح الربط بين الجهات المشتركة والعالم ككل.
- تطوير التطبيقات المصرفية في المصارف وتوحيد الجهد للإستفادة من الخبرات المتراكمة بين المصرفيين والفنيين في المصارف .
- إنشاء الجسم الإداري الذي يتولى التنسيق بين الأطراف المعنية على مستوى المصرف الواحد، المصرف المركزي، البلاد، على مستوى الإقليمي .

٢-٤ نظم الدفع الإلكتروني ووسائلها:

تطورت وسائل ونظم الدفع الالكترونية خاصة منذ إنتشار عمليات التجارة الإلكترونية، وتطورها على الصعيد العالمي وفيما يلي أهم تلك الوسائل[٥٢]:

---

[٥٠] وادي رشدي، أهمية ومزايا البنوك الالكترونية في غزة ومعوقات انتشارها، مجلة جامعة غزةالإسلامية،٢٠١٠،ص٦

[٥١] *يونس عرب* , البنى التحتية لمشروعات البنوك الالكترونية

http://www.arablaw.org/Download/E-banking_Infrastructure_Article.doc , consulté le 25/05/2004 ص٤

٢-٤-١ بطاقات الائتمان:

هي بطاقة بلاستيكية ذات خصائص معينة صادرة عن مؤسسة مالية أو مصرفية تستخدم كوسيلة تعامل عوضا عن النقود. يستطيع حاملها أن يتمتع بواسطتها بالخدمات المالية إضافة إلى إمكانية استفادته من الائتمان الممنوح بموجبها في المصرف المصدر لها، وذلك لتلبية حاجاته المختلفة. إنها بمثابة فتح اعتماد بمبلغ معين لصالح صاحب البطاقة، إذ يستطيع هذا الأخير الوفاء بقيمة مشترياته من السلع باستخدامها.

تحمل البطاقة اسم العميل ورقم حسابه ورمز الفرع، وعليها شريط ممغنط يحمل المعلومات السابقة نفسها ومعطيات محددة سلفا. لكل بطاقة رقم سري يعرفه حامل البطاقة فقط. أول ظهور للبطاقات المصرفية كان في الولايات المتحدة الأمريكية في العام ١٩١٤.

في العام ١٩٥٨م أصدرت بطاقة Américain Express وفي العام ١٩٥٩م أصدرت البطاقة البيضاء carte blanche وفي بداية الستينات تجمع عدد كبير من البنوك ودرسوا إمكانية توفير بطاقة يمكن استعمالها في كل الولايات الأمريكية، واقتضى هذا الأمر خلق عائلتين كبيرتين من البطاقات المصرفية وهما بطاقة VISA وبطاقة "MASTER CARD".

٢-٤-٢ النقد الإلكتروني / أو الرقمي:Digicash /E.cash

عرّفت شركة "إرنست أند يونغ" النقود الإلكترونية بأنها مجموعة من البروتوكولات والتوقيعات الرقمية التي تتيح للرسالة الإلكترونية أن تحل فعليا محل تبادل العملات التقليدية. بعبارة أخرى فإن النقود الإلكترونية أو الرقمية هي المكافئ الإلكتروني للنقود التقليدية التي يتم تداولها. تتميز النقود الإلكترونية بأنها غير ملموسة، تأخذ صورة وحدة إلكترونية، تخزن في مكان آمن جدا على القرص الصلب" الهارديسك" في جهاز الكمبيوتر الخاص بالعميل، والذي يعرف باسم "**المحفظة الإلكترونية**". يمكن للعميل أن يستخدم هذه المحفظة في إتمام عمليات البيع والشراء والتحويل. تعتمد فكرة النقد الرقمي على قيام العميل بشراء عملات إلكترونية من المصرف الذي يقوم بإصدارها، ويتم تحميل هذه العملات على الحساب الخاص بالمشتري، وتكون في صورة وحدات عملة صغيرة ولكل وحدة رقم خاص أو علامة خاصة من المصرف المصدر. عند قيام

---

[52] Edwards, Donald ;Kusel,Jim Oxner,Tom. *Internal Auditing in the Banking Industry Bank Accounting & Finance*, (Euromoney Publications PLC), Fall ٢٠٠٧. vol 15 Issue 1. PP4-63

المستخدم بالشراء من بائع يتعامل بالعملات الإلكترونية، يقوم المشتري باختيار السلع ومعرفة أسعارها، ليقوم بعد ذلك بإصدار أمر عن طريق الكمبيوتر بدفع قيمة مشترياته باستخدام العملات الإلكترونية المسجلة على الحساب الخاص به، يتم بعدها نقل العملات الإلكترونية من خلال المصرف المصدر لها الذي يقوم بالتأكد من صلاحية العملات وعدم تزييفها أو نسخها، ويقوم بتحميلهاعلى الحاسب الخاص بالبائع ليظهر لدى البائع زيادة في قيمه النقدية بالمبلغ الذي تمت إضافته مقابل شراء الأصناف المحددة في طلب شراء المشتري، ويمكن للبائع تحويل العملات الإلكترونية المتاحة لديه إلى عملات حقيقية من خلال المصرف المصدر. تحقق النقود الإلكترونية للمتعاملين بها عدة مزايا منها[٥٣]:

- سهولة الاستخدام حيث يستطيع المشتري سداد قيمة مشترياته بمجرد الامر على حاسبه الآلي، كما تتيح النقود الإلكترونية فرصة التعامل بالعديد من العملات مع إمكانية التحويل بين هذه العملات بصورة لحظية وبأي قيمة
- السرية والخصوصية: حيث يستطيع المشتري أن يقوم بعملية الشراء دون أن يكون مضطرا لتقديم أية معلومات
- الأمان: يتيح نظام النقود الإلكترونية أعلى درجات الأمان الممكنة، حيث يعتمد على نظام التوقيع الرقمي الذي يعتبر أفضل وسائل حماية المعلومات المالية، إضافة إلى استخدام كلمات المرور لحماية مسحوبات العميل من حسابه المصرفي، كما تتقدم البنوك التي تعمل بهذا النظام أجهزة خادمة تدعى بروتوكول الحركات المالية الآمنة، مما يجعل عمليات دفع هذا النظام أكثر أمانا
- انخفاض التكاليف: حيث تنعدم تكاليف المقاصة أو التسوية، لأن العملية تتم أتوماتيكيا وهي في منتهى البساطة
- لا تخضع للحدود: يمكن تحويل النقود الإلكترونية من أي مكان إلى آخر في العالم، وفي أي وقت كان، كونها تعتمد على الأنترنيت والشبكات التي لا تعترف بالحدود الجغرافية والسياسية
- السرعة في الدفع: حيث تجرى حركة التعاملات المالية، ويتم تبادل معلومات التنسيق الخاصة بها فورا، في الزمن الحقيقي دون الحاجة إلى أي وساطة

---

[٥٣]منصوري الزين، "وسائل وأنظمة الدفع والسداد الالكتروني عوامل الانتشار وشروط النجاح "– الملتقى العلمي الدولي الرابع،موسوعة الاقتصاد والتمويل الاسلامي ،٢٠١١،ص١٤

٢-٤-٣ الشيكات الإلكترونية Electronic check

يعتبر الشيك الإلكتروني المكافئ الإلكتروني للشيكات الورقية التقليدية، وهي رسالة إلكترونية موثقة ومؤمنة يرسلها مصدر الشيك لحامله ليعتمده ويقدمه للمصرف الذي يعمل عبر الإنترنت، ويقوم المصرف بعد ذلك بتحويل قيمة الشيك المالية إلى حساب حامل الشيك، وبعد ذلك يقوم بإلغاء الشيك وإعادته إلكترونيا إلى مستلم الشيك (حامله) ليكون دليلا على أنه قد تم صرف الشيك فعلاً. يمكن لمستلم الشيك أن يتأكد إلكترونياً من أنه قد تم بالفعل تحويل المبلغ لحسابه.

تستخدم هذه الشيكات لإتمام عمليات السداد الإلكترونية بين طرفين من خلال وسيط، حيث يتم تحرير الشيكات وتبادلها عبر الانترنت، ويقوم الوسيط بالخصم من حساب العميل والإضافة إلى حساب التاجر، ويحتوي الشيك الإلكتروني على البيانات التالية: رقم الشيك، اسم الدافع، رقم حساب الدافع واسم المصرف، اسم المستفيد، القيمة التي ستدفع، وحدة العملة المستعملة، تاريخ الصلاحية والتوقيع الإلكتروني للدافع[٥٤].

٢-٤-٤ البطاقات الذكية Smart card

هي بطاقة بلاستيكية تضم شريحة إلكترونية ذات سعة تخزينية كبيرة للبيانات، مقارنة بتلك التي تستوجبها البطاقات ذات الشرائط الممغنطة، وتحتوي هذه البطاقات على سجل البيانات والمعلومات والأرصدة والمصروفات المالية، والرقم السري، لذلك سميت بدفتر الشيكات الإلكتروني، كما تتميز هذه البطاقات بعناصر حماية ضد التزييف والتزوير وسوء الاستخدام والسرقة.

تستخدم البطاقات الذكية في تحويل الأرصدة وسداد الفواتير وحجز تذاكر الطيران وشراء المنتجات، ويمكن أن تحول إلى حافظة نقود إلكترونية، كما تستخدم في إجراء التحويلات المالية داخل شبكة الأنترنت ومع التلفون المحمول.

من أهم مزايا هذه البطاقات ما يلي[٥٥]:

- يمكن استخدامها كبطاقة ائتمانية أو بطاقة خصم فوري طبقا لرغبة العميل
- يمكن استخدامها كبديل للنقود في كل عمليات الشراء
- سهولة إدارتها مصرفيا
- وجود ضوابط أمنية حيث لا يمكن التلاعب بها أو تزويرها

---

[54] Kenneth C. Laudon and Carol GuercioTraver, E-commerce business, technology, society. Security + Guide to Network Security Fundamentals ,2009,p88

[٥٥] تاريخ الدخول ٣-١٠-٢٠١٠ http://en.wikipedia.org/wiki/Contactless_smart_card

- يمكن التحويل من رصيد بطاقة لأخرى عن طريق آلات الصرف الآلي دون الرجوع إلى المصرف

مما سبق يتبيّن **أن** العمليات المصرفية الالكترونية هي ممارسة خدمات العمليات المصرفية الكترونيا عبر شبكة الويب من خلال اتصال العميل بموقع المصرف على شبكة الانترنت . يقصد بالعمليات المصرفية الالكترونية تقديم البنوك الخدمات المصرفية التقليدية أو المبتكرة من خلال شبكات اتصال الكترونية، تقتصر صلاحية الدخول إليها على المشاركين فيها وفقا لشروط العضوية التي تحددها البنوك، وذلك من خلال احد المنافذ على الشبكة بهدف[٥٦] :

- إتاحة معلومات عن الخدمات التي يؤديها المصرف كخدمات للمستثمرين
- حصول العملاء على خدمات معينة – يحددها المصرف – كالتعرف على معاملاتهم وأرصدة حساباتهم وتحديث بياناتهم وطلب الحصول على قروض وغير ذلك
- طلب العملاء تنفيذ عمليات مصرفية مثل تحويل الأموال وسداد الفواتير

من كل ما سبق يتضح أن تنوع وتطور الأعمال المصرفية في ظل تكنولوجيا الاتصالات والمعلومات زادت من أهمية الرقابة الداخلية، خصوصا ما يتعلق بأمن البيانات والمعلومات. هذه الاهمية تولدت من المخاطر التي تتأتى من الأعمال المصرفية في البيئة الالكترونية لهذه الأعمال، والتي يتوجب على الرقابة الداخلية تداركها وتجنب آثارها وتخفيف وطأة أعبائها على المصرف والمتعاملين معه. من هنا بات على نظم المعلومات وانظمة الاتصال وتشغيل البيانات بمختلف انواعها تحديد اهداف الامان لبياناتها ومعلوماتها، ورسم سياساتها التي يجب أن تسهم في بلوغ تلك الأهداف، وترجمة تلك السياسات إلى جملة من التعليمات والاجراءات واجبة التطبيق بحيث يمكن من خلالها ضمان أمن البيانات والمعلومات التي ينتجها النظام.

٢-٥ المخاطر المرتبطة بالعمل المصرفي الالكتروني

يصاحب تقديم العمليات المصرفية الالكترونية مخاطر متعددة. وقد أشارت لجنة بازل للرقابة المصرفية إلى أنه ينبغى قيام البنوك بوضع السياسات والإجراءات التى تتيح لها إدارة هذه المخاطر

[٥٦] الكرسانة إبراهيم ، "أطر أساسية ومعاصرة في الرقابة على البنوك وإدارة المخاطر"، صندوق النقد العربي، أبوظبي، مارس ٢٠٠٦، ص ٤٧

من خلال تقييمها والرقابة عليها ومتابعتها. أصدرت اللجنة خلال شهري مارس ١٩٩٨ ومايو ٢٠٠٤ مبادئ لإدارة هذه المخاطر شملت مايلى[٥٧]:

٢-٥-١مخاطر التشغيل

تنشأ مخاطر التشغيل من عدم كفاية إجراءات الأمان للنظام، أو عدم ملاءمة تصميم النظام، أو عدم إنجاز العمل أو أعمال الصيانة، وكذا نتيجة إساءة الاستخدام من قبل العملاء، وذلك على النحو التالي[٥٨]:

- **عدم كفاية إجراءات الأمان للنظام:** تنشأ هذه المخاطر من أمكان اختراق غير المرخص لهم لنظم حسابات المصرف، بهدف التعرف على المعلومات الخاصة بالعملاء واستغلالها، سواء تم ذلك من خارج المصرف أو من العاملين به، الأمر الذي يستلزم توافر إجراءات كافية لكشف وإعاقة ذلك الاختراق
- **عدم ملاءمة تصميم النظام أو إنجاز العمل أو أعمال الصيانة:** وهى تنشأ من إخفاق النظم أو عدم كفاءتها (بطيء الأداء على سبيل المثال) لمواجهة متطلبات المستخدمين، وعدم السرعة في حل هذه المشاكل وصيانة النظم، خاصة إذا زاد الاعتماد على مصادر خارج البنوك لتقديم الدعم الفني بشأن البنية الأساسية اللازمة
- **إساءة الاستخدام من قبل العملاء:** نتيجة عدم إحاطة العملاء بإجراءات الأمان الوقائية أو بسماحهم لعناصر إجرامية بالدخول إلى حسابات عملاء آخرين أو القيام بعمليات غسيل الأموال باستخدام معلوماتهم الشخصية أو قيامهم بعدم إتباع إجراءات التأمين الواجبة.

٢-٥-٢ مخاطر السمعة

تنشأ مخاطر السمعة فى حالة توافر رأي عام سلبى تجاه المصرف، الأمر الذى قد يمتد إلى التأثير على مصارف اخرى، نتيجة عدم مقدرة المصرف على إدارة نظمه بكفاءة أو حدوث إختراق مؤثر لها[٥٩].

---

[٥٧] الساكني وعواودة ،" مخاطر استخدام تكنولوجيا المعلومات وأثرها على أداء نظم المعلومات المحاسبية ، جامعة الأسراء ،٢٠١١،ص ٦

[٥٨] ابو صلاح،مصطفى، " المخاطر التشغيلية حسب متطلبات بازل ٢" ، المؤتمر العلمي السنوي الخامس ، جامعة فيلادفيا ،٢٠٠٧، ص٣

[٥٩] عبدالله ، الريح آدم،" الرقابة على المصارف الاسلامية ومتطلبات مقررات لجنة بازل ، مجلة المصرفي ، بنك السودان المركزي ،العدد ٤٠،٢٠٠٦

٢-٥-٣المخاطر القانونية:

تقع هذه المخاطر فى حالة إنتهاك القوانين أو القواعد أو الضوابط المقررة، خاصة تلك المتعلقة بمكافحة عمليات غسيل الأموال، أو نتيجة عدم التحديد الواضح للحقوق والالتزامات القانونية الناتجة عن العمليات المصرفية الالكترونية[٦٠].

٢-٥-٤المخاطر الأخرى:

يرتبط أداء العمليات المصرفية الالكترونية بالمخاطر الخاصة بالعمليات المصرفية التقليدية، ومن ذلك مخاطر الائتمان والسيولة وسعر العائد ومخاطر السوق مع احتمال زيادة حدتها، فعلى سبيل المثال فإن استخدام قنوات غير تقليدية للاتصال بالعملاء وامتداد نشاط منح الائتمان إلى عملاء عبر الحدود قد يزيد من احتمالات إخفاق بعض العملاء في سداد التزاماتهم[٦١].

٢-٦ مخاطر العمليات المصرفية الالكترونية

تصنف المخاطر على النحو التالي:

٢-٦-١**مخاطر خرق الحماية المادية** ويكون ذلك من خلال:

- **التفتيش في المخلفات التقنية** Dumpster diving يقصد به قيام المهاجم بالبحث في مخلفات المؤسسة من القمامة والمواد المتروكة بحثا عن أي شيء يساعده على اختراق النظام[٦٢]، كالأوراق المدون عليها كلمات السر، او مخرجات الكمبيوتر التي قد تتضمن معلومات مفيدة، او الاقراص الصلبة المرمية بعد استبدالها، او غير ذلك من المواد المكتوبة او الاقراص او الملاحظات او أي أمر يستدل منه على اية معلومة تسهم في الاختراق. فقد حصل ان بيعت من قبل وزارة العدل الأمريكية مخلفات اجهزة تقنية بعد ان

---

[٦٠] البحيصي ، وشعبان ،" مخاطر نظم المعلومات المحاسبية الإلكترونية " دراسة تطبيقية على المصارف العاملة في غزة ، ٢٠٠٨، ص١٠

[٦١] عنانزه ، نايف، عز الدين و عثمان ،داود ، محمد" اختبار مدى كفاءة إدارة مخاطر الائتمان على جودة المحافظ الائتمانية في البنوك الاسلاميه الاردنيه"، المؤتمر العلمي الدولي السابع لجامعة فيلادلفيا،عمان ، ٢٠١٠، ص٦-٧

[٦٢] محمد عبد الفتاح ،الفولي عبد الفتاح " تحديات إنشاء الحكومات الإلكترونية ، القاهرة ،٢٠٠٧،ص١٣

تقرر اتلافها، وكان من ضمنها نظام كمبيوتر يحتوى قرصه الصلب على كافة العناوين الخاصة ببرنامج حماية الشهود، وبالرغم من انه لم يتم فعليا استثمار هذه المعلومات، الا ان مخاطر كشف هذه العناوين استدعى إعادة نقل كافة الشهود وتغيير مواطن اقامتهم وهوياتهم وهو ما تطلب كلفا مالية ضخمة لا لشيء إلا للإخفاق في إتلاف الاقراص بطريقة صحيحة[٦٣].

- **الالتقاط السلكي**:Wiretapping والمقصود هنا التوصيل السلكي المادي مع الشبكة او مع تجهيزات النظام لجهة استراق السمع او سرقة البيانات والاستيلاء عليها، وهي انشطة تتم بطرق سهلة او معقدة تبعا لنوع الشبكة وطرق التوصل المادي٦٤.
- **استراق الأمواج** :Eavesdropping on Emanations ويتم ذلك باستخدام لواقط تقنية لتجميع الموجات المنبعثة من النظم باختلاف أنواعها كالتقاط موجات شاشات الكمبيوتر الضوئية او التقاط الموجات الصوتية من أجهزة الاتصال[٦٥].
- **إنكار او إلغاء الخدمة**:Denial or Degradation of Service والمقصود هنا الاضرار المادي بالنظام لمنع تقديم الخدمة، اما ان كنا نتحدث عن انكار الخدمة مثلا على مواقع الإنترنت فان ذلك يتم عبر تقنيات مختلفة، كضخ الرسائل البريدية الإلكترونية دفعة واحدة لتعطيل النظام[٦٦].

٢-٦- ٢ مخاطر خرق الحماية المتعلقة بالاشخاص وشؤون الموظفين

تعد المخاطر المتصلة بالاشخاص والموظفين، وتحديدا المخاطر الداخلية منها، واحدة من مناطق الاهتمام العالي لدى جهات أمن المعلومات، اذ ثمة فرصة لان يحقق اشخاص من الداخل ما لا يمكن نظريا ان يحققه أحد من الخارج، وتظل أيضا مشكلة صعوبات كشف

---

[٦٣] المري ،عايض، "أمن المعلومات ، ماهيتها وعناصرها واستراتيجيتها،" مركز الدراسات و الاستشارات القانونية ، ٢٠١٣، ص٤

64 Sheila, Frankel, “An Introduction To IP Sec ,”Computer Security Division/Information Technology Laboratory/National Institute of Standards and Technology، ٢٠٠٦ ،p34

[٦٥] حامد محمد،نورالدين" أمن نظم ومعلومات المصارف وحمايتها باشارة خاصة للواقع السوداني"جامعةالنيلين،٢٠٠٧،ص١٣-١٥

66 http://www.dss.mil/training/csg/security/Treason/Infosys.htm Insider Threat to Information Systems, page 1, By Eric D. Shaw, Ph. D., Keven. Ruby, M. A. and Jerrold M. Post, M.D. Political Psycholoogy Associates, Ltd

هؤلاء قائمة ان لم يكن ثمة نظام أداء وصلاحيات يتيح ذلك وبإجراء مسح إحصائي عن حوادث أمن المعلومات من قبل الحكومة الامريكية وجد أن العوامل المؤثرة في أمن المعلومات ومع ما يترتب عن كل عامل منها كالآتي[٦٧]:

- الأفعال غير المقصودة تمثل ٥٠.%
- عدم أمانة العاملين في الحاسب يمثل ١٥٪ إلى ٢٠. .%
- الإبتزاز والضغط المطلبي يمثل .10%
- الإعتداء الخارجي لا يتجاوز .5%
- الكوارث الطبيعية والحريق يمثل .10%.

فقد أثبتت الدراسات أن مهددي الداخل من موظفين وخلافهم هم الأخطر والأعلى نسبة.

ويمكن تصنيف مرتكبي جرائم الحاسوب بصورة عامة على النحو التالي:

إن التهديدات التي تتعرض لها جميع المنشآت تأتي في أغلبها من الموظفين العاملين بالمنشأة كما دلت الدراسات لذلك فإن أكثر من ٨٠٪ منها تأتي منهم، وموظفو الداخل هم الأفراد الذين لهم علاقة مباشرة بالمنشأة، وبحكم طبيعة عملهم وإمكانية إستغلالهم للثقة الممنوحة لهم فانهم يشكلون الخطر الأعظم للمنشأة ويمكن تصنيف هؤلاء الموظفين كما يأتي[٦٨]:

–الموظفون الذين يعملون بصفة مستديمة بنظام الوقت الكامل أو الوقت الجزئي وهؤلاء يخضعون لنظام وآلية التعيين المتبع بالشركة

إن ضعف إجراءات تعيين الموظفين وضعف آلياتها، وطريقة إختيار الموظفين والتحري عن خلفياتهم وسجلاتهم الإجرامية عند التعيين لدى المنشآت بشتى أنواعها، يترتب عليه مشاكل كثيرة، وتعرض المنشآت لمخاطر وخسائر مالية كبيرة كان يمكن تفاديها إذا تم الإختيار والتوظيف وفق معايير وإجراءات محددة.

وأوضحت الدراسة التي أجرتها وور روم عام ٢٠٠٦ أن ٦٢.٩٪ من الشركات التي غطتها الدراسة أبلغت أن سوء استخدام النظم تم داخلياً من قبل الموظفين المعينين بالشركة، كما أوضحت الدراسة التي قام بها معهد أمن الحاسوب بالتعاون مع الشرطة الفدرالية الامريكية عام ٢٠٠٨ أن الاختراقات

---

[٦٧] علي ،حاج عوض و خلف ،أمير حسين،" أمنية المعلومات وتقنيات التشفير "، المكتبة الوطنية، ٢٠٠٥م، ص ٢٠،

[٦٨] بو حروره ، محمود ، و غيث ، عيسى ،" أمن المعلومات " المركز العالي للمهن الشاملة ، اجدابيا ، ٢٠١١ ،ص٧

التي تمت من خارج المؤسسات كانت خساراتها حوالي ٥٦ الف دولار بينما كان متوسط خسارة الشركات من العاملين داخل الشركة ٢.٧ مليون دولار .

كما أفادت الدراسة الشاملة التي قامت بها الأمم المتحدة في مجال الإجرام لعدد ٣٠٠٠ موقع غطت كندا وأوربا و الولايات المتحدة الأمريكية، أن التهديد الاكبر أتى من الموظفين العاملين داخل المنشآت والذين لديهم صلاحيات الدخول لنظم الحاسوب .

وخلصت الدراسات في مجال أمن وحماية نظم المعلومات بأن المشاكل التي يسببها موظفو الداخل هي الأكثر والأخطر في مجال السرقات والتخريب والتجسس، وتأتي من قبل المتخصصين في تقنية المعلومات وذلك لمعرفتهم أسرار النظم ونقاط ضعفها وثغراتها.

ورغم ذلك تشير الدراسات أن الإهتمام الأكبر في الحماية يتركز وينصب على حماية المنشآت من المخاطر الخارجية.

وتتمثل مصادر التهديد في المتخصصين في مجال التقنية من مدراء النظم ومبرمجيها ومشغليها وخبراء شبكات المعلومات، وقد تأتي المخاطر من الموظفين المعينين بالمنشأة كموظفين دائمين أو موظفي نظام الوقت الجزئي أو موظفين مؤقتين أو من الموظفين المتعاقدين. كما يمكن أن يأتي التهديد من الشركاء والعملاء الذين لديهم صلاحية الدخول للنظام والمخولين[٦٩].

والموظفون هم الأكثر خطورة من حيث الدخول على النظام واتلاف نظم المعلومات الحساسة وبحكم انهم موظفون تم انتقاؤهم يتوقعون اهتماماً خاصا تجاه أدائهم ونجاحات مجموعة العمل، ويعتقدون أنهم فوق الشبهات، وهم آخر من يشتبه بهم اذا حدث سؤ اداء او فشل للنظام.

ومع ذلك يمكن للشركات أن تضع الرقابة على موظفيها أكثر من قدرتها على التحكم بالموظفين المتعاقدين أو الموظفين المؤقتين.

ان الموظفين الذين يحدثون التخريب للنظم عادة يستغلون امكانيتهم فى الدخول على مراكز المعلومات وذلك لعدة محفزات منها الطمع أو الانتقام نتيجة لعدم إنصافهم أو عدم سماع شكواهم وتظلمهم من قبل المسؤولين أو لترضية أنفسهم من أجل الأنا أو لحل مشكلة شخصية او مهنية او

---

[69] Eric D. Shaw, Ph. D., Keven. Ruby, M. A. and Jerrold M. Post, M.D. Political Psycholoogy Associates" Insider Threat to Information Systems",٢٠٠٨ , Ltd. 1, page 2

لتحدى النظام وقهره لإظهار مقدراتهم او للتعبير عن غضبهم أو للتاثير على الاخرين او لأكثر من سبب، ومن الأمثلة على ذلك[٧٠] :

–كان أحد المدراء المتخصصبن في مجال التقنية والعاملين بشركة أمريكية عالمية لإنتاج الطاقة يقوم بخلق مشاكل في النظم بفروع الشركة بشتى مواقع الشركة في الخارج وذلك بغرض السفر حول العالم، ولجذب اهتمام الإدارة العليا الى الاعتراف بمهاراتهم وخبراتهم العلمية والتقنية.

– قام المدعو مشيل لوفنبيرج البالغ من العمر ٣١ عاماً والذي يعمل في البرنامج العام لتطوير الصواريخ الديناميكية الأطلسية بزرع قنبلة موقوتة لتقوم بإلغاء المعلومات الحساسة بعد إستقالته، متوقعاً أن يستدعى كخبير لإنقاذ الشركة ويعاد تعيينه بمرتب عالٍ، وذلك نتيجة لإستيائه من قبل إدارته لعدم تقدير جهده تجاه البرامج التي كتبها لضبط وتتبع قطع غيار الصواريخ .

– قام مدير الحاسوب بإحدى الشركات الأمريكية المالكة لمجموعة سوبرماكتات، بالإتفاق مع موظفين من الحسابات بتنفيذ عمليات سرقة كلفت الشركة ٢ مليون دولار في غضون عامين، وبدأت العملية بالحاجة المادية وسرعان ما تحولت إلى طمع. الاستراتيجية المتبعة لتنفيذ السرقة تمت بإجراء تعديل في البرنامج المحاسبي ليقوم البرنامج بإسقاط بعض المشتريات من النظام المحاسبي ومن ثم تحويله إلى حساب وهمي، وفي نهاية اليوم يقوم المجرم بسحب المبالغ من الحساب الوهمي دون أن تظهر الحركة في القيود، ثم يقوم بإلغاء الحساب الوهمي.

في المثالين الأولين نرى أن الموظفين إستغلوا مهاراتهم التقنية للدخول على معلومات النظم الحساسة ومن ثم خلق أزمة وذلك من أجل خلق نوع من الأهمية لأنفسهم وتعظيم قدرهم ورفع قيمتهم لدى الشركة، في حين أن المثال الثالث يوضح بجلاء ويعكس سوء إستغلال الوضع الوظيفي لتنفيذ العملية الإجرامية.

---

[٧٠] حامد محمد، نورالدين " أمن نظم ومعلومات المصارف وحمايتها باشارة خاصة للواقع السوداني"جامع النيلي،٢٠٠٧ ،ص١٣–١٥

-الموظفين المتعاقدون، الشركاء، الاستشاريون والمؤقتون

المتعاقدون والشركاء والاستشاريون والموظفون المؤقتون لا يعتبرون من ضمن موظفي المنشأة لأنهم لا يتم تعينهم واختيارهم بنفس الطريقة التى يتم بها فحص خلفية الموظفين والتحري عنهم، وهم أقل إنتماء للمنشأة من غيرهم من الموظفين، ورغم ذلك نجد ان المتعاقدين والاستشاريين لديهم صلاحيات دخول على الأنظمة لاعتماد المنشآت على العمالة الخارجية فى البرمجة وبعض مهام تقنية المعلومات، وهناك عدة جرائم حدثت من هذه المجموعة منها[٧١]:

- اكتشفت احدى الشركات الامريكية العالمية العاملة فى مجال الطاقة بأن احد المتعاقدين قام بزرع قنبلة موقوتة ليعزز من نفوذه فى الشركة ولحماية نفسه فى حال إكتشاف صحيفة جرائمة، وهذا الموظف كان قد أدين فى خمس جرائم ذات علاقة بتقنية المعلومات من قبل، ولم تكتشفه الشركة لانها لم تقم بعمل الفحص الكامل لهذا الموظف لأنه ليس من موظفيها بل من موظفي شركات التوظيف.

- قام احد الموظفين الصينيين المتعاقدين مع إحدى الشركات الأمريكية باختراق موقع القوات الجوية والدخول فى المعلومات الحساسة للبرامج الدفاعية والقتالية، وقام أيضاً بنقل كلمة سر ذات صلاحيات تمكن مستخدميها من الغاء أي ملف فى شبكة معلومات الشركة ومن ثم بثها فى الانترنت.

فى الامثلة السابقة نجد ان المثال الاول يعبر عن سوء إختبار و إختيار المتعاقدين والمشاكل والمهددات التى تتعرض لها المنشأة جراء الإعتماد على العمالة الخارجية، أما المثال الثانى فيعبر عن عمليات التجسس التى تنجم عن استخدام المتعاقدين والاضرار التى يحدثها عن ذلك .

---

[71] http://www.dss.mil/training/csg/security/Treason/Infosys.htm

Insider Threat to Information Systems, page 1, By Eric D. Shaw, Ph. D., Keven. Ruby, M. A. and Jerrold M. Post, M.D. Political Psycholoogy Associates, Ltd. 1, page 7

- الموظفون السابقون

وهم الموظفون الذين تركوا العمل بالمؤسسة ولكن لديهم إمكانية الدخول مباشرة فى النظام من خلال الأبواب الخلفية، أو بطريقة غير مباشرة عن طريق زميل لديه مشاكل مع رب العمل، أو يتوقع انهاء خدمته من الشركة، ولذا يقوم بترك باب خلفى أو كلمة سر بديلة أو معلومات مخزنة، للاستخدام لاحقا بغرض الإنتقام، وتأتي مثل هذه المشاكل من عدم إطمئنان الموظف لرب العمل ولعدم وجود ضمان ومسار وظيفى واضح ومن أمثلة ذلك:

- قام أحد مبرمجى الحاسوب باحدى الشركات الأمنية – بعد تلقيه توبيخ و تعنييف من مسؤوليه – بإنتاج فيروس يقوم بإلغاء جزء من معلومات الشركة ويقوم بتكرار العملية إذا تحقق شرط معين، وبعد فصله من العمل قام بالدخول للشركة باستخدام نسخة مطبوعة من المفتاح والدخول على شبكة كمبيوتر الشركة باستخدام ثغرة خلفية وتشغيل الفيروس.
- قام أحد الموظفين العاملين فى مجال البرمجة فى شركة متخصصة فى صناعة البرمجيات المتقدمة فى منطقة كلورادو الامريكية بنقل أصل برمجيات Source Code إلى أحد الموظفين الصينيين العاملين بالشركة بمنطقة دنفر الامريكية والذى نقل هذة البرمجيات بدوره الى شركة صينية ونتيجة لسرقة هذة البرمجيات وتسويقها من قبل شركة أجنبية منافسة (الشركة الصينية) تدهورت الشركة مادياً ومن ثم أعلنت افلاسها.

وبالعموم ثمة مسميات وطوائف عديدة للمخاطر (الداخلية الخارجية) فيما سيلي أبرزها[٧٢].:

- **التخفي بانتحال صلاحيات شخص مفوض** Masquerading: والمقصود هنا الدخول الى النظام عبر استخدام وسائل التعريف العائدة لمستخدم مخول بهذا الاستخدام، كلاستغلال كلمة سر أحد المستخدمين واسم هذا المستخدم، أو عبر استغلال نطاق صلاحيات المستخدم الشرعي ومع ان هذا النمط من الاختراقات هو الشائع سواء في البيئة الداخلية للمنشاة او الخارجية، إلا أن وضعه ضمن طائفة الإختراقات المتصلة بالموظفين ومستخدمي النظام من الداخل مصدره

---

[72] Anderson, Ross J.. *Security engineering : a guide to building dependable distributed systems* (2nd ed.). Indianapolis, IN: Wiley. (2008) p. 1040.

ISBN 978-0-470-06852-6. http://books.google.com/books?id=ILaY4jBWXfcC. Chapter 2, page 17

حصوله الغالب في هذه البيئة بسبب أخطاء تشارك الموظفين كلمات السر ووسائل التعريف، وبسبب امكان الحصول عليها عن طريق إستراق النظر أو نحو ذلك من الأساليب التي تتواجد في بيئة العمل الداخلي وتتيح الحصول على كلمات المرور أو وسائل التعريف.

- **الهندسة الاجتماعية** Social Engineering ويصنف هذا الاسلوب ضمن الحماية المادية احيانا ويرجع الى انشطة الحصول على معلومات تهيئ الاقتحام من خلال علاقات اجتماعية وذلك باستغلال الشخص أحد عناصر النظام بايهامه بأي أمر يؤدي الى حصول هذا الشخص على كلمة مرور أو على أية معلومة تساعد في تحقيق اعتدائه، وابسط مثال أن يتصل شخص باحد العاملين ويطلب منه كلمة سر النظام تحت زعم انه من قسم الصيانة او قسم التطوير او غير ذلك، ولطبيعة الاسلوب الشخصي في الحصول على معلومة الاختراق او الاعتداء سميت الهندسة الاجتماعية
- **الازعاج والتحرش**:Harassment وهي تهديدات يندرج تحتها أشكال عديدة من الاعتداءات والأساليب، ويجمعها توجيه رسائل الازعاج والتحرش وربما التهديد والابتزاز او في احيان كثيرة رسائل المزاح على نحو يحدث مضايقة وازعاجا بالغين، وليست حكرا على البريد الإلكتروني بل تستغل مجموعات الحوار والاخبار والنشرات الإلكترونية في بيئة الإنترنت والويب، كما انها ليست حكرا على بيئة الموظفين والمستخدمين، بل هي نمط متواجد في مختلف التفاعلات عبر الشبكة وعبر البريد الإلكتروني، والصحيح انها شائعة كاعتداءات من خارج اطار المصرف وتغلب ان تكون مشكلة تتصل بالاشخاص اكثر منها مؤسسات الاعمال، ومن هنا يصنفها اصحاب هذا التصنيف ضمن هذه الطائفة [٧٣].
- **قرصنة البرمجيات** Software Piracy وقرصنة البرامج تتحقق عن طريق نسخها دون تصريح او استغلالها على نحو مادي دون تخويل بهذا الاستغلال، او تقليدها ومحاكاتها والانتفاع المادي بها على نحو يخل بحقوق المؤلف[٧٤].
- عدم الاقرار بتنفيذ العمليات المالية Non Repudiation ويتمثل هذا الخطر في عدم إقرار الشخص بالعملية التي قام بتنفيذها ، كأن ينكر بأنه قام بإجراء حركات مالية في حسابه لدى المصرف أو ينكر أنه أصدر أمر شراء عبر شبكة المعلومات خصماً على حسابه أو بطاقة الإئتمان الخاص به.

[٧٣] مرجع سابق ، بوحروره ،٢٠١١ ، ص٨

[74] Scribd. http://www.scribd.com/doc/62262162/HP-Pretexting-Scandal. Retrieved 15 August 2011.

- خطأ إدخال البيانات ويحدث هذا النوع من الخطأ في مجال العمل المصرفي وخاصة عند إدخال الحركات المالية لحسابات العملاء والقيود المالية المختلفة ما لم يكن النظام مصمماً بطريقة تضمن الرقابة على المدخلات خاصة أرقام الحسابات وبذلك يتم إيداع المبالغ والقيود المالية في حسابات عملاء آخرين مما يفقد المنشأة مصداقيتها.
- استغلال بواقي وكسور العمليات الحسابية ويحدث هذا النوع من الجرائم دائماً من داخل المنشأة وهنا يقوم المبرمج بوضع أوامر معينة لمراقبة نتائج العمليات المحاسبية وجمع جزء من كسور العمليات المالية في حساب ما واستغلالها دون ترك أي أثر .

٢-٦-٣ خرق الحماية المتصلة بالاتصالات والبيانات

المقصود بهذه الطائفة الانشطة التي تستهدف البيانات والبرمجيات ذاتها. وهي تشتمل على مجموعتين[٧٥]:

المجموعةالأولى: هجمات البيانات Data Attacks

- **النسخ غير المصرح به للبيانات**:Unauthorized Copying of Data وهي العملية الشائعة التي تستتبع الدخول غير المصرح به للنظام، حيث يمكن الاستيلاء عن طريق النسخ على كافة أنواع البيانات، وهنا تشمل البيانات والمعلومات والاوامر والبرمجيات وغيرها.
- **تحليل الاتصالات**:Traffic Analysis الفكرة هنا ببساطة ان الهجوم ينصب على دراسة أداء النظام في مرحلة التعامل ومتابعة ما يتم فيه من اتصالات وارتباطات بحيث يستفاد منها في تحديد مسلكيات المستخدمين وتحديد نقاط الضعف ووقت الهجوم المناسب وغير ذلك من مسائل يجمعها فكرة الرقابة على حركة النظام بغرض تيسير الهجوم علىه.
- **القنوات المخفية**:Covert Channels وهي عمليا صورة من صور اعتداءات التخزين، حيث يخفي المقتحم معطيات او برمجيات او معلومات مستولى عليها كأرقام بطاقات ائتمان

---

75 Cary ,Hayward" ,The Internet Protocol Security (IPSec) Standard: Clearing up the Confusion ," Product Marketing Manager/RedCreek Communications.2008 P73-80

في موضع معين من النظام، وتتعدد اغراض الاخفاء، فقد تكون تمهيدا لهجوم لاحق او تغطية اقتحام سابق او مجرد تخزين لمعطيات غير مشروعة.

المجموعة الثانية: هجمات البرمجيات[٧٦] Software Attacks

- **المصائد أو الأبواب الخلفية**:Trap Doors الأبواب الخلفية ثغرة او منفذ في برنامج يتيح للمخترق الوصول من خلاله الى النظام، انه ببساطة مدخل مفتوح تماما كالباب الخلفي للمنزل الذي ينفذ منه السارق.
- **السرقة او اختلاس المعلومة او الاستخدام اللحظي** (سرقة او اختطاف الجلسات Session Hijacking) وليس المقصود هنا انشطة الاستيلاء على البيانات عبر واحد او اكثر من الاساليب التقنية المتقدمة او اللاحقة، انما المقصود ان يستغل الشخص استخداما مشروعا من قبل غيره لنظام ما، فيسترق النظر او يستخدم النظام عندما تتاح له الفرصة لانشغال المستخدم دون علمه، او ان يجلس ببساطة مكان مستخدم النظام فيطلع على المعلومات او يجري اية عملية في النظام، وذلك بقصد الاستيلاء على بيانات او الحصول على معلومات تستخدم في اختراق او اعتداء لاحق او لتنفيذ نشاط تدميري آني او لكشف معطيات بشكل فوري.
- **الهجمات عبر التلاعب بنقل البيانات عبر انفاق النقل**:Tunneling انفاق النقل في الاصل طريقة تقنية مشروعة لنقل البيانات عبر الشبكات غير المتوافقة، لكنها تصبح طريقة اعتداء عندما تستخدم حزم البيانات المشروعة لنقل معطيات غير مشروعة.
- **الهجمات (الموقوتة)** Timing attacks وهي هجمات تتم بطرق تقنية معقدة للوصول غير المصرح به الى البرامج او البيانات، وتقوم جميعها على فكرة استغلال وقت تنفيذ الهجمة متزامنا مع فواصل الوقت التي تفصل العمليات المرتبة في النظام، وتضم في نطاقها العديد من الاساليب التقنية لتنفيذ الهجوم، منها إساءة استغلال الاوضاع او الانماط العادية للاداء والكيفية في النظام Race conditions والهجمات غير المتزامنة او غير المتوافقة المتصلة باستغلال ترتيب تنفيذ العمليات الاعتياديةAsynchronous attacks .
- **البرمجيات الخبيثة** Malicious Code كالفايروسات Viruses وحصان طروادةTrojan

[76] Allsopp, William. Unauthorised access : Physical penetration testing for it security teams. Hoboken, NJ: Wiley, 2009. 240-241

Horsesوالدودة الإلكترونيةً Warms والسلامي Salamis والقنابل المنطقية Logic Bombs: الجامع المشترك بين هذه البرمجيات انها برمجيات ضارة تستغل للتدمير سواء تدمير النظام او البرمجيات او البيانات او الملفات او الوظائف او تستثمر للقيام بمهام غير مشروعة كانجاز احتيال او غش في النظام، والحقيقة انها ليست تسميات مترادفة للفيروسات الشائعة، انها تختلف عن بعضها البعض من حيث تركيبها احيانا واحيانا من حيث طريقة احداث النتيجة واحيانا اسلوبها في الهجوم.

والفيروسات تمثل حرب الهجمات القائمة والشائعة الان بسبب استغلال الانترنت وتوفيرها فرصة نشر البرمجيات الضارة حول العالم، ولم تعد مجرد هجمة تستهدف نظاما بعينه او تلحق ضررا باحد الملفات، بل عدت هجمات منظمة تلحق خسائر بالملايين[٧٧] .

٣-٦-٤**الهجمات والمخاطر المتصلة بعمليات الحماية**Breaches of Operations Security :

يشار الى خمسة أنواع من الاساليب ضمن هذه الطائفة، بعضها يتصل بالهجمات التي تستهدف نظام او إستراتيجية الدخول، بعضها يستهدف نظام ادخال ومعالجة والبيانات، وبعضها يصنف كفعل اولي لتحقيق عمليات الدخول غير المصرح به الى مختلف أنواع الشبكات. فيما يلي ايجاز لهذه الاساليب والاعتداءات، مع إيضاح لمسميات أخرى من الانشطة والأساليب والاعتداءات تتصل باختراق الشبكات تحديدا وبيان لاهم نقاط الضعف وفقا لما توصلت اليه ادلة أمن المعلومات المتخصصة جراء الدراسات البحثية[٧٨]:

- **العبث (الغش) بالبيانات**:Data Diddling ويستهدف هذا الهجوم او الاعتداء تغيير البيانات او انشاء بيانات وهمية في مراحل الادخال او الاستخراج، ويتم في الحقيقة بعشرات الانماط والأساليب التقنية، جامعها المساح بأمن وحماية مرحلة ادخال البيانات او استخراجها.

- **خداع بروتوكول الإنترنت** IP Spoofing **(التخفي باستغلال بروتوكولات النقل)**: الحقيقة ان اصطلاح Spoofing لا يعني التخفي، فهو اصطلاح يتعلق بالغش والخداع والايهام والتقليد والمحاكاة والسخرية، لكن استخدامه الشائع الان يتعلق بهجمات فايروسات الإنترنت، والفكرة هنا قريبة من فكرة التخفي التي عرضنا لها أعلاه عندما يتخذ شخص او ينتحل صفة مستخدم آخر

---

[77] Mitnick, K: "The Art of Deception", Wiley Publishing Ltd: Indianapolis, Indiana; United States of America،(2002) p. 103. ISBN 0-471-23712-4

[78] Geneva، "WHO Style Guide"، World Health Organization. 2004. p. 43

مخول بالاستخدام، لكن الفرق هنا، اننا نتحدث عن وسيلة تقنية بحتة، بحيث يقوم المهاجم عبر هذه الوسيلة بتزوير العنوان المرفق مع حزمة البيانات المرسلة بحيث يظهر للنظام – طبعا المعتمد في تبادل البيانات على بروتوكولات النقل واهمها هنا بروتوكول الإنترنت الاساسي – على انه عنوان صحيح مرسل من داخل الشبكة، بحيث يسمح النظام لحزمة البيانات بالمرور باعتبارها حزمة مشروعة (ان جاز التعبير)

– **تعقب كلمات السر (جمعها والتقاطها)**:Password Sniffing واذا كانت انشطة الاعتداء التي تتم باستعمال كلمات السر كانت تتم غالبا فيما سبق عن طريق تخمين كلمات السر مستفيدة من ضعف الكلمات عموما وشيوع اختيار الافراد لكلمات سهلة تتصل بمحيطهم الاسري او محيط العمل او حياتهم الشخصية، فان الجديد استخدام برمجيات يمكنها التقاط كلمات السر خلال تجوالها في جزء من الشبكة او أحد عناصرها ومراقبتها ومتابعتها لحركة الاتصال على الشبكة، بحيث يقوم هذا البرنامج من حيث الاصل بجمع اول ١٢٨ بايت او اكثر – مثلا – من كل اتصال بالشبكة التي تجري مراقبتها وتتبع حركة الاتصال عليها، وعندما يطبع المستخدم كلمة السر او اسم المستخدم، فان البرنامج(المتعقب) يجمع هذه المعلومات وينسخها اضافة الى ان أنواع من هذه البرامج تجمع المعلومات الجزئية وتعيد تحليلها وربطها معا كما تقوم بعضها باخفاء انشطة الالتقاط بعد قيامها بمهمتها[٧٩].

– **المسح والنسخ**Scanning وهو اسلوب يستخدم فيه برنامج الماسح ware dialer او (demon dialer processes) الذي هو برنامج احتمالات يقوم على فكرة تغيير التركيب او تبديل احتمالات المعلومة، ويستخدم تحديدا بشان احتمالات كلمة السر او رقم هاتف المودیم او نحو ذلك، وابسط نمط فيه عندما تستخدم قائمة الاحتمالات لتغيير رقم الهاتف بمسح قائمة أرقام كبيرة للوصل الى احدها الذي يستخدم موديم للاتصال بالإنترنت، او اجراء مسح لاحتمالات عديدة لكلمة سر للوصل الى الكلمة الصحيحة التي تمكن المخترق من الدخول لنظام، ومن جديد فان هذا اسلوب تقني يعتمد واسطة تقنية هي برنامج (الماسح) بدلا من الاعتماد على التخمين البشري[٨٠].

– **هجومات استغلال المزايا الاضافية**:Excess Privileges الفكرة هنا تتصل بواحد من اهم استراتيجيات الحماية، فالاصل ان مستخدم النظام – تحديدا داخل المؤسسة – محدد له نطاق الاستخدام ونطاق الصلاحيات بالنسبة للنظام، لكن ما يحدث في الواقع العملي ان مزايا الاستخدام

---

[٧٩] الغثبر سليمان ،خالد ،و القحطاني عبدالله،محمد "امن المعلومات "، مكتبة الملك فهد الوطنية ،٢٠٠٩، ص٤٤-٤٩

[٨٠] Dave Burrows, "Introduction to becoming a Penetration Tester", SANS Institute, part of the Information Security Reading Room, June,2 2003.p210

يجري زيادتها دون تقدير لمخاطر ذلك او دون علم من الشخص نفسه انه يحظى بمزايا تتجاوز اختصاصه ورغباته، في هذه الحالة فان أي مخترق للنظام لن يكون فقط قادرا على تدمير او التلاعب ببيانات المستخدم الذي دخل على النظام من خلال اشتراكه او عبر نقطة الدخول الخاصة به، انه ببساطة سيتمكن من تدمير مختلف ملفات النظام حتى غير المتصلة بالمدخل الذي دخل منه لانه استثمر المزايا الاضافية التي يتمتع بها المستخدم الذي تم الدخول عبر مدخله. واوضح مثال على هذا الخطر في العالم المادي، تمكن شخص من دخول غرفة مدير فندق مثلا بقصد سرقته فيجد في غرفته مفاتيح كافة قاصات الامانات او مفتاح الماستر الذي يفتح غرف الفندق جميعها. وهذا وحده يعطينا التصور لاهمية استراتيجية أمن المعلومات في المصرف فتحديد الامتيازات والصلاحيات قد يمنع في حقيقته من حصول دمار شامل ويجعل الاختراقات غير ذات اثر، ولن تسمح الاستراتيجية الواعية للقول ان أحد المستخدمين لديه مزايا لا يعرف عنها بل لن تسمح بوجودها اصلاً[٨١].

٢-٧بعض نماذج لمهددات ومخاطر القطاع المصرفي الإلكتروني

٢-٧-١المخاطر المتعمدة[٨٢]:

- الاختلاس من حسابات البنك الداخلية من قبل الموظفين

ويتم ذلك عن طريق إستغلال الحسابات الوسيطة والمعلقة والحسابات غير المتحركة وتحدث بسبب سوء إستغلال الصلاحيات الإدارية والمتاجرة بأموال البنك من قبل كبار موظفي البنوك وذلك بمشاركة بعض عملاء البنك في أرباحهم .وتعود جميع هذه المشاكل إلى ضعف الرقابة وعدم وجود نظام مراجعة فاعلة وعدم تطبيق الرقابة الثنائية.

- الإختلاس من حسابات العملاء من قبل الموظفين

ويتم ذلك بالتلاعب في حسابات العملاء من قبل موظفي البنوك بالسحب والإيداع وذلك بتجاوز الصلاحيات الممنوحة أو بإساءة استخدام الصلاحيات أو باستغلال صلاحيات الآخرين وسوء استخدامها أو التزوير، ويعود ذلك أيضاً إلى ضعف الرقابة سواء كان

[81] Dominick Baier, "Improving Application Security through Penetration Testing", Oct, 2004.Conferences.

[82] Warwick Ford "Computer communications security" ،٢٠٠٨، P 17-١٩

الضعف ناتجاً عن النظام أو عن عدم وجود الوعي الأمني لدى العاملين والثقة المفرطة بين الموظفين.

- السرقة من حسابات العملاء باستخدام شبكة الانترنت:

ويتم ذلك بعدة طرق تم ذكرها سابقاً وهي الحصول على المعلومات السرية لعملاء البنك بإختراق أجهزتهم الخاصة وزرع البرامج الخبيثة مثل المصائد Phishing أو برامج رصد حركة لوحة المفاتيح التي تقوم بدورها بنقل البيانات الخاصة بالضحية مثل أرقام الحسابات وأرقام بطاقات الائتمان واسم المستخدم وكلمة السر والأرقام السرية ومن ثم بثها للمجرم ليقوم بالدخول لحسابات العملاء وتنفيذ الحركات المالية منها.

هذا بالإضافة إلى أنه توجد برامج خبيثة يمكن زرعها في جهاز الضحية ومن ثم التحكم في الجهاز – من البعد– في تنفيذ ما يشاء.

- سرقة واستغلال بواقي وكسور الاحتسابات

ويتم ذلك عادة من قبل المبرمجين الذين يقومون باستخدام برامج مدسوسة أو وضع شروط معينة ببعض البرامج وإذا تحقق الشرط يقوم البرنامج بتحويل جزء من الكسر العشري ويتم تجميعه في حساب ما –غير معروف أو مرئي لدي القائيمين بالأمر – ومن ثم يقوم بتحويله لحسابه، والسبب في ذلك عدم فصل المهام، وعدم فصل بيئة العمل، والإعتماد على موظف بعينه، وتفويض الأمر لمبرمج واحد مثلاً ليقوم بكل الأدوار أي دور المبرج والمختبر، وهوالذي يقوم بتركيب وصيانة النظام والمستخدم في آن واحد .

- سرقة الارقام السرية لبطاقات عملاء الصراف الآلي

يتم ذلك إما عن طريق إختراق الملفات الحاوية على الأرقام السرية في حالة ضعف نظام طباعة الارقام السرية أو بفك شفرة الرقم السري باستخدام برامج معينة أو بالمشاهدة من قبل أشخاص آخرين وذلك عند استخدام العميل للبطاقة أو بسرقة المغلفات الحاوية على الارقام السرية.

- سرقة أرقام بطاقات الإئتمان

ويحدث ذللك بطرق عديدة منها الاختراق كما سبق توضيحه وقراءة الملفات التي تحتوي

على هذه الارقام أو تسريبها من قبل الموظفين بشتى الطرق والوسائل مثل النسخ أو عبر البريد الالكتروني أو في شكل تقارير والجريمة الفعلية تبدأ باستخدام أرقام البطاقات في التسوق عبر الإنترنت.

- عدم الاعترا ف بالحركات المالية

من أكبر المهددات التي تجابه التجارة الالكترونية والبنوك –كواحدة من هذه المنظومة – هي عدم امكانية إثبات حق أي من الطرفي التعامل – البنك والعميل– في حالة نشوب خلاف بينهم عند نكران العميل تنفيذه لحركة ما، فقد يكون العميل على حق في حالة حدوث اختراق للبنك من قبل آخرين لضعف في النطام الأمني وعدم القدرة لإثبات الواقعة ومدى قانونيتها والوسائل المستخدمة لاثبات شرعية تنفيذ الحركة والوثوق منها.

- سرقة وتسريب المعلومات

وتتمثل في كشف معلومات العملاء ونشاطهم او كشف أسرار البنك لجهات منافسة وغالباً ما يحدث ذلك في المنتجات المصرفية وفي الصفقات التمويلية..

٢-٧-٢ المخاطر غير المتعمدة[٨٣]

- عدم توفر الخدمة المقدمة وعدم استمراريته

ويتم ذلك من خلال إعاقة الأجهزة والنظم من أداء عملها وجعل مصدر المعلومات غير متاح لاستعمال العملاء.

وعموماً تحث هذه المشكلة لعدة أسباب منها[٨٤]:

–الفيروسات:

وتعود هذه المشاكل إلى عدم وجود سياسات أمنية لإدارة نظم المعلومات ومنها مكافحة الفيروسات والبرمجات الضارة بصورة عامة، لجهل أو تساهل الإدارات في تقدير حجم هذه المشاكل، فعدم وجود السياسات الأمنية يجعل الموظفين ينقلون البرامج والمعلومات

---

[83] http://news.bbc.co.uk/1/hi/uk/4356661.stm

[٨٤] http://www.nytimes.com/2007/01/25/technology/25hack.html?ex=1327381200&en=58990497ce27b2b2&e

دون تحسب لهذه المشاكل، كما أن استخدام البرامج غير المرخصة وغير معروفة المصدر يجعل النظم عرضة للإصابة بالفيروسات.

-مشاكل الكهرباء:

إن عدم إستقرار الطاقة الكهربائية في السودان والقطوعات المستمرة وارتفاع تكلفة البدائل الفاعلة، تعرض أجهزة الحاسوب إلى مخاطر عالية من تلف في الأجهزة وضياع للمعلومات وبالتالي عدم توفر الخدمة للعملاء.

- مشاكل حسابات العملاء:

تتعرض حسابات العملاء لعدة مشاكل إما لخلل في النظام أو لعدم وجود وظيفة رقابية عليها أو لخطأ إدخال البيانات وخلطها بين حسابات العملاء أو لخلل في برامج وأجهزة الصراف الآلي أو مشاكل الشبكات في تنفيذ القيود بين الفروع.

ويمكن عرض ما سبق وإيجازه كما يأتي[٨٥]:

- خطأ إدخال البيانات

كثيراً ما تحدث مشاكل في مجال العمل المصرفي كالخطأ في إدخال أرقام الحسابات عند اجراء الحركات المالية المختلفة فتتم القيود في حسابات عملاء آخرين أو إدخال مبالغ خطأ أو إجراء خصم بدلاً عن الإضافة مما يحدث مشاكل للعملاء، وتعود هذه المشاكل إلى عدم وجود آلية فاعلة في المطابقات اليومية والمراجعة والرقابة الثنائية ، كما تحدث لعدم تصميم النظام بطريقة تضمن الرقابة على المدخلات خاصة أرقام الحسابات عن طريق مراجعة صحة رقم الحساب .

-مشاكل الصراف الآلي:

الصراف الآلي من الوسائل المتطورة في عالم البنوك والخدمات المصرفية التي تقدمها البنوك من حيث سهولة الإستعمال وحرية التصرف ومرونة الزمان والمكان الذين تتيحهما هذه الخدمة، إلا أن هذه الخدمة كغيرها من الخدمات الالكترونية عرضة لبعض

[85] http://news.soft32.com/international-gang-arrested-for-300000-internet-bank-theft_3486.htm

المشاكل التي قد تزعج العميل، ومن هذه المشاكل[٨٦]:

الخلط ما بين حسابات العملاء:

حدث في أجهزة الصراف الآلي لأحد البنوك – لخلل في توفيق الجهاز أو لعدم شمولية برامجه – أن قام الصراف الآلي بصرف المبالغ المالية المطلوبة من حساب العميل السابق حيث كان النظام يقوم بخصم مبلغ الحركة من العميل السابق وهكذا في كل الحركات التالية لان النظام يتعامل مع شخصين مختلفين الاول هو صاحب البطاقة الذي يريد استخدام الجهاز والآخر هو صاحب الحساب وهو الذي استخدم الجهاز قبل الشخص الاول والنتيجة في كل الاحوال أما الخصم من حساب عميل آخر غير صاحب البطاقة أو الإعتذار للعميل بحجة تجاوز حدود الصرف المسموح به خلال اليوم لان العميل السابق قد سحب حد السقف المسموح به أو أن الرصيد لا يكفي، وبنظرة بسيطة نرى حجم المشكلة التي تحدثها هذا الخلل لكل من العميلين.

استرجاع المبالغ :

بعص أنواع أجهزة الصراف يقوم بدفع مبلغ الحركة دفعة واحدة وبالتالي ينتظر فترة محددة لتسيلم المبلغ، في حالة عدم إستلام العميل للمبلغ في الوقت المحدد يقوم الجهاز بسحب المبلغ إلى خزانة خاصة داخل الجهاز، وفي هذه الحالة لا يقوم النظام بعكس القيد أي بارجاع المبلغ لحساب العميل مالم يقم العميل بالمطالبة ومن ثم مراجعة سجل حركات الجهاز **(Jornal)** للتحري لمعرفة تفاصيل الحدث

سحب البطاقات أو إغلاقها:

أجهزة وأنظمة الصراف اللآلي معدة ومجهزة لحماية بطاقات العملاء حيث يقوم الجهاز بسحب بطاقة العميل إذا تركها العميل سهواً لفترة محددة من الزمن لكي لا يأخذها شخص آخر ويسئ استخدامها، أو يقوم الجهاز بايقاف البطاقة إذا أخطأ العميل في

---

٨٦ http://www.zdnet.com.au/news/security/soa/Online_banking_theft_who_pays_/0,130061744,139182217,00.htm

إدخال الرقم السري لأكثر من عدد من المرات محددة وذلك خوفاً من أن تكون البطاقة مسروقة، ولكن عدم رضاء العميل ينبع من بطء اجراءات أستعادة البطاقة او إعادة تشغيلها والتي يتطلب خطوات دقيقة لضمان امن وسلامة الإجراءات.

- مشاكل تنفيذ الحركات المالية بين الفروع عبر الشبكة

من أهم أهداف ربط الفروع بشبكة معلومات واحدة للبنوك، خدمة عملائها بتنفيذ وتبادل القيود فيما بينها، ولكن لوجود مشاكل في الخدمات التي تقدمها شركات الإتصالات، تفشل كثير من البنوك في تقديم هذه الخدمة بالدرجة المأمولة بل وتؤدي إلى مشاكل مالية للعملاء والبنوك معاً من حيث عدم تنفيذ بعض الحركات لحسابات الفروع البعيدة **Remote Branches** ، كما أنها قد تؤدي إلى تكرار القيود في حسابات العملاء بالخصم أو الإضافة، بالإضافة لمشاكل الاتصالات فإن عدم دقة وتكامل النظام المستخدم يودي أيضاً إلى مثل هذه المشاكل.إن المخاطر المذكورة بأنواعها وتأثيراتها تدفع دون شك إلى البحث عن وسائل حماية تبعد المخاطر وتقلل من آثارها [٨٧].

من هنا كان لا بد من تحديد اهداف النظام بدقة في ضوء المخاطر المذكورة، ومن رسم السياسات الواجب اعتمادها لتوفير المناخ الملائم الذي يمكن من خلاله بلوغ أهداف النظام في حماية بياناته ومعلوماته. هذا الاهداف والسياسات يتم ترجمتها إلى تعليمات واجراءات ترافق انجاز الأعمال وتضمن في كل مراحل العمل ومفاصله الحماية الكافية للبيانات.

وتتمثل أهداف أنظمة المعلومات في ضمان سلامة أنظمة المعلومات المختلفة في المصارف من خلال تحقيق ثلاثة مطالب أساسية، تتمثل في سرية المعلومات، سلامة المعلومة، وتوافر المعلومة . ويتطلب تحقيق المطلب الأول المرتبط بسرية المعلومات تأمين المعلومات بشكل يمكن فقط الأشخاص المصرح لهم الوصول إليها دون غيرهم (أصحاب الصلاحية أو المخول لهم). أما المطلب الثاني المتمثل في سلامة المعلومة، فيسعى إلى ضمان سلامة مصادر المعلومات، بحيث لا يمكن تغييرها أو تحديثها إلا من قبل الأشخاص المصرح لهم فقط. فيما المطلب الثالث لضمان أمن المعلومات فيتمثل في إمكانية وسهولة توفير المعلومات وقت الحاجة إليها .

---

87 http://www.xs4all.nl/uk/veiligheid/wireless/Wireless network

ويمكن القول إن مستجدات العمل المصرفي تفرض تحديات نوعية على نظم المعلومات المحاسبية للمصارف باتجاه تطويرها بما يتناسب مع تلك المستجدات وبما يخدم مستخدمي المعلومات التي ينتجها بشكل افضل وخاصة في المصارف التي بدأت تقديم خدماتها الالكترونية، وفرضت بالتالي على نظم معلومات المصارف ضرورة وضع أمن البيانات والمعلومات في اولى أولوياتها، ما دفعها إلى رسم أهدافها في هذا المجال والسعي بالوسائل المتاحة إلى بلوغ تلك الأهداف.

كما أن تنوع وتطور الأعمال المصرفية في ظل تكنولوجيا الاتصالات والمعلومات زادت من أهمية الرقابة الداخلية، خصوصا ما يتعلق بأمن البيانات والمعلومات. هذه الاهمية تولدت من المخاطر التي تتأتى من الأعمال المصرفية في البيئة الالكترونية لهذه الأعمال، والتي يتوجب على الرقابة الداخلية تداركها وتجنب آثارها وتخفيف وطأة أعبائها على المصرف والمتعاملين معه. من هنا بات على نظم المعلومات وانظمة الاتصال وتشغيل البيانات بمختلف انواعها تحديد اهداف الامان لبياناتها ومعلوماتها، ورسم سياساتها التي يجب أن تسهم في بلوغ تلك الأهداف، وترجمة تلك السياسات إلى جملة من التعليمات والاجراءات واجبة التطبيق بحيث يمكن من خلالها ضمان أمن البيانات والمعلومات التي ينتجها النظام.

الفصل الثاني

دور نظام المعلومات المحاسبي في الحد من مخاطر العمل المصرفي الإلكتروني

المبحث الأول : موقع نظام المعلومات المحاسبي في العمل المصرفي الإلكتروني

المبحث الثاني : دور الرقابة الداخلية في التغلب على مخاطر العمل المصرفي الإلكتروني

١- المبحث الأول: موقع نظام المعلومات المحاسبي في العمل المصرفي الإلكتروني

١-١ مفهوم النظام وأهدافه:

قدم النظام وفق تعاريف متعددة منها ما يلي:

"هو مجموعة من العناصر التي ترتبط مع بعضها بسلسلة من العلاقات بهدف أداء وظيفة محددة أو مجموعة من الوظائف وهذه العناصر هي مكونات النظام التي تكون إما مكونات مادية مثل الحواسيب أو الشاشات وإما مكونات معنوية مثل البرامج والملفات والأنظمة والقوانين [٨٨].

"مجموعة من العناصر والأجزاء التي تتحدد فيما بينها وظيفياً وتترابط لتحقيق غاية محددة، ويوجد النظام في إطار بيئة توفر له الموارد وتتلقى منه النتائج ، كما أنه يتصف بالحركة المستمرة والمرونة" [٨٩]

" هو كيان مؤلف من أجزاء أو مكونات متفاعلة تحقق هدف أو عدة أهداف ويعتمد كل عنصر فيها على الآخر وتجتمع العناصر لتكون مكونات النظام الرئيس" [٩٠].

إذا فالنظام هو عبارة عن كيان متكامل، يتكون من أجزاء وعناصر متداخلة فيما بينها تربطها علاقة متبادلة لتحقق أهدافاً محددة هي مخرجات هذا النظام.

يمثل نظام المعلومات في منظمة الأعمال وحدة متكاملة، مكونة من أنظمة فرعية نوعية، تهدف جميعها إلى توفير المعلومات لخدمة اتخاذ القرارات بأنواعها. يشكل نظام المعلومات المحاسبية أحد هذه الأنظمة النوعية، فهو يختص بإنتاج المعلومات المحاسبية التي تعد استنادا إلى ضوابط القياس والإفصاح المحاسبي، وهدفه من ذلك تدعيم قرارات ذوي الشأن للحفاظ على مصالحهم عبر تقديم المعلومات الملائمة والموثوقة. يأخذ تدعيم القرارات أشكالا مختلفة، كتقديم معلومات مرغوبة لم يسبق إعداد مثلها للمستخدمين، أو تقديم المعلومات التي تعد دوريا في الوقت المناسب، وغير ذلك[٩١].

---

[٨٨] القاسم، عبد الرزاق، "تحليل وتصميم نظم المعلومات المحاسبية"، عمان، مكتبة دار الثقافة للنشر والتوزيع، ٢٠٠٤، ص١٧

[89] Kiso، Donald E. and Wgeyganadt، Jerry J، Interbmediate Accounting ،NewYork : John Wiley and Sons Inc، 2002 P 2

[٩٠] جمعة ،أحمد, و العربيد ،عصام, "نظم المعلومات المحاسبية "مدخل تطبيقي معاصر ، جامعة الزيتونة ،عمان، الأردن ،٢٠٠٨ ص١٤

[٩١] دهراوي ، كمال الدين،ومحمد،سمير كامل ،"نظم المعلومات المحاسبية "دار الجامعة الجديدة للنشر ، الإسكندرية ،مصر ،٢٠١٠ ، ص١٦-٢٠

وبالتالي فإن نظم المعلومات تحقق العديد من المنافع بالنسبة للمؤسسة، كالمرونة والسرعة في الإنجاز والانخفاض في التكاليف، وقدرة المؤسسة المستخدمة لنظم المعلومات على تقديم معلومات ذات قيمة وفي الوقت المناسب.

تقوم نظم المعلومات المحاسبية بتنظيم العمل بشكل آلي، مما يقلل نسبة حدوث الأخطاء في الوقت الذي يتم فيه تقديم خدمات جديدة. وعليه فإن إنجاز الأعمال بغياب بيانات النظام المحاسبي أمر متعذر إلى درجة كبيرة.

يمكن حصر بعض المنافع لنظام المعلومات المحاسبي في المصرف بما يلي:

١- توفير المرونة الكافية لتحسين العمل إضافة إلى المرونة التنظيمية

٢- تقليل الأخطار الناجمة عن الأعمال

٣- السرعة في أداء النشاطات

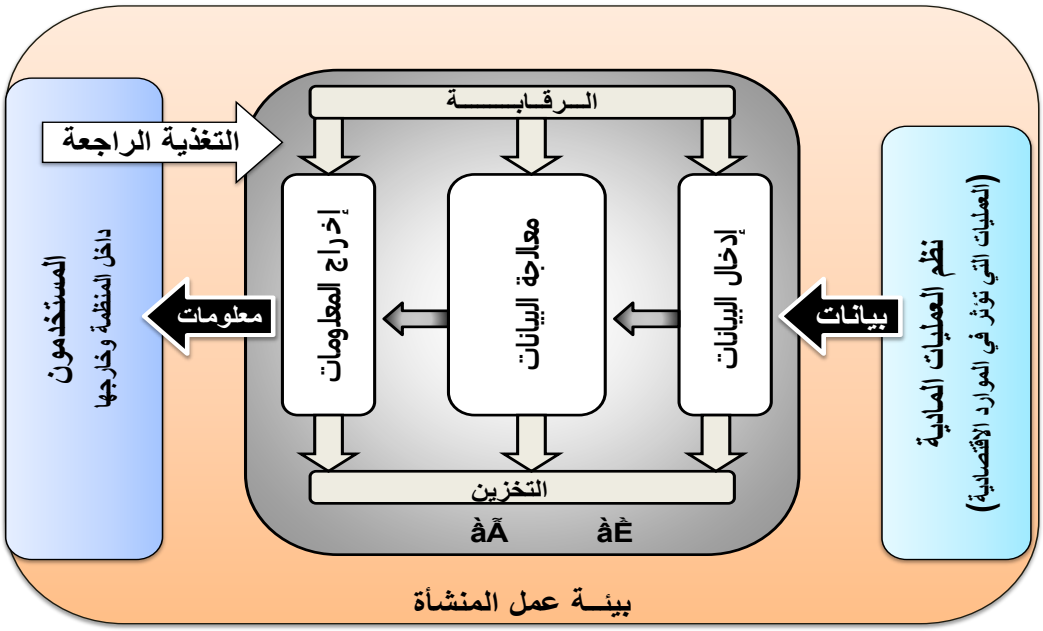
٤- زيادة المبيعات وفتح أفاق جديدة

٥- رفع معنويات العاملين

٦- الميزة التنافسية

٧- تحسين التخطيط والرقابة

يقوم النظام لتحقيق أهدافه والمساهمة في إنجاز الأعمال المصرفية بعدة أنشطة يحوّل من خلالها البيانات إلى معلومات، كما في الشكل رقم (٤). نشاط إدخال البيانات ينتج عنه استلام البيانات (الموارد) من البيئة المحيطة بالنظام ليتم معالجتها عبر أنشطة التشغيل المختلفة داخل النظام بهدف تحويلها إلى معلومات. وهذه تمثل مخرجات النظام، ليبدأ بالتالي نشاط الإخراج. أما نشاط الرقابة فهو يسهم في ضبط العمليات والأنشطة الجارية بحيث يوفر الحماية والأمن للبيانات والمعلومات في كافة مراحل عمل النظام. على حين أن التغذية الراجعة تمكن من معرفة قدرة المعلومات التي أنتجها النظام على تلبية احتياجات المستخدمين إلى المعلومات، أي على دعم قراراتهم. وهذا يمكّن بالتالي من تطوير عناصر النظام وأنشطته وتحسين أدائه لإنتاج المعلومات المطلوبة وبالخصائص اللازم توافرها فيها. المخطط التالي يظهر موقع نظام المعلومات المحاسبي في البيئة التي يعمل فيها والأنشطة التي يمارسها لأداء المهام المطلوبة منه.



الشكل (4) بيئة عمل المنشأة[٩٢]

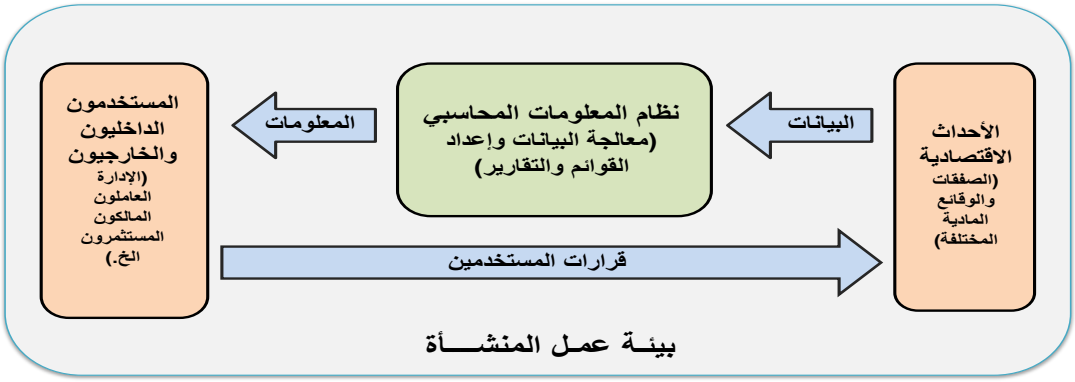
إن أداء النظام المحاسبي لأنشطته المختلفة في بيئة تكنولوجيا المعلومات والاتصالات يجب أن يكون دون شك أداء كفؤاً، يوفر المعلومات اللازمة في الوقت المناسب، خصوصا في الأعمال المصرفية، ويحقق للمعلومات المستخرجة منه خاصية الموثوقية. ولكي تكون المعلومات موثوقة يجب أن يتوافر لها الحماية والأمان بالإضافة إلى دقة وسلامة عمليات النظام وأنشطته المختلفة. وبديهي أنه في حال فقدان عنصر الأمن في النظام فإن الموثوقية تكون شبه معدومة.

تشكل البيانات Data في نظام المعلومات المادة الخام اللازمة لإنتاج المعلومات، فهي تعبر عن حقائق مجردة مرتبطة بأحداث معينة كأرقام الإنتاج وأرقام المبيعات والمخزون، الخ[٩٣]، يتم تلقيها وتسجيلها عن الأحداث موضع الاهتمام. إنها المادة الأولية التي يتم إدخالها إلى نظام المعلومات لمعالجتها, وذلك بهدف الحصول على المعلومات. وهي نتيجة مباشرة لعملية تجريد منطقي للوقائع والأحداث، باستخدام الرموز والأرقام والأحرف. إنها باختصار انعكاسٌ مباشر للأحداث والحقائق

[٩٢] المصري، تيسير ،و يوسف، علي، "نظم المعلومات المحاسبية"، جامعة دمشق، ٢٠١١، ص ٢٤
[٩٣] إبراهيم ,الحبيتي، قاسم، يحى السقا، زياد ,"الإطار العلمي للمحاسبة كنظام للمعلومات"، جامعة الحدباء، الموصل، ٢٠٠٣، ص٢٦

المرتبطة بها، على شكل أحرف وأرقام ورموز، يسهل معه توثيقها وتخزين معطياتها ومعالجة هذه البيانات لأغراض محددة.

إن الباحثة ترى أن المعلومات هي معارف مكتسبة متاحة عن حقائق محددة ترتبط بظاهرة معينة. وهي تمثل في المشروعات الاقتصادية المعارف المتوافرة عن موارد المشروع والأحداث الاقتصادية التي تؤثر فيها وعن الآثار التي تخلفها هذه الأحداث. هذه المعارف يتم توليدها باستخدام المعارف المحاسبية المتاحة. تنتج المعلومات عن عمليات معالجة البيانات التي تصمم لإنتاج المعلومات المرغوبة، وتستخدم لغرض تلبية احتياجات مستخدمها إلى إدراك المعارف التي تحتوي عليها، لتُتّخذ بالتالي القرارات المناسبة استنادا إليها. الشكل التالي يبيّن موقع نظام المعلومات المحاسبي في دورة المعلومات.



موقع نظام المعلومات المحاسبي لمنشأة الأعمال في دورة المعلومات

الشكل رقم (5) موقع نظام المعلومات المحاسبي لمنشأة الأعمال في دورة المعلومات[٩٤]

تحويل البيانات إلى معلومات يمر في مراحل عديدة يشارك فيها كثير من موارد النظام المحاسبي. وهي تتم ضمن اعتبارات كثيرة وتخضع لضوابط متنوعة. تحديد تلك الاعتبارات والأخذ بالضوابط المناسبة، وكذلك إنجاز المراحل المختلفة لعملية التحول، كل ذلك يفرض أن تكون أهداف النظام واضحة محددة بدقة، وأن تكون الرقابة على حركة البيانات متوافرة في كل لحظة ومرافقة لكل خطوة.

يستخلص مما سبق أن هدف نظام المعلومات المحاسبي هو إنتاج المعلومات المحاسبية (باستخدام المعارف المحاسبية) لغرض تزويد المستخدمين بها، ذوي المصالح المادية مع المنشاة،

[٩٤] مرجع سابق ، المصري ،٢٠١١، ص٢٥

لدعم قراراتهم الاقتصادية والصيانة مصالحهم المادية مع المنشأة. تحقيق هذا الهدف يوجب على نظام المعلومات المحاسبي توفير مجموعة من الخصائص النوعية للمعلومات المحاسبية يأتي في مقدمتها الملاءمة والموثوقية. ولغرض توفير هذه الخواص يتم رسم أهداف النظام المختلفة بما فيها تلك التي ترتبط بأمن البيانات والمعلومات.

١-٢.أهمية نظم المعلومات في العمل المصرفي الإلكتروني:

تلعب نظم المعلومات دوراً هاما وجوهرياً في نجاح المصارف والمؤسسات المالية حيث إنها أتاحت الفرصة أمام المصارف لتحقيق المزايا التالية[٩٥]:

١-٢-١ تطوير خدمات مصرفية جديدة: يتيح استخدام تقانة المعلومات والاتصالات في المصارف إمكانية تقديم تشكيلة واسعة من الخدمات المصرفية على مدار الساعة، فأجهزة الصراف الآلي ATM تتيح مواصفات جديدة للخدمة المصرفية مثل: البقاء لساعات طويلة في العمل، التنويع الأوسع للخدمات، وإتاحة خدمات المصرف للعملاء محلياً ودولياً. وهناك خدمة إضافية مهمة في هذا المجال هي العمليات المصرفية على الهاتف التي تسمح للعميل الاستفادة من حسابه بالمصرف وهو في منزله، من خلال تحديد رقم هاتف معين وتفعيل الصوت، إلى جانب استعمال البطاقة الذكية التي تخزن معلومات أكثف من بطاقة (ATM) الاعتيادية. كما أنها سمحت للمصارف بإجراء عمليات التحويلات المالية بين مختلف المؤسسات المالية سواء على الصعيد المحلي أو الدولي بالسرعة اللازمة مع درجة عالية من الأمان كما في استخدام النظام المالي العالمي المعروف باسم (SWIFT)

١-٢-٢ تطوير تطبيقات جديدة للخدمات المصرفية الحالية: لقد أعطت نظم المعلومات في المصارف قدرة إضافية للإدارة المصرفية في إمكانية التوسع والتنوع في الخدمات وفي تطوير كفاءة العمليات، وفي سرعة اتخاذ القرار وفي الرقابة، فلم يعد فتح الفروع الجديدة على السياق التقليدي بشكله السابق، إذ عوضت الاستخدامات التكنولوجية عن ذلك، وصارت الحاجة إلى الخدمة المصرفية في منطقة ما تحل عن طريق الأنظمة الإلكترونية والأجهزة المربوطة بها المكلفة بأداء الوظائف، والتي تستخدم أدوات تقنية متعددة تتيح الربط المتصل والفوري بالفروع والمصارف في المناطق الأخرى داخل البلد وخارجه وبهذه الوسائل يستطيع الزبون وهو في مكان عمله أن يودع ويسحب النقود ويدفع ويحول المبالغ ويقترض الأموال، وغير ذلك دون الحاجة إلى إجراء الزيارة التقليدية إلى فرع المصرف الذي يتعامل معه

[٩٥] القاسم، عبد الرزاق، والمصري، تيسير، والطويل ،ليلى، "نظم المعلومات المحاسبية"، جامعة دمشق ،٢٠٠٥ ,ص ٤-١٠

١-٢-٣ تحسين نوعية الخدمات المصرفية:[٩٦] يساعد استخدام نظم المعلومات المصرف في تحسين نوعية الخدمات المقدمة للعملاء، فسرعة المعالجة التي تتيحها النظم المؤتمتة والربط بين مختلف الحواسب، تتيح للمصرف تخفيض الزمن اللازم لإنجاز الخدمة المصرفية، كما تتيح تكامل الخدمة وإنجازها من خلال النافذة الواحدة، بالإضافة إلى إتاحة إمكانية السحب من فرع من فروع المصرف

١-٢-٤ تحسين الإنتاجية في العمل المصرفي: تعد نظم المعلومات في المصارف من النظم ذات الكثافة العالية للبيانات، أي إن حجم البيانات التي يجب أن تدخل وتعالج كبيرة جداً، وقد تمكنت المصارف عبر نظمها الإلكترونية أن تخفض التكاليف المرتبطة بإنجاز العمليات المصرفية وتحسين كفاءة تقديم الخدمات للعملاء. تحقق ذلك من خلال:

- ❖ خفض عدد القنوات واختصار الدورة المستندية.
- ❖ تخفيض عمليات تسجيل المعاملات.
- ❖ تخفيض تكلفة العمليات.
- ❖ تخفيض التكاليف العامة مثل المرأسلات وغيرها.
- ❖ الدقة في تسجيل البيانات ومعالجتها.

١-٢-٥ تحسين علاقات المصرف مع العميل: إن المصارف التي تقدم مثل هذه الخدمات تتوقع أنها سوف تحقق لعملائها الحاليين الراحة في التعامل مع المصرف، فمثلاً العملاء يتمتعون بالراحة والسرعة عندما يستطيعون تسديد قيم مشترياتهم من السلع في نقطة البيع من خلال استعمال بطاقة مرتبطة بالتحويل الإلكتروني للأموال في نقطة البيع وهناك مؤشرات كثيرة تظهر أن توفير هذه الخدمة من قبل المصرف تمكنه من تحقيق ميزة تنافسية في السوق.

في الواقع، تسهم نظم المعلومات، بما فيها نظم المعلومات المحاسبية، في نجاح العمل المصرفي. فهي تزود الإدارة بالمعلومات المناسبة وبالخصائص المطلوبة وفي الوقت المناسب. فقد تمكنت المصارف الأمريكية، مثلا، من اختصار الوقت اللازم لإنجاز العمليات ووفرت مبلغ ١٢ سنت لكل فاتورة تدفع إلكترونياً.

[٩٦] الموسوي, نوار كحيط ،وعباس ،"أهمية البنوك الإلكترونية في تحسين جودة الخدمة المصرفية"، جامعة واسط – العراق ،٢٠٠٨ ،ص٣-٦

وعليه فإنه لم يعد يوجد أي تباعد بين استخدام تكنولوجيا المعلومات بين القيام بمشاريع الأعمال. لقد أثبتت تكنولوجيا المعلومات قدرتها الفائقة على تخفيض تكاليف الإنتاج والخدمات من خلال أتمتة كافة مراحل العملية الإنتاجية والإدارية، مما أدى إلى توفير في استخدام اليد العاملة والطاقة، بالإضافة إلى أنها تشكل مثلث حلقة الوصل التي تربط بين متطلبات العملاء وأنشطة تصميم الخدمات المصرفية وتسويقها في منظومة كاملة.

لم تعد المصارف الإلكترونية بنكا قائما يقدم خدمات مالية فحسب, بل موقعا ماليا تجاريا وإداريا واستشارياً شاملا. ومن الحقائق التي لابد من إدراكها أن الزبائن أصبحوا بحاجة للحصول على حل لمشاكلهم، وتقديم العروض والخدمات التي تتفق مع رغباتهم وطلباتهم، وهذا ما عجزت عنه البنوك التقليدية التي تقدم جزءا من الحلول ولا تقدم حلولا شاملة[٩٧].

تخلق المصارف الإلكترونية فرصة لتحقيق معدلات أفضل للمنافسة والبقاء في وقت ومكان لتقديم الحلول المبنية على المعلومة الصحيحة. كما أنها تعتبر مؤسسة للمشورة وفتح أفاق العمل والمكان للخدمة السريعة وبأقل التكاليف، ومكان للإدارة المتميزة ومكان لما يمكن تسميته (وقفة التسوق الواحدة(one-stope shopping) لاحتياجات الزبون مهما اختلفت. إن اللجوء إلى المصارف الإلكترونية هو لجوء إلى أحد وسائل المنافسة، ودرءا لمخاطر المنافسة المضادة، وهو أيضا لجوء إلى تقديم خدمات شاملة في وقت قصير وبتكاليف أقل[٩٨].

إن الخدمات التي يقدمها نظام المعلومات المحاسبي للمصرف تبقى فاعليتها محدودة إذا لم يكن النظام قادرا على توفير الأمان لبياناته ومخرجاته وبدرجة عالية من الأمان. من هنا يزداد الاهتمام بأمن النظام الذي يمكن أن يترك آثاراً مباشرة في مستوى أداء الخدمة المصرفية. وهذا يعني ضرورة الاهتمام بكفاءة النظام في بلوغ أهداف الأمان.

[٩٧] قرم، عباس، دراسة بعنوان,"أنظمة الدفع الإلكتروني وتطبيقها في سورية",رسالة ماجستير،الجامعة الافتراضية السورية،٢٠١٢،ص٥٤

[٩٨] معروف، إبراهيم" ,التجارة الإلكترونية والبنوك" , مجلس الغرف التجارية والصناعية السعودية , ٢٠٠٢/٠١/٠٢ ،ص١٣

٢- المبحث الثاني:

دور الرقابة الداخلية في الحد من مخاطر العمل المصرفي الالكتروني

تعتبر الرقابة الداخلية في المصارف جزءاً أساسياً وأولياً من الرقابة المصرفية الشاملة. ولأهميتها فقد أصبحت كل من إدارات البنوك والمراجعين الخارجيين والسلطات النقدية توليها عناية خاصة باعتبارها خط الدفاع الأول في منع وتحجيم المخاطر والأخطاء التي يمكن أن يتعرض لها المصرف. تستند هذه الرقابة ابتداء على وضع قواعد وضوابط أساسية تحكم سير عمل المصارف

وفي هذا الإطار تعتبر أنظمة الرقابة الداخلية في كل مصرف من الأدوات الهامة باعتبارها بمثابة إجراء احترازي يهدف من خلال الوسائل والإجراءات المتبعة التأكد من الصحة الحسابية لما هو مدون في السجلات وحماية أصول المصرف ورفع كفاءة الموظفين وتشجيعهم على التمسك بالسياسات المرسومة.

في الوقت الحالي، أصبحت رقابة أمن أنظمة الكمبيوتر وسلامتها أمراً مهماً. وقد زادت المخاطر في السنوات الأخيرة كما تظهر الدراسات بحسب(Rommney)[٩٩] أن ٦٠٪ من المصارف عانت مؤخراً من فشل رقابي. لذا يجب أن يفهم المحاسب كيف يحمي الأنظمة من التهديدات التي تواجهها. فيجب أن يفهم جيداً تكنولوجيا المعلومات وإمكانياتها ومخاطرها، حيث يمكن لهذه المعرفة أن تساعد تكنولوجيا في تحقيق هدف الرقابة للمصارف.

يجب أن يكون تحقيق الأمن والرقابة الملائمين على مصادر المعلومات هو الأولوية القصوى للإدارة. ومع أن أهداف الرقابة الداخلية تبقى نفسها بغض النظر عن أسلوب معالجة البيانات، تحتاج انظمة المعلومات المحاسبية سياسات وإجراءات رقابة داخلية مختلفة فمثلاً استخدام الكمبيوتر يقلل من الأخطاء ولكنه يزيد مخاطر الوصول أو التعديل غير المسموح للبيانات وأيضا يجب تحقيق فصل وظيفة التفويض عن التسجيل عن وظائف العهدة ضمن الأنظمة المحاسبية بشكل مختلف طالما أن برامج الكمبيوتر قد تكون مسؤولة عن واحدة من هذه الوظائف أو أكثر.

من الأهداف الأولية لنظم المعلومات المحاسبية هو الرقابة فيمكن للمحاسب أن يساعد في تحقيق هذا الهدف بتصميم أنظمة رقابة فعالة وبتدقيق أو مراجعة أنظمة الرقابة لضمان فعاليتها، فالإدارة تتوقع من المحاسبين أن يتخذوا مبدأ وقائي لإزالة تهديدات الأنظمة وكشف التهديدات وتصحيحها والتخلص منها عند حصولها.

---

[99] Marshall B. Romney, Paul John Steinbart, Accounting Information Systems, Prentice Hall 2009 p119-122

فمن الأسهل وضع ضوابط للنظام عند مرحلة التصميم الأولي من إضافتها لاحقاً، ولذلك يجب أن يكون المحاسبون وخبراء الرقابة أفراداً مهمين في الفريق الذي يطور نظام المعلومات أو يطوره.

٢-١ مفهوم الرقابة الداخلية وأهدافها

في بيئة العمل الحالية والتي تتسم بالديناميكية، يجب أن تتفاعل المصارف بسرعة مع الظروف المتغيرة للأسواق، ومن الطرق الجيدة للقيام بذلك هي توظيف موظفين مبدعين ومبتكرين وإعطائهم المقدرة والمرونة لتحقيق متطلبات العمل المتغيرة ومتابعة الفرص الجديدة لإضافة قيمة مؤسساتية للعمل، وفي الوقت نفسه تحتاج المصارف أنظمة رقابة بحيث لا تكون معرضة لمخاطرة قد تؤذي سمعتها.

فالرقابة الداخلية هي المعالجة المطبقة من قبل مجلس الإدارة والإدارة والخاضعين لها لتأمين ضمان معقول أن أهداف الرقابة الآتية قد تحقق[١٠٠]:

- حماية الأصول
- المحافظة على السجلات بتفاصيل كافية لتعكس بشكل دقيق أصول الشركة
- تأمين معلومات دقيقة وموثوقة.
- تأمين ضمان معقول على أنه تم إعداد التقارير المالية بالتوافق مع GAAP.
- تعزيز وتشجيع الكفاءة التشغيلية، بما في ذلك ضمان القيام بالاستلام والانفاق بالتوافق مع تفويض الإدارة والمدراء.
- تشجيع الالتزام بالسياسات الادارية الموصوفة.
- الالتزام بالقوانين والتشريعات القابلة للتطبيق.

إذا الرقابة الداخلية هي معالجة لأنها تتغلغل في النشاطات التشغيلية للمصرف وهو جزء من نشاطات الإدارة الأساسية.

ترى الباحثة أن الرقابة الداخلية تؤمن ضماناً معقولاً وليس مطلقاً لأن تأمين الضمانة الكاملة من الصعب تحقيقها وهي مكلفة جداً، وتكون أحيانا أغراض الرقابة الداخلية متنازعة مع بعضها البعض، فمثلاً بعض الموظفين يضغطون من أجل إعادة هندسة جذرية للعمل بحيث يمكن لهم الحصول على معلومات أفضل وأسرع وتحسين الكفاءة التشغيلية. بينما البعض الآخر يقاوم هذه التغييرات لأنها تعيق حماية أصول الشركة وتحتاج تغييرات مهمة في السياسات الإدارية[١٠١].

---

[١٠٠] Marshall B. Romney, Paul John Steinbart, Accounting Information Systems, Prentice Hall 2009 p 221-222

[101] Romeny K M. and P. Steinbart, Accounting Information System, 3th. ,ed, Prenticehall ,2006 P 227-230

يتم فصل الرقابة الداخلية إلى فئتين [١٠٢]:

- رقابة عامة

صممت الرقابة العامة لضمان أن بيئة رقابة المنظمة ثابتة وذات إدارة جيدة، وهي تنطبق على كل قياسات الأنظمة من الأنظمة الكبيرة إلى أنظمة الكمبيوترات المعقدة إلى أنظمة العميل / المخدم إلى أنظمة الكمبيوترات المكتبية والمحمولة.

ومن أكثر ضوابط الرقابة العامة أهمية هي:

- ضوابط إدارة أنظمة المعلومات.
- ضوابط الإدارة الأمنية.
- ضوابط البنية الأساسية لتكنولوجيا المعلوماتIT.
- ضوابط الحصول على البرمجيات، تطويرها وصيانتها.

- أما رقابة التطبيقات فهي:

–تمنع أخطاء العمليات والاحتيال، تكشفها وتصححها.

– تهتم بدقة البيانات التي تم الحصول عليها، اكتمالها، صحتها والترخيص لها، إدخالها إلى النظام، معالجتها، تخزينها، نقلها إلى الأنظمة الأخرى، ونشرها.

٢-٢ العمليات الرقابية لوثوقية أنظمة المعلومات المصرفية الإلكترونية

إحدى الوظائف الأساسية لنظام المعلومات المحاسبية هي توفير الأمان لمعلومات مفيدة لعملية اتخاذ القرار. ولكي تكون مفيدة، يجب أن تؤمن المعلومات الناتجة عن هذا النظام صورة دقيقة، كاملة وبالوقت المناسب لنشاطات المصرف وأن تكون تلك المعلومات متوافرة عند الحاجة لها. وأيضا يجب حماية المعلومات والنظام ذاته من الفقدان، التهديد والسرقة، ولتأمين معلومات مفيدة لعملية اتخاذ القرار، يجب أن يكون نظام المعلومات المحاسبي موثوقاً[١٠٣].

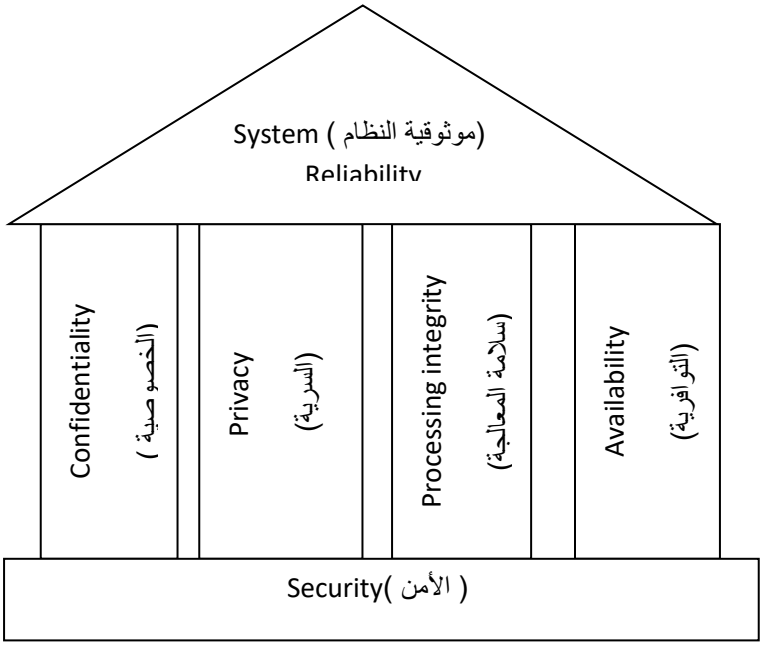
يظهر الشكل التالي خمسة مبادئ أساسية تساهم في الهدف الإجمالي لموثوقية الأنظمة. ونلاحظ أهمية أمن المعلومات حيث تحد إجراءات الأمن من وصول النظام إلى المستخدمين المسموح لهم فقط، ومن ثم تحمي سرية البيانات الحساسة للمصرف وخاصة المعلومات الخاصة بحسابات العملاء.

كما تؤمن إجراءات الأمن معالجة سلامة المعلومات بمنع الموافقة للتبادلات غير المسموحة أو الزائفة بالإضافة إلى منع التغيرات غير المسموحة على البيانات أو البرامج المخزنة، حيث تؤمن إجراءات

[١٠٢] د. المصري تيسير، يوسف علي، نظم المعلومات المحاسبية ،جامعة دمشق، ٢٠١١، ص ٤١١-٤١٩

[١٠٣] د. القاضي حسين، قريط عصام، مراجعة الحسابات (الإجراءات) منشورات جامعة دمشق، ٢٠٠٥ ص ١٢٣ - ١٣٠

الأمن حماية ضد مجموعة من الهجمات بما فيها الفيروسات ومن ثم ضمان توافرية النظام عند الحاجة له وكما نرى في الشكل يعتبر أمن المعلومات أساس موثوقية النظام[١٠٤].



الشكل [١٠٥](6)

٢-٣ أطر الرقابة

تم تطوير عدد من إطارات الرقابة لمساعدة المصارف وغيرها من المنظمات في تطوير أنظمة الرقابة الداخلية لديها وستتناول الباحثة اهم هذه الاطر بالنسبة لموضوع البحث:

٢-٣-١ الخدمات الإئتمانية Trust Services

وهو إطار مطور بالتعاون بين AICPA والهيئة الكندية للمحاسبين القانونيين بشكل خاص يقوم على خمسة مظاهر لأنظمة المعلومات التي تتعلق مباشرة بموثوقية المعلومات[١٠٦]:

- الأمن: يجب الرقابة على الوصول للأنظمة وبياناتها وتقييده لمستخدمين مسموح لهم.

---

[١٠٤] ستيفن أ.موسكوف ، مارك & سيمكن ، نظم المعلومات المحاسبية لاتخاذ القرارات ، مفاهيم وتطبيقات ، دار المريخ ، الرياض ٢٠٠٥، ص ٣٨٨

[105] Marshall B. Romney, Paul John Steinbart, Accounting Information Systems, Prentice Hall 2009,P 272

[106] By Martin J. Coe m, Trust Services: A Better Way to Evaluate I. T. Controls Fulfilling the requirements of section 404,Journal Of Accountin , Sarbanes-Oxley,2009

- السرية: يجب حماية المعلومات الحساسة من غير المصرح لهم.
- الخصوصية: يتم تجميع المعلومات الشخصية عن العملاء تستخدم ويتم المحافظة عليها بالالتزام بالسياسات الداخلية والمتطلبات الخارجية.
- سلامة المعالجة: تتم معالجة البيانات بدقة وبالوقت المناسب وبالتفويض المناسب.
- التوافرية: يكون النظام والمعلومات متوافرين لتحقيق الالتزامات التعاقدية والتشغيلية.

لا يعتبر إطار الخدمات الائتمانية بديلاً عن COBIT لأنه يتعامل فقط مع مجموعة جزئية من القضايا التي تغطيها COBIT.

٢-٣-٢ إطار COBIT

هو إطار أمن أنظمة المعلومات القابل للتطبيق وممارسات الرقابة الخاصة بتكنولوجيا المعلومات، ويسمح هذا الإطار[١٠٧]:

- إدارة لتحديد نقطة إرشاد لممارسات الرقابة والتحكم ببيئات تكنولوجيا المعلومات.
- يعطي الشعور بالأمان لمستخدمي خدمات تكنولوجيا المعلومات بوجود الأمن والرقابة الملائمين.
- الآخذ بآراء المراجعين حول الرقابة الداخلية وأمن تكنولوجيا المعلومات.

يقوم[١٠٨] COBIT على مخاطبة قضايا الرقابة من ثلاث أبعاد:

أهداف الأعمال: لتحقيق أهداف الأعمال يجب أن تتوافق المعلومات مع المعايير المسماة متطلبات الأعمال وقد تم تقسيم المعايير إلى سبعة بنود خططت على شكل أهداف coso وهي:

١-الفعالية: يجب أن تكون المعلومات مناسبة وبالوقت المحدد.

٢ – الكفاءة: يجب إنتاج المعلومات بطريقة اقتصادية.

٣– السرية: يجب حماية المعلومات الحساسة من الكشف غير المصرح به.

٤– السلامة: يجب أن تكون المعلومات دقيقة، كاملة، وصحيحة.

٥ – التوافرية: يجب توافر المعلومات عند الحاجة إليها.

٦ – التوافق: يجب أن تضمن العمليات الرقابية التوافق مع السياسات الداخلية ومع المتطلبات القانونية الخارجية والتنظيمية.

٧-الموثوقية: يجب أن تكون للإدارة إمكانية الوصول إلى المعلومات الملائمة المطلوبة للقيام بالنشاطات اليومية والقيام بمسؤولياتها الائتمانية.

---

[١٠٧] مرجع سابق Romeny ٢٠٠٩ ص ٢٧٣-٢٧٧

[١٠٨] Control Objectives for Information and related Technology

٨-موارد تكنولوجيا المعلومات: متضمنة العاملين، الأنظمة التطبيقية، التكنولوجيا، والبيانات.

٩-عمليات تكنولوجيا المعلومات: ويتم تقسيمها إلى أربعة نطاقات: التخطيط والتنظيم، الاكتساب والتطبيق، التوصيل والدعم المراقبة والتقييم.

في النهاية يتضح أن COBIT قد أتى ووحد المعايير من ٣٦ مصدر مختلف إلى إطار وحيد وكان لذلك تأثير على أنظمة المعلومات وساعد المدراء في التعلم كيفية موازنة المخاطرة والرقابة في بيئة نظام المعلومات.

هناك ثلاث **مواصفات أساسية لأمن المعلومات وفق COBIT** [١٠٩]:

الأولى: الأمن هو قضية للإدارة وليس قضية تقنية فقط

مع أن أمن المعلومات هو موضوع تقني معقد، ولكن من المهم أن نرى أنه وقبل كل شيئ قضية إدارية وليس قضية تقنية معلومات. فبذلك تكون الإدارة مسؤولة عن دقة التقارير الداخلية المختلفة والبيانات المالية الناتجة من أنظمة معلومات المصرف، كما يجب أن تتضمن التقارير السنوية تقريراً لتقويم نظم الرقابة الداخلية للمنظمة حيث تدرك الإدارة مسؤوليتها عن تصميم عمليات الرقابة الداخلية والمحافظة عليها وتقييم كفائتها.

الأمن هو المكون الأساسي للرقابة الداخلية وموثوقية النظام وقد أكدت COBIT في أول أهدافها على أهمية إدارة أمن المعلومات في أعلى مستوى ملائم . ومن المهم معرفة أن الأمن هو هدف متحرك. فالتقدم التقني الحاصل قد أحدث تهديدات ومخاطر جديدة وعليه يجب أن تشمل الرقابة الفعالة على نظم المعلومات تطوير مستمر للسياسات للتعامل مع التهديدات ونقل هذه السياسات لكل الموظفين وتطبيق إجراءات رقابة معينة لتخفيف المخاطر، ومراقبة الأداء والقيام بالتصرفات التصحيحية للمشاكل المحددة وغالباً يشمل التصرف التصحيحي تطوير سياسات جديدة ويأتي هنا دور الإدارة العليا لضمان أن سياسات الأمن تبقى متلازمة مع استراتيجية عمل المصرف وتدعمها.

الثانية: نموذج الأمن المعتمد على الزمن (المستمر) :

لقد أدرك المراجعون أنه لا يمكن للرقابة الوقائية أن توفر حماية ١٠٠٪ وبإعطاء ما يكفي من الوقت والمصادر يمكن التغلب على أي رقابة وقائية ومن ثم تحتاج الرقابة الفعالة إجراءات

[109] Slay ،J.and A.Koronios ،Security & Risk Management، John Willy & Sons ،Australia ،ltd ٢٠٠٦، p 114-120

وقائية مكملة مع أساليب كشف الحوادث والإجراءات لاتخاذ التصرف التصحيحي العلاجي. كما يجب أن تكون أعمال الكشف والتصحيح في الوقت المناسب وهذا هام جداً لأمن المعلومات، فعندما يتم انتهاك الأعمال الرقابية هناك الحاجة للقليل من الوقت لتدمير، تهديد، أو سرقة مصادر معلومات المصرف.

يركز نموذج الأمن المعتمد على الزمن على العلاقة بين إجراءات الرقابة المتعلقة بالوقاية، الكشف والتصحيح. والأنواع الثلاثة من إجراءات الرقابة ضرورية. ودور إجراءات الرقابة الوقائية هو الحد من الأعمال إلى تلك المتوافقة مع سياسة أمن المصرف وعدم السماح بالتصرفات غير المرغوبة. أما دور إجراءات الرقابة الكشفية هو تحديد حالات انتهاك الإجراءات الرقابية الوقائية، أما دور إجراءات الرقابة التصحيحة هو إصلاح الضرر من أية مشاكل حصلت وتحسين وظيفة كل من إجراءات الرقابة الوقائية والكشفية لقليل احتمالية المشاكل المستقبلية.

يقيم نموذج الأمن المعتمد على الزمن كفاءة أمن المصرف بقياس ومقارنة العلاقة بين المتغيرات الثلاث الآتية [١١٠]:

P = الوقت الذي يحتاجه المهاجم لإختراق إجراءات الرقابة الوقائية للمنظمة.

D= الوقت المطلوب لكشف هجمة حاصلة.

C = الوقت المطلوب للاستجابة للهجمة.

ومن ثم يبدأ تقييم هذه المتغيرات الثلاثة كما يلي:

إن كانت P>D+C عندها تكون إجراءات أمن المصرف فعالة وإلا يكون الأمن غير فعال.

يؤمن نموذج الأمن المعتمد على الزمن وسائل لإدارة وتحديد النموذج الأكثر اقتصادية لتحسين الأمن بمقارنة تأثيرات الاستثمارات الإضافية في الرقابة الوقائية، الكشفية، أو التصحيحية فمثلا قد تكون الإدارة تفكر بإستثمار ١٠٠٠٠٠٠ ل.س إضافية لتعزيز الأمن. قد يكون أحد الخيارات هو شراء جدار ناري جديد قد يزيد قيمة P ب ١٠ دقائق. قد يكون الخيار الثاني هو ترقية نظام كشف اقتحام المصرف بطريقة قد تقلل من قيمة D ب١٢ دقيقة.

قد يكون الخيار الثالث هو استثمار أساليب جديدة للإستجابة لأحداث أمن المعلومات بحيث تقلل من قيمة C ب٣٠ دقيقة. في هذا المثال قد يكون الخيار الأوفر هو استثمار عمليات رقابة تصحيحية إضافية تمكن المصرف من الاستجابة للهجمات بشكل سريع.

[١١٠] مرجع سابق Romeny ٢٠٠٩ ص ٢٧٨-٢٧٩

هنا بالرغم من أن نموذج الأمن المعتمد على الزمن يؤمن أساساً تقنياً قوياً لتقييم وإدارة عمليات أمن معلومات المصرف لكن من الصعب تطبيقه مباشرة وأيضا من الصعب اشتقاق معايير موثوقية دقيقة للمعايير P,D,C وأيضاً حتى عندما يمكن حساب قيمة المعايير بشكل موثوق، غالباً ما تضيع موثوقيتها بسرعة بسبب تطورات IT الجديدة.

فمثلاً، اكتشاف ضعف جديد يمكن أن يقلل من قيمة P إلى الصفر ومن ثم يستخدم نموذج الأمن المعتمد على الزمن بالشكل الأمثل كإطار مرتفع المستوى للتحليل الاستراتيجي وللإدارة التكتيكية واليومية للأمن، لذا تتبع معظم المصارف مبدأ الدفاع بالعمق.

الثالثة: الدفاع بالعمق:

فكرة الدفاع بالعمق هي استخدام طبقات متعددة من الرقابة لتجنب الحصول على نقطة فشل وحيدة فيزيد التعدد من الكفاءة لأنه لوفشل واحد أو تمت إعاقته قد يعمل آخر كما هو مقرر. كما أن استخدام معايير الرقابة المتداخلة، المكملة يوفر أيضاً الوقت للمصرف للتفاعل مع الهجمات فمثلاً المصارف تستخدم خليطاً من الأبواب المقفلة، القضبان على النوافذ، الحراس الأمنيين، والخزائن لتأمين معايير رقابة متعددة صممت لتقييد الوصول الفيزيائي إلى الأموال وبشكل مشابه يشمل أمن المعلومات استخدام مزيج من جدران الحماية، كلمات المرور، والإجراءات الوقائية الأخرى لتقييد الوصول لأنظمة المعلومات كما تنطبق الزيادة على معايير الرقابة الكشفية والتصحيحية.

٢-٤ أنواع الرقابة

٢-٤-١ الرقابة الوقائية: هدف الرقابة الوقائية كما يتضمن اسمها، منع حدوث الخروقات الأمنية. وتقوم على [١١١]:

- تمنع حدوث المشاكل قبل نشوئها.
- توظيف طاقم عالي التأهيل.
- فصل مهمات الموظفين بشكل ملائم.
- الرقابة بفعالية للوصول الفيزيائي الى الأصول، أي الرقابة على الموجودات والقيود المحاسبية.
- مراجعة تواقيع العملاء.
- الموافقة على الصرف من الأشخاص المفوضين.

هناك سبعة أنواع لها:

[١١١] مرجع سابق Romeny ٢٠٠٩ ، P 246

رقابة المصادقة: تركز المصادقة على التحقق من هوية الشخص أو الجهاز الذي يحاول الوصول إلى النظام. ويكون هدف رقابة المصادقة هو ضمان أن يستطيع المستخدمين الشرعيين الوصول للنظام. يمكن المصادقة على المستخدمين من[١١٢]:

-شيء يعرفونه، مثل كلمات المرور أو أرقام التعريف الفردية (PIN).

-شيء يمتلكونه، مثل البطاقات الذكية أو بطاقات التعريف.

-شيء فيزيائي (مادي) مميز يسمى "المعرف البيولوجي "مثل البصمات أو الصوت.

ولكن غالباً ما تكون كلمات المرور هي أكثر أساليب المصادقة استخداماً ، كما أن لكل أسلوب مصادقة تقييداته.ومع أنه لا يوجد أياً من أساليب المصادقة الأساسية هذه مضموناً، فإن استخدام اثنين من الأساليب أو الثلاثة كلها بالترافق يكون فعالاً تماماً فتعرف بالمصادقة متعددة العوامل فمثلاً الطلب من المستخدم أن يضع بطاقة ذكية وإدخال كلمة مرور يؤمن مصادقة أقوى بكثير من استخدام أياً من الأسلوبين لوحده.

رقابة التفويض (التخويل)

تقيد المصادقة وصول المستخدمين المخولين للأجزاء المحددة للنظام وتحديداً ما هي التصرفات المسموحة للعمل.

تطبق رقابة المصادقة بخلق مصفوفة رقابة وصول تكون جدولاً يحدد أية أجزاء من مستخدمي النظام يسمح لها بالوصول وأية تصرفات يمكنهم القيام بها. بعد ذلك عندما يحاول موظف الوصول إلى مصادر أنظمة معلومات معينة، يقوم النظام بعملية التوافقية التي تطابق اعتماد الصلاحية مقابل مصفوفة رقابة الوصول ويحدد فيما إن كان سيسمح للموظف بالوصول إلى ذلك المصدر ويقوم بالتصرف المطلوب. ومن المهم أن نقوم بالتحديث المستمر لمصفوفة رقابة الوصول لتعكس التغيرات في مهمات العمل من ترقيات وتنقلات وإلا قد يراكم الموظف مجموعة من الحقوق والمزايا غير المتوافقة مع الفصل المناسب للمهام[١١٣].

يمكن تطبيق المصادقة والتخويل ليس فقط على المستخدمين بل أيضاً على الأجهزة ،عن طريق استخدام الشهادات الرقمية التي توظف تقنيات تشفير معينة تخصص كل معرف مميز الى جهاز. ونستطيع القول هنا أن تطبيق رقابة المصادقة والتخويل لكل من المستخدمين والأجهزة هو مثال آخر عن كيفية زيادة الدفاع بالعمق للأمن.

---

[112] Romney, Marshall B.& Steinbart, Paul John, Accounting Information Systems, 9th Edition, USA: Prentice Hall, 200٦, p 238-240

[١١٣] مرجع سابق Romeny، ٢٠٠٩، p281

التدريب

يلعب الإنسان دوراً مهماً في أمن المعلومات. تعتمد كفاءة إجراءات الرقابة النوعية على مدى جودة فهم الموظفين ومتابعتهم سياسات أمن الشركة. وهكذا يكون التدريب رقابة وقائية مهمة وتنعكس أهميته في حقيقة أن ٣٤ من عمليات الرقابة ذات المستوى الأعلى في إطار COBIT تركز حصرياً على الحاجة لتدريب كل من المستخدمين ومتخصصي الأنظمة.

يكون التدريب مطلوب بشكل خاص لتثقيف الموظفيين بخصوص هجمات الاحتيال (الهندسة الإجتماعية) التي تستخدم الغش للحصول على وصول غير مسموح به لمصادر المعلومات. فمثلاً يجب تدريب الموظفين لعدم إفشاء كلمات السر أو أية معلومات بخصوص حساباتهم أو إعدادات محطات عملهم لأي شخص يتصل بهم هاتفياً، بالبريد الإلكتروني، أو رسائل فورية ويدعي أنه جزء من وظيفة أمن نظام إدارة معلومات المصرف[١١٤].

كما أن تدريب عناصر أمن المعلومات أيضاً مهم فالتطورات الجديدة في التقنية تخلق باستمرار تهديدات أمنية مستمرة وتجعل الحلول القديمة عديمة الجدوى، فمن المهم أن يدعم المصرف استمرارية تثقيف الأخصائيين لمتخصصي أمنهم .

ومن المهم مراقبة هذه المواقع وإيجاد المراسلات المتعلقة بالأنظمة التي تستخدمها منظمتك بحيث يمكن حمايتها من الهجمات. وكمثال على ذلك في سوريا، الهيئة الوطنية لخدمات الشبكة التي أصدرت العديد من التوصيات والثغرات التي تخص أمن المعلومات [١١٥] وخصوصاً "دليل الثغرات الأمنية في نظم تشغيل المخدّمات الخاصة بالمواقع الإلكترونية **على شبكة الإنترنت**"

أخيراً، يكون دعم الإدارة العليا للتدريب مهماً بالإضافة إلى تأمين التمويل للقيام بتدريب كهذا، فيجب على الإدارة إظهار أنها تدعم الموظفين الذين يتابعون سياسات الأمن المقررة.

رقابة الوصول المادي (الفيزيائي) :

تعتبر رقابة الوصول المادي هي طبقة أخرى من الرقابة الوقائية وهي ذات أهمية كبيرة ومطلقة لتحقيق أية درجة من أمن المعلومات ، يحتاج المهاجم المحترف دقائق قليلة من الوصول المباشر غير المراقب من أجل تجاوز رقابة أمن المعلومات الموجودة فمثلاً، يمكن للمهاجم ذو الوصول المادي المباشر غير المراقب أن يقوم بتركيب جهاز ولوج يلتقط ضربات المفاتيح ومن ثم كلمات

[114] Moscove, Stepher," E- Business and Controls" 2003 The CPA Journal,p 1-5

[١١٥] Website: www.nans.gov.sy

التحقق من المستخدمين. ويمكن أن يحصل المهاجم على الوصول غير المسموح به للوصول إلى النظام بالتظاهر أنه مستخدم شرعي.

كما يمكن لشخص ما ذو وصول مادي غير مراقب أن يقوم بإدخال أقراص "إقلاع" تؤمن وصولاً مباشراً إلى كل ملف على الكمبيوتر ومن ثم نسخ الملفات الحساسة إلى وسيط تخزين قابل للإزلة USB. وبالتبادل يمكن للمهاجم ذو الوصول المادي غير المراقب أن يقوم وببساطة بإزالة القرص الصلب، أو حتى سرقة كامل الكمبيوتر. وبمعرفة هذا المجال الواسع من التهديدات المحتملة المترافقة مع الوصول المادي غير الخاضع للإشراف، ولا يجب أن يكون مفاجئاً أن يركز مستوى آخر من أهداف الرقابة العليا ل COBIT بشكل خاص على الأمن الفيزيائي[١١٦].

تبدأ رقابة الوصول المادي مع نقاط الدخول إلى المبنى، حيث يجب أن تكون هناك نقطة دخول منتظمة واحدة تفتح خلال ساعات الدوام الرسمية بالمكتب. بالرغم من أن كودات الحريق تفرض مخارج طوارئ إضافية، ولكن هذه لا يجب أن تسمح بالدخول من الخارج ويجب وصلها إلى نظام إنذار الذي ينطلق أوتوماتيكياً عند فتح مخرج الحريق. وأيضاً يجب وضع موظف استقبال أو حرس أمني في المدخل الرئيسي للتحقق من هوية الموظفين والطلب من كل الزوار التوقيع ويتم مقابلتهم من قبل الموظف الذي يرافقهم إلى حيثما يريدون في المبنى.

وفي داخل المبنى، يجب تقييد الوصول المادي إلى الغرف التي تحتوي معدات الكمبيوتر، كما يجب إقفال الغرف بإحكام وتتم مراقبة كل (الدخول / الخروج) بنظام دارة تلفزيونية مغلقة. يجب أن تطلق عمليات الاقتحام المتعددة الفاشلة الإنذار، كما يجب أن يؤمن للغرف المحتوية على مخدمات تحتوي البيانات الحساسة أقفال اعتيادية ذات تقنية أقوى مثل لوحات المفاتيح الرقمية أو العديد من الأنظمة الأخرى مثل مسح قزحية العين، قارئات بصمات الأصابع، أو أجهزة التعرف الصوتية. [١١٧]

يجب أن يكون أمن الوصول المادي فعالاً، ويحتاج ذلك إلى اهتمام من قبل الإدارة العليا في تخطيط أمن الوصول المادي لضمان أن كل مصادر أنظمة المعلومات محمية بشكل ملائم وأن طبيعة وتركيب رقابة الوصول يعكس قيمة الأصول المحمية.

<u>الرقابة على الوصول عن بعد:</u>

تؤمن معظم المصارف للموظفين، العملاء، والمزودين بالوصول عن بعد لأنظمة معلوماتهم. يحصل هذا الوصول عادة عبر الانترنت ولكن ما تزال بعض المنظمات تحافظ على ملكية WAN أو تؤمن وصولاً عبر اتصال طلب هاتفي عبر مودم. كما تؤمن العديد من المنظمات وصولاً لاسلكياً إلى

---

[١١٦] مرجع سابق ، Romeny،٢٠٠٩، p284

[117] AICPA &CICA, Trust Services, Principles,Criteria and Illustrations,Copy Rights 2007 ,USA, P129-130

أنظمتهم. والاساليب المتنوعة التي يمكن استخدامها مباشر لتحقيق هدف رقابة COBIT لرقابة الوصول عن بعد لمصادر المعلومات هي التالية:الموجهات ، جدران الحماية، نظام منع الاختراق يقوم الموجه بإيصال نظام معلومات المصرف إلى الإنترنت ويكون وراءه هناك جدار حماية رئيسي. كما أن هناك مجموعة من القواعد تسمى الرقابة على الوصول من خلال فلترة الحزم تحدد أية حزم يسمح لها بالدخول وأيها يجب منعها وهناك أيضاً قواعد إضافية التي تحدد الأنواع الأخرى للحزم التي يجب إنكار دخولها،كما تحدد القاعدة الأخيرة أن أية حزمة لم يتم إسقاطها بسبب القواعد السابقة يجب تمريرها إلى جدار الحماية[١١٨].

وهناك أنظمة منع الاختراق Intrustion Prevention Systems (IPS) المصممة لتحديد وإسقاط الحزم العميقة التي تكون جزءاً من هجمة. تستخدم IPS العديد من التقنيات لتحديد الحزم غير المرغوبة ويشمل أحدها تعقب محتويات الحزمة مقابل مقابل قاعدة بيانات لأنماط (تواقيع) من أساليب المعروف الهجوم. ويشمل آخر تطوير مخطط للمرور "الاعتيادي" واستخدام التحليل الإحصائي لتحديد الحزم التي لا تناسب ذلك المخطط. والأكثر أهمية هو استخدام قواعد البيانات التي تحدد أنواع النقل لإسقاط الحزم التي لا تتوافق مع تلك المعايير والذي يميز هذا المبدأ هو أنه لا يوقف فقط الهجمات المعروفة التي توجد لها تواقيع بل أيضاً أية هجمات جديدة تنتهك المعايير.

ومع أن IPS هي إضافة مهمة لمجموعة منتجات الأمن ولكنها أيضاً لا تخلو من المشاكل وقد تكون عرضة لإنذارات زائفة التي تؤدي إلى رفض النقل المقبول ومع ذلك تتم الكثير من البحوث لتحسين ذكاء IPS ومن المحتمل أن تصبح جزءاً مهماً من أمن المصرف. فهي لن تحل محل جدران الحماية ولكنها تعتبر أداة مكملة وتؤمن طبقة أخرى للدفاع، هذا بالإضافة إلى أنظمة حديثة اخرى في منع الإختراق مثل Two-Factor Authentication الذي أثبت نجاحه تجربته من قبل كثير من البنوك[١١٩].

ومن ثم يجب تخصيص المستخدمين الذين يتمتعون بمقدرات إدارية على كمبيوتر معين بحسابين: أحدهما له مزايا إدارية والآخر له مزايا محدودة. وهنا يجب على المستخدمين المستخدمين لحساباتهم المحدودة أن يقوموا بالمهام اليومية التقليدية ويستخدموا حسابهم الآخر عند الحاجة للقيام بعمل ما، مثل تنصيب برنامج. ومن المهم أن نستخدم حساب المستخدم العادي المحدود

---

[١١٨] مرجع سابق ، Romeny، ٢٠٠٩، p285-288

[119] GORDON, WHITSON (3 SEPTEMBER 2012). "Two-Factor Authentication: The Big List Of Everywhere You Should Enable It Right Now". *LifeHacker* (Australia). http://www.lifehacker.com.au/2012/09/two-factor-authentication-the-big-list-of-everywhere-you-should-enable-it-right-now/. تاريخ الدخول 1 November 2012

عند تصفح الإنترنت أو قراءة البريد الإلكتروني فبهذه الطريقة إن زار المستخدم موقعاً خطراً أو فتح بريداً إلكترونياً يحتوي فيروساً سيحصل المهاجم على حقوق محدودة. كما يؤكد هدف رقابة COBIT على أهمية المراجعة الدورية للحسابات بمزاياها المرافقة لها [١٢٠].

التشفير:

هو الطبقة الأخيرة من الرقابة الوقائية. يؤمن التشفير البيانات الحساسة خلال تخزينها حاجزاً أخيراً يجب أن يتغلب عليه المقتحم الذي تمكن من وصول غير مسموح به لمصدر المعلومات. إن التشفير يعزز من إجراءات المصادقة ويلعب دوراً أساسيا في ضمان والتحقق من شرعية صفقات الأعمال الإلكترونية. ومن ثم من المهم على المحاسبين، المراجعين، وأخصائيين النظم فهم التشفير.

التشفير هو عملية تحويل النص العادي، المسمى نص صريح Plaintext إلى نص غير مقروء، يسمى نص مشفر Ciphertext. "**فك التشفير**" Decryption يعكس هذه العملية محولاً النص المشفر إلى نص صريح. يتم استخدام كل من المفتاح والخوارزمية لتحويل نص عادي إلى نص مشفر ولفك التشفير نص ليعاد إلى نص صريح. تمثل الكمبيوترات النص الصريح والنص المشفر كسلسلة من ارقام الثنائية. يكون المفتاح هو سلسلة من الأرقام الثنائية ذات طول ثابت [١٢١].

يحدد هدف رقابة COBIT أهداف الرقابة المهمة المتعلقة بإدارة مفاتيح كودات التشفير. وفي الواقع تكون هذه الناحية الأضعف لنظام التشفير. بغض النظر عن قوة خوارزمية التشفير، إن تم كشف المفاتيح، يمكن اختراق التشفير بسهولة ومن ثم يجب إحكام الوصول إلى مفاتيح التشفير. ويجب أن يكون للمنظمات طريقة لفك تشفير البيانات في حالة مغادرة الموظف الذي يقوم بتشفيرها. الطريقة الأفضل للقيام بهذا هي استخدام برمجيات التشفير التي تخلق مفتاح رئيسي مدمج يمكن استخدامه لفك تشفير أي شيء تم تشفيره من قبل ذلك البرنامج. البديل الآخر الممتاز هو عملية تسمى "إيداع المفتاح" تشمل عمل نسخ لكل مفاتيح التشفير المستخدمة من قبل الموظفين وتخزين هذه النسخ

---

[120] Angela Moscaritolo (2011-07-12). "Zeus for Android steals one-time banking passwords - SC Magazine". Scmagazineus.com. http://www.scmagazineus.com/zeus-for-android-steals-one-time-banking-passwords/article/207286/. تاريخ الدخول 2012-11-07.

[121] Ross Anderson, Eli Biham, Lars Knudsen. Serpent: A Proposal for the Advanced Encryption Standard,2007,p33

بمكان آمن. يكون إيداع الملف أقل تفضيلاً من استخدام المفاتيح الرئيسية المدمجة لأن على المصرف أن يحمي الآن كل من النسخ الأصلية والمقلدة من مفاتيح التشفير [١٢٢]، والعامل الثالث المؤثر على قوة التشفير يهتم بطبيعة الخوارزمية. يكون اختراق خوارزمية قوية صعباً إن لم يكن مستحيلاً، باستخدام تقنيات قوة التخمين المجردة. والسرية ليست مهمة للقوة، الاجراءات المستخدمة من قبل الخوارزميات المقبولة وواسعة الانتشار متوافرة للعامة. لا تكون قوتها نتيجة أن إجراءاتها سرية، بل لحقيقة أنه تم اختيارها بقوة وتبين أنها تقاوم هجمات التخمين [١٢٣].

٢-٤-٢ الرقابة الكشفية

هي ضرورية لاكتشاف المشاكل حالما تنشأ وتقوم على الفحص المضاعف للحسابات وتحضير التسويات المصرفية والمطابقات الحسابية والمراجعة الإدارية والمالية. وتعالج المشاكل المكتشفة ب الرقابة التصحيحية،لا تكون إجراءات الرقابة الوقائية فعالة ١٠٠٪ في إيقاف كل الهجمات ومن ثم يؤكد هدف رقابة COBIT على أن المصرف يحتاج أيضاً لتطبيق إجراءات الرقابة المصممة لكشف الاقتحام بالوقت المحدد. تعزز إجراءات الرقابة الكشفية الأمن بمراقبة فعالية الرقابة الوقائية وكشف الخروقات حيث تم الاحتيال على الرقابة الوقائية بنجاح.

هناك أربعة أنواع للرقابة الكشفية[١٢٤]:

<u>تحليل السجل</u>

تأتي معظم الأنظمة بإمكانيات شاملة لدخول من يصل إلى النظام وما يحدد التصرفات التي قام بها كل مستخدم. تشكل هذه السجلات أثر مراجعة الوصول للنظام. ومثل أي أثر مراجعة، تكون السجلات ذات قيمة فقط إن تمت معاينتها بشكل دوري. فتحليل السجل هو عملية معاينة السجلات لمراقبة الأمن.

وتحليل السجل بحاجة دوماً إلى أن يتم بشكل منظم من أجل كشف المشاكل بالوقت المناسب. وهذا ليس سهلاً لأن حجم السجلات يتزايد بسرعة ومن ثم يستخدم مدراء الأنظمة عدداً من الأدوات البرمجية للتخلص من المدخلات الروتينية للسجل بحيث يمكن تركيز الانتباه بفعالية على السلوك غير السوي الذي قد يمثل علامات الاقتحام. وأيضاً، تقوم معظم المنظمات بتكميل تحليل السجل بالأدوات البرمجية، المسماة أنظمة كشف الاقتحام لأتمتة عمليات المراقبة.

---

[١٢٢] مرجع سابق Romeny ٢٠٠٩, p293,

[123] Forouzan, Behrouz A. Cryptography and Network Security . s.l. : McGraw-Hill, 2007. P127.

[١٢٤] مرجع سابق ،Romeny،٢٠٠٩،p299-303

أنظمة كشف الاختراق

نقطة الضعف الرئيسية لتحليل السجل هي أنها تحتاج لجهد مكثف وعرضة للخطأ البشري. تمثل أنظمة كشف الإقتحام محاولة لأتمتة جزء من وظيفة المراقبة. تخلق أنظمة كشف الاختراق (IDS) سجلات لحركة الشبكة المسموح لها بالمرور عبر جدار الحماية ومن ثم تحليل هذه السجلات من أجل علامات عمليات الاقتحام التي تمت أو غير الناجحة[١٢٥].

الأسلوب الأكثر شيوعاً للتحليل المستخدم من قبل IDS هو مقارنة سجلاتها مع قاعدة بيانات محتوية على أنماط الحركة المترافقة مع الهجمات المعروفة، كما تقارن مضادات الفيروسات الكودات في قواعد البيانات للفيروسات المعروفة. التقنية البديلة المستخدمة من قبل معظم IDS المتقدمة تبني أولاً نموذجاً يمثل حركة "شبكة طبيعية" ومن ثم يستخدم التقنيات الاحصائية المتنوعة لتحديد السلوك غير الاعتيادي أو غير السوي.

تتوضع حساسات IDS في أماكن متعددة والموقع الأشهر هو داخل جدار الحماية الرئيسي كما تكون حساسات IDS متوضعة فقط خارج جدار الحماية الرئيسي. يؤمن هذا وسيلة لمراقبة عدد من عمليات الاقتحام التي تمت بنجاح وتم إيقافها من قبل جدار الحماية ويمكن أن تؤمن إشارات إنذار مبكرة بان المصرف مستهدفة. يمكن تحديد IDS أيضاً على المضيف الفردي لتأمين إنذارات لمحاولات تهديد ذلك النظام.

التقارير الإدارية

التقارير الإدارية هي رقابة كشفية أخرى. يؤمن إطار COBIT للإدارة إرشادات تحدد العوامل المهمة المترافقة مع كل هدف وتقترح عوامل مترافقة مع كل هدف وتقترح مؤشرات أداء رئيسية يمكن للإدارة أن تستخدمها لمراقبة فعالية الرقابة وتقييمها.

وقد ذكرت COBIT حاجة الإدارة لمراقبة وتقييم أداء النظام والرقابة. ومع ذلك، مع أن المراجعة النظامية لتقارير الأداء الدورية، بما فيها تحليل الاتجاهات في مؤشرات الأداء الرئيسية، يمكن أن تساعد لضمان أن الرقابة الأمنية ملائمة. تدل المسوحات أن العديد من المنظمات تفشل في مراقبة الأمن بشكل منتظم. يعتبر هذا مجالاً حيث يمكن للمحاسبين أن يساعدوا بالمشاركة في تصميم بطاقات تسجيل كفاءة الأمن وتشجيع الإدارة على المراجعة المنتظمة لهذه التقارير.

---

[125] Whitman Michael E. (2003), "Enemy at the Gate: Threats to Information Security", Communication of the ACM, (Vol. 46, Iss. 8), pp. 91-95.

اختبار الأمن: كما اتضح سابقاً يؤكد هدف الرقابة في COBIT على الحاجة للاختبار الدوري لفعالية إجراءات الأمن الموجودة. وإحدى الطرق للقيام بهذا هي القيام بعمليات مسح نقاط الضعف، التي تستخدم أدوات مؤتمتة مصممة لتحديد فيما إن كان نظام معين يمتلك أية نقاط ضعف معروفة. وأيضاً، يوجد عدد من مواقع الإنترنت لأمن المعلومات مثل مركز أمن المعلومات (www.cisecurity.org) الذي يؤمننقاط تحديد لأفضل عمليات الأمن وأدواتها التي يمكن استخدامها لقياس مدى توافق النظام مع هذه العلامات.

٢-٤-٣ الرقابة التصحيحية

تعالج مشاكل الرقابة التي تم اكتشافها وهي تشمل جميع الإجراءات المتخذة لتحديد سبب المشكلة، تصحيح الأخطاء أو الصعوبات، تعديل الأنظمة بحيث يتم تقليل المشاكل المستقبلية أو إزالتها ومن أمثلتها النسخ الدعم للملفات الرئيسية والالتزام باجراءات تصحيح أخطاء إدخال البيانات بالإضافة إلى تلك التي تعيد تقديم الصفقات للمعالجة اللاحقة[١٢٦].

لا يكون كشف محاولات الاختراق الناجح كافياً. فقد حدد إطار الخدمات الإئتمانية AICPA الحاجة لإجراءات للتفاعل مع الخروقات وللقيام بالتصرفات التصحيحية بالوقت المحدد. تعتمد العديد من إجراءات الرقابة التصحيحية على الخبرة البشرية. ومن ثم تعتمد فعاليتها إلى حد كبير على التخطيط والتحضير الملائمين، ولهذا يحدد هدف رقابة COBIT الحاجة لتحديد ونقل خصائص الخروقات الأمنية لتسهيل تصنيفها الملائم ومعالجتها. وأيضاً أهداف الرقابة المحددة من أجل الإدارة الفعالة للخروقات والمشاكل[١٢٧].

وفي النهاية وبعد عرض للأنواع الثلاثة للرقابة يمكن القول أن الرقابة الوقائية هي الأهم بالنسبة لأية منظمة. ثم تأتي الأنواع الأخرى لتكمل عملها وخاصة في القطاع المصرفي ولتستطيع تقييم قدرة أي نظم على حماية بياناتها ومعلوماتها يجب أن نختبر قدرتها على تحقيق الرقابة الوقائية أولا ثم تأتي بقية الانواع بالاضافة إلى التحقق من قدرة المصارف على تحقيق أهداف الرقابة **COBIT** .

غير أن السؤال المهم في هذا المجال هو إلى أي مدى توفر النظم المحاسبية المصرفية الضوابط الرقابية للأنواع الثلاثة للرقابة؟.

---

[١٢٦] **الحسبان، عطا الله،**" مدى مواكبة المدققين الداخليين لمتطلبات تكنولوجيا معلومات أنظمة الرقابة الداخلية في شركات المساهمة العامة الأردنية،"الاردن،٢٠٠٧،المنارة ، المجلد ١٤، ص٢٣٨

[١٢٧] مرجع سابق ،Romeny، ٢٠٠٩،p304

٢-٥ متطلبات الرقابة الداخلية على أنشطة المصارف الإلكترونية

٢-٥-١_متطلبات الحماية والأمن:

أقرت لجنة بازل مجموعة من المتطلبات الخاصة بالرقابة على أمان العمليات المصرفية الالكترونية[١٢٨]:

١- على المصارف اتخاذ الإجراءات المناسبة للتحقق من هوية العملاء الذين تقدم لهم الخدمات عبر الانترنت وطبيعة تخويلهم.

٢- يجب على المصارف استخدام طرق التحقق من المعاملات وأن تتولى ترويج "عدم النقض" (Non- Repudiation) وأن تحدد المساءلة عن المعاملات المصرفية الالكترونية.

٣- يجب أن تتأكد المصارف من توافر الضوابط المناسبة للتخويل ومن صلاحيات الدخول للنظم المصرفية الالكترونية وإلى قواعد البيانات والتطبيقات[١٢٩].

٤- يجب على المصارف أن تضمن توافر الإجراءات المناسبة لحماية مصداقية البيانات الخاصة بالعمليات المصرفية الالكترونية السجلات والمعلومات.

٥- لا بد من أن تضمن المصارف وجود مسارات تدقيقية واضحة لكل المعاملات المصرفية الالكترونية.

٦- يجب على المصارف اتخاذ الإجراءات المناسبة لحماية كتمان المعلومات الخاصة بالعمليات الالكترونية كما يجب أن تكون هذه الإجراءات متوافقة مع درجة حساسية المعلومات المطلوب نقلها و/أو خزنها في قواعد البيانات[١٣٠].

٢-٥-٢ المتطلبات التقنية والتكنولوجية:

وهي مجموعة البرامج والأجهزة والمعدات ومواقع الانترنت الخاصة بالأعمال الالكترونية المصرفية. حيث أحدثت التطورات التكنولوجية مزيدا من الحاجة إلى الاستفادة من هذه التطورات المتسارعة

---

[١٢٨] .العنزي سامية "مدى التزام البنوك التجارية الأردنية بمتطلبات الرقابة الداخلية على أنشطة التجارة الالكترونية من وجهة نظر المدقق الخارجي، ٢٠٠٨، مجلة العلوم الانسانية ،جامعة آل البيت- الاردن ،ص٤-٦

[129]Bank for international Settlement ,Basel Committee on Bank Supervision" ,Risk management principles for electronic banking", pp12-18

[130] Information System Audit and Control Association, "IS Auditing guideline Business-to-consumer (B to C) E-commerce Reviews", 1 May 2003, P2. In web www.isaca.org/glossary.htm

لازدياد حدة المنافسة بين المصارف التي تواكب هذه التطورات لتحقيق ميزة تنافسية وتوظيف هذه التكنولوجيا والتقدم التقني في صالح خدمة العملاء بالتالي يجب دراسة المتطلبات التقنية والتكنولوجية من حيث مدى توفر البنية التحتية الملائمة لتطبيق أنشطة التجارة الالكترونية في البنوك.

كما انه يجب تطبيق العديد من الإجراءات الرقابية على التكنولوجيا المستخدمة في العمل من اجل ضمان استمرارية عملها على الشكل الأمثل لتقليل احتمالية فشلها أو قصورها وذلك بإجراء عمليات الصيانة الوقائية المستمرة[١٣١].

٢-٥-٣ المتطلبات التشريعية والقانونية

يتطلب الولوج الى عالم التجارة الالكترونية مواكبة متواصلة وناجحة مع متغيرات العصر الالكتروني، لاسيما في الأعمال المالية والمصرفية، خاصة مع تطور احتياجات ومتطلبات الزبائن واتجاهها للاعتماد على الركائز التكنولوجية عموما والالكترونية بشكل خاص. ويضع ذلك الادارات المصرفية امام تحديات قانونية على المستوى الدولي أمام العمل المصرفي عبر الانترنت مما يتطلب إيجاد بنية قانونية مناسبة تعمل على حماية حقوق كافة الأطراف وتؤكد الهوية القانونية لهذه الأطراف وتعمل على إيجاد القوانين التي تشرع وتنظم وتحكم استخدام وسائل الإبلاغ وتبادل البيانات الالكتروني كبديل لأساليب الإبلاغ والتبادل المتركزة على أساس ورقي والقوانين الخاصة بحماية العميل والسرية.وقد أقرت لجنة بازل مجموعة من المتطلبات لإدارة المخاطر القانونية ومخاطر السمعة الخاصة بالعمليات المصرفية الالكترونية منها:

١- يجب على المصارف أن تضمن تقديم المعلومات المناسبة في مواقعها على الانترنت للسماح للعملاء المحتملين بالتوصل إلى استنتاجات مدروسة حول هوية المصرف ومركزه القانوني وذلك قبل الدخول بمعاملات تنفذ من خلال العمليات المصرفية الالكترونية.

٢- يجب على المصارف اتخاذ الإجراءات المناسبة للتأكد من الوفاء بمتطلبات سرية العميل بحسب الأقطار التي يقدم فيها المصرف منتجاته وخدماته المستندة إلى العمليات المصرفية الالكترونية.

٣- يجب أن تكون للمصارف القدرة الفاعلة واستمرارية النشاط وعمليات التخطيط للطوارئ للمساعدة على ضمان توافر النظم والخدمات من خلال العمليات الالكترونية.

---

[١٣١] احمد عبد الله العموري، اثر التجارة الالكترونية على المراجعة – دراسة ميدانية في اليمن، رسالة ماجستير غير منشورة، جامعة دمشق – سوريا، ٢٠٠٦م، ص١٠٠

٤- يجب على المصارف إعداد خطط مناسبة تتضمن الاستجابة للحوادث والحد منها (السيطرة عليها) والحد من المشاكل الناشئة عن الحوادث غير المتوقعة بما في ذلك أنواع الهجوم الداخلي والخارجي التي قد تعيق تزويد النظم والخدمات المستندة للعمليات المصرفية الالكترونية[١٣٢].

٢-٥-٤ المتطلبات الإدارية:

وتتمثل في التخطيط الجيد والتنظيم الملائم، ولاسيما أن استخدام التجارة الالكترونية في الأعمال يلغي كثيرا من الوظائف التقليدية للفصل بين الواجبات، وتتضمن المتطلبات الإدارية توصيف الهيكل التنظيمي وتحديد السلطات والمسؤوليات وتحديد اجراءات العمل والفصل بين الوظائف المتعارضة في ادارة نظم المعلومات وصياغة آلية إشراف مجلس الإدارة والإدارة العليا على العمليات المصرفية الالكترونية[١٣٣].

إن المتطلبات المذكورة فيما ورد تمثل مرجعية أساسية لمعرفة مدى تحقيق النظم المحاسبية المصرفية لهذه المتطلبات.

---

[132] Bank for international Settlement ,Basel Committee on Bank Supervision" ,Risk management principles for electronic banking",٢٠٠٧ , p 18-21

الفصل الثالث:
حماية البيانات والمعلومات في المصارف

المبحث الأول: مفهوم أمن المعلومات ومقوماته

المبحث الثاني :وسائل ضمان الأمن التقنية

١-المبحث الأول: مفهوم أمن المعلومات ومقوماته

١-١ مفهوم أمن المعلومات وأهدافه:

تشكل المعلومات لمنظمات الأعمال البيئة التحتية التي تمكنها من أداء مهامها، إذ إن نوع المعلومات وكميتها وطريقة عرضها تعتبر الأساس في نجاح عملية صنع القرارات داخل المنظمات المعاصرة، وعليه فإن للمعلومات قيمة عالية تستوجب وضع الضوابط اللازمة لاستخدامها وتدأولها ووضع السبل الكفيلة بحيازتها، لذا فإن المشكلة التي يجب أخذها بالحسبان هي توفير الحماية اللازمة للمعلومات وإبعادها عن الاستخدام غير المشروع لها.

ويقصد بأمن المعلومات ذلك العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها. أما من زاوية تقنية فأمن المعلومات يعبر عن الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية. كما يشير أمن المعلومات كذلك إلى كل موارد معلومات المنظمة من السرقة من قبل أطراف غير مخول لها استخدام النظام.

من الناحية القانونية فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة. وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها[١٣٤].

في ظل هذه الجرائم والمهددات كان لا بد من بروز أمن المعلومات كأمر ملح لتحقيق **الأهداف الأمنية الأساسية** المتمثلة في[١٣٥]:

- **سرية البيانات**

تعني سرية وخصوصية البيانات والمعلومات لدى المنظمة. أن إدارة أمن النظم والمعلومات معنية بتوفير هذه الحماية والخصوصية للنظم والأجهزة والمعلومات وذلك بتطوير السياسات وتطبيق الإطار العام لأمن المعلومات.

---

[١٣٤] زيدان، محمد, وحمو، محمد "متطلبات أمن المعلومات المصرفية في بيئة الإنترنت، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية ", الرياض ٢٠١٠ ص٣

[135] Perrin, Chad. "The CIA Triad". http://www.techrepublic.com/blog/security/the-cia-triad/488. Retrieved 31 May 2012

تكاملية البيانات:

تعني سلامة المعلومات وعدم تعرضها للتغيير والتبديل إلا من خلال القنوات الرسمية وبطريقة شرعية من خلال صلاحيات ممنوحة لهذا الغرض، ولضمان ذلك لا بد من توفر الوسائل والبرامج والإجراءات الرقابية.

توفر الخدمة:

تعني جاهزية وتوفر الخدمة متمثلة في استطاعة مستخدمي النظم والبرامج في استخدام النظام والحصول على المعلومات عند الحاجة والطلب، ولا يتأتى ذلك إلا بأخذ التحوطات اللازمة لمنع ما يمكن أن يؤدي إلى الفشل سواء كان الفشل ناتجًا عن المهددات الداخلية أم الخارجية أم نتيجة لخلل في الأنظمة والبرامج.

بالإضافة إلى الأهداف الأساسية أعلاه هنالك من يرى ضروة أن هذه الأهداف لا تكتمل إلا بتضمين النقاط التالية ضمن الأهداف وهي:

١-الاستخدام الأمثل والشرعي

٢- المسؤولية

٣- عدم النكران

٤-المراجعة والتدقيق

بالنتيجة، يلاحظ أن تحقيق الأساس الأول المرتبط بسرية المعلومات يتطلب تأمين المعلومات بشكل يمكن فقط الأشخاص المصرح لهم الوصول إليها دون غيرهم (أصحاب الصلاحية أو المخول لهم). أما الأساس الثاني المتمثل في سرية المعلومة، فيسعى إلى ضمان سلامة مصادر المعلومات، بحيث لا يمكن تغييرها أو تحديثها إلا من قبل الأشخاص المصرح لهم فقط. فيما الأساس الثالث لضمان أمن المعلومات فيتمثل في إمكانية وسهولة توفير المعلومات وقت الحاجة إليها. بمكن القول إن المصارف السورية تسعى جاهدة لتحقيق هذه الأهداف بالرغم من الصعوبات التي تقف في طريقها والتي من أهمها تعاون طاقم العمل الخاص بقسم IT مع قسم الرقابة الداخلية وبقية الأقسام في المصرف.

١-٢ إختراقات أمن المعلومات

١-٢-١الخطوات الأساسية المستخدمة من قبل المخترقين لأنظمة معلومات المصرف

الاستكشاف:

لا يقومون لصوص المصارف باقتحام المصرف ومحاولة سرقته وإنما يدرسون المخطط الفيزيائي للهدف للتعرف لأجهزة الرقابة التي في مكانها (أجهزة الإنذار، عدد الحرس، وضع الكاميرات.....الخ) يبدأ مهاجمو الكمبيوترات بشكل مشابه بتجميع المعلومات بخصوص هدفهم، فيمكنهم الحصول على الكثير من المعلومات القيمة بتفحص البيانات المالية للمنظمة، ملفات SEC، موقع الانترنت، ويكون الهدف الأولي لهذا الاستكشاف الأولي هو معرفة أكبر قدر ممكن عن الهدف وتحديد نقاط الضعف المحتملة[١٣٦].

الخداع:

غالباً ما يحاولون المهاجمون استخدام المعلومات التي تم الحصول عليها خلال اكتشافهم الأولي وذلك لخداع موظف غير منتبه لمنحهم الدخول. ويمكن الخداع بعدة طرق منها أن ينتحل المهاجم صفة مدير تنفيذي لا يمكنه الوصول من بعيد إلى ملفات مهمة، فيتصل المهاجم بمساعد إداري معين حديثاً ويطلب منه المساعدة في الحصول على الملفات الهامة.

والخديعة الأخرى للمهاجم هي التظاهر بأنه عامل مؤقت بدون دليل لا يمكنه الوصول إلى النظام ويطلب مساعدة المكتب. كما يمكن لهذه الهجمات أن تحصل عبر البريد الإلكتروني، الهجمة المعروفة باسم "صيد السمك بالحربة" تشمل إرسال إيميلات تزعم أنها من شخص آخر في المصرف يعرفه الضحية، أو شخص يجب أن يعرفه. يطلب الإيميل من الضحية النقر على رابط متضمن فيروس تروجان يسمح للمهاجم بالوصول للنظام وهناك تكتيك آخر للإحتيال هو ترك USB في مرآب المصرف المستهدفة، والموظف الذي لا يشك بشيء قد يقوم بوصله إلى كمبيوتره ليقوم بتحميل فيروس التروجان الذي يسمح للمهاجم بالوصول للنظام.

مسح وتخطيط الهدف: إن لم يتمكن المهاجم من الاختراق الناجح للنظام المستهدف عبر الخداع، فتكون الخطوة التالية هي القيام باستكشاف أكثر تفصيلية لتحديد النقاط المحتملة للدخول من بعيد ويكون الهدف هو تحديد الكمبيوترات التي يمكن الوصول إليها من بُعد وأنواع البرمجيات التي تشغلها، ومن ثم استخدام هذه الأدوات نفسها للقيام بمسح النوافذ لكل هدف محتمل، وإرسال سلسلة

[١٣٦] الهادي محمد محمد، مقالة بعنوان توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية، ٢٠٠٦، ص١٥-١٩

من الرسائل التي تكشف البرامج المحددة التي تعمل على ذلك الجهاز، بما في ذلك المعلومات بخصوص نظام تشغيله.

البحث: حالما يحدد المهاجم الأهداف المحددة ويعرف ما هي نسخ البرامج العاملة عليها، تكون الخطوة التالية هي القيام ببحث لإيجاد نقاط الضعف المعروفة لهذه البرامج والاستفادة من نقاط الضعف هذه.

القيام بالهجوم: اي الحصول على الوصول غير المرخص به للنظام.

إخفاء الآثار: بعد اختراق نظام المعلومات، سيحاول معظم المهاجمين إخفاء آثارهم لخلق "بوابات خلفية "يمكن أن تستخدم للحصول على الوصول في حالة اكتشاف الهجمة الأولية وتكون الرقابة مهمة لإيقاف أسلوب الدخول.

وموخراً أصبح هناك وسائل اكثر تعقيداً مثل Main in the Browser attack (MitB) [١٣٧] حيث يحصل الهجوم ما بين المستخدم والموقع الإلكتروني ويتم تغيير التفاصيل التي يجري إدخالها ، كما أن هناك بعض الفيروسات من (MitB)تغير تفاصيل الدفع والمبالغ وتغير الموازين على الشاشة لإخفاء هذه الأنشطة وهذه الفيروسات تكون مركزة ومحددة وهذه التهديدات المتقدمة تركز تحديدا ضد البنوك ويتم إصدار تحديث جديد لهذه البرمجيات فالمؤسسات الأمنية تأخذ عدة أسابيع لمعرفة كيف تكتشف ذلك .

وذكر Mark Bowerman أن خسائر الاحتيال المصرفي عبر الإنترنت قد بلغ ١٦,٩£ مليون في الأشهر الستة الأولى من عام ٢٠١١ في المملكة المتحدة ، كما أنه تم اختراق الموقع الرسمي للبورصة القطرية في الشهر ١٢ من عام ٢٠١١ من قبل هاكرز تطلق على نفسها اسم "قوات ارد المغربية"وهو ما شل جميع التعاملات التي كانت للبورصة مع زبائنها في أوروبا وأمريكا وآسيا ، حيث تم توقيف هذه التعاملات المتاحة من خلال الموقع الرسمي للبورصة بالكامل[١٣٨] ,وتحدثت وكالة رويترز عن عملية القرصنة التي تعرضت لها أنظمة الكمبيوتر بشبكة الشركة السعودية للنفط "آرامكو"في ٢٧-٨-٢٠١٢ وقالت إن الإختراق الذي تعرضت له الشركة عن طريق فيروس يطلق عليه "شامون" وتعد هذه الهجمة من أكبر الهجمات التي تعرضت لها شركة ما ، وقد كلفها هذا الاختراق استبدال نحو ٣٠ ألف جهاز حاسب ، وأوضحت التحقيقات أن موظفيين اثنين لهما صلاحيات في الدخول على الأنظمة يشتبه في أنهما ساعدا في عملية الإختراق[١٣٩] .

---

[137] Spencer, Kelly, Hackers outwit online banking identity security systems ,BBC News Technology , 10 February 2012 ,p2

[138] http://hespress.com/permalink/43431.html تاريخ الدخول ١١-٨-٢٠١١

[139] www.bbc.co.uk/arabic/ تاريخ الدخول ١١-٦-٢٠١١

وبناء على ذلك قرر العديد من شركات البتروكيماويات والمصارف في السعودية منع استخدام أي وصلات الفلاش أو USB بالإضافة الى الأقراص والسيدي.

كما تعرضت أيضاً شركة "رأس الغاز القطرية لهجوم مماثل قبل اسبوع من هجوم آرامكو ولم تفصح عن حجم الأضرار التي تعرضت له أو الفيروس المتسبب بذلك [١٤٠].

بعد أن تم توضيح كيفية مهاجمة المخترقين لنظام معلومات أكبر الشركات والمصرف، ترى الباحثة أنه يجب تخفيف المخاطرة حتى لا تكون هذه الهجمات ناجحة، ويأتي تخفيف المخاطرة من خلال التعمق بالأنواع الرئيسية للرقابة الوقائية، والكشفية، والتصحيحية والتي يمكن استخدامها لتأمين المعلومات بشكل آمن غير الدفاع بالعمق.

١-٢-٢ نماذج الجرائم والاعتداءات بالبنوك العربية

- سرقات مالية تمت في دبي عبر الإنترنت من حسابات لعملاء في ١٣ بنكا محليا وعالميا، قام بارتكابها مهندس حاسوب استطاع الدخول إلى شبكات البنوك الإلكترونية بطريقة اعتيادية وتمكن من تحويل بعض المبالغ المالية عن طريق الإنترنت. توصل الخبراء إلى أن الجاني قام بعمليات الاختلاس الإلكترونية من حسابات عملاء وتحويلها إلى حسابات وهمية كان قد أعدها مسبقا عن طريق أنظمة فتح الحسابات الإلكترونية. استطاع خبراء جرائم الحاسوب تحديد الأسلوب الإجرامي الذي قام به المتهم من اختراق زرع برامج خاصة واختراق حسابات بنكية لأشخاص من دون علمهم وتحويل مبالغ مالية منهاوتبين أيضا أن الجاني قام بشراء بعض المواد من المواقع التجارية عن طريق بطاقات الائتمان لبعض الأشخاص من دون علمهم، إضافة إلى قيامه بفتح مواقع على الإنترنت أحدهم لإيجاد فرص العمل وآخر لاستدراج عارضات الأزياء لجمع بعض البيانات عن الأشخاص واستخدامها في عمليات السرقة الإلكترونية تمكن الجاني من الوصول إلى أرقام حسابات العملاء والأرقام السرية بطريقة عشوائية ومن ثم قام بعمليات التحويل لحسابات ومشتريات خارجية[١٤١] .
- تمكن أحد القراصنة من تصميم موقع لأحد البنوك السعودية وإرسال رسائل باللغتين العربية والإنجليزية إلى عملاء البنك يحثهم فيها على أهمية تحديث البيانات ليكون التعامل عبر الإنترنت أكثر أمنا وسرعة، واستطاع من وضع صور وبيانات تطابق الموقع الأصلي للبنك

[140] www.alwatan .com.sa/economy/news تاريخ الدخول ١١-٨-٢٠١٢

[141] http://aljareema.com/newss/wmview.php?ArtID=20 تاريخ الدخول ٤-٤-٢٠١٠

تمهيدا لنقل البيانات المدخلة من قبل العملاء إلى موقعه إلكترونياً مما يتيح له إمكانية التلاعب في الأرصدة أو إجراء عمليات تحويل وهمية،ولم يعرف ما إذا كان القرصان قد استطاع الأضرار بأرصدة العملاء أم تم تداركه قبل ذلك لاعتذار البنك عن التصريح عن ذلك.

هذه العملية تصنف ضمن جرائم المعلومات التقنية الدولية، ولم يكن لبرنامج الحماية الذي يستخدمه البنك، أية علاقة بعملية التزوير الحأصلة، كونها عملية تضليل مشابهة للموقع وليس اختراقا لبرنامج الحماية.

كما يشار إلى أن المؤسسات المالية السعودية عرضة دائما إلى الاختراقات حيث تمثل النسبة الأكبر بين تلك العمليات، حيث تتجاوز الـ ٨١ % بمعدل نحو ٣ آلاف موقع شهريا[١٤٢]..

- في منطقة الحدود الشمالية بالمملكة العربية السعودية تم ضبط شبكة مكونة من اربعة أشخاص سعوديين يقومون باختلاس أموال المواطنين عن طريق شبكة الإنترنت الإلكترونية من البنوك المحلية بطريقة القرصنة حيث يقوم أحدهم باختراق الحسابات البنكية بطريقة ماهرة ويقوم بتحويل مبالغ مالية إلى حسابات أشخاص آخرين تربطه صلة بهم وبعد رصد أمني دقيق لهذه القضية، تمت متابعة أحد أفراد المجموعة بطريقة سرية، ورصد كامل لتحركاته، حتى تم القبض عليه متلبسا بعد أن أجرى أول عملية تحويل مبلغ مالي من حساب شخص إلى حساب شخص آخر تربطه به صلة.

وقد لوحظ أن حجم المبالغ المالية التي سحبت من أرصدة العملاء في البنوك المحلية السعودية بلغ (٣٥٠٠٠٠) ألف ريال مثل هذه الاختلاسات لا تحصل إلا بسبب ضعف البوابة الإلكترونية للبنوك التي تحافظ دائما على الأرباح ولا تحافظ على أموال العملاء.[١٤٣]

- ومن السرقات الإلكترونية في السعودية أيضاً تم تحويل مبلغ (٨٤٤٦٥) ريالاً من حساب أحدهم إلى حساب عميل آخر في نفس البنك دون علمه وقد أبلغه صاحب الحساب المحول له المبلغ بأنه صاحب محل لأجهزة الهاتف الجوال بالرياض، وكان قد إتفق مع شخص على شراء كمية كبيرة من الأجهزة، على أن يسدد المبلغ بتحويل بنكي وهو ما تم بالفعل خلال نصف ساعة.[١٤٤]

---

142 http://web.1asphost.com/attasaa/News...ject.asp?NO=80 تاريخ الدخول ١٠-٦-٢٠١١

143 http://www.alwatan.com.sa/daily/2006-07-03/local/local10.htm تاريخ الدخول ٤-٤-٢٠١١

144- http://212.119.67.87/okazarchive/Data/2006/1/24/Art_310706.XML تاريخ الدخول ٤-٤-٢٠١١

- حدثت ٣ حالات اختراق في أشهر البنوك المصرية وبنك امريكي فقد تمكن المخترقون خلال أيام قليلة من سحب حوالي مليون جنيه مصري من حسابات خاصة في البنوك الأمريكية لم يزر أصحابها مصر ولا مرة واحدة. وقد تم تصنيف المخترق في عالم الجريمة الإلكترونية باعتباره الخامس عالميا بين أقرانه من قراصنة الحاسوب والإنترنت المعروفين عالميا باسم "القراصنة"

تبدأ الحكاية عندما تقدم المسؤول عن مراقبة مخاطر بطاقات الائتمان في البنك الأهلي ببلاغ حول اكتشافه قيام شخص ما باستخدام بطاقة ائتمانية صادرة من بنك "ميريل لنش" الأمريكي بطريقة تتنافى مع السلوك المالي المعتاد لمستخدمي البطاقات، حيث تم استخدامها في إجراء ثماني عمليات جارية متتالية في فترة زمنية تقارب الدقيقتين بمبلغ يتجاوز سبعة آلاف جنيه لدى أحد المحال التجارية الكبرى بالقاهرة، فقام المراقب بالاتصال بمدير المحل الذي أخبره ان مستخدم البطاقة شخص مصري الجنسية وأنه سيحضر بعد عدة أيام لاستلام باقي مشترياته.

قام المراقب بالاتصال بالمسؤولين في البنك الأمريكي من أجل تحصيل المبلغ الذي قام المستخدم المجهول للبطاقة بسحبه. وكانت مفاجأة عندما أكد مسؤولو البنك أن صاحب تلك البطاقة الحقيقي أمريكي الجنسية ولم يسبق له الحضور إلى مصر من قبل. وأضاف مسؤولو البنك أن هناك ٢٤ بطاقة ائتمانية أخرى صادرة من البنك نفسه وتم استخدامها داخل مصر بالرغم من وجود البطاقات مع أصحابها في الولايات المتحدة.

بعد إلقاء القبض على أحد الأشخاص أثناء توجهه إلى المحل لاستلام باقي المشتريات أقر باستخدام بعض البطاقات المزورة في عمليات الشراء من المحلات التجارية. وبتفتيشه عثر على ثلاث بطاقات ائتمانية مزورة صادرة من بنك مصر. وقد أكد الجاني أن البنك غير مسؤول عن إجراء عملية التزوير وأن المسؤول عن ذلك هو صديق له (المتهم الأول) وبعد ضبط المتهم الأول وتفتيش منزله تم العثور على بطاقة ائتمانية خاصة به على شاكلة البطاقات السابقة وعلى جهاز كمبيوتر وماكينة "تكويد" يتم استخدامها في عمليات تزوير البطاقات الائتمانية وإدخال الأرقام المعاد تكويدها على الشريط الممغنط. هذه الأرقام حصل عليها المتهم عن طريق اختراق موقع بنك ميريل لنش الأمريكي علي شبكة الإنترنت، وعن طريق العديد من أعوانه بالخارج من 'القراصنة'. وبعد أن يقوم بعملية التزوير المتقنة.

يقوم المتهم بتوزيع البطاقات المزورة على ثلاثة من أصدقائه لاستخدامها في المحال التجارية.

١ـ ٣ تطوير السياسات والمعايير والإجراءات في المصارف

١-٣-١السياسات والمعايير:

السياسات والمعايير الأمنية هى عبارة عن قوانين تسيطر على نظام المعلومات وتزوده بمستوى حماية موثوق به، وهي المنظمة لكل الأنشطة ذات الصلة في موقع ما. هذه السياسة تصدرها جهة مسؤولة تقر بمسؤوليتها تجاه أمن وحماية معلومات المصرف من جميع مصادر التهديد، فالسياسة المكتوبة والمطبقة بشكل جيد تحتوي معلومات كافية لما يجب عمله لحماية المعلومات والعاملين في المنظمة، كذلك فإن سياسات ومعايير أمن نظم المعلومات تؤسس قواعد لاستخدام الحاسوب للموظفين فيما يتعلق بمهامهم العملية[١٤٥].

السياسة الأمنية ومعاييرها بالإضافة إلى هدفها الرئيس في حماية المصرف، **تسهم في**[١٤٦]:

أ. تحسين طرق الاتصالات بين الأطراف

ب. نقل المعرفة بين الأطراف المعنية

ت. تحسين الأداء والإنتاجية

ث. تخفيض تكلفة أداء العمل

إن مصطلح "**سياسة**" هو تعبير عام وفضفاض، يشمل مواضيع عديدة. ولتطبيقها بسهولة لا بد من تطوير إطار عام للسياسة الأمنية يتمثل في وضع المعايير وخطوط الأساس والإرشادات والإجراءات.

هناك فرق بين الأهداف الإستراتيجية والأهداف التكتيكية للسياسات الأمنية، فالأهداف الاستراتيجية هي الأهداف المنشود تحقيقها في نهاية المطاف، أي إنها الأهداف النهائية، بلوغها يستوجب رسم السياسات الأمنية. بينما الأهداف التكتيكية هي أهداف فرعية مرحلية، بلوغها يستوجب اتخاذ الخطوات اللازمة التي يمكّن تنفيذها السليم من بلوغ تلك الأهداف. رسم تلك الخطوات يعني وضع المعايير وخطوط الأساس والموجهات والإرشادات والإجراءات.

---

[145] Spagnoletti, Paolo; Resca A.. "The duality of Information Security Management: fighting against predictable and unpredictable threats". *Journal of Information System Security* (2008)4 (3): p46–62. http://eprints.luiss.it/955/.

[١٤٦] محمد, محمد الهادي، "توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية", Cybrarians Journal، العدد ٩، يونيو ٢٠٠٦، تاريخ الاطلاع ٢٥ -١١-٢٠١١-www.journal.cybrarians.info/index.php

المعايير، في المصرف، هي المرجعية التي يقاس عليها ويحدد بناء عليها كيفية تهيئة وإعداد وتنفيذ عمل الأجهزة والبرامج، وذلك لضمان أن كل خطوات توفيق البرامج تم تبصورة متطابقة وبطريقة موحدة.

خطوط الأساس هي الحد الأدنى من متطلبات أمن النظم والمعلومات التي يجب توفرها قبل الشروع في بناء السياسات الأمنية، والمعايير تبنى عادة من خطوط الأساس لأمن النظم والمعلومات.

الموجهات والإرشادات هى عبارة عن توصيات إجرائية ودليل تشغيل وتنفيذ عمل للمستخدمين من موظفي التقنية ومشغلي الحاسوب والآخرين من ذوي العلاقة عندما لا تكون هناك سياسة أو موصفات لتطبيقها، ويستدل الموظف بالدليل لتنفيذ العمل المعني إذ إن الدليل يتمتع بمرونة التطبيق على عكس المواصفات التي يجب اتباعها وتطبيقها بدقة.

الإجراءات هي المعنية بتفاصيل تنفيذ أي عمل خطوة بخطوة، وهذه الخطوات تنطبق على المستخدمين وموظفي التقنية ومشغلي الحاسوب، والإجراءات هي الدرجة السفلى من درجات السياسة الأمنية لأنها معنية بالتفاصيل وتتعامل مع الحاسوب مباشرة مثل تركيب البرامج وتوفيقها وتنفيذها.

١-٣-٢ أنواع السياسات

هناك ثلاثة أنواع من السياسات الأمنية مصنفة على حسب إلزامية السياسة وتطبيقها وهى سياسات ملزمة التطبيق، سياسات توضيحية إرشادية وسياسات إعلامية[١٤٧]

- **السياسة الملزمة**

هذه السياسة تصاغ للتأكد من أن المصرف يطبق وينفذ المعايير التى تم كتابتها من قبل جهات محددة والتي قد تم تعميمها بقوة القانون.

- **السياسة التوضيحية**

هذا النوع من السياسة يصاغ لتقديم النصح لتوجيه سلوك أو أنشطة ستطبق بالمصرف، وأيضًا لتوضيح الآثار المترتب لعدم تطبيق السياسات للموظفين، وهذه السياسة تطبق في المعلومات الطبية، الحركات والقيود المالية ولمعالجة المعلومات السرية الأخرى.

[١٤٧] تقرير وزارة رئاسة مجلس الوزراء في السودان،المركز القومي للمعلومات، الإدارة الفنية، ٢٠١٠، ص١٢-١٤

- **السياسة الإعلامية**

هذه السياسة تصاغ لتعريف الموظفين بأمور محددة وهي ليست قابلة للتطبيق الإلزامي بقدرما هي لإعلام الموظفين بأمر ما ذي علاقة بالمصرف، كأن يعرف الموظف كيفية التعامل مع الآخرين، وتوضيح أهداف المصرف وطريقة ونظام كتابة وتقديم التقارير.

١-٣-٣ مستويات السياسات الأمنية

يمكن تقسيم وتصنيف السياسة الأمنية إلى:

- السياسة العامة: هى تعبير أو إفادة عامة عن مدى رغبة المصرف في حماية أصوله.
- السياسة الأمنية للمصرف: هي مجموعة القواعد والقوانين والإجراءات والمواصفات التي تنظم كيفية إدارة وحماية وتوزيع مصادر المعلومات من أجل تحقيق أهداف المصرف
- السياسات الأمنية للنظم: هى مجموعة القواعد التى يجب إنفاذها والإجراءات التى يجب اتباعها لتوفير القدر المطلوب من الحماية والأمن لنظم المعلومات بما يضمن تحقق أهداف السياسة الأمنية للمصرف.

إن المصارف السورية وخاصة العينة المستخدمة في البحث تسعى جاهدة لتطبيق المستويات الأمنية لتوفير حد أعلى من الأمان لنظمها الإلكترونية إلا أنها تعاني من بعض الصعوبات في تطبيق هذه المستويات كما سيتم عرضه في الدراسة العملية

١-٣- ٤ شروط نجاح السياسات في حماية المصارف:

لضمان تطبيق السياسات تطبيقًا فعليًا وتنفيذها من قبل المعنيين فلا بد من توفر الشروط الآتية عند صياغة السياسة وتطويرها وتطبيقها:

١-شمولية السياسة الأمنية

٢- مشاركة الجهات المعنية وذات الصلة في تطوير السياسة

٣- مراجعة السياسة بصفة دورية لمواكبة التطورات والتهديدات المستجدة

٤- تحديد المسؤوليات بوضوح

٥-عدم المغالاة في التطبيق

٦- اطلاع الموظفين على السياسات الأمنية.

ويجب التنويه هنا إلى أن أغلب المصارف السورية لم تستطع تطبيق هذه الشروط لنجاح السياسات الأمنية المتبعة وذلك لعدة أسباب سيتم ذكرها كنتائج في الفصل الرابع

١-٣-٥ تطبيق السياسات الأمنية

١-٣-٥-١التحوط

يرتكز تطبيق سياسات أمن النظم والمعلومات وحمايتها على ثلاثة محاور هي :التحوط والاكتشاف والتصويب. من أهداف أمن النظم والمعلومات عمل التحوطات اللازمة لحماية المصرف من المخاطر والمهددات الأمنية قبل حدوثها وذلك بتطبيق السياسات الأمنية الكفيلة بحماية كل من البيانات، الاتصالات والشبكات وتوفير الحماية المادية.

إن حماية البيانات هو المقصد النهائي من أمن النظم والمعلومات ولا بد من أن تشمل الحماية جميع الإجراءات الفنية للنظم والأجهزة والإجراءات الإدارية المتبعة في المصرف وتتمثل في:

- حماية النظم والبرامج التشغيلية والبرمجيات
- حماية قواعد البيانات
- فرض نظام التحكم في الوصول إلى النظم
- عمل النسخ الوقائي
- التحكم في تركيب البرامج الجديدة والتعديلات
- اختبار البرامج والنظم واعتمادها.
- فصل وظائف ومهام موظفي التقنية
- حماية الاتصالات والشبكات

إن الشبكات والاتصالات هي منفذ المصرف للعالم الخارجي وإن عدم وضع الخطط والبرامج لحماية الشبكات يعرض معلومات المصرف لمخاطر جمة لا يمكن التكهن بها، وهناك عدة طرق ووسائل لحماية الشبكات وتتمثل في:

- التشفير
- جدار النار
- بروكسي
- التوقيع الرقمي والشهادة الرقمية
- الأمن المادي

لا يكتمل أمن النظم والمعلومات وحمايتها إلا من خلال التأمين المادي للمنشأة والذى يشمل:

- اختيار مواقع غرف الحاسوب
- تصميم الغرفة

- إجراءات الدخول للمنشأة ومراكز المعلومات
- إيجاد الطاقة الكهربية البديلة
- حماية الوسائط
- حماية المستندات
- إجراءات التخلص من المستندات والوسائط الإلكترونية

إن أغلب المصارف السورية التي تستخدم الأنظمة الإلكترونية تتبع سياسة التحوط في حماية أنظمتها من المخاطر والتهديدات التي يمكن أن تتعرض لها.

١-٣-٥-٢الكشف عن الجريمة:

بما أن استخدام أنظمة المعلومات والشبكات أصبح أمرًا ملازمًا لجميع أعمالنا اليومية والتى تتجاوز استعمالاتها حدود المصرف إلى العالم الخارجي، وكما بينا في الصفحات السابقة فإن المخاطر والمهددات قائمة سواء كان مصدر هذه المهددات والمخاطر من داخل المنشآت أم خارجها وبالتالي لا يمكن معرفة ما يتم داخل هذه الأنظمة من تجاوزات أو اختراقات أو سرقات ما لم يكن هناك نظام رقابي يتحكم في جميع أنشطة هذه النظم، لذا لا بد لنا من وضع عين رقيبة لمعرفة ما يدور فيها وتزويد الجهات الرقابية بتقارير ووسائل تمكنهم من معرفة الاختراقات والتجاوزات، وتتمثل وسائل الرقابة والتحكم في:

التقارير الرقابية:

تشمل التقارير الرقابية الأتى:

١- تقرير التجاوزات

٢- تقرير أنشطة إدارة النظم

٣-تقرير الأخطاء

٤- تقرير إدارة المستخدمين

بالإضافة إلى تقارير الرقابة المتعلقة بالأنشطة، كل حسب نشاط المصرف.ونتيجة البحث وإجراء المقابلات والاطلاع على التقارير نرى أن هناك ضعف في عملية إعداد التقارير الرقابية فمثلا في المصرف العقاري الذي يقوم بإعداد التقرير حول قسم الـIT هو مفتش الرقابة الداخليةالمرسل من المصرف المركزي والأجدر هنا أن يعد التقرير شخص اختصاصي في مجال النظم والرقابة.

المشاهدة والمتابعة:

كثير من نظم الحماية مزودة بمزايا عرض الأنشطة التي تتم، كما في أنظمة جدار النار، بها إمكانيات تؤهلها من اكتشاف الاختراقات وتصنيفها وتوجيه رسائل إلى مسؤولي المراقبة عن طريق أجهزة الهاتف والهاتف النقال والنداء الآلي أو الرسائل الإلكترونية القصيرة، كما أن هذه

الأنظمة مزودة بإمكانية إصدار تقارير بالمخالفات والتجاوزات والاختراقات، فعليه، لا بد من

تركيب مثل هذه الأجهزة بحيث يستفاد من إمكانياتها لأقصى درجة ممكنة.

أنظمة اكتشاف الاختراقات:

مع تطور التقنية وتطور وسائل وتقنيات جرائم الحاسوب، وما تنتج عنها من خسائر مادية كبيرة، دأبت الشركات المهتمة والمتخصصة في أمن النظم والمعلومات وحمايتها في تطوير أنظمة الحماية ومنها أنظمة اكتشاف ومنع الاختراقات .وهذه الأنظمة مزودة كذلك بإمكانيات إصدار التقارير وإرسال الرسائل عند حدوث أي تهديد لشبكة وأنظمة المعلومات، فعلى المنشآت السعي لتزويد آلية الحماية لديهم بمثل هذه الأنظمة.

المراجعة والتدقيق:

من الطبيعي وجود إدارة متخصصة ومناطة بمراجعة وتدقيق نظم المعلومات لدى أى منشأة، ويجب أن تتمتع هذه الإدارة بكامل الإستقلالية والصلاحيات التي تمكنها من أداء مهمتها دون تأثير من أي جهة، وأن تدعم بكوادر مؤهلة ومتخصصة وخبيرة، لتؤدي هذه الإدارة عملها بمهنية وحيادية وتغطي جميع الجوانب المناطة بها.

١-٣-٥-٣ التصويب:

إن عملية التصويب والتصحيح لاتتم إلا بعد وقوع الحدث ومثول الخطر، لذا يجب أن ينصب اهتمام المنشآت في اتخاذ التحوطات اللازمة لمنع وقوع الخطر، وبما أن احتمالات حدوث الخطر وارد في ظل المهددات الأمنية المتفاقمة، فلا بد من وضع الترتيبات الكفيلة لإيقاف التدهور الأمني وتخفيف الآثار الناتجة عن الخطر وذلك باتباع الخطوات التالية:

١- إيقاف عملية الاختراق

٢- البحث عن نقاط الضعف

٣- البحث عن نتائج وآثار الاختراق والتجاوزات

٤- معالجة المشاكل الناتجة عن الاختراق والتجاوزات

٥- تنشيط الإجراءات الوقائية

٦- ترقية وتحديث مستوى الحماية وتنشيطها

٧- استئناف العمل

٨- التوثيق

يمكن القول من خلال الدراسة العملية أن المصارف موضوع الدراسة تتبع أغلب هذه السياسات مع وجود بعض النقاط التي تحتاج إلى تحديث كترقية وتحديث مستوى الحماية كبرامج مضادات الفيروسات وغيرها.

١-٤ مقومات أمن المعلومات

إن أغراض ابحاث واستراتيجيات ووسائل أمن المعلومات – سواء من الناحية التقنية او الأدائية-، ضمان توفر العناصر التالية لأية معلومات يراد توفير الحماية الكافية لها[١٤٨]:

١) السرية أو الموثوقية :Confidentiality وتعني التأكد من ان المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.

٢) التكاملية وسلامة المحتوى :Integrity التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغيره أو العبث به في اية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.

٣) استمرارية توفر المعلومات او الخدمة:Avallability التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وإن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله اليها.

٤) عدم إنكار التصرف المرتبط بالمعلومات ممن قام به:Non- repudiation ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها انكار أنه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة إثبات ان تصرفا ما قد تم من شخص ما في وقت معين..

ومما سبق نستنتج أنه لا بد لأي مصرف من اتخاذ الخطوات والإجراءات الكفيلة بحمايتة. ولا يتأتى ذلك إلا بإنشاء إدارة مختصة لأمن النظم والمعلومات،و تطوير السياسات والمعايير والإجراءات مع الإلتزام التام بتطبيق وتنفيذ السياسات والإجراءات الأمنية مما يؤدي إلى ضمان

[١٤٨] محمد,محمد الهادي,"توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية", - .cybrarians journal -ع ٩ ,يونيو ٢٠٠٦

كفاءة النظام في توفير الأمن في المصارف،كما تبين أن المصارف السورية(عينة الدراسة) تتوافر فيها مقومات أمن المعلومات وذلك من خلال التحليل الذي تم في الفصل الرابع.

١-٥ معايير أمن نظم المعلومات:

1-5-1معاييرالآيزو:

المنظمة الدولية للتوحيد القياسي (آيزو)(ISO)، الذي أنشئ في عام ١٩٤٧، هو هيئة غير حكومية تتعاون مع اللجنة الدولية الكهرتقنية (IEC) والاتحاد الدولي للاتصالات (ITU) على تكنولوجيا المعلومات والاتصالات (ICT).[١٤٩]

وهنا أشهر المعايير التابعة لها:

١-. <u>آيزو ٢٧٠٠٢:</u>

هذا المعيار يتضمن بعض السياسات والتوجيهات، منها:

أ- السياسة الأمنية Security policy

ب- تنظيم أمن المعلومات Organization of information security

ت- وإدارة الأصول Asset management

ث- أمن الموارد البشرية Human resources security

ج- الأمن البيئي والمادي Physical and environmental security

ح- الاتصالات وإدارة العمليات management Communications and operations

خ- التحكم في الوصول access control

د- اقتناء نظم المعلومات وتطويرها وصيانتها acquisition Information systems development and maintenance

ذ- إدارة الحوادث الأمنية للمعلومات management Information security incident

ر- إدارة استمرارية الأعمال Business continuity management

ز- إدارة الامتثال أو التوافق Compliance management

[١٤٩] بحث علمي :An overview of information security standards لحكومة منطقة هونغ كونغ الإدارية الخاصة.

إن معيار قواعد ممارسه أمن المعلومات ISO 27002 يتطابق في هيكليته مع مرفق –أ– من ISO 27001 لكنه أكثر تفصيلاً من حيث المضمون، فهو يسهب في شرح كيفية تطبيق الضوابط الأمنيه عند اختيارها، فتطبيق التوجيهات والمعلومات الاضافية هي في صلب تركيبته لكل من الضوابط المدرجه ضمن ١١ هدفاً محدداً كما في الرسم أدناه:

إنه لمن الممكن استخدام كل أو جزء من هذا المعيار منفصلاً عن ISO 27001 من لدن أي منشأ يسعى وراء رفع مستواه الأمني عبر اختيار الضوابط الأمنيه المناسبه لدرء الأخطار المحيطه. مع العلم أن ليس هناك أولويات أو تسلسل عند إنتقاء الضوابط،وكما تنبه المنظمة الدولية إليه فإنه لا يتحقق الأمن الكامل بمجرد العمل بهذه الضوابط بل إنها تحث على تدخل إضافي من المنشأ لرصد وتقييم وتحسين فعالية الضوابط الأمنية الداعمة لأهدافها.

٢– آيزو ٢٧٠٠١:

هذا المعيار[١٥٠] يقدم نموذجاً دورياً يعرف بـ(PDCA) وهو اختصار لـ (Plan–DO–Check–Act) وهو يهدف إلى تحديد الاحتياجات اللازمة لإقامة وتنفيذ وتشغيل ورصد واستعراض وصيانة وتحسين وتوثيق نظام إدارة أمن المعلومات داخل المصرف. وعادة ما ينطبق على جميع أنواع المنظمات، بما في ذلك المؤسسات التجارية والوكالات الحكومية، وغيرها.

وكما ورد سابقا فإن هذا النموذج يتم في أربع مراحل متتابعة:

أ– الخطة (Plan): تأسيس نظام لإدارة أمن المعلومات.

ب– التنفيذ (Do): البدء في تنفيذ الخطط وتشغيلها.

ت– التحقق (Check): مراجعة النظام بعد تنفيذه.

ث– العمل (Act): صيانة وتحسين النظام.

هذا المعيار لا يفرض كما قد يظن بعضهم ضوابط أمنية معينة أو يعالج فقط النواحي الأمنيه لتقنية المعلومات، بل أنه يقف فقط عند مستوى إدارته للنظام. أما من يقوم بدور إرشادي لتفسير وتطبيق الضوابط المعرفه في ملحقه فهو معيار قواعد الممارسه لإدارة أمن المعلومات ٢٧٠٠٢ ISO المنتمي إلى نفس العائله والذي من المقصود استخدامه سوياً.

[150] E.H. Freeman, "Holistic Information Security: ISO 27001 and Due Care.," *Information Systems Security*, vol. 16, Sep. 2007, pp. 291-294

وكما يعنى هذا المعيار إنشاء نظام إدارة أمن معلومات تدار من خلاله المخاطر الأمنيه، فإن المؤسسات تسعى من خلال إثباتها لإدارة نظامها وضوابطها الامنيه وفق توصيفات النظام الحصول على شهادة أمن معترف بها دولياً. ومع وجود هذا النظام يكون بمقدور الإدارة العليا للمؤسسة التحكم ومراقبة الأمن كما باستطاعتها التخفيف من وطأة المخاطر المحيطه بعملها[١٥١].

ويعـد ISO 27001 معيار الحماية الدولي الرسمي المقدم لأي منظمة (بغض النظر عن كونها صناعيةً كانت أم خدمية) ترغب بالحصول على شهادة مستقلة لنظام إدارة حماية المعلومات الخاصة بها. لهذا تحدد المواصفة المتطلبات الإلزامية لتأسيس وتطبيق وتوثيق نظام ISMS، وتحديد متطلبات السيطرة لحماية المعلومات التي ستطبق وفق حاجات المصرف الخاصة بها، وتشمل (١١) مركزاً للسيطرة و(٣٩) هدفاً للسيطرة بالإضافة إلى (١٣٣) موقعاً للسيطرة متوافقاً مع المواصفة ISO 17799 والتي تعمل من خلال أنموذج Plan – Do – Check – Act(PDCA) الذي يقوم بعمل التحسين المستمر، وبهذا تستند المواصفة ISO 27001 في عملها على تسعة أجزاء للمعالجة التي حددها تحالف صناعة حماية شبكات الإنترنيت CSIA *يمكن تلخيصها بالاتي[١٥٢]:

١. تعريف المجال لنظام إدارة حماية المعلومات ISMS.
٢. تعريف سياسة حماية المعلومات.
٣. تقييم الأخطار /التحليل.
٤. إدارة الخطر.
٥. تحديد الأهداف للسيطرة والسيطرة الفعلية عليها / التطبيق.
٦. تجهيز بيان (كشف) التطبيق.
٧. تطبيق وتشغيل ISMS.
٨. استمرار المراقبة ومراجعة ISMS.
٩. إدامة وتحسين ISMS.

[151] Calder, A. and J. Van Bon, *Information Security Based on ISO 27001/ISO 17799: A Management Guide*. 2009

[*] Cyber Security Industry Alliance

[152] CSIAISO 27001: Get The Facts, , 2007, www.csialliance.org

ولإنجاز نظام ISMS فعال تستعين منظمة المواصفات الدولية ISO معايير ISO 27002 كتعليمات تساعد في تطبيق ISO 27001 من خلال الأتي[١٥٣]:

١. تقييم المخاطر والمعالجة.

٢. سياسة الحماية.

٣. تنظيم حماية المعلومات؟

٤. إدارة الموجودات.

٥. حماية معلومات الموارد البشرية.

٦. حماية الطبيعة والبيئة.

٧. إدارة العمليات والاتصالات.

٨. السيطرة على دخول قواعد البيانات.

٩. الحصول على نظم المعلومات، التطوير، الإدامة.

١٠. إدارة حوادث لحماية المعلومات.

١١. إدارة استمرارية العمل.

١٢. الالتزام (الالتزام بتطبيق بنود المواصفة)

فوائد الحصول على شهادة المواصفة ISO27001:2005

هناك عدة أسباب التي تدفع المصرف للحصول على الشهادة وذلك للحصول على عدة منافع هي[١٥٤]: (Hinson، 3 ,2008)

١. المصداقية وزيادة الثقة.

٢. تحسين الشراكة (العمل مع الشريك).

٣. زيادة ثقة الزبائن وأصحاب العلاقة.

٤. التنظيم وحماية الشريك التجاري.

٥. شهادة تفيد بأن المصارف مؤهلة ومطبقة لكل القوانين النافذة والتعليمات.

---

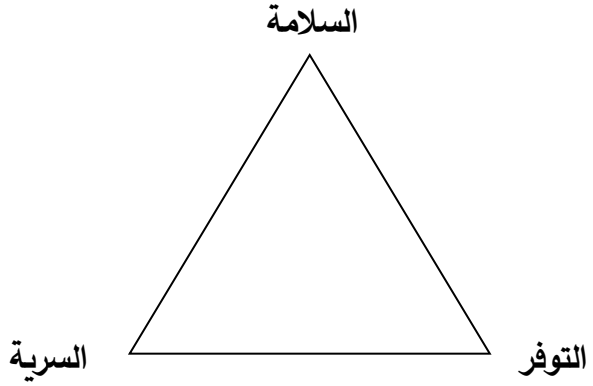
[153] Arnason, Sigurjon Thor & Willett, Keith D., How to Achieve 27001 Certification : An Example of Applied Compliance Management, Taylor & Francis Group, LLC, USA. ,2008 p203

[154] Hinson,Gary, ,ISO27001 Security :The Financial Implications of Implementing ISO/IEC27002, Ageneric Cost Benefit Model, ISECT Ltd , 2008 www.ISO27001 security .com

٦. المفاضلة بين المنافسين وكذلك الحصول على تعليمات بكلف منخفضة.

الأبعاد الثلاثة لحماية المعلومات:

يمكن أن يتعرف المصرف على كيفية إدارة حماية المعلومات من خلال ثلاثة أبعاد (السرية، السلامة، التوفر) أو كما وصفتها هيئة معايير معالجة البيانات الاتحادية FIPS Federal Information Processing Standers بأحجار الزاوية لحماية المعلومات عام ٢٠٠٤، وذلك من خلال تطبيق نظم إدارة حماية المعلومات، أو باستعمال معايير ISO27001 كدليل لتطوير ISMS، كما في الشكل(٥):



الشكل (٧) الأبعاد الثلاثة لحماية المعلومات

الأبعاد الثلاثة لحماية المعلومات[١٥٥]

ويمكن توضيح هذه الأبعاد الثلاثة بإيجاز كالاتي [١٥٦]:

١. **السرية** Confidentiality: يوفر هذا البعد للمنظمة السرية التامة لكافة المعلومات، حتى لو كانت المعلومات صغيرة وبسيطة.

٢. **السلامة** Integrity: تقدم المواصفة ISO27001 معياراً لحماية وكمال المعلومات وطرائق معالجتها، وهذا يضمن الاستمرارية وإعادة العمل في حالة وقوع الكوارث.

٣. **التوفر** Availability: ويقصد بالتوفر هو توفر المعلومات المقيد، إذ إن استخدام ISO27001 لحماية نظام المعلومات يؤكد للمنظمة بأن المستخدمين المخولين هم الوحيدون القادرون على الوصول إلى هذه المعلومات وأصولها، وهذا يجعل إدارة حماية المعلومات مهمة سهلة المعالجة.

---

[155] Arnason, Sigurjon Thor & Willett, Keith D. ,2008, مرجع سابق

[156] www.intertek-semkocertification,se, 2007

2-5-1 معيار الكوبيت

COBIT:(The Control Objectives for Information and related Technology)

هو عبارة عن إطار للسيطرة أو التحكم تربط تقنية المعلومات بمتطلبات العمل، وتنظيم أنشطة تكنولوجيا المعلومات في نموذج العملية المقبولة، وتحديد الموارد الرئيسة لتكنولوجيا المعلومات، وأهداف الرقابة الإدارية التي سينظر فيها"

وقد تم بناء هذا المعيار من قبل معهد حوكمة تقنية المعلومات .IT.ITIG Governance Institute في عام ١٩٩٥م.[١٥٧]

١- النظرة التنفيذيةExecutive overview .

٢- إطار الكوبيت. COBIT framework

٣- التخطيط والتنظيم. Plan and Organize

٤- الاكتساب والتنفيذ. Acquire and Implement

٥- التسليم والدعم. Deliver and Support

٦- الرصد والتقييم. Monitor and Evaluation

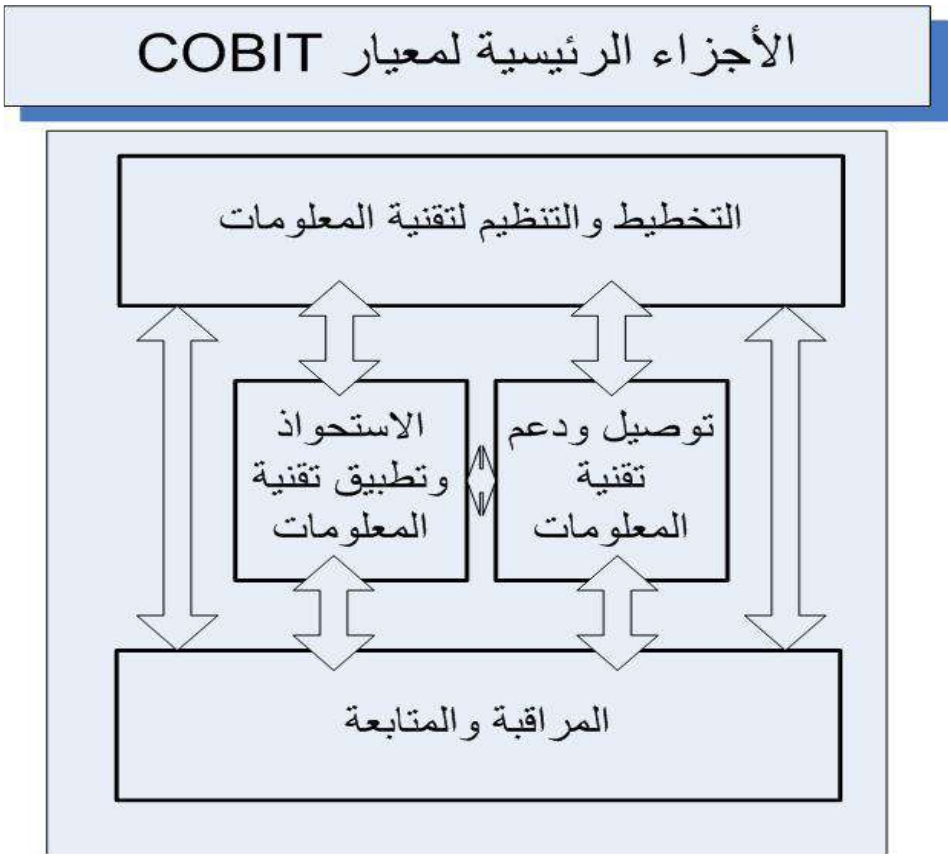
٧- الملاحق، بما في ذلك المعجم أو المصطلحات Appendices

والكوبيت هو مجموعة من المواد التوجيهية الدولية تستخدم لحوكمة تقنية المعلومات وكذلك تتيح للمديرين سد الفجوة بين متطلبات الرقابة والقضايا التقنية والمخاطر التجارية. واستناداً إلى أبرز النقاط في الكوبيت تبين أنه يركز على مخاطر محددة حول أمن تكنولوجيا المعلومات بطريقة بسيطة لمتابعة وتنفيذ المنظمات الصغيرة والكبيرة. والشكل التالي يبين العلاقة بين هذه الأجزاء[١٥٨].

---

[157] 93 Wood, David J.. "Assessing IT Governance Maturity: The Case of San Marcos, Texas". Applied Research Projects, 2010Texas State University-San Marcos

[158]ITGovernanceInstitute. *COBIT® 4.1*. 2008 [cited 22\11\2009]; Available from: http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/ContentManagement/ContentDisplay.cfm&ContentID=34172



الشكل رقم(٨) الاجزاء الرئيسة لمعيار COBIT

١-٥-٣ معيار ITIL

هو اختصار لـ The Information Technology Infrastructure Library ويسمى أيضاً آيزو ٢٠٠٠٠.

وهذا المعيار عبارة عن مجموعة من المفاهيم والسياسات لإدارة وتطوير خدمات تقنية المعلومات والعمليات المتعلقة بها. وفي هذا المعيار هناك وصف تفصيلي للمهام والعمليات المتعلقة بتقنية المعلومات مع قوائم مرجعية متكاملة بحيث تستطيع أي منظمة تستخدم تقنية المعلومات موائمته حسب احتياجاتها.

وبالرغم من عدم وجود جزء مستقل في هذا المعيار مخصص لأمن المعلومات إلا أنه يعتبر الأمن عملية مستمرة وتكاملية مع باقي العمليات خصوصاً عملية إيصال الخدمة [١٥٩]

وفي هذا المعيار يجب أن تتوافق إدارة أمن المعلومات في المصرف مع ما يلي:

- السياسات الحالية والمستقبلية لأمن إدارة الأعمال.

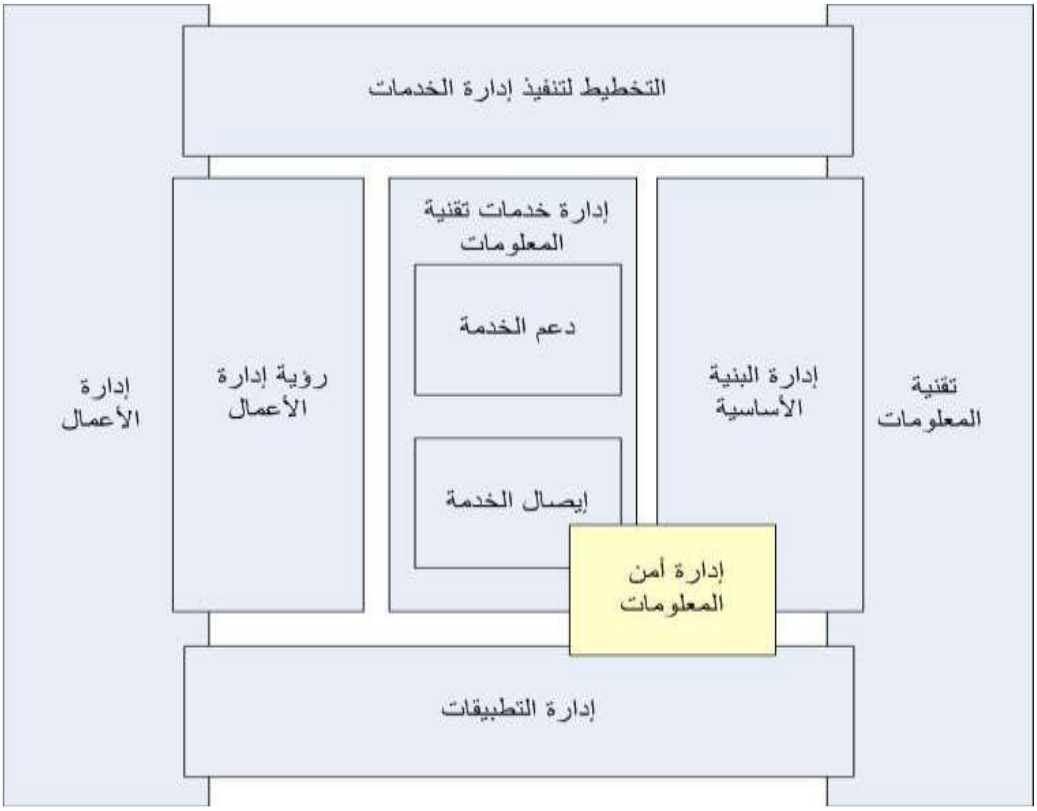
[159] Van Bon, J., *Foundations of IT service management based on ITIL V3*.: Van Haren ،2008،p66

- متطلبات الأمن.
- المتطلبات التشريعية والقانونية.
- إدارة تقييم مخاطر الأعمال وتقنية المعلومات.

كما يجب أن توضح إدارة أمن المعلومات ما يلي:

- سياسة أمن المعلومات.
- أنظمة إدارة المعلومات.
- خطة استراتيجية متكاملة لأمن المعلومات ومتوافقة مع استراتيجيات الأعمال.
- هيكلية فعالة لإدارة الأمن.

وذلك كما يظهر في الشكل التالي [١٦٠]:



.....

الشكل رقم (٩) إدارة أمن المعلومات في COBIT

[160] Sallé, M., *IT Service Management and IT Governance: review, comparative analysis and their impact on utility computing.* Trusted Systems Laboratory: HP Laboratories Palo Alto, 2004، p98

ورغم أن هناك عددا من معايير أمن المعلومات المتاحة، وهي منظمة بحيث لا يمكن الإستفادة منها إلا إذا تم تنفيذ هذه المعايير بشكل صحيح. الأمن هو شيء ينبغي أن تشارك فيها جميع الأطراف سواءً من الإدارة العليا والعاملين في أمن المعلومات، والمحترفين في تكنولوجيا المعلومات والمستخدمين والكل منهم له دور يؤديه في تأمين أصول المؤسسة. نجاح أمن المعلومات يمكن تحقيقه من خلال التعاون الكامل على جميع مستويات المصرف، سواء في الداخل والخارج.

بالعودة إلى نظم المعلومات المحاسبية للمصارف السورية فإن توافر معايير لأمن وسلامة البيانات أمر لا بد منه، ليتم من خلالها ضبط أمن المعلومات وتقييم إجراءات الأمان القائمة وتحديد نقاط ضعفها، تمهيدا لتدارك هذا الضعف عبر تطوير إجراءات الأمان.

٢-المبحث الثاني: وسائل ضمان الأمن التقنية

٢-١ نطاق معالجة وسائل الأمن ومنطلقاته.

توافر الوسائل التقنية الضرورية لضمان الأمن لمعلومات النظام، يسهم بشكل مباشر في بلوغ النظام أهدافه الأمنية. الحديث هنا ليس عن منتجات الأمن التي لا يمر يوم دون وجود منتج جديد، ولا يمر يوم أيضا دون إعادة تقييم لوسائل الأمن. إنها وسائل ومنتجات تتوزع بين الوسائل المادية للحماية وبرمجيات وحلول الحماية، ونظريات وبروتوكولات الحماية. إن سوق وسائل الأمن أصبح يتقدم في عدد منتجاته على سوق الأجهزة ذاتها والحلول، لأن كل منتج وكل برنامج جديد يتطلب قدرا معينا من وسائل الحماية الفنية [١٦١].

كما أن هذا الدليل لا يقيم وسائل الأمن القائمة، فيتحدث مثلا عن مدى فعالية الجدران النارية أو مدى مقدرة الشبكات الخاصة الافتراضية على توفير الأمن والثقة، انما يعرض فقط للشائع من طوائف وسائل أمن المعلومات بوجه عام والتي تندرج في نطاق كل طائفة منها آلاف الوسائل التي تتباين تبعا للاحتياجات وتبعا لطبيعة محل الحماية. ولهذا، وعند الحديث عن اية وسائل، ثمة منطلق رئيس، وثمة ادلة تفصيلية: المنطلق- لكل وسائله، والخطأ في الاستنساخ وإغفال الاحتياج الحقيقي كالخطأ في إغفال الحماية.

الخطأ السائد يكمن في الاعتقاد أن نظم الكمبيوتر والشبكات تتشابه من حيث احتياجاتها الأمنية، إذ حتى في نطاق الطائفة الواحدة من أنظمة الكمبيوتر التي تستخدم نفس برمجيات التشغيل أو تعتمد نفس وسائل التشبيك وحلول الشبكات وتجهيزاتها، فإن اختلافا في متطلبات الحماية لما يزل قائما ومرد لك التباين بين طبيعة العمليات التي يقوم بها النظام والتباين بين طبيعة البيانات نفسها، والتباين بين وسائل الاستخدام والمستخدمين، واخيرا، التباين في درجة التوازن المطلوبة ما بين إجراءات الأمن وأداء وفعالية النظام نفسه.

إن بناء وسائل أمن فاعلة يتطلب الانطلاق من احتياجات المؤسسة الخاصة وأغراض الأمن فيها، ويقوم على إدراك الاحتياجات الداخلية فما نحميه يختلف عما يحميه غيرنا، ومصادر الخطر التي تواجه مؤسسة مالية مثلا تختلف عن المخاطر التي تواجه مؤسسة عسكرية أو تواجه نظام كمبيوتر مستخدم فرد. واحتياجات حماية جهاز الكمبيوتر وبرمجياته والبيانات المخزنة فيه يتخلف عن

[161] P. Puhakainen and M.T. Siponen, "Improving employees' compliance through information systems security training: An action research study," *MIS Quarterly*, vol. 34, Dec. 2010.

احتياجات حماية شبكة داخلية او حماية الارتباط بشبكة عالمية.[١٦٢]

ولهذا فإن تقنيات الحماية مرتبطة بعامل الاحتياجات الخاصة المعتمدة على تقدير قائم على ركائز وحقائق سليمة، ويعتمد أيضا على التوازن بين متطلبات الحماية وسرعة الأداء، والتوازن أيضا بين متطلبات الحماية والميزانية المرصودة لتوظيف وسائل الأمن. ومنطق استخدام تقنيات أحدى الشركات لمجرد أنها عالمية أو مميزة، منطق لا يتفق مع إستراتيجية الأمن ذاته، ولا نبالغ إن قلنا أن مئات المؤسسات – وتحديا المالية – استخدمت حزما من التقنيات في ضمنها مثلا جدران نارية وبرمجيات تشفير – كانت فاعلة في حالات أخرى– لم تكن لتحل مشكلاتها الأمنية، وفي الوقت ذاته اذا تمكنت من حلها فإنها أحدثت أثرا سلبيا على كفاءة الأداء وفعالية النظام. الأدلة التقنية– لكل طائفة من وسائل الأمن مؤسساتها وأدلتها التقنية وثمة تخصصية متنامية في نطاق كل وسيلة منها.

إن سوق الوسائل التقنية في مرحلة ما كان مجرد منتجات وخدمات مضافة إلى طائفة منتجات وخدمات شركات تكنولوجيا المعلومات المختلفة وغالبا ما تكون وسائل في خدمة بقية منتجاتها وخدماتها ومع ان شركات تقنيات المعلومات لما تزل في غالبيتها تخصص وحدات من بين وحدات نشاطها لوسائل الأمن فان سوق تكنولوجيا المعلومات انتقل إلى التخصصية، فنشأت شركات عملاقة تعمل في حقل أمن المعلومات، ووسائله ووحلوله، واتجهت الدراسات البحثية والاستراتيجية والعلمية والقانونية إلى التعامل مع وسائل الأمن على استقلال، فثمة أدلة ودراسات شاملة في ميدان الفيروسات ووسائل مكافحتها وثمة مثله في ميدان التشفير وحلوله، وأخرى في ميدان وسائل التعريف والتحكم في الدخول إلى النظام، وهكذا[١٦٣]

[162] J.M. Hagen, E. Albrechtsen, and J. Hovden, "Implementation and effectiveness of organizational information security measures," *Information Management & Computer Security*, vol. 16, 2008, pp. 377 - 397.

[١٦٣] المهتدي، زهير سوسن، "تكنولوجيا الحكومة الإلكترونية "، دار أسامة للتوزيع والنشر، الأردن، ٢٠١١، ص١١١-١١٦

٢-٢إستراتيجية أمن الإنترنت

تشكل استراتيجية أمن النترنت أحد الأركان الأساسية لنجاح النظام في بلوغ أهدافه الأمنية، المرتبطة بالعمليات المصرفية عبر الإنترنت. يقوم بشكل أساسي أمن المعلومات في حقل تحقيق أمن الإنترنت على مواضع ثلاث: **أمن الشبكة، أمن التطبيقات، أمن النظم**[١٦٤]. وكل منها ينطوي على قواعد ومتطلبات تختلف عن الأخرى ويتعين أن تكون أنظمة الأمن في هذه المواضع الثلاث متكاملة مع بعضها حتى تحقق الوقاية المطلوبة لأنها بالعموم تنطوي أيضا على اتصال وارتباط بمستويات الأمن العامة كالحماية المادية والحماية الشخصية والحماية الإدارية والحماية الإعلانية. وفيما تقدم اشرنا إلى العناصر المتصلة بأمن النظم والبرمجيات والبيانات وبقي ان نشير في هذا المقام إلى أمن الشبكات:

إن ما يحمى من خلال أمن الشبكة هو عملية الاتصال والتبادل بين أحد كمبيوترات الشبكة النظام النهائي سواء اكان نظام الزبون أن نظام المستضيف (الخادم) وبين كمبيوتر آخر ضمن الشبكة، فإذا ارتبط النظام النهائي بالإنترنت مباشرة دون وجود وسائل أمن ما بين هذا النظام والشبكة فإن أية حزمة بيانات مرسلة قد يلحق بها ما يلي[١٦٥]:

أ- قد يتم تغيرها خلال عملية النقل

ب- قد لا تظهر من حيث مصدرها من الجهة التي قدمت منها

ت- قد تكون جزء من هجوم يستهدف النظام

ث- قد لا تصل إلى العنوان المرسلة اليه

ج- قد يتم قراءتها والاطلاع عليها وافشاؤها من الغير.

ويهدف أمن الشبكات من جهة أخرى إلى حماية الشبكة نفسها وإظهار الثقة لدى مستخدم النظام النهائي بتوفر وسائل الحماية في تعامله مع الشبكة وكذلك إظهار الشبكة ذاتها بأنها تحتوى على وسائل أمن لا تتطلب معها ان يكون كمبيوتر المستخدم محتويا على وسائل خاصة.

تتضمن وسائل أمن الشبكة ما يلي[١٦٦]:

---

[164] M.T. Siponen and H. Oinas-Kukkonen, "A review of information security issues and respective research contributions," *SIGMIS Database*, vol. 38, 2007, pp. 60-80.

[165] K. Hong, Y. Chi, L.R. Chao, and J. Tang, "An integrated system theory of information security management," *Information Management & Computer Security*, vol. 11, 2003, pp. 243 - 248.

[166] M. Dlamini, J. Eloff, and M. Eloff, "Information security: The moving target," *Computers & Security*, vol. 28, May. 2009, pp. 189-198.

١-التعريف والسلامة: من خلال تزويد نظام المستقبل بالثقة في حماية حزم المعلومات والتأكد من ان المعلومات التي وصلت لم يتم تعديلها.

٢- السرية: حماية محتوى حزم المعلومات من الإفشاء إلا للجهات المرسلة إليها.

٣-التحكم بالدخول: تقيد الاتصالات بحصرها ما بين النظام المرسل والنظام المستقبل.

٢-٣ متطلبات أمن المعلومات والمعاملات المصرفية الإلكترونية:

تشير حصيلة دراسات أمن المعلومات وما شهده هذا الحقل من تطورات على مدى الثلاثين عاما المنصرمة أن مستويات ومتطلبات الأمن الرئيسة للبنوك في بيئة تقنية المعلومات تتمثل فيما يلي[١٦٧]:

٢-٣-١ الوعي بمسائل الأمن لكافة مستويات الأداء الوظيفي، الحماية المادية للتجهيزات التقنية، الحماية الأدائية(استراتيجيات رقابة العمل والموظفين) الحماية التقنية الداخلية، والحماية التقنية من المخاطر الخارجية.

٢-٣-٢ الأمن الفاعل هو المرتكز على الاحتياجات المدروسة التي تضمن الملاءمة والموازنة بين محل الحماية ومصدرالخطر ونطاق الحماية وأداء النظام والتكلفة، وبالتالي فان استراتيجيات وبرامج أمن المعلومات تختلف من منظمة إلى أخرى ومن بيئة إلى أخرى تبعا لطبيعة البناء التقني للنظام محل الحماية وتبعا للمعلومات محل الحماية وتبعا للآليات التقنية للعمليات محل الحماية، إلى جانب عناصر تكامل الأداء وأثر وسائل الأمن عليه وعناصر التكلفة المالية وغيرها، كما أن الحماية التقنية وسيلة وقاية ودفاع، وفي حالات معينة وسيلة هجوم، ولا تتكامل حلقات الحماية دون الحماية القانونية عبر التشريعات القانونية التي تحمي من إساءة استخدام الحواسيب والشبكات فيما يعرف بجرائم الكمبيوتر والإنترنيت والاتصالات وجرائم المعلومات المصرفية، وبالتالي تتكامل تشريعات البنوك والتجارة الإلكترونية مع النصوص القانونية لحماية المعلومات، وبدونها يظل جسم الحماية بجناح واحد [١٦٨]

٢-٣-٣ تمثل بيانات البنوك أموالا رقمية وحقوقا مالية وعناصر رئيسة في الائتمان، ومنه فالمطلوب هو وضع إستراتيجية شاملة لأمن المعلومات تتناول نظام البنك وموقعه الافتراضي وتتناول نظم الحماية الداخلية من أنشطة إساءة الاستخدام التي قد يمارسها الموظفون المعنيون، إلى

---

[١٦٧] مصطفى ,سمارة،"استيعاب استراتيجيات التجارة الإلكترونية المنطلق الأساسي نحو البنوك الإلكترونية"، مجلة انترنت، العدد الحادي والعشرون،تشرين الثاني، ٢٠٠٧، تاريخ الدخول ٢٢-١٠-٢٠١٠

[١٦٨] الغثبر،سليمان خالد،و القحطاني، عبدالله محمد، "أمن المعلومات بلغة ميسرة"، الرياض، مكتبة فهد الوطنية، ٢٠٠٩،ص ١٠٨

جانب إستراتيجية الحماية من الاختراقات الداخلية، وهذه الاستراتيجيات يجب أن تمتد إلى العميل لا للمصرف وحده، حتى نضمن نشاطا واعيا للتعامل مع المعلومات وتقدير أهمية حمايتها، ولكل إستراتيجية أركانها ومتطلباتها ومخرجاتها، وتقييم كفاءة الإستراتيجية يقوم على مدى قدرتها على توفير مظلة أمن شاملة لنظام المصرف والعميل والنظم المرتبطة بهما.

٢-٣-٤ الرقابة الإلكترونية والتي تركز على الأساليب التكنولوجية للرقابة على المخاطر وفحص البنوك في بيئة هيكلية تتسم بالانفتاح، وسوف تخضع جهات الرقابة والفحص لتبديل في الاتجاهات خلال السنوات القادمة، وبما أن الصناعة المصرفية قد مرت بتغيير في الثقافة مع الاعتماد المتزايد على أجهزة الكومبيوتر والإنترنيت، ومنه فالتامين اللازم عند أي تعامل مصرفي إلكتروني سوف يضل العامل الرئيس المراد الوصول إليه لتجنب الجرائم المعلوماتية التي تواجه البنوك في بيئة الإنترنيت

٢-٣-٥ إن أهم استراتيجيات أمن المعلومات توفير الكفاءات التقنية القادرة على كشف وملاحقة الاختراقات وضمان وجود فريق تدخل سريع يدرك جيدا ما يقوم به لأن أهم الاختراقات في حقل الكمبيوتر أتلفت أدلتها لخطأ في عملية التعامل التقني مع النظام، ومن جديد تظل الحماية القانونية غير ذات موضوع إذا لم تتوفر نصوص الحماية الجنائية التي تخلق مشروعية ملاحقة أفعال الاعتداء الداخلية والخارجية على نظم الكمبيوتر وقواعد البيانات.

٢-٣-٦ أمن نظام التحويلات المالية الإلكترونية، حيث توجد وسيلتان أساسيتان لتأمين المعاملات المالية والمصرفية الإلكترونية وهما:

-الأمن البرمجي ويعتمد هذا النوع من الأمن على تشفير المعلومات البنكية عن طريق برنامج خاص يعمل على تشفير المعلومات الخاصة بإتمام عمليات الشراء، بحيث لا يمكن قراءتها في حالة اعتراضها، ومن أمثلة هذه البرامج بروتوكول الطبقات الأمنية وهو بروتوكول تابع لشركة Netscape Communication Corp، يسمح بمعرفة هوية البائعين، بل وقد يربك حتى المشتري نفسه الذي يتعين عليه إرسال رقم بطاقته للبائع على الخط، إذ قد يؤدي ذلك إلى استعمال رقمه من طرف غيره، وأهم ميزة في هذا البروتوكول البساطة في الاستعمال، حيث يتم إدماجه ضمن برامج التعامل عبر الإنترنيت المعروفة مثلNetscape ، Internet explorer، أوOpera ، وبالتالي فهو لا يتطلب توفير أجهزة خاصة وهو متاح لك مستخدمي الإنترنيت.

- الأمن العتادي ويتم هذا النوع من الأمن باستعمال البطاقات الذكية الخاصة بالمستهلك، ومن أمثلة البرامج المستخدمة لتحقيق الأمن العتادي نجد بروتوكول الحركات المالية الآمنة،والذي

يسمح لشركتي Master Card و Visa International بمعرفة أطراف التبادل من خلال التوقيعات الرقمية، حتى إنه أضحى يعتبر بمثابة الحلم في أغلب عمليات الدفع التي تتم عبر الإنترنيت.

٢-٣-٧ التوقيع الإلكتروني: وهو شهادة رقمية تستخدم في إرسال أي وثيقة أو عقد تجاري أو تعهد أو قرار، وهو مكون من أحرف أو أرقام أو رموز أو صوت أو نظام معالجة إلكتروني. واللجوء إلى التوقيع الإلكتروني يرفع، من مستوى الأمن والخصوصية للمتعاملين على شبكة الإنترنت، حيث يضمن سرية المعلومات والرسائل والبيانات،فمن خلاله يمكن تحديد هوية المرسل والتأكد من مصداقية الأشخاص والمعلومات، والتوقيع الإلكتروني يتم عن طريق صورتين أحداهما التوقيع الرقمي أو إعطاء شيفرة باستعمال عدة أرقام يتم تركيبها للتوقيع بها، ويستعمل كثيرا في التعاملات الهامة كالتعاملات البنكية ومزايا هذا التوقيع هو أنه يؤدي إلى إقرار المعلومات التي يتضمنها السند وهو دليل على الحقيقة، كما يسمح التوقيع الرقمي بإبرام صفقات عن بعد وتسهيل التعاملات دون ضياع الوقت في التنقل وضياع المال وبذلك يزيد في تنمية وضمان التجارة الإلكترونية.

وفي النهاية يمكن القول إن المصارف السورية تحاول جاهدة النهوض بعملها وهذا ما يظهر في الناحية التطبيقية وخاصة المصارف التي تتبع الأنظمة الإلكترونية في معالجة بياناتها فتقوم بتطبيق السياسات الأمنية ووسائل الأمن الشائعة والاستراتيجيات المتبعة لحماية أمن الشبكات أثناء نقل البيانات التي تضمن الحماية لأنظمتها وفق الإمكانيات المتاحة على أرض الواقع وبذلك تكون قد ضمنت تحقيق مطلب أساسي لكفاءة النظام وهو أمن المعلومات وسيظهر ذلك بشكل واضح من خلال الدراسة العملية التي أجريت على المصرفين عينة الدراسة

الفصل الرابع
التحقق من قدرة نظام المعلومات المحاسبي المصرفي على حماية البيانات والمعلومات

المبحث الأول: منهجية الدراسة

المبحث الثاني: إجراءات أمن البيانات والمعلومات المطبقة في المصارف

المبحث الثالث: تقييم واقع أمن البيانات والمعلومات في المصارف عينة الدراسة

المبحث الرابع: مقارنة اجراءات أمن البيانات والمعلومات المتبعة في المصارف بمعايير الجودة ومعايير cobit بهدف تقييم كفاءة النظام

المبحث الخامس: التحقق من الفرضيات والحكم على كفاءة نظم المعلومات المحاسبية في حماية البيانات والمعلومات في المصارف السورية

١-المبحث الأول: منهجية الدراسة

١- ١أداة الدراسة

لبلوغ هدف البحث قامت الباحثة بتحديد مرجعية أساسية للمقارنة تمثلت في معايير الجودة ومعايير **cobit**.ثم قامت بزيارات ميدانية متكررة إلى المصرف العقاري ومصرف عودة جمعت خلالها البيانات والمعلومات اللازمة لعمليات المقارنة والتحليل. وقد اعتمدت في سبيل ذلك مجموعة وسائل منها:

١. الملاحظة المباشرة لكيفية إنجاز الأعمال من قبل العاملين في الأقسام ذات الصلة
٢. قائمة استقصاء موجهة إلى جهات محددة ذات صلة بموضوعات البحث، في حال تعذر المقابلة الشخصية، لغرض الحصول على معلومات تُمَكِّن من معرفة واقع أمن البيانات في المصرف (وليس لغرض معرفة رأي الأشخاص المعنيين وتقييمهم الشخصي)
٣. المقابلات الشخصية مع رئيس قسم نظم المعلومات والعاملين في القسم للمصرفيين وتوجيه الاسئلة لإستخدامها في اختبار الفرضيات حول :

<u>الإجراءات الإدارية في البنوك عينة الدراسة وتشمل</u>

- اهتمام الإدارة العليا بأمن المعلومات
- استخدم تقنية النظم والمعلومات في أداء الأعمال
- ربط جميع فروع البنك بشبكة واحدة
- ربط البنك بشبكة الإنترنت
- إنشاء دائرة خاصة بأمن وحماية المعلومات
- تجهيزات غرف الحاسوب

·التوعية العاملين الأمنية

·تحفيز الموظفين العاملين التقنيين

·التدريب والمجلات والدوريات عن أمن ونظم المعلومات

·إجراءات المتبعة عند الاستغناء عن موظفي الحاسوب أو استقالتهم

·الإجراءات الإدارية والقانونية تجاه الأفراد الذين يسربون المعلومات.

·اعتماد البنك كلياً على التقانة في أداء أعمالها.

الإجراءات الامنية المتبعة في البنوك عينة الدراسة وتشمل

·إجراءات استمرار العمل عند حدوث خلل في النظام والشبكات

·التخلص من الوسائط والمستندات والتقارير

·إجراءات استمرار العمل ومراجعتها وتحديثها

·عمل نسخ وقائية احتياطية للمعلومات وطريقة حفظها

·طريقة حماية شبكات نظم المعلومات بالبنك

·استخدام كلمات السر وحفظها

·تركيب وصيانة الشبكات

·استخدام البرامج الأصلية المرخصة

·وضع إستراتيجية مكافحة الفيروسات

·تفعيل برامج ونظم حماية المعلومات

·إجراءات الدخول لنظم الحاسوب

·الاختراق وسوء استخدام النظام

·المصرح لهم للدخول في نظم البنك

الإجراءات الرقابية والحماية لدى البنوك عينة الدراسة

·مراجعة وتدقيق نظم المعلومات

·التخويل بإجراء التعديلات على البيانات

·موظفون متخصصون بأمن المعلومات وحمايتها

·سياسات وإجراءات ومواصفات قياسية لأمن المعلومات

·سياسات ومواصفات قياسية لتطوير وتشغيل نظم المعلومات

·متخصصون لمراجعة وتدقيق نظم المعلومات

·تطبيق سياسات نظم المعلومات بالبنك

·الدخول لغرفة الحاسوب

·إدخال الأجهزة إلى البنك وإخراجها

·الإجراءات المتبعة حيال نظم المعلومات بعد نهاية ساعات العمل الرسمية

٤. اختبارات تجريبية لبعض إجراءات الأمان وذلك عن طريق إجراء اختبارات فعلية في المصرف العقاري، وأيضاً من خلال الاختبار الذي تم إجراؤه لفحص الثغرات وإعطاء تقرير تفصيلي لمعرفة مناطق الضعف والثغرات الموجودة في هذا الموقع وبالتالي تعديلها وتحديث ما يلزم منها. الأداة التي استخدمت في هذا الإختبار هي: **Acunetix Website Audit**
وذلك لاختبار الفرضية الثانية

بعد ذلك تم تحليل المعلومات التي تم جمعها ومطابقتها مع المرجعية ذات العلاقة (معايير الجودة ومعايير **Cobit** ومقومات أمن المعلومات) ثم تم استخلاص أوجه الاختلاف والتشابه بين المعايير المرجعية للمقارنة وبين الواقع في المصارف ذات العلاقة. كما تم معالجة البيانات التي تم الحصول عليها من خلال أداة الدراسة باستخدام البرنامج الإحصائي SPSS (Statistical Package for Social Sciences) حيث تم استخدام التحليلات الوصفية و استخدام المتوسطات الحسابية والانحرافات المعيارية ،كما تم استخدام اختبار ت ستودينيت لاختبار الفرضيات .

١-٢ مجتمع الدراسة وعينتها:

مجتمع الدراسة هو المصارف العاملة في سورية التي يبلغ عددها: **23** مصرفا، منها ٦ مصارف حكومية و**17** مصارفاً خاصاً.

تكونت عينة الدراسة من مصرفين: المصرف العقاري باعتباره مصرفا حكوميا، ومصرف "عودة" كمصرف خاص، حيث شملت هذه العينة جميع العاملين في قسم نظم المعلومات وقد تم اعتماد هذين المصرفيين دون غيرهما لسببين: أولاً لأن هذين المصرفيين متميزان بتجربتيهما الرائدتين في مجال العمل المصرفي الإلكتروني، على حين أن كثيراً من المصارف الأخرى لم تقدم بعد خدمات مصرفية إلكترونية . ثانياً نظرا لعدم تعاون المصارف الأخرى مع الباحثة لإنجاز العمل.

١-٣ محددات الدراسة:

واجهت الدراسة عدة صعوبات تجلت في:

- تحفظ شديد من قبل المصارف الخاصة على تقديم المعلومات التي تساهم في إجراء عملية المقارنة
- عدد المصارف الخاصة التي تستخدم Internet Banking محدود جداً وكون مصرف عودة هو الوحيد الذي لديه Switch ، تم اختياره لكي تكون عملية المقارنة متماثلة

وفيما يلي تعريف بالخدمات التي يقدمها المصرفيين المذكورين:

١-٤الخدمات الإلكترونية للمصرف العقاري

- خدمة الصراف الألي
- بنك الإنترنت
- خدمات نقاط البيع [١]
- سيريا كارد
- بطاقات الائتمان
- خدمة توطين الرواتب (التوطين المصرفي Salary File)
- خدمة الرسائل القصيرة
- تسديد الفواتير
- الحسابات والودائع
- القروض العقارية

١-٥الخدمات التي يقدمها مصرف عودة

يقدّم مصرف عودة – سورية مجموعة واسعة من الخدمات التجارية ومنتجات البيع بالتجزئة، من خلال عمليّات مصرفيّة تندرج تحت الفئات التالية:

١. الحسابات المصرفية، وبشكلٍ خاص حسابات التوفير، والحسابات الجارية، والودائع الزمنية، وحسابات الحوالات.

٢. القروض التجارية والتسهيلات المتنوّعة، بما فيها تمويل مشاريع طويلة ومتوسّطة الأجل، والاعتمادات المستندية والكفالات.

[١] : لايمكن استخدام هذه الميزة على الموقع الجديد لبنك الإنترنت حالياً، وسيتم تفعيلها قريباً

٣. قروض المؤسسات الصغيرة والمتوسّطة الحجم الموجّهة إلى أصحاب الحرف والمهن الحرّة، والمنشآت الصغيرة والمتوسّطة الحجم، ومؤخراً تم إطلاق قرض العاملين في القطاع الصحي (الأطباء، والصيادلة، والمخبريين) بحد أدنى وسقف غير محدد لمبلغ القرض.

٤. منتجات البيع بالتجزئة: القروض الشخصية، والقروض السكنية، وقروض السيارات، والخدمات المصرفية الإلكترونية كبطاقات الائتمان العالمية وبطاقة التسوق على الإنترنت، وقرض الحاسب المحمول، وقرض الشاشات المسطّحة، وقرض سخّان الطاقة الشمسية، قرض كاميرات الفيديو والكاميرات الرقمية، بالإضافة إلى المنتجات التأمينية المصرفية، وخدمات التوطين المختلفة للرواتب والفواتير

وفي مبادرة رائدة في سورية، أطلق مصرف عودة – سورية وبالتعاون مع ماستركارد العالمية خدمة مصرفية جديدة في ميدان البطاقات الإلكترونية وهي بطاقة الدفع الفوري ٢٤/٧ المحلية والعالمية والتي تتمتع بمميزات عديدة، وذلك بعد حصوله على الترخيص الرسمي من ماستركارد العالمية التي تخول مصرف عودة سورية إصدار بطاقات ماستركارد على اختلاف أنواعها (دفع مباشر، ائتمان، دفع مسبق) كما تخوله توزيع نقاط البيع POS لدى التجار والصرافات الآلية على جميع الأراضي السورية بالإضافة لقبول كافة بطاقات ماستركارد على أجهزة الصراف الآلي الخاصة بمصرف عودة سورية. لقد جاء إطلاق هذه البطاقة تطبيقاً للقرار رقم ٣٩٦ /م ن / ب ١ الصادر عن مجلس النقد والتسليف في سورية.

وضع مصرف عودة خطة استراتيجية للتركيز على سوق الخدمات الإلكترونية والبطاقات، والتي تهدف إلى تعزيز موقعه في هذا السوق ليس فقط كإحدى المؤسسات المالية الرائدة في المنطقة، بل كأحد أكثر البنوك إبداعاً في إصدار بطاقات الدفع الإلكترونية وتقديم الخدمات الإلكترونية. وكانت تتمثل خطته، بالنسبة للسوق السوري، بتقديم العديد من حلول الدفع الإلكترونية الموجهة للافراد والشركات والتجار عبر إصدار عدد كبير ومتنوع من البطاقات المصرفية، وتطوير شبكة نقاط البيع POS والصرافات الآلية في سوريا وتسويق نظام الدفع عبر الإنترنت والتجارة الإلكترونية E-commerce.

وبعد استعراض الخدمات الإلكترونية المتطورة التي يقدمها المصرفان مع التنويه أن المصرف العقاري خطى خطوة كبيرة باتجاه الدفع الإلكتروني تميزه عن مصرف عودة بات من الواضح أهمية بيان مدى كفاءة نظم المعلومات للمصرفيين في حماية البيانات والمعلومات لديهم .

٢-المبحث الثاني: إجراءات أمن البيانات والمعلومات المطبقة في المصارف

تم تحليل نظام المعلومات المحاسبية لتحديد نقاط القوة والضعف الموجودة باستخدام تحليل "سووت" (SWOT analysis[١]) وهو تحليل "القوة، مواطن الضعف، الفرصة والتهديدات" (**S**trength, **W**eakness, **O**pportunities &**T**hreats) " للأنظمة الإلكترونية. اعتمد التحليل على إطارين مرجعيين:

١-إطار COBIT

٢-إطار الخدمات الائتمانية (خدمات الثقة) Trust Services

٢-١ توصيف النظام المصرفي في مصرفي عينة الدراسة Core Banking في المصرف العقاري

النظام الذي يعمل على أساسه هو نظام Phenix، (الشكل رقم ١٠). يمثل هذا النظام نواة كل عمل مصرفي يستند إلى نظام محاسبي متكامل. يتألف النظام من:

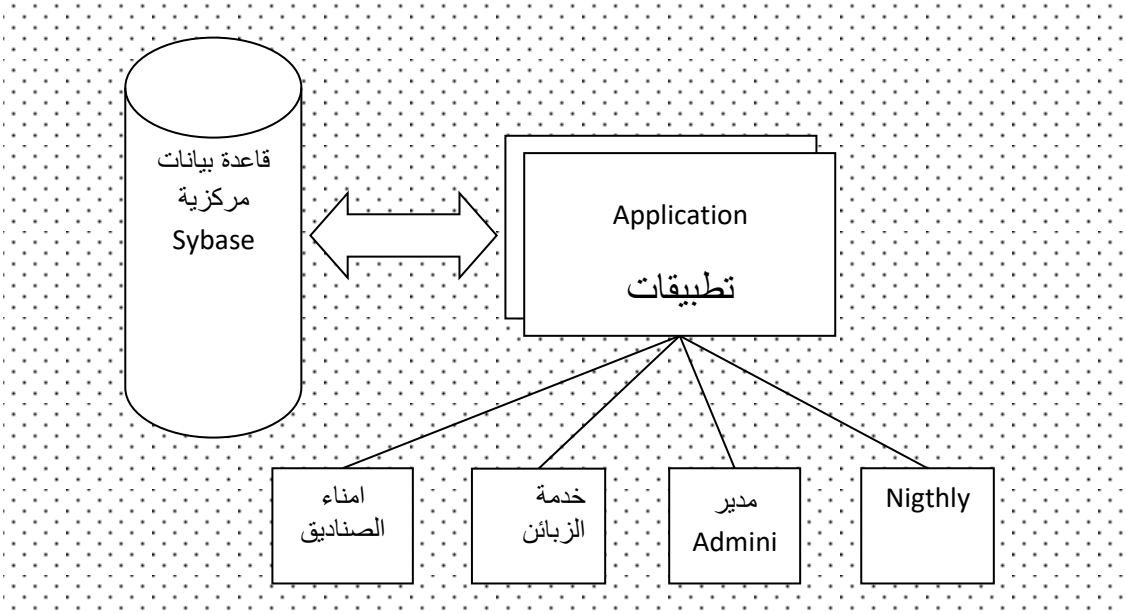
١- قاعدة بيانات مركزية Sybase.

٢- تطبيقات Applications. وهذه تتفرع وترتبط: بأمناء الصناديق Tellers، – بإيداعات ومسحوبات العملاء، – بخدمة الزبائن CS (يشمل كل ما يخص التعامل مع الزبائن من فتح حساب إلى الودائع والقروض وحساب التوفير.. . . . الخ) – بمدير قواعد البيانات

[١]- **تحليل الفرص والمخاطر SWOT وهو اختصار لـ** Strength, **W**eakness, **O**pportunities &Threats ويعتبر تحليل **SWOT** أداة مفيدة لفهم عمل المؤسسة من الداخل والخارج. حيث يأخذ تحليل القوة والضعف بالاعتبار العوامل الداخلية للشركة أو المؤسسة، ويصنف كل عامل من هذه العوامل كعامل قوة أو ضعف بالنسبة لها. حيث يهتم تحليل الفرص والمخاطر SWOT بالبيئة الداخلية والخارجية لأي شركة أو مشروع استثماري في محأولة للتركيز على اتجاهها في المستقبل.. **فنستطيع من خلال هذا التحليل** أن نفهم الفرص المتوفرة لنا والتي يمكن أن تكون على شكل تكنولوجيا جديدة أو تطوير البنية التحتية التي يمكن أن توسع قاعدة الزبائن.. فهو يسمح ببناء قوة المؤسسة وخلق فرص جديدة للوصول لمزيد من الزبائن..

Administrator الذي يقوم بدوره بتحديد صلاحيات الموظفين ومحددات المصرف بشكل عام، – وبنظام العمل "الليلي"Nightly.

٣- واجهات تسهل العمل مع قاعدة بيانات



الشكل (١٠)Core banking في المصرف العقاري

المصدر:الشكل من إعداد الباحثة

يبدأ نظام **العمل الليلي** Nightly في المصرف العقاري في نهاية كل يوم عمل، بعد إغلاق امناء الصناديق لصناديقهم. بداية العمل تكون في الرابعة والنصف مساءاً وتنتهي الساعة العاشرة ليلاً. تقوم مجموعة العمل الليلي بإقفال الحسابات. أثناء عملية الإقفال تظهر بعض المشاكل كأخطاء فنية وأخطاء محاسبية تعالج من قبل الموظف المختص في صباح اليوم التالي كما في الجدول التالي.

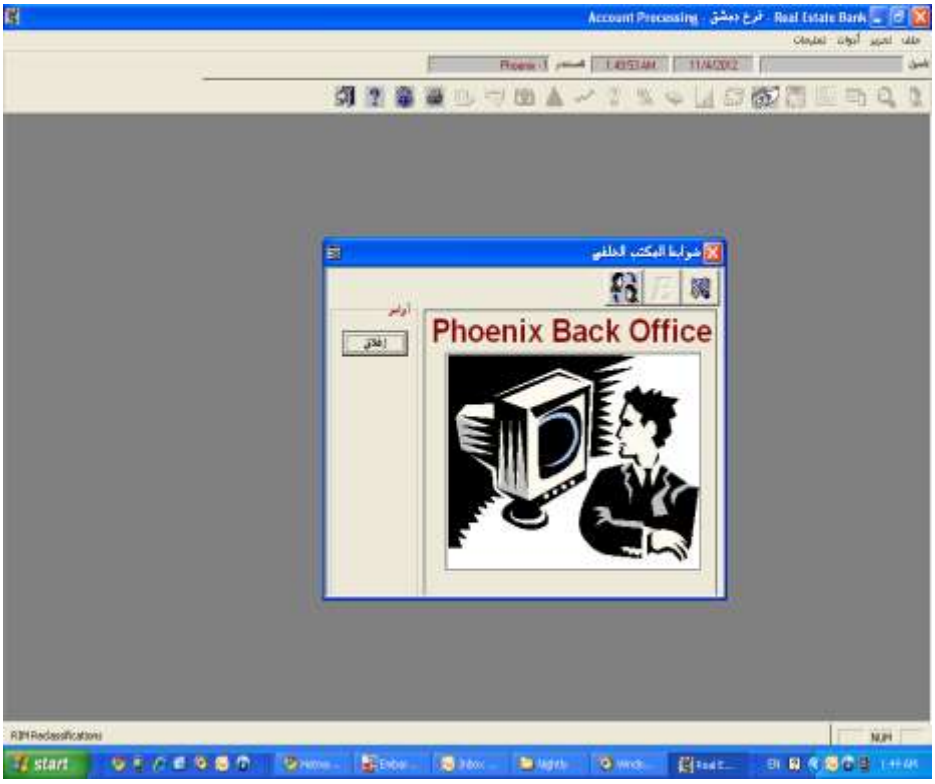
اخطاء تقنية قد تظهر اثناء إغلاق الحساب الجاري
17603 Account has holds placed against it. There are one or more holds placed against this account. A closing withdrawal/redemption transaction cannot be posted to an account until all holds placed against the account have been removed.
17601Account has an invalid.. A closing withdrawal/redemption cannot be posted to an account with a status of 'Closed'
17662Account has a plan with invalid status. The retirement plan for this account does not allow distribution and/or the distribution for the plan was not set up properly.

17651Invalid account and/or account type. The account number and/or account type specified for this transaction is invalid. Verify the information and re-post the transaction. If this error persists, contact Phoenix International.
17654 Could not close account. ^The system could not set the account's status to 'Closed'
.. display record. The system could not update one or more fields on this account's deposit display record

الجدول رقم (٢) اخطاء تقنية قد تظهر أثناء إغلاق الحساب الجاري

تتم عمليات التسوية للمشكلات وتصحيح الأخطاءعن طريق ما يسمى بـ "**ضوابط المكتب الخلفي**" وحسب التسلسل التالي:

١- يفتح ما يسمح بضوابط المكتب الخلفي وهي النافذة التي يتم عن طريقها البدء بتصحيح الأخطاء المحاسبية وذلك حسب الشكل رقم (١١)



الشكل رقم (١١) ضوابط المكتب الخلفي

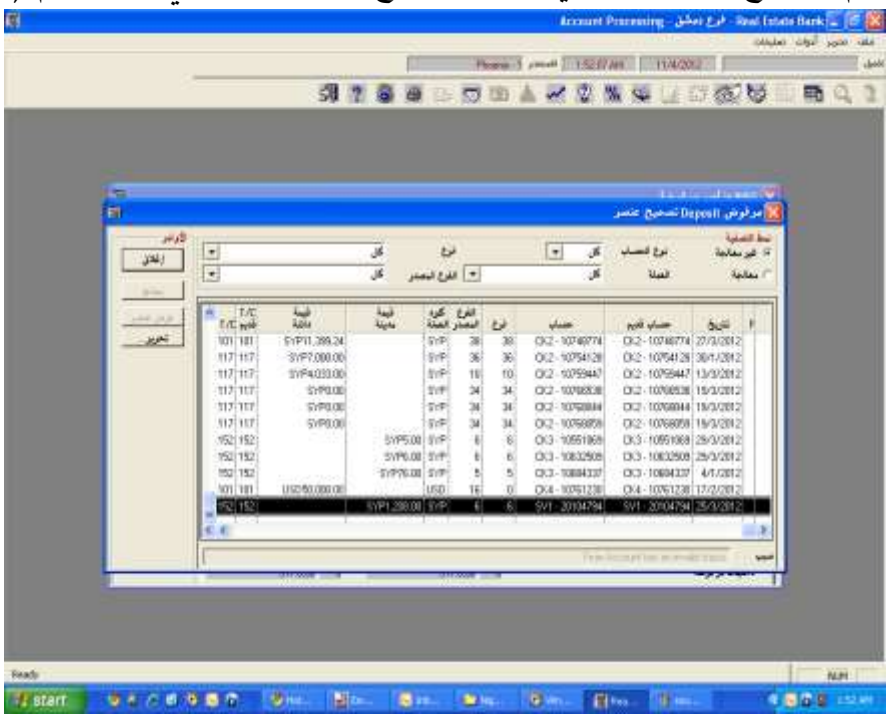
المصدر نظام phoenix في العقاري

٢- ثم يتم الانتقال إلى معالجة الخطأ عن طريق تحرير العناصر غير المرصدة وذلك كما هو واضح في الشكل رقم (١٢)

الشكل رقم (١٢) تحرير العناصر غير المرصدة

نفس المصدر السابق

٣- ثم يتم تصحيح الخطأ عن طريق نافذة تصحيح عنصركما هو في الشكل رقم (١٣)



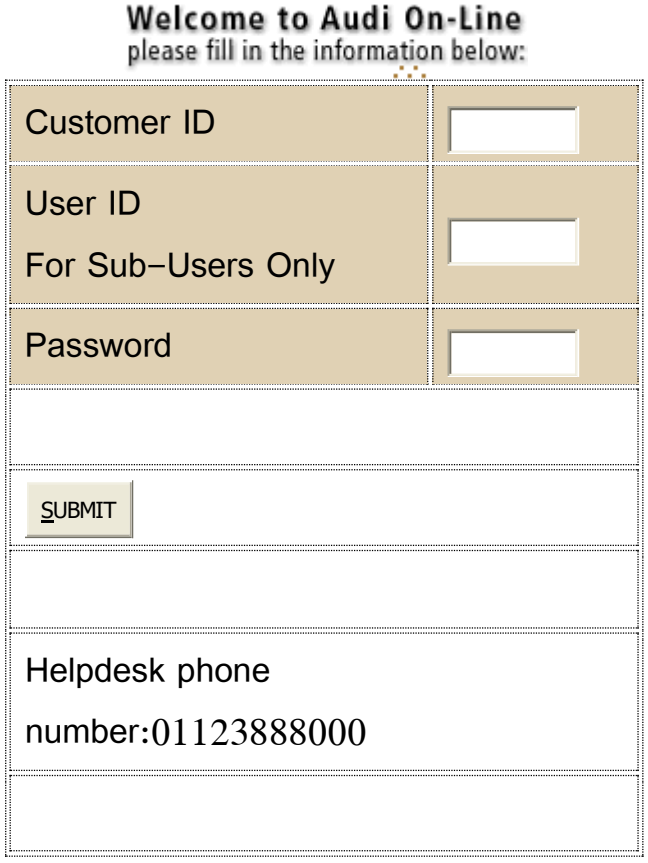
الشكل (١٣) نافذة تصحيح عنصر

نفس المصدر السابق

مصرف عودة

أما مصرف عودة (Core Banking) فإنه يعمل على نظام Bank mate من شركة ADTEK. هذا النظام شبيه بنظام المصرف العقاري. يقوم على قاعدة بيانات مركزية وتطبيقات Applications تتفرع وترتبط: بأمناء الصناديق Tellers – الإيداعات والسحوبات التي تتم عبر العملاء – خدمة الزبائن (يشمل كل ما يخص التعامل مع الزبائن من فتح حساب إلى الودائع والقروض وحساب التوفير.. . . . الخ) – ومدير قواعد البيانات Administrator الذي يقوم بدوره بتحديد صلاحيات الموظفين ومحددات المصرف بشكل عام. كما أن لديه واجهات تسهل العمل مع قاعدة البيانات.

يوزع لكل موظف قوائم خاصة حسب صلاحياته والمهام الموكلة له ولكل موظف مستوى محدد يسمح بدرجة معينة من العمليات وإذا تجاوزت هذه الدرجة يجب الموافقة على العملية من المستوى الأعلى وهكذا ، فيما يلي الصفحة التي يتم من خلالها الدخول إلى مصرف عودة On Line



الشكل (١٤) صفحة عودةOn Line

المصدر : موقع مصرف عودة على الانترنت

منافع Audi On– Line إن الخدمة الآنية عبر الإنترنت تمكن عميل مصرف عودة سورية من:

١. الاطلاع على أرصدة الحسابات وتفاصيل حركاتها.
٢. الاطلاع على العمليات المنفذة على الحسابات بين تاريخين معينين
٣. فرز حركات الحسابات حسب التاريخ أو القيمة أو طبيعة الحركة (سحب أو إيداع)
٤. تحميل نتائج البحث وحفظها في ملفات إلكترونية.
٥. التحويل الداخلي بين حساباته المدرجة تحت رقم تعريف (ID) الخاص به
٦. ربط جميع الحسابات الخاصة به (الشخصية و/ أو المشتركة) للاطلاع عليها كافة عند الدخول، باستعمال اسم تعريف واحد وكلمة مرور واحدة

بالإضافة إلى ذلك يمكن الاستفادة من إحدى الميزات الجديدة التالية أو جميعها:

١. طلب دفتر شيكات عبر Audi On– Line: يمكن لمستخدمي Audi On– Line طلب دفتر شيكات عبر هذه الخدمة. في حال كان العميل يطلب دفتر شيكات للمرة الأولى، يتوجب عليه عندئذ زيارة فرعه للتقدم بالطلب. في حال وافق المصرف على إصدار دفتر الشيكات، سيتم استلامه من الفرع المحدد خلال مدة قصيرة من تاريخ التقدم بالطلب.
٢. طلب كشف حساب رسمي عبر Audi On– Line: يمكن لمستتخدميAudi On– Line طلب كشف حساب رسمي عبر Audi On– Line، حيث يتم تحديد فترة الكشف (على ألا تتجاوز السنة). يتم استلام الكشف من فرع العميل خلال مدة قصيرة من تاريخ التقدم بالطلب.
٣. إرسال الاستفسارات والشكاوى: يمكن لمستخدمي Audi On– Line تدوين أي استفسارات أو شكاوى أو اقراحات حيث يتوجب تحديد الفرع ورقم التعريف الخاص بالعميل (ID) وسيتولى المصرف الرد على الاستفسارات والشكاوى بحسب طبيعتها وكما يرتئي.
٤. تفعيل خدمة التحويل الداخلي للحسابات المربوطة Group: أصبح بإمكان مستخدمي Audi On– Line المستفدين من ميزة ربط الحسابات طلب تفعيل خدمة التحويل الداخلي بين حساباتهم (PLs) المدرجة تحت أرقام تعريف شخصية أو حساباتهم المشتركة وبغية الحصول على هذه الخدمة، يتوجب على العميل زيارة فرعه لطلب تفعيلها على حساباته المربوطة Grouped. للمحافظة على أمان العمليات، سوف يطلب من العميل تغيير كلمة المرور لدى أول زيارة للموقع الإلكتروني قبل دخول الصفحة الأولى. كما يمكن للعميل السماح لأشخاص آخرين بدخول حساباته عبر Audi On– Line ومنحهم حق

التصرف بالحسابات كما هو محدد من قبل العميل وبذلك يتوجب إدخال اسم التعريف الإضافي وكلمة المرور لكل شخص.

١- ٢ توصيف الأنظمة الإلكترونية وكيفية حمايتها

في المصرف العقاري:

البنية التحتية تشمتل على:

تجهيزات وتحوي:

- غرفة التحكم: وفيها مركز البيانات Data Center والمخدمات والمبدلات Swtich والموجهات .... الخ.
- الشبكة التي تربط بين المصرف وأقسامه وبين المصرف وفروعه وبين المصرف وصرافاته.

برمجيات وتضم:

١- نظام الـ Core Banking الذي يحوي معلومات عن الزبائن وإيداعاتهم وسحوباتهم وحسابهم وقروضهم وأقساطهم اي كل عمليات السحب والإيداع.

٢- نظام تبديل (تحويل)ATM Swtich الذي هو ATM الصرافات ومخدم خدمة الصرافات ومخدم وصل المصرف بالبنوك الأخرى، بالإضافة إلى نظام توليد البطاقات المصرفية وطباعتها ونظام التحقق منها. تكمن وظيفة ATM في إصدار البطاقات والتحقق منها ودعم بطاقات البنوك الأخرى والربط مع الـ Core Banking. ومن وظائفه الهامة حماية الاتصال بين الصراف والمصرف (Man In The Middle).

٣- نظام مصرف الإنترنت Internet Banking.

٤- نظام الدفع الإلكتروني وهو يؤمن الاتصال بين المصرف ومزودي الفواتير لإتاحة خدمة دفع الفواتير لزبائن المصرف.

٥- نظام أتمتة الفرع Branch Automation الذي يحوي مجموعة البرمجيات التي تتيح لموظفي المصرف في الفروع إجراء العمليات المصرفية للزبائن (فتح حساب-وإيداع – وسحب- ودفع قسط قرض – ودفع فاتورة.. . . الخ).

٦- نظام المجيب الصوتي الآلي الذي يتيح بعض العمليات المصرفية للزبائن عن طريق الهاتف سواء خط أرضي أم موبايل.

٧- نظام قناة الرسائل القصيرة SMS الذي يتيح للزبائن إجراء بعض العمليات المصرفية عن طريق الرسائل القصيرة.

٨- نظام قناة USSD مشابه للرسائل القصيرة وهي قناة الاتصال الدائمة بين الموبايل وبرج الاتصال وهي قناة تفاعلية فيها قوائم تتيح للزبون اختيار الأوامر التي يريدها.

٩- أنظمة أُخرى: وهي الأنظمة التي ليس لها علاقة مباشرة بزبون المصرف مثل أنظمة المستودعات – أنظمة التحكم بالأبواب – أنظمة مراقبة البنية التحتية – أنظمة مراقبة الكاميرات – نظام مراقبة الدوام، الخ.

<u>في مصرف عودة</u>

البنية التحتية تشمتل على:

<u>تجهيزات وتحوي:</u>

- غرفة التحكم: وفيها مركز البيانات Data Center والمخدمات والمبدلات Swtich والموجهات .... الخ.
- الشبكة التي تربط بين المصرف وأقسامه وبين المصرف وفروعه وبين المصرف وصرافاته.

<u>برمجيات وتضم:</u>

١-نظام الـ Core Banking الذي يحوي معلومات عن الزبائن وإيداعاتهم وسحوباتهم وحسابهم وقروضهم وأقساطهم أي كل عمليات السحب والإيداع.

٢-نظام تبديل (تحويل)Swtich ATM الذي هو ATM الصرافات ومخدم خدمة الصرافات ومخدم وصل المصرف بالبنوك الأخرى، بالإضافة إلى نظام توليد البطاقات المصرفية وطباعتها ونظام التحقق منها. تكمن وظيفة ATM في إصدار البطاقات والتحقق منها ودعم بطاقات البنوك الأخرى والربط مع الـ Core Banking. ومن وظائفه الهامة حماية الاتصال بين الصراف والمصرف (Man In The Middle).

٣-نظام عودة اون لاين Audi On- Line.

بعد توصيف الأنظمة الإلكترونية في المصرف العقاري ومصرف عودة بات من الواضح أهمية حماية هذه الأنظمة في عمل المصارف لذلك يجب فحص هذه الأنظمة من خلال تحليل كل قناة من قنواتها وبيان نقاط الضعف والقوة في كل منها والوقوف على الآليات المتبعة في حمايتها .

٢-٣ كيفية حماية المصارف لقنوات الاتصال بين الزبون والمصرف

بما أن معلومات الزبائن تمر عبر هذه القنوات ومن هنا بات حماية هذه القنوات أمن أمراً مهماً،هذه الأهمية تولدت من المخاطر التي تتأتى من الأعمال المصرفية في البيئة الإلكترونية وأنظمة الاتصال وتشغيل البيانات بمختلف أنواعها وبالتالي بات من الضروري تحديد أهداف الأمان لبياناتها ومعلوماتها، ورسم سياساتها التي يجب أن تسهم في بلوغ تلك الأهداف، وترجمة تلك السياسات إلى جملة من التعليمات والإجراءات واجبة التطبيق بحيث يمكن من خلالها ضمان أمن البيانات والمعلومات التي ينتجها النظام.

القناة الأولى: عبر الفرع حيث يتطلب حضور الزبون شخصياً في الفرع ومعرفة هويته ودفتر حسابه.

القناة الثانية:عبر ATM الصراف الآلي يتصل بالفرع عن طريق بطاقة الصراف.

القناة الثالثة: عبر Internet Banking يستطيع الزبون الوصول عن طريق الشبكة.

القناة الرابعة: عبر الهاتف (المجيب الصوتي الآلي)

القناة الخامسة: عبر شبكات الهواتف النقالة "الموبايل" عن طريق الرسائل القصيرة SMS

القناة السادسة: قناة الاتصال الدائمة بين الهاتف الخليوي "الموبايل" وبرج الاتصال

هنا ترى الباحثة أن القناة الأولى فيها محدودية في السعة لاستقبال الزبائن، والتوزع الجغرافي يلعب دوره ايضاً. أما القناة الثانية فمحدوديتها في التوزع الجغرافي للصرافات الآلية وآليات إصدار البطاقات. كما تستقبل الزبائن بالدور. القناة الثالثة ليس لها محدودية الا انها تعرض المصرف لخطر كبير كمحاولات الاختراق، لكنها بالمقابل تعطيه عمل وسمعة وتسهل الخدمات. لذا في مثل هذه القنوات يجب اخذ احتياطات لحماية البيانات والمعلومات أثناء نقلها خلال الشبكة.

٢-٣-١ واقع قنوات الاتصال في المصرف العقاري

/١/ - قناة بنك الإنترنت (IB):

يتم التعرف على الزبون من خلال: اسم المستخدم User name وكلمة السر Password ويجب عدم معرفة كلمة السر إلا من قبل الزبون. يتم الدخول بعدها إلى واجهة خدمات متعددة هي:

١- استعلام عن الرصيد

٢- كشف حساب

٣- التحويل المغلق بين الحسابات، سقفه ١٠٠٠٠٠٠ ل. س بمعدل ٣٠٠٠٠٠ ل. س للحركة الواحدة

٤- التحويل المفتوح من حسابات الزبون لحساب زبون آخر في المصرف ومحدودية المبلغ ٢٠٠٠٠٠ ل. س يوميا و٢٥٠٠٠ ل. س بالحركة الواحدة.

٥- دفع قسط قرض من حساب له أو لأي زبون آخر في المصرف.

٦- الاستعلام عن الأقساط المدفوعة والمتبقية لقرض حصرا لصاحب الحساب.

٧- دفع الفواتير:

- فاتورة سيرياتلSyriatel وMTN
- تحويل رصيد للخطوط لاحقة الدفع ومسبقة الدفع
- دفع اشتراك انترنت لشركة آية
- شراء بطاقات انترنت مسبقة الدفع من شركة آية
- خدمة دفع فواتير الهاتف الثابت ودفع فواتير الكهرباء

٨- التحويل المفتوح المجدول زمنيا.

٢-٣-٢المخاطر التي تتعرض لها الأنظمة الإلكترونية

على خدمة Internet Banking في المصارف عينة الدراسة وكيفية حمايتها

أ-حماية الاتصال بين الزبون والمصرف

- هوية بنك الإنترنت: يمكن خداع الزبائن من خلال السطو على موقع المصرف أو انتحال هوية المصرف بإظهار موقع مشابه لموقع المصرف. من خلال هذه الواجهة يمكن سرقة اسم المستخدم وكلمة المرور عندما يقوم الزبون بإدخالهما.
- هوية الزبون: (كلمة السر واسم المستخدم)لا يمكن لأي شخص أن ينتحل شخصية الزبون إلا من خلال كلمة المرور وهي حاليا مؤلفة من عشرة أرقام.
- التجسس على الاتصال بين الزبون والمصرف. مثال على ذلك إن الاتصال بين الزبون والمصرف موجود عليه طرف ثالث هو مزود خدمة الإنترنت والمؤسسة العامة للاتصالات والإنترنت الدولية وكل الراوتر والسيرفر بكل انحاء العالم, مما يعني أن أي شخص من هذه الاطراف قادر على التجسس على الاتصال لمعرفة كلمة السر واسم المستخدم. والمصرف يقوم بتشفير قناة الاتصال بمفتاح تشفير صعب التخمين وتغييرها عند كل اتصال والمعيار الدولي المستخدم هو بروتوكول اتصال لتأمين الوصلة SSL.
- محاولات خرق السماحيات:

ينقسم مستخدمو بنك الإنترنت إلى:

– مستخدمين عاديين

– مدراء مواقع لهم صلاحية تغيير أو تعديل الحساب

والمصرف يقوم بـ:

– تحديد الأدوار واستخدامها وحماية الوصول إلى تطبيقات تغيير الأدوار والسماحيات

– وضع سياسة صارمة للمدراء، وهي موجودة في المصرف ولكنها سياسات شفهية غير مكتوبة.

وهنا يكمن الخطأ في عدم كتابة السياسة الخاصة بالأدوار وادارة الموقع وعدم تحديثها وتطويرها.

والمشكلة هنا أن أحد الزبائن يستطيع أن يزيد سماحياته من زبون عادي إلى مدير موقع.

- **بالنسبة لكلمة المرور**

–من الممكن اختلاس كلمة المرور في حال وقوف شخص خلف مستخدم الإنترنيت الذي يدخل إلى بنك الإنترنت وهذا ضعف في النظام مثلا يجب أن يكون هناك غرف صغيرة تتسع لشخص واحد امام الجهاز باب الغرفة يفتح باستخدام بطاقة المصرف سارية المفعول. وبهذا الشكل يضمن النظام عدم حدوث مثل هذه الحالة

–إذا اضطر العميل إلى استخدام بنك الإنترنت من حاسب شخص آخر، وكان هذا الحاسب مزودا ببرنامج اسمه (Key Logger)، يقوم البرنامج بتسجيل كل ضغطة على مفتاح من مفاتيح اللوحة ويحتفظ بهم في ملف خاص به. بهذه الطريقة يتم سرقة كلمة السر واسم المستخدم. وهذا ايضاً ضعف في إجراءات الحماية المتبعة لذلك هنا ينصح بمنع إدخال كلمة السر عن طريق لوحة المفاتيح واستبدالها بالفأرة عن طريق اظهار لوحة المفاتيح على الشاشة وينقر عليها باستخدام الفأرة

وهنا ايضا نقع امام مشكلة ال (Mouse Logger) وهو برنامج يسجل كل تحركات الفأرة فنوصي هنا بإظهار لوحة المفاتيح بشكل عشوائي كل مرة بتغيير ترتيب الحروف على لوحة المفاتيح الظاهرة بشكل عشوائي في كل مرة .

ولكن هناك حلاً مثالياً لكل من الحالتين السابقتين وهو :

جزء من كلمة المرور يتم توليده بشكل عشوائي كل فترة زمنية تختلف كل ساعة بواسطة جهاز (Token) هدفه توليد أرقام عشوائية بالتزامن مع المخدم اي التقنية استخدام مولدات أرقام عشوائية متزامنة أي التزامن بين المخدم وجهاز (Token) ومشكلة هذا الجهاز إن كلفته عالية والزبون الذي يريد حماية بياناته ومعلوماته وحسابه البنكي يجب عليه اقتناء هذا الجهاز .

ب.حماية الاتصالات بين بنك الإنترنت والأنظمة الأخرى في المصرف يكون عبر:

- عزل بنك الإنترنت عن كل الأنظمة الداخلية في المصرف والسماح فقط للاتصال بين بنك الإنترنت والأنظمة التي يحتاجها فقط ال Core Banking ونظام دفع الفواتير الإلكترونيوهو محقق في المصارف عينة الدراسة.
- حماية الاتصالات بين بنك الإنترنت والأنظمة التي يحتاجها. والحماية الموجودة هنا تكون من خلال استخدام الجدران الناريةFirewall وقوائم التحكم بسماحيات المرور AccessControl List وهو ما تطبقه المصارف عينة الدراسة

/٢/- قناة نظام المجيب الصوتي الآلي

تتم هذه الخدمة عن طريق رقم هاتف أرضي أو رقم هاتف نقال. كما يتم عن طريق التفاعل مع اسم المستخدم خلال مكالمة هاتفية، من خلال الأرقام الموجودة على أزرار الهاتف. خدمات المجيب الصوتي الآلي هي: الاستعلام عن الرصيد – تحويل مبلغ – دفع فواتير: MTN- Syriatell، الهاتف الثابت والكهرباء.

لكل قناة اتصال بين الزبون والمصرف أوراق اعتماد إلكترونية خاصة يقدمها الزبون لتأكيد هويته. هنا يقدم الزبون رقم الهاتف ورقم حسابه في المصرف والرقم السري لكل حساب.

وهنا يمكن التنصت على خط الهاتف وذلك عن طريق أخذ فرع من خط الهاتف وبطريقة محددة يستطيع أخذ المعلومات الحساسة المتبادلة خلال المكالمة ومنها كلمة السر. الحل يكون بعدم ثبات كلمة السر أو كلمة السر المتغيرة ومن آليتها:

كلمات السر التي تستخدم لمرة واحدة فقط. ومشكلتها هي توزيع كلمات السر المولدة على الزبائن مثلاً لكل زبون ١٠٠٠ كلمة سر والملف الذي يعطى للزبون مشفر ويفترض كل ستة اشهر أن يولد ملف جديد. يمكن إعادة إظهار الأرقام المستخدمة في المكالمة من خلال زر Redial. الحل هو عادة تنبيه الزبون لوجود المخاطر الامنية المتعلقة بهذا الموضوع.

/٣/-قناة SMS

يتم خلال هذه القناة إرسال الأوامر للمصرف على شكل رسائل قصيرة. يقوم المصرف بالاستجابة لها برسائل. الخدمات التي تقدمها هي: الاستعلام عن الرصيد, وكشف حساب مختصر, ودفع الفواتير, ودفع القرض.

هوية الزبون هو رقم هاتفه النقال وكلمة سر معتمدة. هذه القناة لها محدودية لأن الرسالة لها طولاً محدداً والجواب أيضا له طول محدد ومكلفة والرسائل تمر عبر مزودات خدمة الموبايل

الذي هو طرف ثالث, كما أن رسائل SMS لا تشفّر ولا تحمى أي نص صريح وواضح حيث يجب أن ينتبه الزبون أنه باشتراكه بهذه الميزة سيرفع عن نفسه السرية المصرفية.

السؤال الذي يطرح نفسه هنا: هل يمكن حماية المعطيات الحساسة مثل رقم الحساب – الرصيد– كشوف الحسابات – الرقم السري – والفواتير؟ الجواب لا يمكن، لأنه لا يوجد تشفير. هنا المشكلة غير قابلة للحل لأن الرسالة نص صريح وواضح. لكن الذي يمكن حمايته هنا هو هوية الزبون عن طريق جعل كلمة السر ديناميكية وليست ثابتة أو استخدام الـTokken.

/٤/ –قناة USSD

هذه القناة لا تزال قيد الإطلاق

/٥/ –الصراف الآلي Switch ATM

هو الوسيط بين طريقة الدفع الإلكتروني (البطاقة) وبين CoreBanking وهو في المصرف العقاري قسمان:

- صراف خاص بالعقاري
- قسم يرتبط مع(مبدِّل أو مُحَوِّل)Switch آخر

طريقة التخاطب بين المبدّل(أو مفتاح التبديل) Switch والصراف هو مفتاح تشفير(HSM)

أنواع الصرافات:

- Banket
- NCR
- Win core

يعتبر NCR أحدث الصرافات الموجودة لدى العقاري من ميزاته أن خزنته أثقل خزنة بالوزن وآلية حمايتها تعتبر الأقوى بين الصرافات عالمياً وتستخدم الهواء في ضخ الأموال.

الأساليب المتبعة في حماية ATM:

١- يتعامل المصرف العقاري مع شركات Visa وMaster ويفرض على المصرف تطبيقه لمعايير الايزو 8583 حتى تتعامل هذه الشركات مع المصرف وبالتالي يحقق المصرف اسلوب الحماية المطلوب.

٢- في الصرافات كاميرات تسجل كل عملية سحب فنظام التشغيل التابع للكاميرا يخاطب نظاماً آخر (Icome) وهومخدِّم (سيرفر) مربوط مع المبدّلSwitch تأخذ هذه الكاميرات ثلاث لقطات للزبون أثناء سحبه بالبطاقة من الصراف.

٣- يوجد على البطاقات التابعة للصرافات شريط ممغنط وهو اسلوب الحماية المتبع لحماية البطاقة.

فيما يلي مقارنة بين قنوات المصرف تتجلى فيها النقاط التالية:

	نظام المجيب الصوتي الآلي IVR	قناة SMS	الصرافATM	بنكالإنترنت Internet Banking
محدودية القناة	لها محدودية في التفاعل لأنها أرقام فقط	لها محدودية	محدود التفاعل والاظهار	غير محدود بالإظهار والتفاعل
التشفير والحماية	تشفر وتحمى	لا تشفر ولا تحمى	تشفر وتحمى	تشفر وتحمى
عزل القناة	يجب عزلها جميعهاعن الأنظمة الداخلية بالمصرف شبكيا وبرمجياً			

الجدول رقم (٣) مقارنة بين قنوات المصرف العقاري

منظومة الدفع الإلكتروني:

يقدم المصرف العقاري بوابة الدفع الإلكتروني (بوابة العقاري) كوسيلة للدفع والتحصيل من خلال العديد من القنوات كشبكة الإنترنت أو الهاتف أو الموبايل (خدمة الرسائل القصيرة) إضافة إلى أجهزة الصراف الآلي ونقاط البيع.

وهي تشابه إلى حد كبير عملية الدفع من خلال ال visa card والبطاقات الأخرى للدفع الإلكتروني إضافة إلى أنها موثوقة أكثر كونها تتم لدى المصرف العقاري الذي يؤمن هذه الحماية لنقل المعلومات.

تعتبر هذه البوابة ذات أهمية للشركات التي لا تقدم خدمات لدى المصرف العقاري وتريد أن تسمح لزبائنها بشراء منتجاتها أو تحصيل رسومها عن طريق الإنترنت.

ومن خلال الإحصائيات التي قمنا بها بين عام ٢٠٠٧ و ٢٠١١(ملحق رقم ١) التي تبين التطور الشهري الملحوظ لعمليات الدفع الإلكتروني للشركتي MTN و Syria tell وهذا يدل على أن الخدمة موثوقة بين المصرف وشركة الاتصالات فنظام بوابة الدفع الإلكتروني في المصرف هو **تكامل لأنظمة عديدة**، منها أنظمة المؤسسات المستفيدة خارج المصرف، ومنها الأنظمة التالية الخاصة بالبنك:

١. النظام المصرفي Core Banking.
٢. نظام محولة الصرافات الآلية ATM Switch.
٣. نظام بنك الإنترنت Internet Banking.

٤. النظام الوسيط لدفع الفواتير الآني Online Bill Payment Gateway(OBPG)

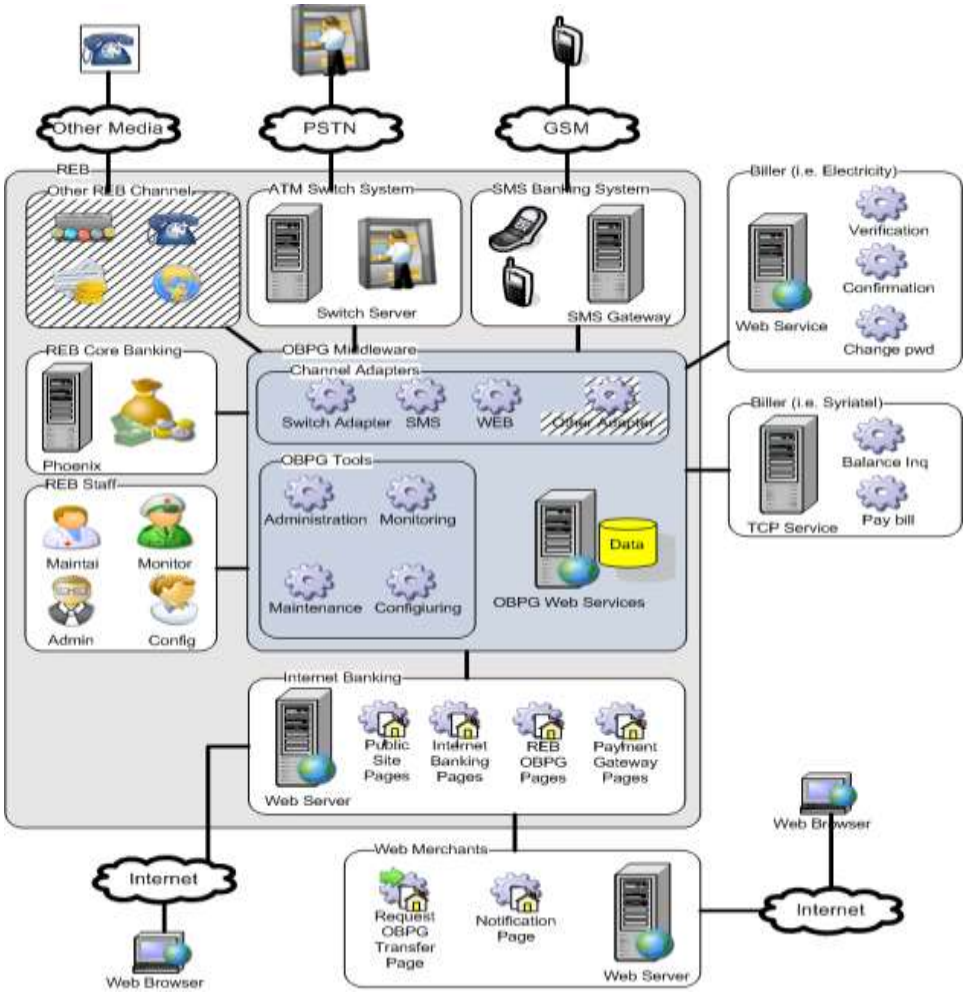
٥. بوابة التجارة الإلكترونية على موقع بنك الإنترنت، وقد قدمت هذه البوابة في مؤتمر الحكومة الإلكترونية الأول لعام ٢٠٠٧.

٦. نظام المجيب الصوتي.

٧. نظام طلبات الرسائل القصيرة.

٨. البنية التحتية الاعتيادية الموجودة في المصرف وفروعه (كالشبكة الداخلية)، وبنية الربط مع المؤسسات والجهات الخارجية.

- تعدد القنوات
- تعدد المفوترين
- تعدد الخدمات
- SOA



الشكل (١٥)بنية النظام في بوابة الدفع الإلكتروني

تختلف آليات حماية الاتصالات مع مزودي الفواتير باختلاف التقنيات التي يستخدمها هؤلاء المزودون. ولكن هناك أساسيات يجب تنفيذها دائما وهي عبارة عن مقومات لأمن المعلومات:

أ. التأكد من الهويات Authenticationأي ضمان هوية طرفي الاتصال وهي مطبقة من المصرفيين عن طريق الشهادة الرقمية المعتمدة من قبل الطرفين معاً واستخدام تقنية التحدي والجواب كاسم المستخدم وكلمة المرور.

ب. التخويل (أي منح الصلاحيات) Authorization أي التأكد أن طرفي الاتصال مخولان بالعمليات التي تمت بهذا الاتصال وآلية تنفيذها هي توثيق الادوار والسماحيات وهو معتمد من قبل المصرفيين .

ت. التشفير للمعلومات الحساسة: هو استخدام خوارزميات التشفير المعيارية بغرض حماية المعلومات المتناقلة من الانكشاف لطرف ثالث مثل اسم المستخدم وكلمة المرور. وآلية تنفيذها: تشفير متناظر وتشفير غير متناظر. أما المشكلة الأساسية هنا هي تبادل مفاتيح التشفير غالباً يتم عن طريق قناة غير القناة المعتمدة للاتصال.

ث. الأختام الزمنية Time Stamping وهو مطبق من المصرفيين باستخدام . ختم زمني على كل رسالة متبادلة والهدف منه التأكد أن كل رسالة لها زمن محدد (زمن صلاحية).

ج. عدم الإنكار Nun Repudiation: عدم إنكار الإرسال يتحقق المستقبل من عدم قدرة المرسل على إنكار الرسالة. وهي مستخدمة في المصرفيين عن طريق التوقيع الرقمي.

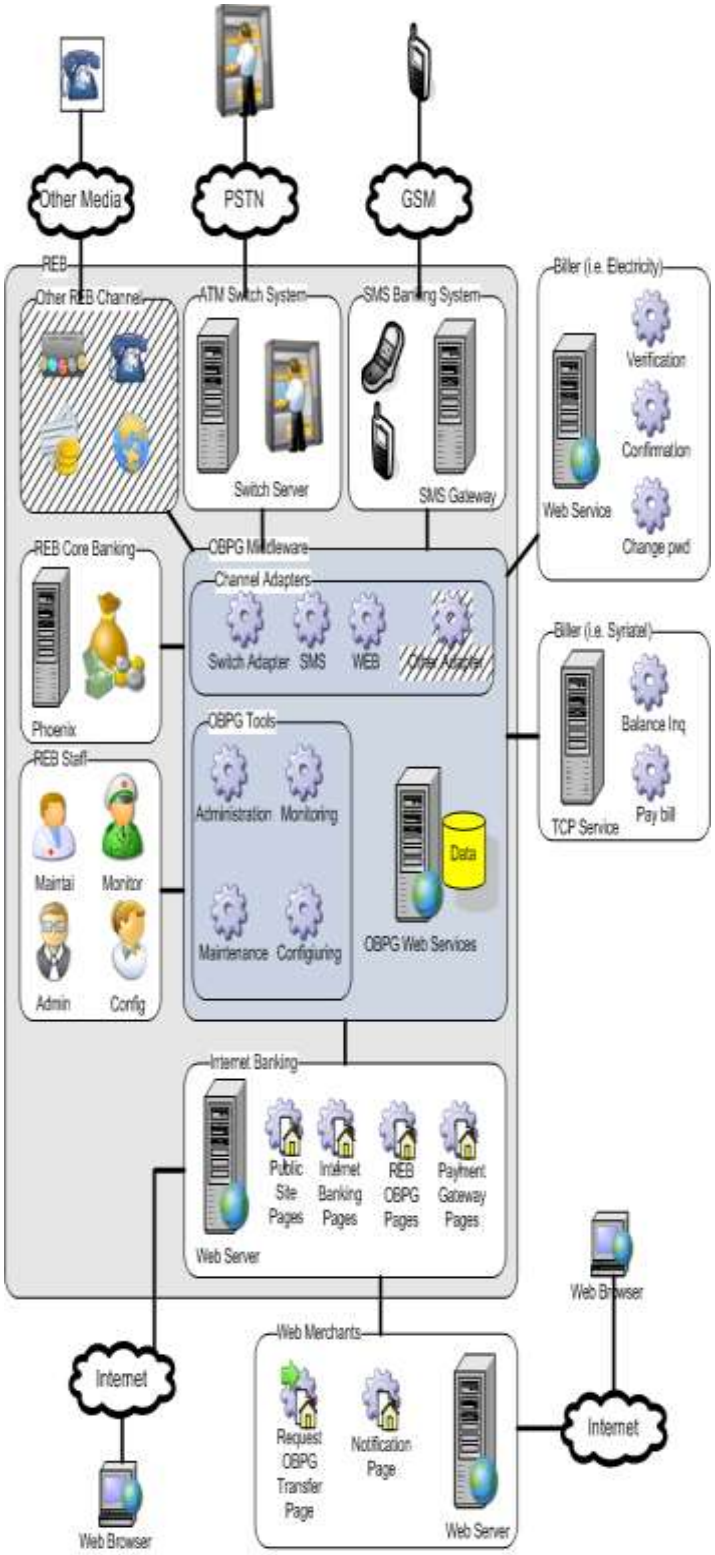
ولكن ما لفت انتباه الباحثة اثناء عملية التحليل أن أحد الزبائن قام بعدة عمليات تحويل رصيد إلى خط مسبق الدفع، في أحد مزودي خدمة الهاتف الجوال، وذلك بعد حوالي الثالثة مساءً. وقتها لم تستطع شركة الاتصالات معالجة عمليات التحويل بشكل فوري (خلال الوقت المطلوب). بعد عملية التحويل هذه قام الزبون بتحويل خطه إلى خط لاحق الدفع. في صباح اليوم التالي، قبل الساعة الثامنة (وقت اكتشاف موظفي المصرف المشكلة)، حاول موظف المصرف إتمام العملية ولكن بسبب تحويل الزبون خطه إلى خط لاحق الدفع أصبحت العملية غير قابلة للإتمام أبداً، مع أن عملية الدفع قد تمت أي جرى إنقاص المبلغ من حساب الزبون الذي قام بعملية التحويل والزبون المحول له لم يستفد منها. هنا القانون لا يتيح للمصرف إلغاء عملية التحويل المالي. وإذا قام المصرف بإلغاء التحويل لا يوجد قانون يضمن عدم اعتراض شركة مزودي الخدمة على الموضوع.

المصرف حل المشكلة بأن ألغى التحويل بناء على اتفاقية بين المصرف ومزودي الخدمة، تلزم مزود الخدمة على عدم الاعتراض على إلغاء التحويل. يتضح هنا أن القوانين التشريعية التي تحكم عمليات الدفع الإلكتروني غير كافية وغير واضحة, كما أن بعض مزودي الخدمة ليس لديهم تخطيط أمني إلى الدرجة التي يتطلبها العمل المصرفي.

أما القنوات الواجب حمايتها في البوابة فهي :

- إن الوصلات الإلكترونية التي تحتاج الحماية هي
  - من الزبون إلى القناة
  - من القناة إلى نظام الدفع الإلكتروني
  - من نظام الدفع الإلكتروني إلى النظام المصرفي
  - من نظام الدفع الإلكتروني إلى أنظمة الجباية لمزودي الخدمات
- من التقنيات المستخدمة لتأمين تلك الوصلات
  - التحقق من الهوية باستخدام شهادات رقمية أو أسماء مستخدمين وكلمات سر
  - التشفير: سواءً المتناظر أم غير المتناظر
  - بروتوكلات الاتصالات الآمنة كـ SSL وIPSEC
  - السماحيات: ربط المستخدمين بالأدوار
  - التدقيق المستمر Real-time Auditing

- Channel-OBPG
- OBPG-Core Banking
- OBPG-Operator
- Customer-Channel



الشكل (١٦) القنوات الواجب حمايتها

3-المبحث الثالث: مقارنة واقع أمن المعلومات في المصارف بمعايير الجودة ومعايير cobit بهدف تقييم كفاءة النظام

بنتيجة التحليل وفق SWOT تبين أن بوابة العقاري وعودة حققت بعض أهدافها بما ينسجم مع معايير COBIT و ISO (٢٧٠٠١) وذلك وفق نقاط قوة تتجلى بالجدول التالي:

	المصرف العقاري	مصرف عودة
١-الأمن والحماية	أ. حماية كافة الاتصالات الإلكترونية بين أجزاء البوابة والأنظمة الأخرى المختلفة. ب.التخطيط لسياسات أمنية معيارية والصرامة في تطبيقها. ت.استخدام تقنيات الحماية الحديثة، ومنها: • التحقق من الهوية باستخدام الشهادات الرقمية (التوقيع الرقمي)، وغيرها كأسماء المستخدمين وكلمات المرور. • تقنيات التشفير (المتناظر وغير المتناظر) الحديثة. • بروتوكولات الاتصال الآمنة SSL وIPSEC. • ربط السماحيات بالأدوار Role-based Authorization. ث.التدقيق المستمر Real-time Auditing. ج. تنفيذ اختبارات الأمن والاختراق Vulnerability Tests بشكل دوري.	أ. حماية كافة الاتصالات الإلكترونية بين أجزاء البوابة والأنظمة الأخرى المختلفةفجميع الاتصالات مشفرة باحدث نظم التشفير العالمية وعن طريق تجهيزات نوعية من احدث الأنواع العالمية. ب.التخطيط لسياسات أمنية معيارية والصرامة في تطبيقها. منذ اطلاق البوابة قام المصرف بشكل دوري ودائم بتطبيق معايير امنية عالمية والتطوير عليها وتحديثها بشكل لحظي بما يتوافق مع احتياجات المصرف والزبائن ومراقبة تطبيقها عبر عدة طبقات من التدقيق: أ. استخدام تقنيات الحماية الحديثة، ومنها: • التحقق من الهوية باستخدام الشهادات الرقمية (التوقيع الرقمي)، وغيرها كأسماء المستخدمين وكلمات المرور. بالإضافة لما ذكر من قبل العقاري يقوم المصرف باعتماد أعلى معايير حماية كلمات المرور مثل التغيير الدوري وعدم السماح بكلمات السر البسيطة • تقنيات التشفير (المتناظر وغير المتناظر) الحديثة • بروتوكولات الاتصال الآمنة SSL وIPSEC. • ربط السماحيات بالأدوار Role-base Authorization. ب.التدقيق المستمر Real-time Auditing. من قبل جهات خارجية معتمدة ومن قبل موظفي المصرف المعتمدين من المصرف المركزي

		ت.تنفيذ اختبارات الأمن والاختراق Vulnerability Tests بشكل دوري. سواء من داخل أم من خارج سوريا من خلال شركات عالمية ومحلية
٢-أمان المعلومات والمحافظة على الخصوصية	أ. لا تخزن البوابة أي معلومة خاصة بالعلاقة بين المؤسسات المستفيدة وزبائنها إلا ما له علاقة بعملية الدفع فقط (كالأرقام المعرّفة والمبالغ المدفوعة). ب. لا تُطلب من المؤسسات المستفيدة معلومات عن زبائن لا يستخدمون البوابة. ت. تخزّن جميع المعلومات المتعلقة بالبوابة في قواعد معطيات معيارية تدعم التخزين الهائل وتكامل المعطيات مع سرعة الحصول على المعلومة. ث. تُظهر تطبيقات المراقبة معلومات دقيقة ومفصلة عن جميع الطلبات مما يمكن موظفي المصرف والمؤسسات المعنية من مراجعتها كلّ حسب سماحياته. ج.يمكن لموظفي المصرف أو المؤسسات المعنية توليد تقارير تقاص Reconciliation آلياً.	أ. لا تخزن البوابة أي معلومة خاصة بالعلاقة بين المؤسسات المستفيدة وزبائنها إلا ما له علاقة بعملية الدفع فقط (كالأرقام المعرّفة والمبالغ المدفوعة). ب.لا تُطلب من المؤسسات المستفيدة معلومات عن زبائن لا يستخدمون البوابة. ت.تخزّن جميع المعلومات المتعلقة بالبوابة في قواعد معطيات معيارية تدعم التخزين الهائل وتكامل المعطيات مع سرعة الحصول على المعلومة. ث.تُظهر تطبيقات المراقبة معلومات دقيقة ومفصلة عن جميع الطلبات مما يمكن موظفي المصرف والمؤسسات المعنية من مراجعتها كلّ حسب سماحياته. ج. يمكن لموظفي المصرف أو المؤسسات المعنية توليد تقارير تقاص Reconciliation آلياً.
٣-التكامل	أ. تدعم البوابة واجهات تخاطب معيارية، منها: • المعيار ISO 8583 (فيزا)، الخاص بالتخاطب مع محولة الصرافات. • تقنياتSOAP وXML (خدمات الويب). • SSL (بروتوكول طبقة المنافذ الآمنة) لحماية قنوات الاتصال.	تدعم البوابة واجهات تخاطب معيارية، منها: • المعيار ISO 8583 (فيزا)، الخاص بالتخاطب مع محولة الصرافات. • تقنيات SOAP وXML (خدمات الويب). • SSL (بروتوكول طبقة المنافذ الآمنة) لحماية قنوات الاتصال. ب. تدعم البوابة واجهات تخاطب خاصة، منها: • XAPI: واجهة التخاطب مع النظام المصرفي لدى المصرف العقاري.

	ب. تدعم البوابة واجهات تخاطب خاصة، منها: • XAPI: واجهة التخاطب مع النظام المصرفي. • البروتوكول الخاص بدفع فواتير الخطوط لاحقة الدفع من سيرياتل. ت. تتكامل البوابة مع نظام إعلام Notification يتيح إرسال رسائل نصية أو بريد إلكتروني للمعنين في حالات المشاكل والحالات الطارئة وغيرها من الأحداث.	• لا تتوافر هذه الخدمة الخاصة بدفع فواتير الخطوط لاحقة الدفع من سيرياتل لدى المصرف حاليا مع إمكانية اضافتها عند الضرورة وبحال التوافق بين الشركة والمصرف (أو أي شركة اخرى وذلك نتيجة التصميم المعياري العالي الأداء للبوابة والمعتمد على البرمجة Modular) ت. تتكامل البوابة مع نظام إعلام Notification يتيح إرسال رسائل نصية أو بريد إلكتروني للمعنين في حالات المشاكل والحالات الطارئة وغيرها من الأحداث.
٤-الدقة	أ. تعالج جميع الطلبات آنياً Online مع جميع الأطراف (المصرف والمؤسسات المستفيدة). ب. البوابة مزودة بتطبيقات مراقبة تتيح معلومات دقيقة ومفصلة عن جميع الطلبات.	أ. تعالَج جميع الطلبات آنياً Online مع جميع الأطراف (المصرف والمؤسسات المستفيدة). ب. البوابة مزودة بتطبيقات مراقبة تتيح معلومات دقيقة ومفصلة عن جميع الطلبات.
٥-المرونة وقابلية التوسع	أ. بنية خدماتية التوجه SOA بالتصميم والتنفيذ. ب. خدمات قائمة على تدفق العمل Workflow •لكل خدمة طريقة عمل خاصة تمثل Workflow. •يعتمد تدفق العمل على إجراءات بسيطة Primitives تمثل تنفيذاً لإحدى واجهات الاتصال. •تُسجل بدقة كافة تفاصيل تدفق العمل وجميع المعلومات المرسلة عبر كل واجهة تخاطب مع أجوبتها. •نعتمد توزيع الأدوار في أجزاء التدفق ذات المعالجة البشرية. ت. مرونة إضافة واجهات تخاطب جديدة للبوابة، وبالتالي:	أ. بنية خدماتية التوجه SOA بالتصميم والتنفيذ. ب. خدمات قائمة على تدفق العمل Workflow •لكل خدمة طريقة عمل خاصة تمثل Workflowوجميع هذه المعلومات معتمدة ومتم فحصها من قبل جهات متخصصة بهذا المجال •يعتمد تدفق العمل على إجراءات بسيطة Primitives تمثل تنفيذاً لإحدى واجهات الاتصال. •تُسجل بدقة كافة تفاصيل تدفق العمل وجميع المعلومات المرسلة عبر كل واجهة تخاطب مع أجوبتها. •نعتمد توزيع الأدوار في أجزاء التدفق ذات المعالجة البشرية. ت. مرونة إضافة واجهات تخاطب جديدة للبوابة، ومن ثَمَّ: •سهولة إضافة قنوات جديدة. •سهولة إضافة خدمات جديدة.

	• سهولة إضافة قنوات جديدة. • سهولة إضافة خدمات جديدة. • سهولة تقديم الخدمات ذاتها لبنوك أخرى كما أشرنا سابقاً. • سهولة تقديم الخدمات ذاتها لمؤسسات جديدة.	•سهولة تقديم الخدمات ذاتها لبنوك أخرى كما أشرنا سابقاً. •سهولة تقديم الخدمات ذاتها لمؤسسات جديدة.
٦-التوفر والجاهزية	أ. إن قنوات البوابة متاحة لكل الزبائن في سورية على مدار الساعة •موقع بنك الإنترنت •الصرافات الآلية •نظام المجيب الصوتي •نظام الرسائل القصيرة ب. يؤمن المصرف فريقاً دائم الجاهزية لمراقبة أداء الخدمات والاستجابة السريعة.	أ. إن قنوات البوابة متاحة لكل الزبائن في سورية على مدار الساعة •موقع بنك الإنترنت •الصرافات الآلية •لا تتوفر خدمة نظام المجيب الصوتي حاليا •نظام الرسائل القصيرة ب. يستطيع زبائن المصرف المقيمين خارج سورية استخدام قنوات موقع بنك الإنترنت والمجيب الصوتي والرسائل القصيرة الاستفادة من خدمات بوابة العقاري على مدار الساعة. ث. يوجد لدى المصرف العقاري فريق دائم الجاهزية لمراقبة أداء الخدمات والاستجابة السريعة٢٤/٢٤.
٧-مراقبة وقياس الأداء	١. إذ تؤمن البوابة العديد من التقارير، منها: أ. تقارير تشغيلية: تؤمنها أنظمة مراقبة أداء الخدمات. ب. تقارير تحليلية • تتولد من مخزن المعلومات Data warehouse الخاص بالبوابة. • تقارير لقياس مؤشرات الأداء لكل خدمة ولكل نظام وسيط.	١. إذ تؤمن البوابة العديد من التقارير، منها: أ. تقارير تشغيلية: تؤمنها أنظمة مراقبة أداء الخدمات. ب. تقارير تحليلية • تتولد من مخزن المعلومات Data warehouse الخاص بالبوابة. • تقارير لقياس مؤشرات الأداء لكل خدمة ولكل نظام وسيط.
٨-الاستجابة السريعة لمعالجة المشاكل	أ. تتكامل البوابة مع نظام إعلام Notification يتيح إعلام القائمين على البوابة في حالات المشاكل والحالات الطارئة وغيرها من الأحداث. ب. تُظهر تطبيقات المراقبة معلومات	أ. تتكامل البوابة مع نظام إعلام Notification يتيح إعلام القائمين على البوابة في حالات المشاكل والحالات الطارئة وغيرها من الأحداث. وذلك على مدار ٢٤/٢٤ ب. تُظهر تطبيقات المراقبة معلومات دقيقة ومفصلة عن جميع الطلبات مما يمكن المعنيين من تحديد

	دقيقة ومفصلة عن جميع الطلبات مما يمكن المعنيين من تحديد أسباب المشاكل وآلية حلها بسرعة. ت. تتيح أنظمة التدخل اليدوي اتخاذ الإجراء المناسب لحل أي مشكلة. ث. تعالج معظم الأخطاء والمشاكل بسيناريوهات آلية تقوم بها خدمة التدخل الأوتوماتيكي.	أسباب المشاكل وآلية معالجتها بسرعة. ت. تتيح أنظمة التدخل اليدوي اتخاذ الإجراء المناسب لحل أي مشكلة. ث. تعالج معظم الأخطاء والمشاكل بسيناريوهات آلية تقوم بها خدمة التدخل الأوتوماتيكي.
٩- نوع الرقابة	الرقابة الوقائية والتصحيحية	الرقابة الوقائية والتصحيحية
تعتبر المواصفة (ISO 27001:2005) قاعدة لتقييم إدارة حماية المعلومات، باعتبارها وثيقة لتقييم النظام		

الجدول رقم (٤) جدول مقارنة وفق COBIT

٤-المبحث الرابع :التحقق من الفرضيات والحكم على كفاءة نظم المعلومات المحاسبية في حماية البيانات والمعلومات في المصارف السورية

بعد توصيف واقع عمل نظام المعلومات المصرفي في مصرفي العينة، وأمن البيانات والمعلومات فيه، طبقا لما ورد في الفصلين الثاني والثالث . وبعد إجراء المقارنة المرجعية لتقييم ما هو مطبق فعلياً من هذه المعايير والسياسات والإجراءات كان لا بد من تدعيم الدراسة عن طريق إجراء الاختبارات الفعلية لأنظمة الأمن المتبعة وإجراء المقابلات الشخصية مع رئيس قسم نظم المعلومات للمصرفين وكشف نقاط القوة والضعف فيهما و ذلك بإجراء الآتي :

٣-١ اختبار Acunetix Website Audit

أجري اختبار قوة أنظمة الأمن في المصرف العقاري ومقارنتها مع عدد الخروقات في الاشهر السابقة وقد تم استخلاص النتائج من التقرير بعدد الاختراقات وكيفية اقتراح حلها كما في التالي:

١-٣-١ إداة الاختبار

acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit
28 November, 2012

Developer Report

Generated by Acunetix WVS Reporter (v8.0 Build 20120423)

Scan of https://ebank.reb.sy:443/

Scan details

Scan information	
Starttime	11/28/2012 12:36:37 AM
Finish time	The scan was aborted by the user
Scan time	50 minutes, 4 seconds
Profile	High_Risk_Alerts

Server information	
Responsive	True
Server banner	Microsoft-IIS/6.0
Server OS	Windows
Server technologies	ASP.NET

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Knowledge base

SSL server running [443]

A SSL3 server is running on TCP port 443.

-
SSL server information:
- Version: SSL2,SSL3,TLS1- Ciphers suported:
- SSL3_CK_RSA_RC4_128_MD5(OpenSSL ciphername: RC4-MD5, Protocol version: SSLv3, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: RC4(128), Message authentication code: MD5) - High strength
- SSL3_CK_RSA_RC4_128_SHA(OpenSSL ciphername: RC4-SHA, Protocol version: SSLv3, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: RC4(128), Message authentication code: SHA1) - High strength
- SSL3_CK_RSA_DES_192_CBC3_SHA(OpenSSL ciphername: DES-CBC3-SHA, Protocol version: SSLv3, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: 3DES(168), Message authentication code: SHA1) - High strength

- Certificate 1:

Issuer:
Common Name: TRKTRUST Elektronik Sunucu Sertifikas Hizmetleri
Country Name: TR
Organization Name: TRKTRUST Bilgi letiim ve Bilim Gvenli Hizmetleri A.. (c) Kasm 2005

Recipient:
Country Name: SY
State Or Province Name:
Locality Name: Damascus
Organization Name: REB
Organizational Unit Name: IT
Common Name: ebanik.reb.sy

Certificate version: 2
Serial number: 0601
Finger print: 678ad246e70f9696f5cf7826ecea86fc
Algorithm ID: 1.2.840.113549.1.1.5
Validity start: Mon Feb 14 17:46:50 UTC+0200 2011
Validity end: Thu Feb 13 17:46:50 UTC+0200 2014
Expire in: 442 days

- Certificate 2:

Issuer:
Common Name: TRKTRUST Elektronik Sertifika Hizmet Salaycs
Country Name: TR
Locality Name: Ankara
Organization Name: TRKTRUST Bilgi letiim ve Bilim Gvenli Hizmetleri A.. (c) Kasm 2005
Recipient:
Common Name: TRKTRUST Elektronik Sunucu Sertifikas Hizmetleri
Country Name: TR
Organization Name: TRKTRUST Bilgi letiim ve Bilim Gvenli Hizmetleri A.. (c) Kasm 2005

Certificate version: 2
Serial number: 03
Finger print: 133c94cac5dba0ebe7bdfc1b239029dc
Algorithm ID: 1.2.840.113549.1.1.5
Validity start: Mon Nov 7 13:14:43 UTC+0200 2005
Validity end: Tue Sep 15 14:14:43 UTC+0300 2015
Expire in: 1021 days

A TLS1 server is running on TCP port 443.

-
SSL server information:
- Version: SSL2,SSL3,TLS1- Ciphers suported:
- TLS1_CK_RSA_WITH_RC4_128_MD5(OpenSSL ciphername: RC4-MD5, Protocol version: TLSv1, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: RC4(128), Message authentication code: MD5) - High strength
- TLS1_CK_RSA_WITH_RC4_128_SHA(OpenSSL ciphername: RC4-SHA, Protocol version: TLSv1, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: RC4(128), Message authentication code: SHA1) - High strength
- TLS1_CK_RSA_WITH_3DES_EDE_CBC_SHA(OpenSSL ciphername: DES-CBC3-SHA, Protocol version: TLSv1, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: 3DES(168), Message authentication code: SHA1) - High strength

- Certificate 1:

Issuer:
Common Name: TRKTRUST Elektronik Sunucu Sertifikas Hizmetleri
Country Name: TR
Organization Name: TRKTRUST Bilgi letiim ve Bilim Gvenli Hizmetleri A.. (c) Kasm 2005
Recipient:
Country Name: SY
State Or Province Name:

Locality Name: Damascus
Organization Name: REB
Organizational Unit Name: IT
Common Name: ebanik.reb.sy

Certificate version: 2
Serial number: 0601
Finger print: 878ad246e70f9696f5cf7826ecea86fc
Algorithm ID: 1.2.840.113549.1.1.5
Validity start: Mon Feb 14 17:46:50 UTC+0200 2011
Validity end: Thu Feb 13 17:46:50 UTC+0200 2014
Expire in: 442 days

- Certificate 2:

Issuer:
Common Name: TRKTRUST Elektronik Sertifika Hizmet Salayc
Country Name: TR
Locality Name: Ankara
Organization Name: TRKTRUST Bilgi letim ve Bilim Gvenli Hizmetleri A.. (c) Kasm 2005
Recipient:
Common Name: TRKTRUST Elektronik Sunucu Sertifikas Hizmetleri
Country Name: TR
Organization Name: TRKTRUST Bilgi letim ve Bilim Gvenli Hizmetleri A.. (c) Kasm 2005

Certificate version: 2
Serial number: 03
Finger print: 133c94cac5dba0ebe7bdfc1b239029dc
Algorithm ID: 1.2.840.113549.1.1.5
Validity start: Mon Nov 7 13:14:43 UTC+0200 2005
Validity end: Tue Sep 15 14:14:43 UTC+0300 2015
Expire in: 1021 days

Alerts summary

ASP.NET Padding Oracle Vulnerability

Affects	Variation
/	1

Application error message

Affects	Variation
/	8

Login page password-guessing attack

Affects	Variation
/ebanik/public/login.aspx	1

GHDB: Typical login page

Affects	Variation
/ebank/public/login.aspx	1
/ebank/public/login.aspx (03cca719916cf6465f44b0af238a7eee)	1
/ebank/public/login.aspx (0515de7cc9f71fa9686bd66e5285c6a1)	1
/ebank/public/login.aspx (07f789c2cceb2b539607f4b6953bd38f)	1
/ebank/public/login.aspx (10838753840ae257450e8d8d37ee25eb)	1
/ebank/public/login.aspx (1c48d2383d066abccbd3c564dc55924b)	1
/ebank/public/login.aspx (1fd9dbbacf93b79b498573cdf7efbae4)	1
/ebank/public/login.aspx (224bce9ba1df1862937d9a3e70fad153)	1
/ebank/public/login.aspx (2e6a74b88d6809a3b6eeba560dec3171)	1
/ebank/public/login.aspx (32c499fe0864f0887f5ae20db4968ba6)	1
/ebank/public/login.aspx (3bf3ab18414ebedf0feb4a98b11cf77b)	1
/ebank/public/login.aspx (44c019186819f9f9ed42e45f9ee5c54d)	1
/ebank/public/login.aspx (4aed83b28d1ffba0e1774dd914b7ee28)	1
/ebank/public/login.aspx (4e19cf38542054c3605d649037118b59)	1
/ebank/public/login.aspx (56e9d616258570b9be453def89c21d3e)	1
/ebank/public/login.aspx (5c992f60995badce245e06004b98f52a)	1
/ebank/public/login.aspx (665ffac2c93d6ebb661b3b53ec039016)	1
/ebank/public/login.aspx (68cfd29d3867335c179a423d0882d9f2)	1
/ebank/public/login.aspx (6ac691db1d45a3a5898dd54b7ca56af4)	1
/ebank/public/login.aspx (6f0cd84a05d27c62f345bffcb38a54b0)	1
/ebank/public/login.aspx (753155096dd85fcb59939b839996cc34)	1
/ebank/public/login.aspx (7b398ebb2f6638493430d0a674fd4c8d)	1
/ebank/public/login.aspx (84ceed00e002f44ccc4e79bc87d1502d)	1
/ebank/public/login.aspx (86bd5a209ec7262ae24622305cb17af5)	1
/ebank/public/login.aspx (883095c7ea2c3c5eacf0b47e20c2aabc)	1
/ebank/public/login.aspx (936408e5883176b03bbb8fed865f270f)	1
/ebank/public/login.aspx (96860c8525843b92abf76bd8fa44e1ff)	1
/ebank/public/login.aspx (9afb769fc5a4c29543e23f6d4d3d83ca)	1
/ebank/public/login.aspx (ac019ea9c1aac625b6bf0c4e761ff185)	1
/ebank/public/login.aspx (b672e4a912abc98acf7d205a59e371ca)	1
/ebank/public/login.aspx (c490694b3d57e1833e3cb9a3ceef7913)	1
/ebank/public/login.aspx (ca4ff78b6bd934273ef4cd7e44c40b3b)	1
/ebank/public/login.aspx (db64d2edc6557903deb94332d2c3cc39)	1
/ebank/public/login.aspx (deddaf4d1063ffbd9a48e046737837c6)	1
/ebank/public/login.aspx (eda148df60ae39f4b544faa56e4d8195)	1
/ebank/public/login.aspx (f826e380eea5f366e9d010b22a45da7a)	1
/ebank/public/login.aspx (f9c6855795e55c2dbbbfc3d5e560f202)	1

Alert details

ASP.NET Padding Oracle Vulnerability

Severity	High
Type	Validation
Reported by module	Scripting (ASP_NET_Oracle_Padding.script)

Description

ASP.Net uses encryption to hide sensitive data and protect it from tampering by the client. However, a vulnerability in the ASP.Net encryption implementation can allow an attacker to decrypt and tamper with this data. This vulnerability exists in all versions of ASP.NET. An attacker who exploited this vulnerability could view data, such as the View State, which was encrypted by the target server, or read data from files on the target server, such as web.config. This would allow the attacker to tamper with the contents of the data. By sending back the altered contents to an affected server, the attacker could observe the error codes returned by the server.

A workaround to prevent this vulnerability is to enable the <customErrors> feature of ASP.NET, and explicitly configure your applications to always return the same error page - regardless of the error encountered on the server. By mapping all error pages to a single error page, you prevent a hacker from distinguishing between the different types of errors that occur on a server.

Impact

An attacker who exploited this vulnerability could view data, such as the View State, which was encrypted by the target server, or read data from files on the target server, such as web.config. This would allow the attacker to tamper with the contents of the data. By sending back the altered contents to an affected server, the attacker could observe the error codes returned by the server.

Recommendation

Microsoft released a workaround to prevent this vulnerability from being exploited.

Enabling the Workaround on ASP.NET V1.0 to V3.5
If you are using ASP.NET 1.0, ASP.NET 1.1, ASP.NET 2.0, or ASP.NET 3.5 then you should follow the below steps to enable <customErrors> and map all errors to a single error page:

1) Edit your ASP.NET Application's root Web.Config file. If the file doesn't exist, then create one in the root directory of the application.
2) Create or modify the <customErrors> section of the web.config file to have the below settings:

```
<configuration>
  <system.web>
    <customErrors mode="On" defaultRedirect="~/error.html" />
  </system.web>
</configuration>
```

3) You can then add an error.html file to your application that contains an appropriate error page of your choosing (containing whatever content you like). This file will be displayed anytime an error occurs within the web application.
Notes: The important things to note above is that customErrors is set to "on", and that all errors are handled by the defaultRedirect error page. There are not any per-status code error pages defined – which means that there are no <error> sub-elements within the <customErrors> section. This avoids an attacker being able to differentiate why an error occurred on the server, and prevents information disclosure.

Enabling the Workaround on ASP.NET V3.5 SP1 and ASP.NET 4.0
If you are using ASP.NET 3.5 SP1 or ASP.NET 4.0 then you should follow the below steps to enable <customErrors> and map all errors to a single error page:

1) Edit your ASP.NET Application's root Web.Config file. If the file doesn't exist, then create one in the root directory of the application.
2) Create or modify the <customErrors> section of the web.config file to have the below settings. Note the use of redirectMode="ResponseRewrite" with .NET 3.5 SP1 and .NET 4.0:

```
<configuration>
  <system.web>
    <customErrors mode="On" redirectMode="ResponseRewrite" defaultRedirect="~/error.aspx" />
  </system.web>
</configuration>
```

3) You can then add an Error.aspx to your application that contains an appropriate error page of your choosing (containing whatever content you like). This file will be displayed anytime an error occurs within the web application.
4) We recommend adding the below code to the Page_Load() server event handler within the Error.aspx file to add a random, small sleep delay. This will help to further obfuscate errors.

References

Important: ASP.NET Security Vulnerability
Vulnerability in ASP.NET Could Allow Information Disclosure
How to check if your application is vulnerable to the ASP.NET Padding Oracle Vulnerability
Understanding the ASP.NET Vulnerability

Affected Items

/

Details

Acunetix detected this vulnerability by comparing the HTTP response status and body for two different requests (one request when the padding is incorrect and another one where the encrypted text is not valid). If the body AND/OR status are different, this vulnerability can be exploited.

First request:
Status code 500
Response body (first 500 bytes) <html> <head> <title>Runtime Error</title> <style> body
{font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;} p
{font-family:"Verdana";font-weight:normal;color:black;margin-top: -5px} b
{font-family:"Verdana";font-weight:bold;color:black;margin-top: -5px} H1 {
font-family:"Verdana";font-weight:normal;font-size:18pt;color:red } H2 {
font-family:"Verdana";font-weight:normal;font-size:14pt;color:maroon } ...

Second request:
Status code 404
Response body (first 500 bytes) <html> <head> <title>The resource cannot be found.</title> <style> body
{font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;} p
{font-family:"Verdana";font-weight:normal;color:black;margin-top: -5px} b
{font-family:"Verdana";font-weight:bold;color:black;margin-top: -5px} H1 {
font-family:"Verdana";font-weight:normal;font-size:18pt;color:red } H2 {
font-family:"Verdana";font-weight:normal;font-size:14pt;co ...

Request headers

```
GET /WebResource.axd HTTP/1.1
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

Application error message

Severity	**Medium**
Type	Validation
Reported by module	Scripting (Error_Message.script)

Description

This page contains an error/warning message that may disclose sensitive information.The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

Impact

The error messages may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Review the source code for this script.

References

PHP Runtime Configuration

Affected Items

/

Details

Path Fragment (suffix .aspx) Input / was set to
Error message found: <H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

Request headers

```
GET //Public/Faq.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/

Details

Path Fragment (suffix .aspx) Input / was set to
Error message found: <H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

Request headers

```
GET //Public/HomePage.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/

Details

Path Fragment (suffix .aspx) Input / was set to
Error message found: <H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

Request headers

```
GET //Public/PrivacyStatement.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/

Details

Path Fragment (suffix .aspx) input / was set to
Error message found: <H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

Request headers

```
GET //Public/Aboutus.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/

Details

Path Fragment (suffix .aspx) input / was set to
Error message found: <H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

Request headers

```
GET //Public/ActiveAccount.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/

Details

Path Fragment (suffix .aspx) input / was set to
Error message found: <H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

Request headers

```
GET //Public/Contactus.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/

Details

Path Fragment (suffix .aspx) input / was set to
Error message found: <H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

Request headers

```
GET //WebChannel/Aya.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/

Details

Path Fragment (suffix .aspx) input / was set to
Error message found: <H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>

Request headers

```
GET //User/AccountSummary.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
```

```
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

Login page password-guessing attack

Severity	Low
Type	Validation
Reported by module	Scripting (Html_Authentication_Audit.script)

Description

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

References

Blocking Brute Force Attacks

Affected Items

/ebank/public/login.aspx

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/Electricity.aspx HTTP/1.1
Content-Length: 3907
Content-Type: application/x-www-form-urlencoded
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...flyo2BLzbvJYV9Pg21j%2b0ix%2b5Adldolxwzr Atyz4z%2b%2b11autGd2aGgC7VwV4ttR%2bwm0Mr5hMWbF
P84BRl5FzXsbR0wagyY2O5d35F5fOUQDe%2fW1D1OD3DmuvgmEC1tFVNDY9q9Dvkt%2bBh2w2cFqY5kh1U%2b%2f
yAaBP%2fCTaVNodChMYGvgAzTbptJjWv5vYla810w2fonJCjvsbDiLy5%2b6MONgheQa%2f8IVniwZZwjJrO5SrN
NK404D22hzx%2buTwRcf%2fH2rqL%2b5W1FOUBg98Yuee5clVgYWpOp7EwEyw1QkhXTuRZ4c%2fb2Rp67UpsmP5R
JLiJD%2bsdYD2Hdc0DBz5QtQgTsOYRSgs%2fSeE6URXODXy3jHsJcb2c%2fuRGTZf4jIh1LdaER2k36N9EBa967
lxWrIw51WXFINVAljJTAlRc59IMclzszyLtmrXTwLFa5JcOd2WNcFFA5eVlM%3d
```

GHDB: Typical login page

Severity	Informational
Type	Informational
Reported by module	GHDB

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.
Category : Pages containing login portals

This is a typical login page. It has recently become a target for SQL injection. Comsec's article at http://www.governmentsecurity.org/articles/SQLInjectionBasicTutorial.php brought this to my attention.

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Recommendation

Not available. Check description.

References

The Google Hacking Database (GHDB) community
Acunetix Google hacking

Affected Items

/ebank/public/login.aspx

Details

We found Inurl:login.asp

Request headers

```
GET /ebank/public/login.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/EBank
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/ebank/public/login.aspx (03cca719916cf5465f44b0af238a7eee)

Details

We found Inurl:login.asp

Request headers

```
GET /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/SteBillPayment.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/WebChannel/SteBillPayment.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=ar-SY
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/ebank/public/login.aspx (0515de7cc9f71fa9686bd66e5285c6a1)

Details

We found inurl:login.asp

Request headers

```
GET /ebank/public/login.aspx?ReturnUrl=/EBank HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/EBank
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/ebank/public/login.aspx (07f789c2cceb2b539607f4b6953bd38f)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/EBank HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 3907
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=ar-SY
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...FonUzBeMFWJaw%2b6PSCbPn2ac7ZoQZr2pM6iIXuwQUscXMi6Ob86WO8L11D1KvE547alCnD7pntP1Xqr%2bd
psofgz%2f8bVQryix3ZpKtGCtcAHETMQNDmxwdkc1oGJv92jmWy39NxIWyeR6OHQJ1N3C86ln4rG3Jnh5WwKcO%2
b9gPxK2eqsxSs43Uk362dDxjaochDhbF9nFlz6ZK1tFYGlao7ANH3jEJ%2ffHynpjLQI4dSBl81DeJ8vTMTD8O8C
b3G2NnXaYki%2bTx4GPvQrUtDMKP%2bMnAyOxbVyXpz%2bOcwQlppzlUA1CFunEJOaV9%2bpy2tRHf%2ffRkFXpF%
2fsPJx9kJ%2fNhaNTS1e9T8tpm3CJ1bhc9juDuVKJJhy1nNTMn3F8yculNS1nN7RP4pp3%2bgD%2bx%2bi0S1oVP
s47shBqn0XCB2csaQx%2b%2f8IoWxJQwFjtRoqftIQdk8Urjj%2feWANGCBM%3d
```

/ebank/public/login.aspx (10638753840aa257450e8d8d37ee25eb)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/SteBillPayment.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 3915
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

```
(line truncated)
...QxWF7xgbg2Fdzp4jUnraaGQ94rydo%2bsnMSjacvE0Ns%2bpbmEdCE67qFbO8hmfy45x7XE2HQ3gwXkU5CwTY
TLHu7s5D784InczGzM4l2WYlI9pu2SCWYOgII3%2fNOOhRN6X03n%2f%2bBOcO8R3V4CMHF9RqnE86cWVFOeqLIw
vJJ8Bpg2fIC2NedCBsn3RF8Mg%2bN0phgbiEu4YxqurCIRarkc2mfkqKgf0rtwWjHXqGJ66FhqD8RtcfJPYm2dF6
oT3mFamauPRQeth6ulK8OZagAeFn33yU188JG9BARapG7IaoO7757AJeIhUh1ysDDZ%2bgohHh3eqIOrPvY8oYHP
GvarHN%2fPx3OysoHb0V%2fQO64I4%2bP1qDgsTqtvUD5wZQ1qLag119WBl2jc5VWyHRxtowWnmGcX%2bLWP%2fv
7aI8prjTa04jr8yQ4rKdrEMNPy9Qt4RTE8hu6llLArDHnmTrDJhqTv0%2fePGPa
```

/ebank/public/login.aspx (1c48d2383d066abccbd3c564dc55924b)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 3825
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwceon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...FdKbEcVCQhL9RtgrNQN%2fJsNlsmvIm28ozZNxgLc0WDQULqK%2bK04UR8voRa1QcGY47VTcYksO2k7d97vx2
uzxyrVFIE822Pxr644dKV7BNcD8Qahbe08Nu6GBYshhYvgzIDaoMq0rnlwh7tnDzRTdTyYjO7LtPOTN%2bI8yzEr
8OrXhI2ArnIM8d4gp%2ff%2bzBxl8fo4mZQkj3ax3znuiLc4Sc4cPM4pJeM5wBoqKtltgF%2fYA%2bj250mcKKO
8g87XD8Fp1L7GpTWJOUqOODcWqdRp7oqaHamaDXr9pCjfI7SymNDdpOX0nJj6%2fxIUwIYuu4UCw5RQlmoeWADak
s42btZ98v6o2dXD32C0BOV%2bD8xDluwDtpnn5YJHa2Qkqmqx3R8kxn6X8kfJ53LDox6XjfcYchjxGbcDpLOabI9
h4Ov%2bxl17MbtZS5h8gJQgMaaSWHrx7I2lddZyZE5WCcd06DugCZPQtMEx8%3d
```

/ebank/public/login.aspx (1fd9dbbacf33b79b496573cdf7efbae4)

Details

We found inurl:login.asp

Request headers

```
GET /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/Mtn.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/WebChannel/Mtn.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwceon; __IbLanguageCookie__=Culture=ar-SY
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/ebank/public/login.aspx (224bce9ba1df1862937d9a3e70fad153)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/Electricity.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 4124
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
```

```
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...%2bx3Xsupc1xfZgl1jr1hQH1BuHZ9oRj5Ggg7aR%2btTyMWwK33CyVwscGcjf4UZ5fMyK12YtZHzVRRQeMX7r
hPmCIhU3L5D%2fH3C0brXRc92xRvcrZT%2fGZLCeczgfe8hXN8w7lmaVtVFhuA25jrw152%2fT1aSGPfoVLEKUTd
rUZdiW8%2fFagEPM5rcvg%2bCV8sta%2fR2bymOMPpkfmXT2RnLwlcw3WNlfV5RMM40qrONXPOPrJevaGRWLTOpZ
2O3Zx%2b51s1w85dqhOMtTbW1ZV0mdQPGyF9zD7jAoFuUtFsvgF8O8F1KhWdmVQzyMOkptckY941Kg5a7DQba8g0
XUp8tnnYATSk%2bC3R8bxJnOMPYLXGdFw9cUa4z%2baRSmdwNVPQ9gld9pqLgL3%2bp1KZ%2bdAJYI%2f4rnD16F
r%2fE%2bHzvZX4Fm7Ju%2b1lD6wfyWh4ukPQRprCbcquxPdvA%2fGFyXQ%3d%3d
```

/ebank/public/login.aspx (2e6a74b88d6809a3b5eeba560dec3171)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/AyaAdslCard.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 4124
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...%2bx3Xsupc1xfZgl1jr1hQH1BuHZ9oRj5Ggg7aR%2btTyMWwK33CyVwscGcjf4UZ5fMyK12YtZHzVRRQeMX7r
hPmCIhU3L5D%2fH3C0brXRc92xRvcrZT%2fGZLCeczgfe8hXN8w7lmaVtVFhuA25jrw152%2fT1aSGPfoVLEKUTd
rUZdiW8%2fFagEPM5rcvg%2bCV8sta%2fR2bymOMPpkfmXT2RnLwlcw3WNlfV5RMM40qrONXPOPrJevaGRWLTOpZ
2O3Zx%2b51s1w85dqhOMtTbW1ZV0mdQPGyF9zD7jAoFuUtFsvgF8O8F1KhWdmVQzyMOkptckY941Kg5a7DQba8g0
XUp8tnnYATSk%2bC3R8bxJnOMPYLXGdFw9cUa4z%2baRSmdwNVPQ9gld9pqLgL3%2bp1KZ%2bdAJYI%2f4rnD16F
r%2fE%2bHzvZX4Fm7Ju%2b1lD6wfyWh4ukPQRprCbcquxPdvA%2fGFyXQ%3d%3d
```

/ebank/public/login.aspx (32c439fa0864f0887f5ae20db4968ba6)

Details

We found inurl:login.asp

Request headers

```
GET /ebank/public/login.aspx?language=en HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/ebank/public/login.aspx (3bf3ab18414ebedf0feb4a38b11cf77b)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/EBank HTTP/1.1
```

```
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 4302
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswriin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...%2bOels7GlnzBq5%2ffaHRa%2fd7%2b5kreOkAPx%2bgopJIPDCax2oG%2ffbuQMFLN81EWmeS3YQpULgY382
V9RlrUy5ZZmDcZCOvRxqkRzucJJxuthK4YhD6n9mVKh%2bONDir7XI%2blR9RXPloo%2faI85B19EZyCY%2fqCli
DIXdKOwXqB39p%2f08jlfgxit4MKUHlXXWYxUwTCDv62%2b%2fV0qMewXldOE%2bIIT%2budHaMFueLRetpXNKXT
2ls6GTKIulR2Vkh3Yxs%2bWUCfOQUooWwiIE%2bxm2Yt691BGCjyEKeWtmoJ4M5f4bg%2fgPO7jDOve07NXNVei0
XiiQw%2fvRupZUkoQlJh1CKpb5L6U2b%2b3%2foG1U2%2bhVvKjbffHIbfWBlW%2bbWk%2fJ5AiaDTNxNvTu3zL4
kYnCuwJ4zaklslmxQtMd%2f%2fLy%2fMNQbO4HqF8C96c87o5mQCk6l9Q98k%3d
```

/ebank/public/login.aspx (44c019186819f9f9ed42e45f9ee5c54d)

Details

We found inurl:login.asp

Request headers

```
GET /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/AyaAdslCard.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/WebChannel/AyaAdslCard.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswriin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=ar-SY
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/ebank/public/login.aspx (4aed83b26d1ffba0e1774dd314b7ee28)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 4198
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswriin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...OcxWjstsk17wR6gQ2aWOlojo6k1T5dkjQi8x1Tg9vaxOaC2JFqpj0q5zrqKX1j%2bqxeIIg1GzxSnUFVI%2ft
1yQtbRoCRF3ktL%2bRH%2fAD8CkCIE1sI%2bXd%2bPPJBGpyYktV8Aq4vgw98EOuuiogWVjBjhZlrxnyDS%2bfyS
LxQKjauO88xXcTiIWxktASC9b%2bhkJOGKIlOCxB91W8d52FvcVitnjjviD9vyC1x35Tp8Qg%2folPoJoLTGjkbd
U2VWPaSQPJndWE3n8HUe8VLBuKGja%2fn1bws9GhHAmDHYE%2fgEgRMpYdPoEwzGucvTXfWt1ih3QrZdw8m2vsaL
aL4hDhCPzLayJPHg4UjuliozlaeEfpnGaHlG0ftNuc5%2fuqjLQFhLWd4Ow%2bBt3Oge1pR4Gw%2fWCPdDllUpDA
4QC9upcNq54M7qo2n%2boOCOXwlqA5RrTrVIJ%2ffMoBL5hxvemTTWyrA%3d%3d
```

/ebank/public/login.aspx (4e19cf38542054c3805d649037118b59)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/Default.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 4220
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswriin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...5U%2fHOmOgkOvwX47A%2fsO7A80pAZhYq9RPzOuAn2tP3gXpMCHJtKB5uLJH9f%2bWBwPGaPGO%2fazKAAd8o
aD3jz5Ie07L28dJ9kx7f4avom3zTWgQa3dwSPH6%2fqCoE%2b44qI8DRa8MJv4vJL6mfqnDUwe7NM8V3N2dze%2f
KpR4laCHdJP%2bQUc7kNNr1xdAvewN%2b1B%2bIH6kTwtojjo%2fVXk9cruvjJBIzEPNdljvZqWBfg5Pwccw%2b5
2TJfn1caix9%2f5GVmfTun%2f6nbeM70i5hwOEldcL8UXcBcoDlLQ33utPPipRZ27fWePMVOwyONBgan10CyPeC2
IQbca7hJ0NF1A32X7d8zvQD3wgMpzBeHcE1PV3ulwi6Ygs5iEWwlmTUdOIA8BmqMx79a0vwzemVNuJ9GRP2Nns87
NbFhKGonF%2bMAfUn4IbsOsuKZxe7jf4x5hY6UKyM5zxr0k86wgmcerOQ%3d%3d
```

/ebank/public/login.aspx (56e9d616258570b9be453daf89c21d3e)

Details

We found inurl:login.asp

Request headers

```
GET /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/Aya.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/WebChannel/Aya.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswriin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=ar-SY
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/ebank/public/login.aspx (5c992f90995badce245e06004b96f52a)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/Tasdid.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 4124
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswriin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

```
(line truncated)
...%2bx3Xsupc1xfZg1ljrlhQHlBuHE9o8j5Ggg7aH%2btTyMWwK33CyVwscGcjf4U85fMyK12Yt2HzVRRQeMX7r
hPmCIhU3L5U%2fH3C0brXRc92xKvcr2T%2fGZLCeczgfe8hXN8w7LmaVtVFhuA25jrw152%2fYlaSGPfoVLEKUTd
zUZd1W8%2fPagEPM5rcvg%2bCV8sta%2fK2bymOMFpkfmXT2RnLwlcw3WNlfV5RM040qrONXPOPrJevaGRWLTOp%
2O3Zx%2b51a1w85dqh0MtYbW1ZV0mdQPGyF9zD7jAoFuUtFsvgF8O8F1KhWdmVQzyMOkptckY941Kg5a7DQba8g0
XUp8tnnYATSk%2bC3H8bxJnOMPYLXGdPw9cUa4z%2baRSmdwNVPQ9gld9pqLgL3%2bpiKZ%2bdAJYI%2f4rnD16F
r%2fS%2bHzvZX4Fm7Ju%2b11D6wfyWh4ukPQRprObcquxPdvA%2fGFyXQ%3d%3d
```

/ebank/public/login.aspx (665ffac2c93d6ebb661b3b53ec039016)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/Syriatel.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 3909
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswr1in43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...nbJTlW%2b1nCxAtEO0yvwO%2fMsalaoPQ6TXaVJeyT4w4tH6uLIMpOM4ICoZ1kgtIqfd9Ar1s47584HImcwQG
w8OITEC9%2fW014yH5DIpbc%2fE6wkIAP4Wy5uFjIfGS5ywBx8qEwarkX3meGlsoT2CRivOKAYbad4HyfdVzkdzm
HQT6AJMV76dzajgNloW%2fWxNwawMZfqPZGha3rY2sCMYFWHGxbdNMyBz3k2%2f5Y6KJ%2bVaKVHf5p8tddgyHbY
4gCzvYXl%2bfHPuucdQ75TLV72TqzDgjvGaP2Vp%2fboBnOgasKOrs23fnhs8FsJ7L7o8ApZ1j5MHI0zXmQxgCOC
75QV%2fboXpx2bNWP7fcFaCfouCIS9WGTYxk8JxPycpxpAgUDKzMKJUsFyF1EqG%2fOENwdgJ7nw5GrXG4hTAmfJq
glSFjukYzvznVbu%2b%2bB8SleTGfXKVFcHDdRE4GWkQkBVCXyOyTKnYgsWbN6
```

/ebank/public/login.aspx (68cfd29d3867335c179a423d0682d9f2)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/MtnBillPayment.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 4220
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswr1in43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...5U%2fHOsOgkOvwX47A%2fsO7AR0pAZhYq9RPzUuAn2tP3gXpMCRJtKB5uLJH9F%2bWBwPGaPGU%2fazKAAd8o
ab3jz5Ie07L28dJ9kx7f4avxm3zTWgQa3dwSPH6%2fqCo8%2b44qI8DRa9MJv4vJL6mfqnDUwe7NM8V3N2dze%2f
KpR4laOHdJP%2bQUc7kNNr1xdAvewN%2b1B%2bIH6kTwtojjo%2fVXk9cruvjJBIzEFMdljvZqwBfg5Pwccw%2b5
2TJfn1csix9%2f5GVwfTun%2f6nbeM7015hwOE1dcLBUXcBcoD1LQ33utPPipR227fWeFMVOwyONBgan1OCyPeC2
1Qbcs7hJ0NF1A32X7d8zvQD3wgMpzBeRcE1PV3ulwi6Yga5iEWwlmTUdO1A8BmgMx79a0vwzemVNuJ9GRF2Nna87
NbFnKGonF%2bMAFUm4LbaOauKZxe7jf4x5hY6UkyM5zxrOk86wgmcerOQ%3d%3d
```

/ebank/public/login.aspx (6ac691db1d45a3a5898dd54b7ca56af4)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/Electricity.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 3907
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswriin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...flyo2BLzbvJYV9Pg21j%2b0ix%2b5AdIdolxwzrAtyz4z%2b%2b1lsutGdZsGgC7VwV4ttE%2bwmOMr5hMWbF
PS4BR15FzXabR0wsgyY2O5d35F5fOUQDe%2fWiDiOU3DmuvgmEC1tFVNDY9q9Dvkt%2bBh2w2cFqY5kh1U%2b%2f
yAaHP%2fCTmVNodChMYGvgAzTbptJjWv5vY1a8i0w2fonJCjvabDiLy5%2b6MOMgheQa%2f8IVnlw2ZwjJzO58rN
NK404D2Zhzx%2boTwKcf%2fH2rqL%2b5WiFOUBg9BYuee5clVgYWpOp7EwEywiQkhXTuR24c%2fb2Rp67OpamPSR
JLiJD%2badYD2HdcODBz5QtQgTaOYRSga%2fSeE6URXODXy3jHaJcb2cZ%2fuRGTZf4jIh1LdaER2k36N9EBa96T
ixWr1w51WXFINVAljJYAlHc59IMclzazyLtmrXTwLFa5JcCd2WNcFFA5eViM%3d
```

/ebank/public/login.aspx (6f0cd84a05d27c62f345bffcb38a54b0)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/Tasdid.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 3833
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswriin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...6Cme12cQkacWkJbvENpPEyx74tbAgQJAfUJVHfFo5osmPO4pEugYaCgSAWLJFKgTwincjcJdoRUhz51TG2nzx
v4SGVNccK5ejCjeu3oIFzIkdyGbj42bRKlrZ2C9W9FSVLN%2bCNyQGzPwDxw48OO1Ne3vsdxG%2fbXVm0LnH6z81
5zdwauoKDpeEXhLrHt1lqNcWW52TBGGa5lAazqau7DyaE%2b7%2b1K6laYK%2bApASzupjqa4ZQX2BTcjeu%2f61
2UwBJn3n841jLv8Y9ypdL6z5eWdt2TcWuc82beCbM5VltF3O58xEa97iccSt%2bhIpaRhU%2f%2bQGB1SXANHsF3
Awj5dRuKBx8Q7FD9yGVzz7sM%2b12KNnrMThVdPUIovwoSyeu96o5X7fQ9mOYWJVK7sqPoV8hZ2jf1%2bb7JMT9x
u6%2fP36UTmqF1bQ61q7Klu7J145o8d0FabXnc03TooL2643x%2bGR%2ff7I%3d
```

/ebank/public/login.aspx (753155096dd65fcb55939b839996cc34)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/Aya.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 3903
Content-Type: application/x-www-form-urlencoded
```

```
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswriin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...oXwy2NygFLi%2bjjjjyTLnBnMQ56KdS%2bkpNDBrWnLLYrCDY%tt7w2uxSgJPoU0VdbAJz6VdchuPezwEe4Gl
3cwaqaVE%2bltjSIeoUYM22RGv7xY2OOx87cIc3bDdJg1aL6fhJZ1rqBf9PT9wY7YaurIO2PYOxlp%2fPuOADHwB
0ucAkiusD2pjhJAAXmpNUPwk2for7yquiQmZRm%2b90WzkbjfPWG4SbzfefIs8v7SlizYBCF%2fBiLfPtFIJxU2A
4%2f6YkhLu6VBQCrAHA0I4BJxfmFAth3ozzcFDuVau5jajtnd10nfIykdDVhqtrbV2g09%2fJFCVTqcZoucAo%2b
3%2bqYDz2ELQydgHHKvJcV52DF1f%2fpvFBaWJyFSn3TmrPxvtKl32wCFeK2C6VX7nbDKtInEIP44AOfDciKcl%2
b%2fuJlL3YWP1KFQX22Uf2O5wAxg%2fz8FX4ocGah%2fErQJRTMdgJwYVJlo%3d
```

/ebank/public/login.aspx (7b398ebb2f6638433430d0a674fd4c8d)

Details

We found inurl:login.asp

Request headers

```
GET /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/Tasdid.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/WebChannel/Tasdid.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswriin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=ar-SY
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/ebank/public/login.aspx (84ceed00e002f44ccc4e75bc87d1502d)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/Default.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 3829
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswriin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...wSTfAZlcmDCgLraMDTroTlsJajIeawGB%2fG2gWHUZbxT7bOzWZMb6uvUC3rHnyFRHWPOqyBZlvWInKH22JJb
74Y4M14w2qDDdf%2fKlXmd%2f8najaljEZjCom5N5xUmYko8l1RBe0GcKpz20uIMBTg7dCb67I4cRUV11RfqGLB7
JFxJJagaQnzgmxt5gUFBJw1HbgE4lV%2frKa5KZOhT8DfpB5aPCnyEjChc%2fndqxGh9AFYL%2bi6axvZkvz%2bb
%2f0QJII2Kbu4L4WEvE29e5EoaqZluDCaH4oYaVMV%2fUiIErW%2f3oz3EsQkPxHW61fvOc0wVty2t7Vq2A8Mvbh
jUqDAu27051wqYI6Laqu4s0BgPtInfnryaoHlhvm%2fujMiBexfUQnsNvUh%2fpsz2qtcYBItXzaRxu6PVQX2OOz
glvLcl%2baKNNwaRGtO2KJ9Au8Ltj%2bWlegBQusM6ulTTGlwuRiagTg%2ba%3d
```

/ebank/public/login.aspx (86bd5a209ec7262ae24622305cb17af5)

Details

We found inurl:login.asp

Request headers

```
GET /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/Syriatel.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/WebChannel/Syriatel.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswriin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=ar-SY
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/ebank/public/login.aspx (883095c7aa2c3c5eacf0b47e20c2aabc)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/MtnBillPayment.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 3845
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswriin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...dwLUNoGIc1G%5HV%30bWv0HzhKn9GASxUh3dCJ3GJEkF72FPGvR1ER%2bDC%2fbjG81AdIEm72%2baTawJc47
3uWg6BbPIE3LTb4TN8xPPTvktce%2fuoxzVDuVc%2bQLVbg1JaLX5cNabex6krUK3wgQFMgF220v%2fXvh1Q9Qdf
IMkTJDdehQW4PO1WWTgQaM8BGgaaUv8kc8DYb%2fpgDa1k4Y1UHeGqqvEWMS17DM9Uu2J8fq%2fhEO5Ag1cLaHZi
yJN3yS0vgbe%2fd%2b81kzjIy88FbJYRpz6BTCBeQqbYpuLgo%2b%2by4uGX%2fpXdGc37hhrkbsAD0IuSHqdeJU
WVKVOIJSG75EuPxgYxQDW3g8Cz46It5Ithc5%2foCgUBkde5loUBwRfK9zAc2aBA7yQge4Y6vAqeT1c2G%2b%2bP
MeKb82QZPvV5Dd895PYk5z42PptK4h9AxX5HDasAkA8c4GtlbPJWGctpn7zo%3d
```

/ebank/public/login.aspx (336408e5883176b03bbb8fed865f270f)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/Aya.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 4220
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswriin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

```
(line truncated)
...5G%2fHOmOgkOvwX47A%2fsO7ARGpAEhYqSRPzUuAn2tP3gXpMCHJtKH5uLJH9F%2bWBwPGaPGO%2fazKAAd8o
aD3jz5Ie07L28dJ9kx7f4avxm3zTWgQa3dwSPH6%2fqCoE%2b44qI8DRa8MJv4vJL6mfqnDUwa7NM8V3N2dze%2f
KpR4laOHdJP%2bQUc7kNNr1xdAvewN%2b1B%2bIH6kTwtojjo%2fVXk9cruvjJBIzEFHd1jv2qwBfg5Pwcow%2b5
2TJfn1caix9%2f5GVnfTun%2f6nbeM7Oi5hwOE1dcL8UXcBcoD1LQ33utPPipR227fWePMVOwyONBgan1OCyPeC2
1Qbcs7hJ0NF1A32X7d8zvQD3wgMpzBeHcSiPV3ulwi6Yga5iEWwlmTUdOIA8RmgMx79a0vwzemVNuJSGRF2Nna87
NbFnKGonF%2bMAfUm4IbsOauK2xe7jf4x5hY6URyM5zxrOk86wgmcerOQ%3d%3d
```

/ebank/public/login.aspx (38860c8525843b92abf7Sbd8fa44e1ff)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/Syriatel.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 4124
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...%2bx3XsupclxfZglljr1hQHlBuHZ9oBj5Qgg7aH%2btTyMWwK33CyVwacGcjf4UX5fMyK12YtZHzVRAQeMX7r
hPmCIhU3L5O%2fH3C0brXRc92xKvcrZT%2fG2LCeczgfe8hXN8w7lmaVtVFhuA25jrw152%2fTlaSGPfoVLERUTd
rUZdiW8%2fFagEPM5rcvg%2bCV8ata%2fA2bymOMPpkfmXT2RnLwlcw3WNlfV5MM40qrONXPOPrJevaGKWLTOp2
ZO3Zx%2b5lslw85dgh0MtTbWIZV0mdQPGyP9zD7jAoPuUtFsvgF8O8F1KhWdmVQzyMOkptckY941Kg5a7DQbaSg0
XUp8tnnYATSk%2bC3H8bxJnOMPYLXGdPw9cUa4z%2baR8mdWNVPQ9gld9pgLgL3%2bp1K2%2bdAJYI%2f4rnDi6F
r%2fE%2bHzv2X4Pm7Ju%2blID6wfyWh4ukPQRprObcquxPdvA%2fGFyXQ%3d%3d
```

/ebank/public/login.aspx (9afb769fc5a4c29543e23f6d4d3d83ca)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 4194
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=ar-SY
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...jstsk1TwR6gQ2aWOlojo6k1T5dkjQ18x1TqSvaxOaCZJFqpj0q5zrgKX1j%2bqxeIIg1GzxSnOFVI%2ft1yQt
bRoCRF3ktL%2bRH%2fAD8CkCIEisI%2bXd%2bPPJBGpyYktV8Ag4vgw98EOuu1ogWVjBjh2lrxnyD8%2bfySLxQK
jau0Z8zXcTiIWxktASC5b%2bhkJ0GKIlOCG%2baqXRw5hiVo4tUi3y8%2fV8UqFHAeneK9%2fo8Mcu80nCTNNbFB
AKoLXc%2b66H%2bo33t4tl%2bCtyTscVOn2BH%2byAzXICrUcdXF%2bEIhafzav6DDdH5X5hFWVT%2feNhxflK5p
cTA8Fyd%2bQ9nImhBleHiorJdd9mGXxI9Oq1tWDf9Wokoev965M6zLpzGwEbCXfYIyKzZJYXqYawA0W111QnIA6Y
zzqoBlQhT8L2f2HNC7tDojXa7KdIuyFtJNhe5J5CSo9ytjgQkBuoOzevQ%3d%3d
```

/ebank/public/login.aspx (ac019ea9c1aac625b6bf0c4e761ff185)

Details

We found inurl:login.asp

Request headers

```
GET /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/Default.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/WebChannel/Default.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswr1in43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=ar-SY
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/ebank/public/login.aspx (b672e4a912abc98acf7d205a59a371ca)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/Mtn.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 4220
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswr1in43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...5U%2fHOmOgkOvwX47A%2faO7A8CpAZhYg9RPzUuAn2tP3gXpMCHJtKB5oLJR9F%2bW8wPGaPGU%2fazKAAd8o
aD3jz5Ie07L28dJ9kx7f4avxm3zTWgQa3dwSPH6%2fqCo8%2b44qI8D8a8MJv4vJL6mfqnDOwa7NM8V3N2dze%2f
KpR4laOHdJP%2bQUc7kNNr1xdAvewN%2b1B%2bIH6kTwtojjo%2fVXk9cruvjJBIzEFRdljv2qwBfg5Pwccw%2b5
2TJfnlcsix9%2f5GVmfTun%2f6nbeM7015hwOE1dcL8UXcBcoDILQ33utPP1pRZ27fWeFMVOwyONBgsn1OCyPeC2
1Qbcs7hJ0NF1A32X7d8zvQD3wgMpzBeKcRiPV3ulwi6Ygs5iEWwlnT0dOlA8BmqMx79a0vwzemVNuJ9GRF2Nns87
NbFnKGonF%2bMAfUn4LbaOsuKZxe7jf4x5hY6UkyM5zxr0k86wgmcerOQ%3d%3d
```

/ebank/public/login.aspx (c490634b3d57e1633a3cb9a3ceef7913)

Details

We found inurl:login.asp

Request headers

```
GET /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/MtnBillPayment.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/WebChannel/MtnBillPayment.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswr1in43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=ar-SY
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*
```

/ebank/public/login.aspx (ca4f78b6bd934273ef4cd7e44c40b3b)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/AyaAdslCard.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 3833
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...s00nWPs6V5bfrNT58kub4QOj7rzuUKlfDv8jqJxTrv3pU9CBmlWuAu9A03i%2fNfL7oKMMtGwDMqCmEXeBf89
CUOwUWGH5VKl7yH%2fORApBBVz1I1pA6xAe6%2biAGM5LHryOZ3VkbXbFzGQ%2bNvyK6xp%2bl3T%2fSaszmTytT
URfI7evgWWD6AzNpPP1s8y4oy5TbyB0gtyfC6RcBiVV8rNaVWQQIq9ng6z54P8tHm2dS5kwowy8gxQzE4a93tscj
rQenGszn8eg9DwH6Ka%2be%2ffWtROZMlQfvtx3G%2bgCivVxkmw5gEw0zEx1Ujbo3anJJ6rxHzELY4pKFN%2b7z
E%2f53UhbM342CaQF5I7VJ9XPpK6zx9Ut4yxvxO4nl1e1oww9nAV8Fm49wZv1aP%2b1Vg1QC3YUGCaxCvgAbstA2
rZL97LiY3f2RqcAKUxK%2ffZ8TaTXblyo9zXh67rvyWwMB86nO8zAUzC9zlk%3d
```

/ebank/public/login.aspx (db64d2edc6557903deb94332d2c3cc39)

Details

We found inurl:login.asp

Request headers

```
POST /ebank/public/login.aspx?ReturnUrl=/ebank/WebChannel/SteBillPayment.aspx HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Content-Length: 4124
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: ASP.NET_SessionId=ygswrlin43fpv3lwqexwoeon; __IbLanguageCookie__=Culture=en-US
Host: ebank.reb.sy
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

(line truncated)
...%2bx3Xsupc1xfXg11jr1hQH1BuHZ9oBj5Ggg7aR%2btTyMWwK33CyVwscGcjf4UX5fMyK12Yt2HzVRRQeMX7r
hPmCIhU3L5U%2fH3C0brXRc92xKvcrZT%2fGZLCaczgfe8hXN8W7LmaVtVFhuA25jrw152%2fTlaSGPfoVLEKUTd
rUZd1W8%2ffagEPM5rcvg%2bCV8ata%2fR2bymOMFpkfmXT2RnlwlcW3WNlfV58MM40qr0NXPOPrJevaGRWLTOpZ
2O3Zx%2b51s1w85dqhOMtTbW1ZV0mdQPGyF9zD7jAoFuUtFsvgF808F1KhWdmVQzyMOkptckY941Kg5a7DQba8g0
XUp8tnnYATSk%2bC3H8bxJnOMPYLXGdFw9cUa4z%2baR8mdwNVPQ9gld9pqLgL3%2bp1KZ%2bdAJYI%2f4rnDi6F
r%2f8%2bHzvZX4Fm7Ju%2b1lD6wfyWh4ukPQRprObcquxPdvA%2fGFyXQ%3d%3d
```

/ebank/public/login.aspx (deddaf4d1063ffbd9a48e046737837c6)

Details

We found inurl:login.asp

Request headers

```
GET /ebank/public/login.aspx?language=ar HTTP/1.1
Pragma: no-cache
Referer: https://ebank.reb.sy/ebank/public/login.aspx
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
```

وبعد الانتهاء من إجراء الاختبار لمعرفة الخروقات والثغرات تبين منه النتائج التالية:

- الصفحة ٦ من التقرير الاختراقASP.NET Padding Oracle Vulnerability

مستوى الاختراق خطير:والحل من خلال تنزيل نسخة من net framework 4.0. التي تحل هذه المشكلة

ASP.Net uses encryption to hide sensitive data and protect it from tampering by the client. However, a vulnerability in the ASP.Net encryption implementation can allow an attacker to decrypt and tamper with this data. This vulnerability exists in all versions of ASP.NET. An attacker who exploited this vulnerability could view data, such as the View State, which was encrypted by the target server, or read data from files on the target server, such as web.config. This would allow the attacker to tamper with the contents of the data. By sending back the altered contents to an affected server, the attacker could observe the error codes returned by the server.

- الصفحة ٩ من التقرير**Application error message**

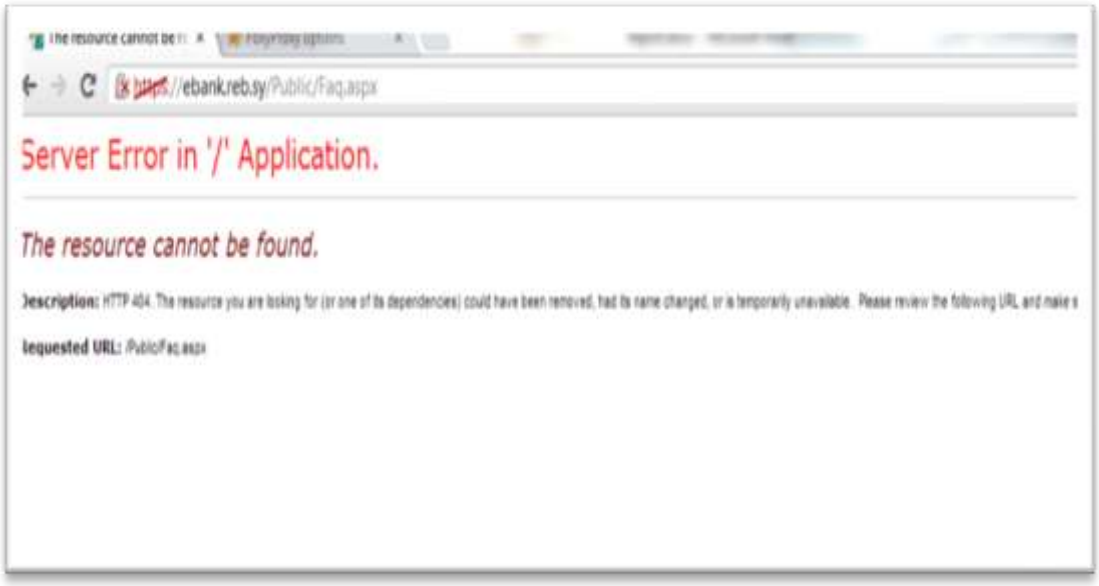
مستوى الاختراق متوسط :هذا الخطأ بسبب طلب عنوان لا يحوي ebank

مثلhttps://ebank.reb.sy/Public/Faq.aspx

والصحيح هو

https://ebank.reb.sy/Ebank/Public/Faq.aspx

والحل هو وضع صفحة Error.html بحيث يظهر توصيف الخطأ أن الصفحة المطلوبة وفق العنوان المطلوب غير موجودة بدلا من ظهور الصفحة



- الصفحة ١٢ من التقرير **Login page password-guessing attack**

مستوى الاختراق منخفض :هذا التهديد يتم حله من خلال إغلاق الحساب بعد خمس محاولات وذلك عندما يكون الحساب موجوداً.

في الحالة التي يتم فيها محاولة اكتشاف كلمة سر لحساب غير موجود بالأساس لا يوجد ضرورة لحل كون الحساب غير موجود اصلا.

- الصفحة ١٣ من التقرير **GHDB: Typical login page**

مستوى الاختراق إعلام :مادام المستخدم لم يسجل دخولاً فإن الدخول إلى أي صفحة من الموقع تتطلب دخوله من خلال صفحة تسجيل الدخول وهذا طبيعي.

وبمقارنة عدد الخروقات في هذا التقرير مع الستة أشهر السابقة كان عدد الخروقات كالتالي :

التاريخ	عدد الخروقات
٢٠١٢-٨-٢٦	١٣ اختراق
٢٠١٢-٩-٣٠	١١ اختراق وستة اختراق منها مستوى الاختراق اعلام
٢٠١٢-١٠-٣١	١٠ أغلبها مستوى الاختراق منخفض
٢٠١٢-١١-٢٨	٤ كما وردت سابقا
٢٠١٢-١٢-٣٠	٥
٢٠١٣-١-٣٠	٣

الجدول رقم (٣) عدد الخروقات على موقع العقاري

عن طرق اختبار Acunetix Website Audit

ونلاحظ من الجدول السابق أن عدد الخروقات والثغرات ينخفض بشكل ملحوظ ولكن الاختراقات لم تزل موجودة وهذا دليل على أن إجراءات الأمان المتبعة في المصرف العقاري لا تعزز كفاءة النظام من شهر الى آخر وهو ما يثبت عدم صحة الفرضية الثانية .

٣-٢ من خلال المقابلة الشخصية التي أجريت مع رئيس قسم نظم المعلومات والعاملين في القسم للمصرفيين وبعد طرح مجموعة من الاسئلة عليهم كما في الملحق رقم (٢)
تم معالجة البيانات التي تم الحصول عليها من خلال أحد أدوات الدراسة باستخدام البرنامج الإحصائي SPSS (Statistical Package for Social Sciences) الملحق رقم (٣) حيث تم استخدام التحليلات الوصفية و استخدام المتوسطات الحسابية والانحرافات المعيارية ،كما تم استخدام اختبار ت ستودينيت لاختبار الفرضيات .
وفيما يلي نتائج الاختبار

جدول رقم (٥): الإحصاءات الوصفية للفرضية الأولى

One-Sample Statistics				
	N	Mean	Std. Deviation	Std. Error Mean
spo1	10	1.8125	.12148	.03841

من الجدول السابق نلاحظ أن قيمة المتوسط بلغت 1.8125 والانحراف المعياري 12148.

جدول رقم (٦): اختبار ت ستودينت للفرضية الأولى

One-Sample Test						
	Test Value = 1.5					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
spo1	8.135	9	.000	.31250	.2256	.3994

- بلغت قيمة t 8.135 بإشارة إيجابية لأن المتوسط اعلى من المتوسط المحسوب 1.5 أي النتائج في صالح العينة، وقيمة sig أصغر من 0.05 أي نرفض الفرضية الابتدائية ونقبل الفرضية البديلة التي تقول أن السياسات والاجراءات الادارية المتبعة في المصارف لا تعزز كفاءة نظم المعلومات

جدول رقم (٧): الإحصاءات الوصفية للفرضية الثانية

One-Sample Statistics				
	N	Mean	Std. Deviation	Std. Error Mean
spo2	10	1.8571	.09524	.03012

من الجدول السابق نلاحظ أن قيمة المتوسط بلغت 1.8571 والانحراف المعياري 0.09524 .

جدول رقم (٨): اختبار ت ستودينت للفرضية الثانية

One-Sample Test						
	Test Value = 1.5					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
spo2	11.859	9	.000	.35714	.2890	.4253

بلغت قيمة **t 11.859** بإشارة إيجابية لأن المتوسط اعلى من المتوسط المحسوب **1.5** أي النتائج في صالح العينة، وقيمة **sig** أصغر من **0.05** أي نرفض الفرضية الابتدائية ونقبل الفرضية البديلة التي تقول أن السياسات والاجراءات الامنية المتبعة في المصارف لا تعزز كفاءة نظم المعلومات.

جدول رقم (٩): الإحصاءات الوصفية للفرضية الثانية

One-Sample Statistics				
	N	Mean	Std. Deviation	Std. Error Mean
spo3	10	1.7810	.24302	.07685

من الجدول السابق نلاحظ أن قيمة المتوسط بلغت 1.7810 والانحراف المعياري 24302 .0.

جدول رقم (١٠): اختبار ت ستودينت للفرضية الثالثة

One-Sample Test						
	Test Value = 1.5					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
spo3	3.656	9	.005	.28095	.1071	.4548

بلغت قيمة **t 3.656** بإشارة إيجابية لأن المتوسط اعلى من المتوسط المحسوب **1.5** أي النتائج في صالح العينة، وقيمة **sig** أصغر من **0.05** أي نرفض الفرضية الابتدائية ونقبل الفرضية البديلة التي تقول أن السياسات والاجراءات الامنية المتبعة في المصارف لاتعزز كفاءة نظم المعلومات.

نستنتج من تحليل النتائج التي حصلت عليها الباحثة من المصرفيين ما يلي :

- **بالنسبة للإجراءات والسياسات الإدارية**

١-إن المصرفيين يستخدمان تقنية النظم في أداء الأعمال المصرفية .

٢-جميع فروع المصرفيين مربوطة بشبكة معلومات .

٣-إن المصرفيين لهما اتصال بالشبكة العالمية (الانترنت).

٤- مصرف عودة به نسبة عالية من الوعي الأمني أكثر من المصرف العقاري.

٥-إن المصرفيين لا يتبعان طريقة معينة لتحفيز الموظفيين العامليين وكسب انتمائهم .
٦-إن اهتمام المصارف بشكل عام ضعيف في مجال التدريب وتوفير المجلات الدورية .
٧-إن المصرفيين يقومان بتغيير كافة الإجراءات التي كانوا يقومون بها الموظفون عند تركهم العمل .
٨-إن المصرفيين لديهم إجراءات إدارية وقانونية ضد الأفراد الذين يسربون المعلومات لجهات اخرى .
٩- التهديد في المصرفيين يأتي من مستخدمي النظام من الموظفيين وأنهم الذين يقومون بإساءة استخدامه .

- **بالنسبة للإجراءات والسياسات الأمنية**

١- إن المصرفيين يرون أن اعتماد استخدام التقنية لا يشكل خطورة على أموال المودعيين .
٢- إن المصرفيين يرون أن استخدام التقنية يساعد في السرقات المالية .
٣- إن المصرفيين ليس لديهم إجراءات لاستمرار العمل عند حدوث خلل أو أعطال في النظم والشبكات .
٤- إن المصارف لا تقوم بتلف الوسائط والمستندات والتقارير .
٥- إن المصرفيين لديهم تجهيزات مكافحة الحريق .
٦- إن المصرفيين ليس لديهم إجراءات لاستمرار و تحديث العمل بصفة دورية .
٧- إن المصرفيين يقومان بحفظ النسخ الاحتياطية خارج غرفة الحاسوب في مكان آمن خارج المصرف .
٨- إن موظفي المصرف من مستخدمي النظم ومبرمجيها هم فقط المصرح لهم بالدخول واستخدام النظم .
٩- إن المصرفيين يعتمدان كلياً على الجهات الاخرى في تركيب وصيانة الشبكات .
١٠- إن المصرفيين يستخدمان برامج ونظم حماية المعلومات يتركون جزء منها لموظفي التقنية والمستخدمين ويقومون بوضع خطط للمراقبة .
١١- إن تستخدم مضادات الفيروسات الأصلية المرخصة ولا تواكب تحديثها .

١٢- إن المصارف حريصة على تطوير إستراتيجية لمكافحة الفيروسات ولكن مصرف عودة مهتم أكثر بهذا الموضوع .

١٣- إن المصرفيين يستخدمان برامج أصلية ومرخصة .

١٤- إن الموظفيين يعتمدون على كلمة السر للدخول في نظم الحاسوب .

١٥- إن الموظفيين في المصرف العقاري يتهاونون في المحافظة على كلمة السر أكثر من مصرف عودة .

١٦- إن المصرفيين يستخدمون أكثر من وسيلة لحماية الشبكات .

- **بالنسبة للإجراءات والسياسات الرقابية**

١- إن المصرفيين لا يمنعون مدخلي البيانات من اجراء التعديلات .

٢- إن نسبة إهتمام الإدارات العليا بأمن وحماية المعلومات مقبولة في المصرفيين .

٣- لا توجد في المصرفيين دوائر مختصة بمراجعة وتدقيق نظم المعلومات .

٤- إن المصرفيين لديها سياسات وإجراءات ومواصفات قياسية لأمن المعلومات ولكن هذه السياسات تضعها المصارف بنفسها .

٥- المصرف العقاري لديه سياسات ومواصفات قياسية لتطوير وتشغيل نظم المعلومات أفضل من مصرف عودة .

٦- لا يوجد في المصرفيين موظفون متخصصون بمراجعة وتدقيق نظم المعلومات .

٧- إن الإدارة العليا لدى المصرفيين لا تشارك في تطبيق السياسات وتوكل مهام التطبيق لإدارة نظم المعلومات .

٨- إن المصرفيين لديهم إجراءات للمراقبة والتحكم في إدخال الأجهزة وإخراجها .

٩- إن المصارف عينة الدراسة لا تعتمد نظام الحراس في الدخول لغرف الحاسوب ، والاجراء المتبع في عودة هو أرقام سرية و العقاري أيضاً يتبع نفس الأسلوب ولكن أغلب الموظفيين يعرفون الرقم السري الموضوع للدخول إلى قسم نظم المعلومات .

وبنتيجة التحليل نستطيع القول أنه بالرغم من تطبيق المصرفيين لنسبة كبيرة من السياسات والاجراءات الادارية وإجراءات الامان والرقابة على النظم كما هو موضحاً في التحليل السابق إلا أنه غير كافي لتعزيز كفاءة النظم في المصارف وهذا ما يثبت عدم صحة الفرضيات الفرعية الثلاث .

وبالاعتماد على عدم صحة الفرضيات الثلاث نستطيع القول أن الفرضية الرئيسية قد تحققت وذلك بسبب عدم قدرة المصرف على بلوغ أهدافه في تحقيق الأمان فالموارد الموظفة في البنك لم تمكن النظم من بلوغ أفضل مستوى لأهداف أمن البيانات، وكان قد بيّن البحث أن الموارد البشرية والتجهيزات التقنية المستخدمة والبرمجيات التي تدعم بلوغ الأهداف والتي وظفها المصرف غير كافية لبلوغ المستوى الأعلى من الأهداف. كما أن تطور هذه الموارد، سواء من ناحية تدريب العنصر البشري أو تحديث التقنيات المستخدمة بما يناسب التطورات المحيطة بالعمل المصرفي الإلكتروني، كان يمكن أن يكون أفضل بما يساعد بشكل أفضل على تحقيق أمن البيانات والمعلومات.

فأهداف النظام في تحقيق الأمان للبيانات والمعلومات، وصولا إلى أبسط الأهداف، يستتبعها السياسات المعتمدة لبلوغ هذه الأهداف والإجراءات المرسومة في ضوء تلك السياسات والأهداف. وهذا تدعمه الفرضية الفرعية الثالثة. فالسياسات والإجراءات المطبقة في المصرف وخاصة المتعلقة بالرقابة الداخلية تحتاج إلى إعادة هيكلة بما يناسب أنظمة المصرف.

فعندما بدأ المصرف العقاري وعودة بوضع منظومتهما الإلكترونية كانا قد وضعا أهدافاً معينة للأمان ورسما سياساتهما وإجراءات أمان بياناته ومعلوماته في ضوئها وانطلقا في ذلك من الموارد. كمثال على ذلك حماية كافة الاتصالات الإلكترونية بين أجزاء البوابة والأنظمة الأخرى المختلفة. والتخطيط لسياسات أمنية معيارية والصرامة في تطبيقها. واستخدام تقنيات الحماية الحديثة، ومنها: كالتحقق من الهوية باستخدام الشهادات الرقمية (التوقيع الرقمي)، وغيرها كأسماء المستخدمين وكلمات المرور. تقنيات التشفير (المتناظر وغير المتناظر) الحديثة. بروتوكولات الاتصال الآمنة SSL وIPSEC. ربط السماحيات بالأدوار Role-based Authorization. التدقيق المستمر Real-time Auditing. تنفيذ اختبارات الأمن والاختراق Vulnerability Tests بشكل دوري. ولكن المصرف لم يتمكن من تنفيذها بشكل كامل وأيضا عدم اتباع المعايير(الآيزو) بشكل كاف فالمصرف يحاول جاهدا بما لديه من إمكانيات تطبيق هذه المعايير إلا أن وجود عقبات في المصرف وقفت عائقاً في تنفيذ هذه المعايير.

بذلك يمكن القول إن فرضية البحث الرئيسة قد تحققت الأمر الذي يستوجب أخذ المصارف السورية بنتائج هذا البحث للعمل على تطوير نظم الأمان لديها. وعليه يمكن الحكم على أن كفاءة نظم المعلومات المحاسبية في تحقيق الأمان للمصرفين محدودة نسبيا، وكان من الممكن أن تكون أفضل. فهي لم تتمكن من بلوغ مستوى متقدم من أهداف الأمان من خلال سياساتها وإجراءاتها الادارية والأمنية والرقابية التي كانت رسمتها. هذه المحدودية كانت محكومة بالمتغيرات الثلاثة المذكورة (الفرضيات الفرعية) التي شكلت متغيرات مستقلة تؤثر بشكل مباشر في المتغير التابع وهو الأمان للبيانات والمعلومات .

الفصل الخامس

النتائج والتوصيات

المبحث الأول : النتائج

تبين بعد الدراسة العملية التي قامت بها الباحثة إن المخاطر التي تتعرض لها المصارف موضوع الدراسة في أعمالها وفي أنظمة معلوماتها والتي تؤثر على كفائتها ما يلي :

١- بينت النتائج أن امتلاك برنامج لمكافحة الفيروسات هو أهم أولوية أمنية بينما يمثل نقص موظفي أمن المعلومات المدربين تدريبا جيدا أشد المخاوف الأمنية للمصرف العقاري ومصرف عودة. الجدول (١١)التالي يعرض قائمة بأهم خمس أولويات في حماية المعلومات بينما يعرض الجدول (١٢)قائمة بأشد خمسة مخاوف

الدرجة	أولويات أمن المعلومات
الأول	برامج مكافحة الفيروسات
الثاني	الوقاية من فقد البيانات
الثالث	جدار الحماية
الرابع	كشف ومنع الاختراق
الخامس	التحكم في الوصول للشبكة

الجدول (١١)أشد خمسة مخاوف في أمن المعلومات داخل المصرف العقاري وعودة

الدرجة	مخاوف حماية المعلومات
الأول	نقص موظفي حماية المعلومات المدربين تدريباً جيداً
الثاني	غياب سياسة الأمن الكافية داخل المصرف
الثالث	نقص الممارسات العملية الكافية على حماية البيانات
الرابع	غياب الممارسات الجيدة في اختيار كلمة المرور وتطبيق التحديثات واتخاذ الحماية
الخامس	عدم الالتزام بمعايير أمن المعلومات

الجدول (١٢) أهم خمس أولويات في حماية المعلومات داخل المصرف العقاري ومصرف عودة

٢-وجدت الباحثة أن المصارف عينة الدراسة لديها إجراءات أمنية عالية مقارنة بباقي البنوك الأخرى.

٣- وجود رغبة عالية لدى المصارف في استخدام ومواكبة التقنية ولا يرونها تشكل في حد ذاتها خطورة وتهديداً لودائع العملاء.

٤-بالرغم من النظرة الإيجابية لدى المصارف تجاه التقنية إلا أنهم يرون أن السرقات تتم بسوء استخدام التقنية والاستغلال السيئ للثقة الممنوحة لهم.

٥-المصارف تنقصها مواصفات قياسية ومعايير وسياسات نظم المعلومات وأمنها وحمايتها

٦-أما بالنسبة لبرامج التوعية الأمنية لدى المصارف محل البحث وجدت أنها ضعيفة ولا توجد خطط تدريبية أو مجلات ونشرات دورية لرفع الوعي الأمني لدى الموظفين.

٧-وجدت أن المبرمجين لديهم تعامل مباشر في تغيير ومعالجة مشاكل النظم والبرامج لدى المصارف في البيئة التنفيذية (Production) بدلا من أن يتم ذلك في بيئة تطوير البرامج (Development)ومن ثم تركيبها في البيئة التنفيذية.

٨- وجدت الباحثة أن المصارف عينة الدراسة يسمحون لمدخلي البيانات بإجراء التعديلات بأنفسهم.

٩- اتضح أن المصارف مربوطة بالشبكة العالمية للإنترنت دون فصل الشبكات المصرفية الخاصة بها بوسائل الحماية اللازمة، ودون وجود برامج رقابية، مما يجعل المصارف عرضة للاختراقات والتسلل والبرامج الخبيثة، ولا يخفى على أحد ما ينتج عن ذلك من مخاطر أمنية، كما أن المصارف ليست لها أي معلومات عَما إذا كانت هناك اختراقات أم لا، وذلك لانعدام أو عدم فاعلية وسائل الحماية والرقابة.

١٠- كما وجدت الباحثة عدم وجود دائرة خاصة لمراجعة وتفتيش نظم المعلومات بالمصارف هذا بالاضافة لعدم وجود كوادر مؤهلة في مجال أمن نظم المعلومات ومراجعتها والرقابة عليها

١١- كما إتضح عدم تطبيق السياسات أو ضعفها وعدم تطبيق الأجراءات الأمنية وعدم وضوح الجهات المسؤولة والمناطة بها.

١٢- في الوقت الذي يمثل فيه الاجراءات عادة أكثر من ٦٠٪ من حماية النظم و٤٠٪ وسائل

حماية تقنية نجد أن المصارف عينة الدراسة تغفل عن الإجراءات وتعتمد على البرامج والنظم الأمنية.

١٣- وجدت الباحثة أن الحماية المستخدمة للدخول والتعامل مع النظم والبرامج هي استخدام كلمة السر وهناك شيوع في استخدام كلمات سر الموظفين مع بعضهم البعض.

١٤- رغم إظهار الإستبانة بوجود استراتيجية لمكافحة الفيروسات وجد الباحث أن هناك ضعفاً في آلية توزيع وتركيب ومراقبة وتحديث برامج مكافحة الفيروسات وبما أن المصارف متصلة بالإنترنت فان نسبة الإصابة بالفيروسات تظل عالية حيث أن برامج المكافحة لا تأتى عادة إلا بعد اكتشاف الفيروس .

١٥- بالنسبة لاستمرارية العمل عند حدوث خلل بالأنظمة والبرامج، وجدت الباحثة أن هناك عدم اهتمام لدى المصارف لإيجاد بدائل عملية فاعلة لتقديم خدمات مصرفية للعملاء، مما يجعل العميل يرضخ للأمر الواقع والانتظار حتى حل المشكلة، ويتحمل ما ينتج عن ذلك من أعباء والتزامات مالية قد لا تحمد عقباها وما ذلك إلا لعدم وجود منافسة حقيقية في تقديم الخدمات المصرفية بين المصارف.

١٦-وجدت الباحثة أن المصارف عينة الدراسة تقوم بعمل نسخ احتياطي بصورة دورية ، يحتفظون بهاخارج مبنى المصرف.

١٧- يعتبر العنصر البشري (مستخدمو النظام) محور الخطر في المصرف. حدوث المخاطر في نظم المعلومات المحاسبية الإلكترونية يرجع إلى أسباب تتعلق بموظفي المصرف، نتيجة ضعف الخبرة والوعي والتدريب، إضافة إلى أسباب تتعلق بإدارة المصرف نتيجة غياب السياسات الواضحة والمكتوبة، ولضعف الإجراءات والأدوات الرقابية المطبقة لدى المصرف. كما أن المشكلة تكمن في عدد موظفي تكنولوجيا المعلومات في المصرف، حيث تعتمد الفروع على موظف واحد أو اثنين، مهمتهم تشغيل أنظمة الحاسوب. بينما الموظفون المتخصصون يكون مقر عملهم في المراكز الرئيسة للفروع. ولو حدث أن اضطر أحدهم للتغيب يؤدي ذلك إلى حدوث أزمة في العمل.

١٨-يلاحظ عدم حدوث مخاطر متكررة لنظم المعلومات المحاسبية في المصرف العقاري، لكن لوحظ أن مخاطر الإدخال غير المتعمد، ووجود مستوى واحد لكلمة المرور، وتوجيه البيانات

والمعلومات إلى أشخاص غير مصرح لهم بذلك، هي من أكثر المخاطر تكرارا. فقد تحدث أكثر من مرة شهريا إلى مرة أسبوعيا.

١٩- يلاحظ أن المصرفيين لديهما مدير Administrator مسؤول عن توزيع المهام والصلاحيات على العاملين في المصرف. لكن هذا التوزيع يتم شفهيا. بينما يفترض أن يكون مكتوباً بشكل واضح وموزعا على العاملين

٢٠-تبين أن المصارف عينة الدراسة تتوافر فيها بعض نظم إدارة أمن البيانات وليس جميعها. والمشكلات التي تعوق توافرها جميعها تقع على عاتق المصرف المركزي لعدم وضعه سياسات ومعايير محددة وواضحة للمصارف عموماً فكل مصرف يضع ما يناسبه من السياسات والمعايير بما ينسجم مع عمله والشركات العالمية التي يتعامل معها.

٢١-تبين أيضاً أن المصرفيين لا يعتمدان وجود فريق الاستجابة لطوارئ الكمبيوتر المسؤول عن التعامل مع الخروقات الرئيسة عن طريق إدراك وجود المشكلة وإحتوائها وإصلاح الضرر الناتج عنها والمتابعة لمعرفة كيف تم الخرق لكي يتم تفاديه في المستقبل .

٢٢- هناك ضعف في الرقابة الوقائية في المصرفيين عينة الدراسة اتضح ذلك من خلال استخدام الأبواب الإلكترونية التي تفتح برقم سري يفترض أن يعرفه فقط من يعملون بقسم IT ولكن الواقع أن كل الموظفين يعرفونه فما الداعي إلى استخدامه؟ ومن خلال أيضاً تدريب الموظفين فيجب الاهتمام أكثر بتدريب المستخدمين وليس فقط موظفين أنظمة المعلومات

٢٣-من خلال المقابلات الشخصية وبعد الاطلاع على تقارير رقابية في البنوك عينة الدراسة لوحظ أن هناك ضعفا في عملية إعداد التقارير الرقابية فمثلا في المصرف العقاري الذي يقوم بإعداد التقرير حول قسم الITهو مفتش الرقابة الداخلية المرسل من المصرف المركزي والأجدر هنا أن يعد التقرير شخص اختصاصي في مجال النظم والرقابة.

٢-المبحث الثاني: التوصيات

بما أن كفاءة نظم المعلومات المحاسبية في تحقيق الأمان للمصرفين محدودة نسبيا، وكان من الممكن أن تكون أفضل. فهي لم تتمكن من بلوغ مستوى متقدم من أهداف الأمان من خلال سياساتها وإجراءاتها الأمنية التي كانت رسمتها. كما ظهر جلياً من نتائج الدراسة وجود مهددات ومخاطر كبيرة تواجه استخدام التقنية في العمل المصرفي وأن معظم هذه المهددات والمخاطر حتى الآن داخلية ، وقد قسمت الباحثة التوصيات إلى توصيات خاصة لسد الثغرات في البنوك السورية لرفع كفاءة الأنظمة في المصارف في الوقت الراهن وتوصيات لوضع حلول شاملة لحماية نظم المعلومات عامة بما فيها المصارف من المخاطر والمهددات التي ستجابهها مع التوسع في تقديم خدمات مصرفية متنوعة باستخدامات التقنيات الحديثة لمواكبة التطور في العالم.

أولاً التوصيات الخاصة لسد الثغرات في المصارف السورية في الوقت الراهن

في ضوء نتائج البحث التي حصلنا عليها من المصارف عينة الدراسة من نتائج المقابلات التي أجرتها الباحثة نرى أن معظم المشاكل تنحصر في سوء إدارة مستخدمي النظم، ومشاكل كلمات السر ، وضعف الرقابة المصرفي نتيجة لضعف التقارير الرقابية، وعدم وجود سياسات ومواصفات ومعايير واجراءات أمنية، هذا بالإضافة للفجوة المعرفية الكبيرة بين التقنيين والتنفيذيين لعدم وضوح المهام وقلة التدريب وعدم مشاركة الموظفين التنفيذين في تطوير النظم، وعدم معرفة الموظفين

وجهلهم بالمخاطر الامنية والثقة المفرطة وسوء إستغلال هذه الثقة .

وعليه يمكن حصر التوصيات الخاصة بمعالجة المصارف السورية بالنقاط الآتية:

١- إنشاء دائرة خاصة لأمن المعلومات تزود بكوادر مؤهلة لإدارتها ومنحها صلاحيات قوية تؤهلها لتطوير وتطبيق السياسات الأمنية وذلك بدعم الإدارة العليا لها.

٢-رفع الوعي الأمني لدى جميع موظفي البنوك على اختلاف مستوياتهم وذلك بعمل دورات تدريبية خاصة مع عمل إصدارات دورية.

٣-عمل كتيب بملخص السياسات والمعايير والمواصفات القياسية مع إقرار وتعهد أمني يوقع عليه جميع الموظفين بمختلف مستوياتهم الإ دارية بعد قراءة الكتيب والاطلاع عليه.

٤-ألاَ يتم إجراء أي تعديل أو إلغاء من النظام المصرفي إلا بنظام تحكم ثنائي أي أن يقوم طالب العملية بإجراء العملية ومن ثم تتم الموافقة عليها من قبل المشرف أو المدير من خلال النظام بعد الاطلاع على القيود وعلى مستند طلب الإلغاء.

٥- لمعالجة سوء استخدام الشاشات المفتوحة من قبل الموظفين يجب تركيب برامج لحماية الشاشة ، ونظام الوندوز مزود ببرامج حماية الشاشات فما عليهم إلا إختبار عدم تعارضها مع البرامج التطبيقية ومن ثم تفعيلها، هذا بالإضافة إلى تضمين مثل هذه الميزة في البرامج التطبيقية بحيث تغلق النظام بعد فترة معينة من الزمن إذا ترك من غير عمل.

٦- ولمعالجة سوء استخدام كلمات سرالآخرين لتنفيذ عمليات مالية يجب إضافة الميزات التالية بالبرامج التطبيقية:

·ربط رقم المستخدم بموقع معين بالشبكة إذا أمكن، وذلك لمنع استخدام اسم المستخدم أو رقمه في شاشة أخرى غير شاشة أو موقع صاحب الرقم حتى لو عرفت كلمة سره من قبل الآخرين.

·إضافة ميزة إغلاق رقم المستخدم بعد ثلاثة محاولات فاشلة وذلك لمنع محاولة الدخول على النظام بتخمين كلمة السر.

·تطبيق سياسة صارمة تجاه كلمة السر، إذ يجب وضع مواصفات قياسية لكلمة السر من حيث عدد الحروف وتنوعها بالحروف والارقام والرموز، وعدم تكرار الحروف، وعدم إعادة استخدام نفس الكلمة حتى انقضاء فترة من الزمن وليكن عاماً، وطلب تغير الكلمة بصورة دورية، وتضمين هذه المواصفات في البرامج التطبيقية لفرض السياسة على جميع المستخدمين .

·إمكانية تجميد المستخدم بعد عدم استخدامه لفترة من الزمن.

٧- تطبيق الإدارة الثنائية في إنشاء المستخدمين بالنظم وفي منح الصلاحيات.

٨-يجب تطبيق السياسات المبنية على المهام الوظيفية ، بمعنى أن تجمع الوظائف ذات

الصلاحيات المتشابهة معاً، مثل صلاحيات الصراف – صلاحيات المشرفين – صلاحيات المدراء بحيث لا يتجاوز أحد حدود صلاحياته .

٩- تزويد النظام بإمكانية إصدار تقارير رقابية خاصة بإدارة المستخدمين تصدر يومياً وبصورة آلية وتعكس كل الأنشطة التي تمت على سجل المستخدمين من إضافة وحذف وتعديل ويراجع ويوقّع عليه من قبل المدير.

١٠-تزويد النظام بإمكانية إصدار تقارير لكل المستخدمين يعكس كل الأنشطة التي تمت لكل مستخدم.

١١-لمعالجة مشاكل تعطل النظم وعدم إستمرارية الخدمة يتم طباعة تقرير شامل بأرصدة العملاء للإستمرار في تقديم الخدمة يدوياً في أسوأ الفروض.

١٢- مراجعة قائمة المستخدمين بالنظم التشغيلية وإلغاء جميع المستخدمين الغير نشطة.

١٣-إصدار تقرير يومي بالحسابات الداخلية غير النشطة ومراجعة الحركات التي تجرى فيها مقابل المستندات.

١٤-إصدار تقارير بالتغييرات التي تحدث على وضع الحسابات كالحسابات التى يتم تجميدها والحسابات المغلقة وبالحسابات التي تم تنشيطها والحسابات التي أزيل تجميدها أو إيقافها.

١٥-إصدار تقارير بالحساب ذات الأرصدة الكبيرة ومراقبة حركاتها .

١٦-فصل شبكة بيئة التطوير عن بيئة التنفيذ فعلياً أو إفتراضياً .

١٧- عدم السماح للمبرمجين والإختصاصين الفنيين من إجراء التعديلات مباشرة على برامج النظم في بيئة التنفيذ.

١٨-عدم ربط البيئة التنفيذية الداخلية بالبيئة الخارجية بما فيها الإنترنت إلا إذا دعت الضرورة لذلك، في هذه الحالة يجب تطبيق سياسة صارمة لذلك من حيث فصل الشبكات وتركيب وسائل حماية قوية من طوق أمني و غير ذلك.

١٩-بما أن معظم الأعطال ناتجة عن إصابة الأنظمة بالفيروسات والبرامج الخبيثة فعلى البنوك وضع إستراتيجية شاملة لمكافحة الفيروسات وذلك بجلب وتركيب برامج المكافحة المعروفة والمشهود لها بفاعليتها، بحيث تشمل الإستراتجية تركيب برامج مراقبة واكتشاف الفيروسات وبتوفيق البرامج بالخوادم بحيث لا تسمح للأجهزة الطرفية بالدخول إليها إذا لم تكن بها برامج إكتشاف الفيروسات وحديثة ومتوائمة مع ما بالخادم من برامج الحماية كما يجب أن تتضمن الاستراتيجية عدم نقل أو جلب البرامج والبيانات لنظم المصرف بأي وسيلة ما لم يتم فحصها وتوثيقها من قبل الجهة المختصة بالمصرف بخلوه من الفيروسات والبرامج الخبيثة .

٢٠- سد الفجوة المعرفية بين التنفيذيين والتقنيين بالبنوك وذلك بالتدريب المستمر وتحديد مهام كل طرف بوضوح وإشراك التنفيذيين في المراحل المختلفة من إختيار أو تطوير وإعداد النظم التقنية المصرفية.

٢١- قيام البنك المركزي بفرض الإطار العام للسياسات الامنية لحماية نظم معلومات المصارف وحقوق المودعين،وذلك بالمتابعة والتفتيش المستمر للتأكد من إلتزام البنك في تطبيق السياسات بدقة .

٢٢- تخصيص المستخدمين الذين يتمتعون بمقدرات إدارية على كمبيوتر معين بحسابين:

أحدهما له مزايا إدارية والآخر له مزايا محدودة واستخدام حساب المستخدم العادي المحدود عند تصفح الإنترنت أو قراءة البريد الإلكتروني فبهذه الطريقة إن زار المستخدم موقعاً خطراً أو فتح بريداً إلكترونياً يحتوي فيروساً سيحصل المهاجم على حقوق محدودة.

٢٣- تطبيق ما يعرف بـ "المعيار الثنائي للتحقق من الهوية"، وهو نظام إلكتروني يستخدم لإضافة المزيد من الأمان إلى المعاملات المصرفية الخاصة بالعملاء، وذلك عن طريق التحقق من هوية العميل وحماية سلامة المعلومات المالية الخاصة به. يعمل هذا المعيار بمجرد إدخال اسم المستخدم وكلمة السر التي تعد بمثابة خطوة واحدة للتحقق من هوية العميل، ومن ثم يقوم المصرف بإرسال رقم سري إضافي وبشكل تلقائي إلى هاتف العميل المقيد لدى المصرف في كل مرة يقوم فيها بتسجيل الدخول إلى حسابه، وهذه الخطوة الاحترازية تعتبر الثانية للتحقق من الهوية قبل أن يتمكن العميل من الدخول إلى حساباته وتنفيذه للعمليات المصرفية المختلفة، ما يحقق المزيد من الحماية للمعلومات والمعاملات المالية الخاصة بالعملاء، ويقلل من فرص الوصول غير المصرح أو غير المشروع إلى حساباتهم.

24- اصدار تعليمات مكتوبة للعملاء لتوخي الحذر تتعلق بـ :

أ. استخدام الحواسب في الأماكن العامة وخاصة عند إجراء التعاملات المالية أو إرسال المعلومات الشخصية.

ب.تنبيه العملاء تجنب إرسال أية معلومات تتعلق بالبيانات المالية بالبريد الإلكتروني. وتجنب إرسال أو ذكر أية معلومات شخصية أو مالية عبر مواقع الإنترنت (مثل أرقام البطاقات المصرفية أو رقم الهاتف الشخصي) أو أية معلومات تدل على تفاصيل بيئة العمل كالعنوان ونوع العمل أو اسم الشركة وما إلى ذلك.

٢٥- من الأفضل عدم إدخال كلمة السر عن طريق لوحة المفاتيح أو الماوس حيث يمكن إظهار لوحة المفاتيح بشكل عشوائي بحيث يتغير في كل مرة ترتيب الحروف على لوحة المفاتيح الظاهرة بشكل عشوائي . ولكن هناك حل مثالي وهو كالتالي:

جزء من كلمة المرور يتم توليده بشكل عشوائي كل فترة زمنية تختلف كل ساعة بواسطة جهاز (Token)،هدفه توليد أرقام عشوائية بالتزامن مع المخدم، واستخدام مولدات أرقام عشوائية متزامنة بين المخدم وجهاز (Token). مشكلة هذا الجهاز أن كلفته عالية والزبون الذي يريد حماية بياناته ومعلوماته وحسابه المصرفي يجب عليه اقتناؤه.

٢٦- بالإضافة إلى الرقابة الوقائية والتصحيحة يجب تعميم فكرة الدفاع بالعمق والتي تقوم على استخدام طبقات متعددة من الرقابة وذلك لتجنب الفشل في أي نقطة فتعدد طبقات الرقابة يزيد من الكفاءة لنظم المعلومات المحاسبية في المصارف

ثانياً : توصيات وحلول لحماية شاملة لنظم المعلومات :

و ذلك وفق الترتيب التالي :

أولاً: السياسات و الإجراءات الإدارية والفنية التي تضمن حماية المصرف من المخاطر

١-سياسة الدخول للمعلومات:

يجب أن تكون عملية الدخول الى المعلومات محدده ومحكمة بحيث تراعي متطلبات العمل والحماية وقواعد الدخول الخاصة بكل نظام من نظم المعلومات ونأخذ بعين الاعتبار هذه القواعد:

- المتطلبات ذات الصله بالحماية لتطبيق أو تطبيقات العمل.
- وجود حاجة محددة ذات صله بالعمل لدى المستخدم للدخول إلى المعلومات أو عمليات العمل.
- يتم حجب كافة أنواع الدخول ما لم يتم الموافقة عليه بموجب أحكام هذه اللائحة.
- تعريف ملفات دخول المستخدمين وإدارة صلاحيات دخول المستخدمين على امتداد البنية التحتية لتقنية المعلومات بالمصرف.يجب تطبيق ضوابط الدخول عبر تحديد إعدادات لمجموعات مستخدمين ترتبط بصلاحيات محدده، وينبغي أن لا يتم منح المستخدمين

الفرديين دخولاً مخصصاً، حيث عوضا عن ذلك تمكينهم من الدخول من خلال العضوية ضمن مجموعات محدده مسبقا.

- يجب سحب حقوق دخول المستخدمين إلى نظم المعلومات أو الخدمات فور حدوث أي تغيير على الدور المناط بهم أو في حالة الاستقالة أو نهاية الخدمة.

أ.سياسة إدارة الدخول للمعلومات: لضمان دخول المستخدمين المصرح لهم إلى النظام والحيلولة دون الدخول غير المصرح به لنظم المعلومات:

- ينبغي توثيق وتطبيق تسجيل دخول وإجراءات المستخدم حسب الوصول.
- لا يجب أن يتم منح أي مستخدم رسميا حق الدخول قبل الانتهاء بالكامل من إجراءات تحديد صلاحياته.
- يخصص لكل مستخدم من مستخدمي نظم المعلومات هوية مستخدم فريدة ويفوض من قبل مالك الأصل أو الإدارة بالدخول للأصول المعلوماتية للجامعة.
- لا يسمح للمستخدمين وتحت أي ظرف من الظروف بتبادل أسماء وكلمات المرور بينهم. وفي هذه الحالة يتحمل المستخدمون المسئولية المباشرة عن كافة أنشطة النظام التي تمت من خلال صلاحيات المستخدم المخصصة لهم.
- ينبغي عدم تخصيص هويات المستخدمين التي سبق وإن كانت مخصصة لمستخدمين آخرين لمستخدمين جدد.
- على إدارة تقنية المعلومات اتخاذ تدابير إضافية واستخدام ضوابط ملائمة (كالتوعية بأهمية حماية المعلومات مثلا) للحيلولة دون سرقة الهوية واعتراض بيانات المستخدم من خلال أساليب الاختراق والاعتراض أو الاستدراج.
- يتم تخصيص كافة الامتيازات عالية المستوى (كتلك الخاصة بالإداري أو بالحسابات الجذرية) للمستخدمين من خلال الالتزام بإجراءات تفويض رسمية، بحيث لا يتم تخصيص أي امتياز قبل الانتهاء من إجراءات التفويض.
- على مركز تقنية المعلومات وبالتنسيق مع الإدارة المعنية مراجعة كافة صلاحيات دخول المستخدمين كل ٦ أشهر. وتخضع صلاحيات الدخول للإداريين للمراجعة كل ٣ أشهر.
- على مركز تقنية المعلومات القيام بعمليات تدقيق منتظمة على نظم المعلومات للكشف عن الحسابات غير المستخدمة. وينبغي تعطيل مثل هذه الحسابات ومن ثم إزالتها.
- عند اكتشاف أي إساءة استخدام لصلاحيات حقوق الدخول تقوم إدارة المركز بتقييد هذه الصلاحيات وإبلاغ الإدارة المعنية لاتخاذ اللازم.

- يجب الحفاظ على خصوصية وسرية اسم المستخدم وكلمة المرور للنظم وأن يتم تخصيصها واستخدامها بصورة آمنة.
- عند اقتناء النظم، يجب تغيير كافة اسماء المستخدمين وكلمات السر الافتراضية وذلك قبل ربطها بالبنية التحتية بالمصرف ووضعها في بيئة الانتاج.
- على مركز تقنية المعلومات توفير سجل متكامل وتوثيق التغييرات على أسماء المستخدمين وعلى كلمات المرور الخاصة بهم للدخول للنظم.
- على كافة مستخدمي نظم المعلومات الالتزام بالقواعد التالية بوصفها مرجعاً لهم عند اختيارهم لكلمات المرور الخاصة بهم.
- ان لا يقل الحد الادنى لطول كلمة المرور عن (٨ حروف ورموز).
- أن تتكون كلمة المرور من حروف وأرقام ورموز.
- أن لاتتضمن كلمة المرور اسم المستخدم أو جزء منه.
- أن لا تكون كلمة المرور قابلة للتخمين أو كلمة من القاموس.
- لا يسمح بترك كلمة المرور خالية.
- على المستخدمين تغيير كلمة المرور عند تسجيل الدخول لأول مرة الى أى نظام.
- يجب تغيير كلمة المرور كل ١٨٠ يوم.
- يجب تغيير كلمة المرور في حالة الشك باكتشافها وإبلاغ مدير الإدارة المعنية.

ب.سياسة مسئوليات المستخدمين: لمنع دخول المستخدمين غير المصرح لهم أو تعرض المعلومات أو عمليات معالجة المعلومات للخطر أو سرقتها.

- يجب على كافة المستخدمين تشغيل شاشات التوقف بكامات مرور على الحواسيب الشخصية، الحواسيب النقاله، والخوادم للحيلولة دون الدخول غير المصرح بها.
- على كافة المستخدمين وعند الانتهاء من أداء أعمالهم إنهاء كافة فترات الاتصال النشط بالشبكة.
- عدم استخدام الأوراق ووسائط الحاسوب وخصوصا فيما بعد ساعات العمل الرسمي، ينبغي حفظها في خزانات مناسبة ومغلقة.
- يجب إزالة الأوراق والتي تحتوي على معلومات حساسة أو سرية من الطابعات فور طباعتها.

ت.سياسة الدخول لنظام التشغيل:

- ينبغي تهيئة نظام التشغيل بحيث يعمل على تشغيل خدمات مقيده ووفقا للحاجة.

- عرض معلومات محدودة فقط عن النظام والهدف من استخدامه عند تسجيل الدخول لأي نظام.
- ينبغي للنظام عرض تنبيه عام مفاده بأن الدخول للحاسوب يقتصر على المستخدمين المصرح لهم فقط.
- يكون الدخول للبرامج الخدمية محدودا ويخضع للسيطرة وذلك بهدف منع أي ضرر محتمل لسلامة ضوابط الحماية الخاصة بمعلومات المصرف.

ث.سياسة الدخول للتطبيقات:

- يجب أن يعمل المصرف على تقييد دخول المستخدمين وموظفي الدعم الى نظم المعلومات والتطبيقات.
- يجب وضع ضوابط بهدف ضبط المخرجات من نظم التطبيقات التي تتعامل مع المعلومات الحساسة.
- يجب تنفيذ عملية عزل مادية و/أو منطقية للنظم الحساسة.
- يجب تشغيل التطبيقات الحساسة التى تتعامل مع البيانات الحساسة على أنظمة تشغيل مخصصة.
- يجب تهيئة التطبيقات لتعمل على تشغيل خدمات محدودة فقط، وذلك طبقا لمتطلبات المصرف.

ج. سياسة الدخول من الأجهزة النقالة:

- يجب أن لا يتم السماح بالدخول إلى المعلومات الخاصة بالعمل، عبر الشبكات العامة وباستخدام تسهيلات الحوسبة المتنقلة، إلا بعد القيام بعملية تحقق ومصادقة ناجحة، مع توفير آليه لضبط الدخول.
- في حالات السفر يجب عدم ترك الأجهزة والوسائط دون إشراف في الأماكن العامة.
- يجب توفير كافة ترتيبات وضوابط الحماية قبل التفويض بالعمل عن بعد.
- عند استكمال أنشطة العمل عن بعد يجب وعلى الفور إلغاء التفويض وصلاحيات الدخول وإعادة الأجهزة.
- يجب حفظ سجل دقيق وحديث بكافة الأنشطة المتعلقة بالعمل عن بعد.
- عند فقدان أي جهاز متنقل ينطوى على بيانات حساسة أو حصول أي انتهاك آخر للحماية يجب القيام فورا بإبلاغ مركز تقنية المعلومات.

- ينبغي للمستخدمين أن يكونوا على معرفة بمسئوليتهم الشخصية عن الأجهزة وكافة البيانات والمعلومات الموجودة أو المخزنة على الأجهزة ووسائط التخزين الموجودة أو المخزنة على هذه الأجهزة.

ثانياً :سياسة حماية المعلومات:

- يتوجب على إدارة المصرف إدراك مسئوليتها نحو دعم أهداف حماية المعلومات وتقديم التوجيه والدعم للمبادرات الخاصة بالحماية.
- تقوم الإدارة بتطوير واعتماد سياسة حماية المعلومات، وضمان مراقبة عملية تطبيقها.
- يجب العمل على توفير التنسيق بين الإدارات المختلفة بخصوص الأدوار المرتبطة بالحماية ووظائف العمل. وعلى كافة وحدات المصرف وبدعم من إدارة مركز تقنية المعلومات ضمان توفر مستويات مقبولة من الحماية للاصول المعلوماتية الموجودة لديهم.
- تلتزم المصرف بتبني معايير عالمية وأفضل الممارسات المعتمده، إضافة إلى تبني المتطلبات التنظيمية والتشريعية وذلك بهدف ضمان:
  - التزام موظفي المصرف بالمحافظة على حماية الأصول المعلوماتية الموجودة بحوزتهم .
  - عدم الدخول للمعلومات إلا من قبل الأفراد المصرح لهم بذلك، والذي له تفويض رسمي بذلك.
  - تطبيق الضوابط الملائمة لحماية كافة المعلومات السرية.
  - عدم تغيير أو تحديث المعلومات إلا من قبل الأفراد المصرح لهم بذلك والذي لديهم تفويض رسمي معتمد بذلك.
  - ديمومة توفر المعلومات لكافة الأفراد المصرح لهم بذلك.
  - إن كافة الموظفين الذين حصلوا على أي نوع من التفويض بالدخول إلى المعلومات يتحملون كامل المسئولية عن الاستخدام المناسب لهذه المعلومات.
  - إن كافة موظفي المصرف على إدراك تام ويقرون بمسئوليتهم فيما يتعلق بالالتزام بسياسات وإجراءات ومعايير حماية المعلومات.
- تقوم إدارة مركز تقنية المعلومات بمراجعة وتحديث سياسات وإجراءات ومعايير حماية المعلومات كل عام.
- يقوم مركز تقنية المعلومات بإجراء قياس سنوي لفعالية الضوابط المطبقة بهدف تجنب حوادث انتهاك حماية المعلومات وتقليص الآثار الناتجة عن ذلك، بالإضافة إلى مقارنة مستوى نضج الحماية في المصرف مع مؤسسات اخرى مماثلة.

- توافق سياسات وإجراءات ومعايير حماية المعلومات ذات الصلة مع المتطلبات القانونية والتنظيمية والمعايير العالمية.
- تقوم إدارة مركز تقنية المعلومات بالتعاون مع الإدارة بضمان التحقيق الفعَال لأهداف وغايات حماية المعلومات والأنشطة الاخرى ذات الصلة.

٣- سياسة التعامل مع حوادث أمن المعلومات:

أ الإبلاغ عن الحوادث المرتبطة بحماية المعلومات: بحيث يضمن الإبلاغ عن حوادث أم المعلومات المرتبطة بنظم المعلومات اتخاذ إجراءات تصحيحية دون تأخير:

- يتوجب على الموظفين ذوي العلاقة الإبلاغ عن كافة حوادث أمن المعلومات المؤكدة أو المحتملة.
- ينبغي العمل فورا على إبلاغ مركز تقنية المعلومات بكافة الحوادث التي يشك بوجودها.
- على كافة موظفي المصرف إدراك مسئولياتهم فيما يتعلق بالإبلاغ عن أي حادثة ذات صلة بأمن المعلومات يكون لها آثار معروفة أو محتملة على أمن المعلومات.

ب إدارة الحوادث المرتبطة بحماية المعلومات: بحيث يضمن تطبيق نهج متجانس وفعال لإدارة حماية أمن المعلومات:

- يتولى مركز تقنية المعلومات مسئولية تطوير وتطبيق إجراءات للقيام بالأنشطة الروتينية للتحقق من الكشف عن الحوادث، والإبلاغ عن حوادث أمن المعلومات، وضبط الأضرار ومعالجتها والحيلولة دون إلحاق اضرار مستقبلية بموارد المصرف.
- ينبغي أن لا يسمح بدخول إلا الموظفين المحددين والمفوضين بدخول الأنظمة المتأثرة خلال الحادثة، ويجب توثيق كافة الإجراءات العلاجية بحيث يتم توفير أكبر قدر من التفاصيل.
- يتوجب على مركز تقنية المعلومات وبناء على المعلومات المتوفرة ودرجة حيوية وأهمية الحادثة، إرسال تحذيرات بخصوص الحادثة إلى الإدارات التي قد تتأثر بمثل هذه الحوادث.
- تقوم إدارة المصرف بإجراء تحقيق واف في جذور وأسباب الحادثة وتعمل على اتخاذ إجراءات مناسبة بهدف:
  - تحذير، معاقبة، أو مقاضاة المسئولين عن الحادثة.
  - تحديث ضوابط الحماية الحالية أو استحداث ضوابط جديده بهدف الحليولة دون تكرار وقع نفس الحادثة.

٢-سياسة اقتناء وتطوير نظم المعلومات:

أ تحليل ومواصفات متطلبات الحماية: بحيث يتم التأكد من أن الحماية تمثل جزءاً لايتجزأ من نظم المعلومات:

- ينبغي تحليل متطلبات الحماية بخصوص نظم المعلومات الجديدة أوالتحسينات على النظم الحالية، واستحداث الضوابط الضرورية عبر اتباع إجراءات رسمية.
- يتولى المصرف ضمان أن كافة عمليات تطوير نظم المعلومات أو اقتنائها تتم وفقاً للمتطلبات، والمعايير والإجراءات الموثقة.
- يتولى المصرف ضمان تحديد وتوثيق وتطبيق ومراقبة ضوابط حماية مخصصة لمخاطر معينة بخصوص كافة النظم الحيوية التي تدعم العمل بالمصرف.
- تتولى إدارة مركز تقنية المعلومات ممثلة في قسم أمن المعلومات، وبدعم من مالك الأصل المعلوماتي، مسئولية تنفيذ الإجراءات المحددة.
- تقوم المصرف بإجراء تقييم للتهديدات والمخاطر خلال مرحلة المتطلبات عند تطوير أوتطبيق إجراءات رئيسة أو اقتناء نظام حماية معلومات وذلك بهدف:
  - تحديد متطلبات الحماية الضرورية لحماية نظم المعلومات.
  - تخصيص تصنيف حماية للمعلومات ولنظم المعلومات.
  - يلتزم المصرف بضمان توفر الضوابط الكافية للحد من مخاطر فقدان أو أخطاء أو إساءة استخدام المعلومات في نظم المعلومات.
  - على المصرف ضمان التوثيق الكافي لكافة خطط حماية النظام وبأنه يتم إدامة هذه الخطط بخصوص كل نظام من نظم المعلومات.

ب معالجة التطبيقات: الحيلولة دون حدوث الأخطاء في المعلومات أوفقدانها أوتعديلها بدون تفويض أو إساءة استخدامها في التطبيقات:

- يجب تطبيق عمليات تحقق ومصادقة ملائمة على التطبيقات ونظم قواعد البيانات للتأكد من صحة وسلامة مدخلات ومخرجات بيانات نظم المعلومات وفي حالة البيانات الحساسة، ينبغي تطبيق ضوابط إضافية حسب الحاجة .
- يجب تصميم ضوابط المعالجة ضمن نظم التطبيقات وقواعد البيانات، وذلك للكشف عن عدم دقة المعلومات سواء أكان ذلك بسبب أخطاء المعالجة أو الأعمال المتعمدة.
- يجب تصميم ضوابط المخرجات ضمن التطبيقات، للتحقق من صحة وسلامة معالجة البيانات المخزنة .

- تخضع عملية إجراء التغييرات على الوثائق والموارد الخاصة بالبيانات المدخلة لإجراء التفويض .
- يجب تحديد وتوثيق مسئوليات كافة الموظفين القائمين على إجراءات إدخال وإخراج البيانات.
- يجب وضع آلية ومعايير لتسجيل الأعطال للتعامل مع الأعطال التي يتم الإبلاغ عنها وينبغي العمل على مراقبة البيئة باستمرار بحثاً عن أية أحداث سلبية.

ت. ضوابط التشفير: بحيث يضمن حماية سرية وأصالة وسلامة المعلومات عبر استخدام وسائل التشفير:

- يجب تطبيق ضوابط التشفير حسب الحاجة على تطبيقات العمل الحيوية التي يتم الدخول إليها عبر الإنترنت، أوعلى أية نظم قد تتواجد عليها معلومات حساسة.
- يجب توفر حماية كافية للبيانات التي تبث عبر الإنترنت وذلك باستخدام تقنيات تشفير مناسبة.
- تتم عملية الاستيراد والتصدير واستخدام منهجيات التشفير بما يتوافق مع القوانين والنظم ذات الصلة.

ث. حماية عمليات التطوير والدعم: إدامة حماية برامج ومعلومات نظم التطبيق:

- يجب عزل بيئة الإنتاج عن بيئة التطوير والإختبار.
- يتم تنفيذ التغييرات في أوقات ملائمة، بحيث لاتؤثر سلباً على إجراءات العمل في المصرف.
- يجب وضع كافة الضوابط الضرورية للحد من تسرب المعلومات من الأجهزة التي تقوم بمعالجة المعلومات الحساسة، بحيث تتوافق تدابير الحماية مع سياسة إدارة الأصول.
- يجب التخطيط لمتطلبات سعة النظام قبل إدخال تطبيقات عمل حساسة جديدة، وأن تتم مراجعتها عند التحديث. وينبغي اتخاذ تدابير احتياطية ملائمة لتجنب أية إشكالات تتعلق بتوافر التطبيقات أوالنظم الحالية

ج. إدارة نقاط الضعف الفنية في الحماية: تقليص المخاطر الناجمة من استغلال نقاط الضعف الفنية:

- يتولى المصرف القيام بإجراءات استباقية لتحديد وتقليص نقاط الضعف في بيئة التقنية الخاصة بها، قبل قيام جهة ما باستغلال هذه النقاط.

- تتولى مركز تقنية المعلومات مسئولية إتخاذ الخطوات الاحتياطية لتوفير الحماية للبنية التحتية في المصرف.
- على الموظفين الذين يتولون مسئولية إدارة نقاط الضعف التأكد مما يلي:
  - استخدام أدوات المسح الأمني وفقاً لأسس محددة في التعرف على نقاط ضعف الحماية التي يمكن أن يتم استغلالها من قبل أشخاص يقومون بعمليات مسح غير مصرح بها باستخدام نفس الأدوات.
  - يجب استخدام أدوات متعددة تعتمد على تقنيات مختلفة في تحديد أكبر قدر ممكن من نقاط الضعف.
  - يجب القيام بمسح للأصول المربوطة بكل من الشبكة الداخلية وبشبكة الإنترنت.
  - يجب إبلاغ مالك المعلومات بالآثار المحتملة لأنشطة المسح في البيئة المستهدفة وقبوله لها، وذلك قبل بدء المسح.
  - يتم تركيب برامج الأصلاح على كافة الأجهزة المربوطة بالشبكات التي تحتوي على نظم تشغيل وتطبيقات يعرف عنها احتوائها على نقاط ضعف في الحماية، وذلك بهدف التعامل مع هذه النقاط.

٥-سياسة إدارة الاتصالات والعمليات:

أ. ضوابط الحماية من الكودات الضارة والمتنقلة: حماية سلامة البرامج والمعلومات:

- ينبغي أن يعمل المصرف على تحديد وتطبيق آلية ملائمة لمنع واكتشاف البرامج الضارة ومعالجة النظم المتأثرة بصورة ملائمة، ودون أي تأخير.
- ينبغي تطبيق برنامج مركزي للحماية من الفيروسات على المستويات المختلفة في البنية التحتية للشبكة.
- ينبغي أن يعمل الخادم المركزي للحماية من الفيروسات تلقائياً على تحديث تواقيع الفيروسات من مزود الخدمه، وكذلك القيام بهذه المهمة عند توفر تحديث للتوقيع أو لمحرك الفيروس.
- يجب اتخاذ كافة التدابير الممكنة والعملية الكفيلة بتوفير الوقاية من إدخال البرامج الضارة الى نظم المعلومات وشبكة المصرف.
- ينبغي تهيئة برنامج الحماية من البرامج الضارة بحيث يقوم تلقائياً بمسح أمني لسواقات (drives) وسائط التخزين النقالة وذاكرة الفلاش عند ربطها.

- على المصرف القيام بوضع وتطبيق إجراءات ملائمة للعمل بانتظام على جمع المعلومات، كالتسجيل في القوائم البريدية و/أو زيارة مواقع الويب التي توفر معلومات عن البرامج الضارة الجديدة.
- على المصرف منع تركيب البرمجيات غير المصرح بها أو غير القانونية على أي نظام للمعلومات.
- على المصرف توفير الحماية الفعالة ومنع المستخدمين من تغيير تهيئة أو إزالة أوتعطيل أو العبث بأي برنامج لمنع اكتشاف البرامج الضارة قد يكون تم تركيبه على الأجهزة المستخدمة من قبلهم.
- على المستخدمين استيعاب مسئوليتهم فيما يتعلق بإبلاغ مركز تقنية المعلومات عن أية مواضيع بخصوص أية كودات ضارة يشك في وجودها.
- ينبغي تفقد كافة الوسائط المتبادلة بين الدوائر والمؤسسات بحثاً عن البرامج الضارة قبل استخدامها أو تبادلها.
- ينبغي تهيئة برنامج الحماية من البرامج الضارة بحيث يقوم تلقائياً بمسح أمني لكافة الحواسيب الشخصية، الخوادم، الحواسب النقالة وأية مكونات اخرى من مكونات بنية النظم في المصرف لاكتشاف الكودات الضارة المحتملة.
- يتولي إداري النظام مسئولية مراقبة برامج الحماية من الفيروسات بصورة منتظمة، وذلك لضمان التعامل دون تأخير مع الحوادث المتعلقة بالفيروسات.

ب. النسخ الاحتياطي للمعلومات: المحافظة على سلامة وتوافر المعلومات وتسهيلات معالجة المعلومات:

- على مركز تقنية المعلومات، ومن خلال التعاون عن كثب مع مالكي النظم والبيانات والتنسيق معهم، تحديد متطلبات الحفظ الاحتياطي واستعادة البيانات لكافة نظم المصرف وبما يراعي الجوانب القانونية والتنظيمية، وتوصيات الموردين والعوامل الاخرى ذات الصلة.
- يجب إجراء حفظ احتياطي، وفقاً للإجراءات التي يوصي بها المورد/ المطبّق لكافة برامج التطبيقات ونظم التشغيل، والبيانات (بما في ذلك قواعد البيانات)، ومعلومات التهيئة الخاصة بالمستخدم.
- يجب الحصول على التفويض المناسب للقيام باستعادة البيانات من النسخ الاحتياطية، وأن تتم عملية الإستعادة وفقاً لإجراءات الحفظ الاحتياطي للبيانات واستعادتها.

- وجوب تفقد واختبار كافة نسخ الحفظ الاحتياطي على فترات منتظمة، وذلك لضمان سلامة وفعالية البيانات، وذلك من خلال القيام باستعادة بعض البيانات على أساس انتقائي.
- عنونة النسخ الاحتياطية وترقيمها تلقائياً حسب الأصول من قبل نظام الحفظ الاحتياطي أو يدوياً من قبل الإداري الذي يقوم بعملية الحفظ.
- ينبغي توفير وتحديث سجلات الحفظ الاحتياطي.
- يجب مراجعة سجلات الحفظ الاحتياطي من قبل إداري النظام ذي العلاقة لضمان تنفيذ عملية الحفظ حسب الأصول.
- العمل على تشفير نسخ الحفظ الاحتياطي التي تتضمن معلومات حساسة، فيما لو كان ذلك ممكناً.
- يقوم إداري النظام باختيار وسائط حفظ احتياطي ملائمة بناء على أهمية وحيوية البيانات ومدة الحفظ.
- على إداري النظام تفهّم مسئوليته عن الإبلاغ عن أية أوضاع قد تؤدي الى التأثير على سلامة البيانات المحفوظة أو على سريتها أو توافرها لأي سبب كان.

ت. إدارة حماية الشبكة: ضمان حماية المعلومات في الشبكات وحماية البنية التحتية المساندة:

- حماية سرية وسلامة وتوافر البيانات التي يتم تمريرها عبر الشبكات العمومية أو الشبكات اللاسلكية.
- حماية النظم والتطبيقات المربوطة.
- يجب الفصل بين مسئولية تشغيل الحواسيب لتجنب حدوث تداخل.
- يجب تسجيل ومراقبة أنشطة الدخول والخروج من وإلى الشبكة بهدف تسجيل أية أعمال تتعلق بالحماية.
- على المصرف تطبيق تدابير وخصائص حماية ملائمة للشبكة لحماية البنية التحتية لتقنية المعلومات.
- يتم وضع اتفاقية خدمات الشبكة بخصوص خدمات الشبكة التي يتم توفيرها داخلياً أو من خلال أطراف ثالثة على أن تتضمن خصائص الحماية ومتطلبات الإدارة ومستويات الخدمة.

ث. إدارة الوسائط: الحيلولة دون الإفشاء غير المصرح به أو التعديل أو إزالة أو إتلاف الأصول أو تعطيل أنشطة العمل

- على مالكي الأصول المعلوماتية التأكد من إدارة وضبط الوسائط وفقاً للسياسات والإجراءات المعمول بها في المصرف.
- يجب تخزين كافة الوسائط ضمن بيئة آمنة ومحمية وفقاً للمواصفات التي توفرها الجهات الصانعة لهذه الوسائط.
- يجب تخزين المعلومات الموجودة على وسائط والتي يحتاج إليها المصرف لفترة زمنية تزيد عن فترة الصلاحية وسائط التخزين في مكان آخر للحد من فقدان المعلومات بسبب تدهور حالة وسائط التخزين.
- تحفظ المعلومات الشخصية على الوسائط النقالة فقط عندما تكون هناك حاجة ماسة لذلك وينبغي أن تكون مشفرة.
- يجب تفعيل محركات الوسائط القابلة للنقل فقط في حالة وجود حاجة حقيقية لها تكون مرتبطة بالعمل.
- يجب تسجيل كافة الوسائط القابلة للنقل ضمن سجل يتم تحديثه لتقليص فرص فقدان البيانات.
- ينبغي أن يتم إعادة تهيئة الوسائط القابلة للنقل والتي يمكن إعادة الكتابة عليها، وذلك للحيلولة دون الكشف عن المعلومات عن غير قصد خلال عمليات تبادلها بين الموظفين والأطراف الاخرى.
- يجب التخلص بصورة ملائمة من كافة الوسائط وفقاً لإجراءات تصنيف وعنونة وتداول المعلومات ومدة الإحتفاظ بها أو الانتهاء من استخدامها.
- يحتفظ بسجل حديث بخصوص كافة وسائط التخزين التي تم التخلص منها وذلك بهدف توفير إمكانية تعقب التعديلات عليها.
- يجب حماية الوسائط أثناء النقل من الدخول غير المصرح به أو إساءة الاستخدام أو التلف.

6- سياسة حماية الموظفين :

- يتلقى كافة الموظفين، فيما إذا دعت الحاجة تدريباً في مجال التوعية بأهمية حماية المعلومات، بالإضافة الى تزويدهم على أساس منتظم بالتحديثات التي تتم على السياسات والإجراءات ويكون لها صلة بمسئولياتهم الوظيفية.

- يقوم المصرف بالتاكد من أن كافة الموظفين على دراية بمتطلبات حماية المعلومات، وبأنهم يتم تدريبهم على متطلبات وإجراءات الحماية المرتبطة بأعمالهم.
- تتولي المصرف، وبهدف ردع الآخرين، إيقاع إجراءات تأديبة رسمية بالموظفين الذين يصرون على انتهاك سياسات حماية المعلومات.
- ينبغي للإجراءات التأديبية أن تنطوي على معاملة الموظفين، الذين يشك في قيامهم بإنتهاك الحماية، بصورة صحيحة ومنصفة.
- تعمل المصرف على اتخاذ تدابير احتياطية للفصل بين واجبات الموظف بهدف تقليص فرص التعديل غير المصرح به للمعلومات أو إساءة استخدامها.
- يجب عدم استخدام تسهيلات معالجة المعلومات لأغراض ليست لها صلة بالعمل . وفي حالة اكتشاف أية عمليات تحايل فإنه سيتم التعامل معها وفقا للإجراءات التأديبية.
- على كافة الموظفين تفهم مسئوليتهم فيما يتعلق بسرعة إبلاغ المصرف، عن أي أحداث أو مخاطر ذات صلة بحماية المعلومات.
- على كافة الموظفين إعادة كافة الأصول المعلوماتية والمادية الموجودة بعهدتهم عند إنهاء الوظيفة أو العقد.
- ينبغي أن يتم سحب حقوق الدخول الى المعلومات وتسهيلات معالجة المعلومات عند إنهاء خدمة الموظفين أو الاتفاقية التعاقدية .

٧-الأدوار والمسئوليات

أ.دور الإدارة:

- دعم تنفيذ الحماية في بيئة المصرف لحماية الأصول المعلوماتية والبرامج الحيوية للعمل.
- الموافقة على استخدام كافة نظم المعلومات المستخدمة في معالجة وتخزين أو طباعة المعلومات الحساسة.
- الموافقة على السياسات الجديدة أو على التعديلات التي تتم على السياسات الحالية.

ب.دور مركز تقنية المعلومات:

- توزيع وثائق حماية المعلومات، بحيث تحصل الجهات التي تحتاج إليها على نسخ منها، أو تمكينها من الحصول عليها عبر موقع على الشبكة الداخلية.
- ضمان حماية نظم المعلومات والبنية التحتية وفق للآليات التقنية التي تحدد لجمايتها.
- مراقبة حماية النظم، التطبيقات والشبكة.

- تحديد وإدامة سياسات حماية المعلومات. إعدادات كتيبات حماية المعلومات اللازمة لتعزيز مستوى حماية المعلومات في المصرف، وتحديث هذه الكتيبات بشكل دوري.
- تطبيق الضوابط الملائمة لحماية سرية وسلامة وأصالة المعلومات الحساسة.

ت.دور المستخدم:

- الالتزام بسياسات الحماية وإرشادات وإجراءات حماية البيانات الحساسة.
- إبلاغ رئيس القسم الذي يتبع له عن نقاط الضعف التي تؤثر بالفعل، أو هنالك شكوك قد تؤثر على سرية وسلامة وتوافر البيانات والمعلومات الحساسة.
- استخدام وتوظيف المعلومات في الأغراض التي تنسجم مع أهداف المصرف.

ثانياً: توحيد كل بوابات الدفع الإلكتروني الخاص بالبنوك والمؤسسات ببوابة واحدة تتيح:

- هوية واحدة للزبون
- برمجية واحدة يحوي كل حساباته في البنوك وإدارتها معاً
- إتاحة عمليات الدفع الإلكتروني لكل المؤسسات عن طريق هذه البوابة وبالتالي لا داعي لأن يكون للمؤسسة أكثر من حساب واحد في أي مصرف وهذا يوفر على البنوك تكلفة الدارات والبرمجيات والربط مع المؤسسات.
- يوفر نقطة نفاذ موحدة قابلة للضبط والحماية بجهد أقل ودقة أكبر.

ثالثاً: إنشاء هذه البوابة وفق معايير اتصال موحدة ومعايير حماية موحدة، اي بالنسبة لهوية الزبون يجب أن يكون لديه هويتان، الهوية الافتراضية أي اسم المستخدم وكلمة المرور وهوية للصرافات أي البطاقات.

ملاحظة: من التوصية دمج كل مبدلات الصرافات في البنوك بمبدلة وطنية واحدة هي جزء من البوابة الموحدة.

رابعاً: حماية هذه البوابة وذلك من خلال :

أ. إنشاء شهادة رقمية تصدر عن الهيئة الوطنية لخدمات الشبكة واعتماد التوقيع الرقمي كجزء أساسي بكل عمليات التحويل المالي في البوابة.

ب. حماية الاتصالات مع المؤسسات المشتركة بالبوابة بطريقة موحدة تضمن:

- شهادة رقمية خاصة لكل مؤسسة تصدر عن الهيئة الوطنية لخدمات الشبكة.
- اعتماد التوقيع الرقمي على كل التعاملات بين البوابة والمؤسسات.
- تشفير كل المعطيات المتبادلة بالتعاملات المالية لحماية معلومات الزبون وخصوصيته.
- اعتماد الختم الزمني لضبط توقيت عمليات التعاملات المصرفية.

- حماية الخصوصية (بنوك، مؤسسات، أفراد)

خامساً:البدء بتنظيم جديد لبطاقات الصراف الآلي لحماية عملائها من عمليات الاحتيال والغش والسرقات، وذلك بإصدار بطاقات الصراف الآلي التي تتميز بخاصية احتوائها على شريحة ذكية Smart Chip تجعل البطاقة أكثر أماناً من السابق. وبتوفير هذه الإجراءات الأمنية الاحترازية المختلفة للعملاء أصبح لدى العملاء خيارات متعددة لحماية حساباتهم من الاختراق أو التعدي.

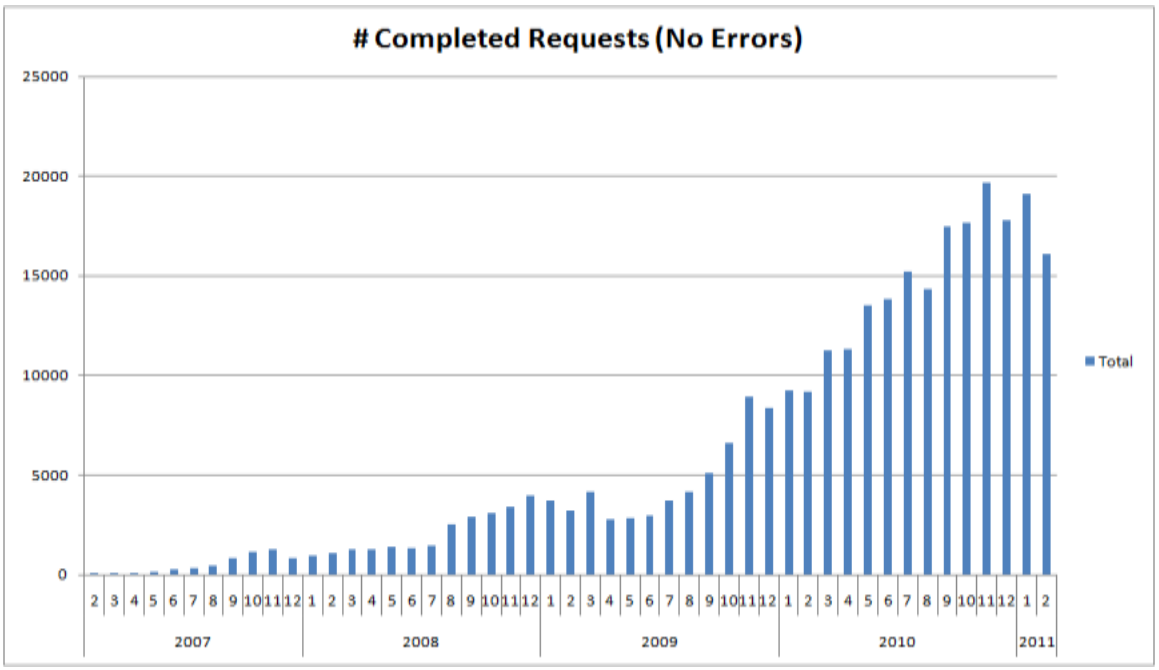
سادساً: الإسراع في تفعيل آليات عمل الهيئة الوطنية لخدمات الشبكة.

سابعاً:ضرورة ربط المصارف، فعليا، بين المعلومات والمواصفة **(ISO 27001)**، إذ إن هذا الربط سيوفر وسائل فاعلة وناجحة للتعامل مع المعلومات، فضلاً عن أن حصول المصارف على شهادة **ISO** في هذا المجال سوف يمّكن المنظمات من الحصول على ميزة تنافسية، وإكسابها الطابع العالمي من خلال حصولها على شهادة دولية.

الملاحق

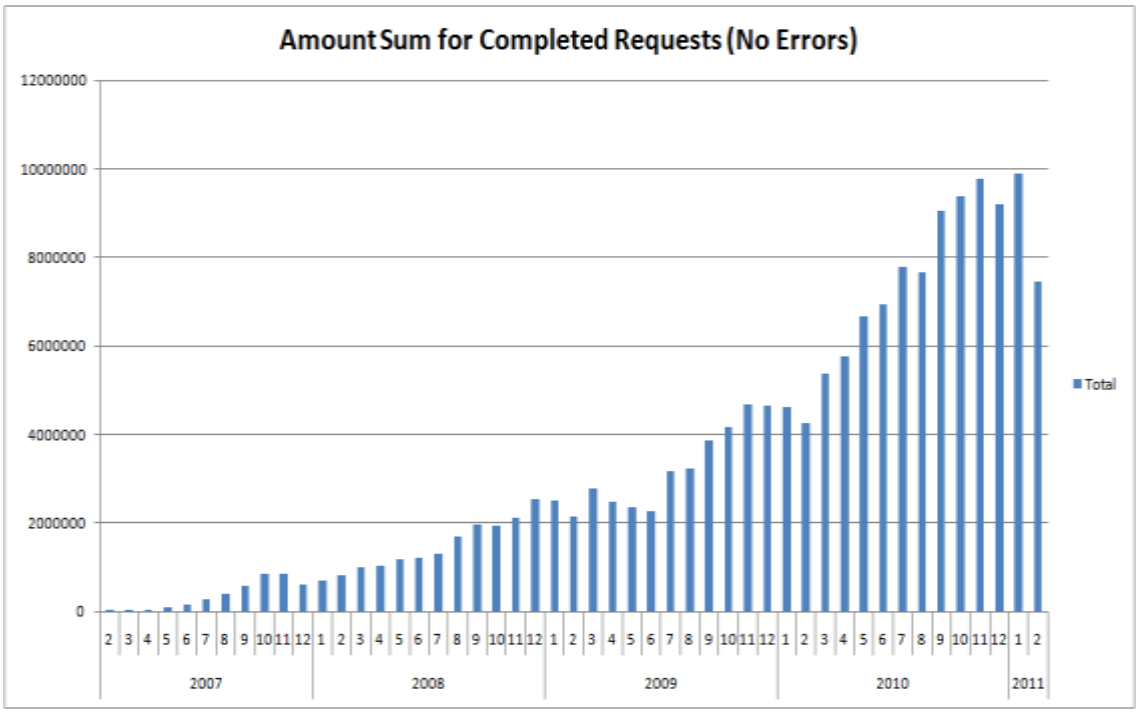
الملحق رقم (1)

إحصائيات: تطور عدد الطلبات شهرياً



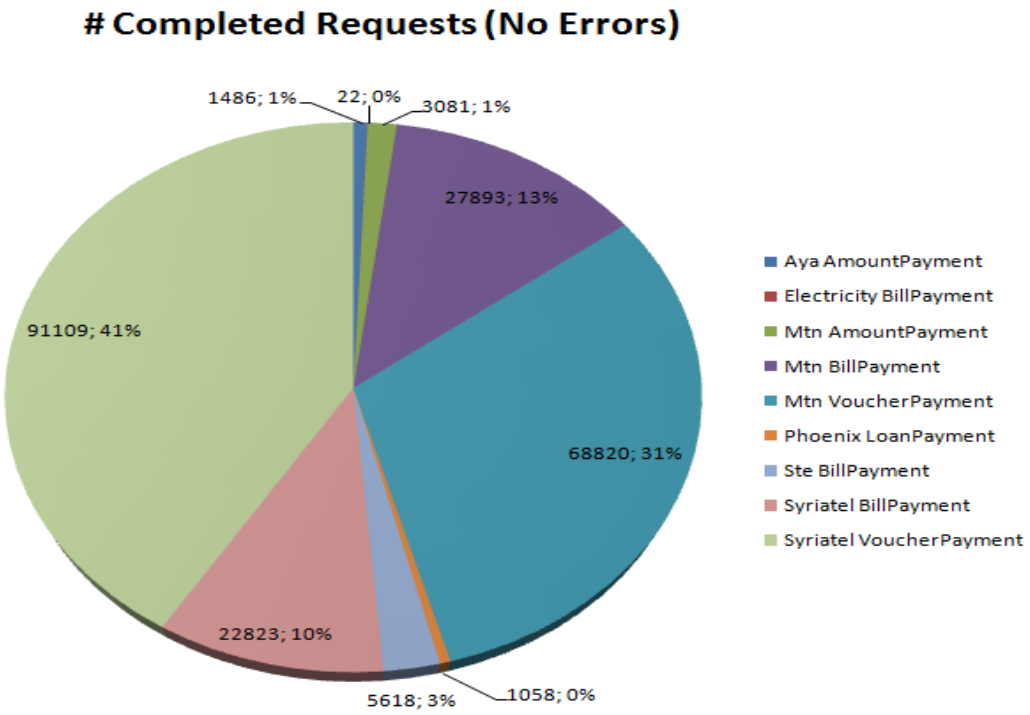
الشكل (١٧) إحصائيات تطور عدد الطلبات شهرياً

إحصائيات: تطور المبالغ المدفوعة شهريا



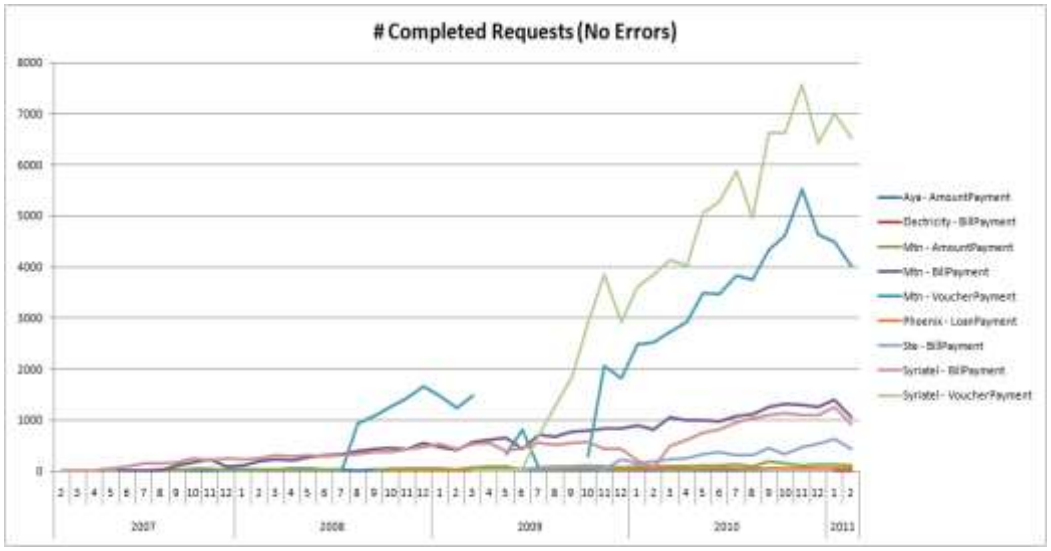
الشكل (١٨) إحصائيات: تطور المبالغ المدفوعة شهريا

إحصائيات: تطور كل خدمة شهرياً



الشكل (١٩) إحصائيات تطور كل خدمة شهرياً

إحصائيات: تطور كل خدمة شهرياً



الشكل (٢٠) إحصائيات تطور كل خدمة شهرياً

الملحق رقم (٢)

قائمة بالاسئلة التي وجهت إلى المصرفيين عينة الدراسة للاستعانة بها في عملية التحليل

السؤال رقم (١) هل تستخدم تقنيات نظم المعلومات في أداء جميع الأعمال لديكم ؟ نعم لا
السؤال رقم (٢) هل البنك مربوط بشبكة معلومات بجميع الفروع ؟ نعم لا
السؤال رقم (٣) هل ترى الاعتماد كلياً على التقانة ؟ نعم لا
السؤال رقم (٤) هل ترى الاعتماد على تقنية المعلومات في النظام المصرفي أكثر خطورة على أموال المودعين من النظام اليدوي ؟ نعم لا
السؤال رقم (٥) عادة ما تتم السرقات المالية بالبنوك باستخدام التقنية ؟ نعم لا
السؤال رقم (٦)من هم المصرح لهم بالدخول في نظم البنك ؟ المستخدمون – المبرمجون – موظفو شركة الصيانة – آخرون
السؤال رقم (٧) من هم المخول لهم باجراء التعديلات على البيانات ؟ مدخل البيانات – المشرف – آخرون
السؤال رقم (٨) من هو المسؤول عن تركيب وصيانة الشبكات ؟ موظفو البنك – عمل مشترك– جهات أخرى
السؤال رقم (٩) هل البنك مرتبط بالشبكة العالمية (الإنترنت) ؟ نعم لا
السؤال رقم (١٠) ما درجة اهتمام الإدارة العليا بأمن المعلومات ؟ اهتمام كبير– نوعا ما – لا يهتمون
السؤال رقم (١١) هل توجد دائرة خاصة بأمن وحماية المعلومات ؟ نعم لا
السؤال رقم (١٢) هل يوجد بالبنك جهة مختصة بمراجعة وتدقيق نظم المعلومات ؟ نعم لا

السؤال رقم (١٣) هل هناك موظفون متخصصون بأمن المعلومات وحمايتها ؟ نعم لا
السؤال رقم (١٤) هل هناك سياسات وإجراءات ومواصفات قياسية لأمن المعلومات؟ نعم – جزئياً– لا

السؤال رقم (١٥) هل توجد لدى البنك سياسات ومواصفات قياسية لتطوير وتشغيل نظم المعلومات ؟ نعم جزئياً لا
السؤال رقم (١٦) هل هناك موظفون متخصصون بمراجعة وتدقيق نظم المعلومات؟ نعم لا
السؤال رقم (١٧) من الذي يقوم بتطبيق سياسات نظم المعلومات بالبنك ؟ الإدارة العليا –إدارة نظم المعلومات – آخرون
السؤال رقم (١٨) ما نوع الحماية المستخدمة لدى البنك ؟ برامج – إجراءات – اخرى
السؤال رقم (١٩) ما الطريقة المتبعة في حماية شبكات نظم المعلومات بالبنك ؟ تركيب طوق أمني – تركيب برامج حماية الشبكات – عزل الشبكات عن بعضها – نظم أخرى
السؤال رقم (٢٠) ما الطريقة المستخدمة للدخول في نظم الحاسوب؟ بصمات اليد – الصوت – كلمة السر – البطاقات الذكية – بدون رقم سري وبطاقات
السؤال رقم (٢١) العلاقات الجيدة والثقة بين الموظفين عادة تجعلهم يستخدمون كلمات السر فيما بينهم. هل هذا ينطبق على بنككم ؟ نعم – لا – أحياناً
السؤال رقم (٢٢) هل يستخدم البنك برامج أصلية ومرخصة ؟ نعم – لا
السؤال رقم (٢٣) هل لدى البنك إستراتيجية مكافحة الفيروسات ؟ نعم – لا
السؤال رقم (٢٤) هل يستخدم البنك مضادات للفيروسات المرخصة ويواكب تحديثها؟ نعم – لا

السؤال رقم (٢٥) ما الإجراءات التي يتخذها البنك لتفعيل برامج ونظم حماية المعلومات ؟وضع خطة لمراقبة الأجهزة – ترك أجهزة الرقابة تقوم بها آلياً– ترك الأمر لموظفي التقنية والمستخدمين
السؤال رقم (٢٦) ما الإجراءات المتخذة للدخول إلى غرفة الحاسوب ؟ الرقم السري – نظم البطاقات – نظم المفتاح العادي – نظم الحارس
السؤال رقم (٢٧) هل هناك إجراءات لإدخال الأجهزة إلى البنك وإخراجها؟ نعم – لا
السؤال رقم (٢٨) من الذي يقوم بالاختراق، أوسوء استخدام النظام ؟ موظفو نظم المعلومات – مستخدمو النظم من الموظفين – مستخدموا النظم من الاداريين – باشتراك أكثر من طرف
السؤال رقم (٢٩) ما الوسائل المستخدمة في التخلص من الوسائط والمستندات والتقارير ؟ الاتلاف داخل البنك بإشراف لجنة – الاتلاف خارج البنك – عدم الاتلاف
السؤال رقم (٣٠) هل غرفة الحاسوب والمكاتب مجهزة ضد الحريق والمهددات الأخرى؟ نعم – نوعا ما – لا
السؤال رقم (٣١) هل هناك إجراءات لاستمرار العمل في حالة وجود خلل في النظام والشبكات ؟ نعم – لا – نوعا ما
السؤال رقم (٣٢) ما نوع الإجراءات المتخذة لاستمرار العمل في حالة وجود خلل في النظام؟ تشغيل النظام الاحتياطي – استخدام الطريقة اليدوية – الانتظار حتى معالجة العطل
السؤال رقم (٣٣) هل تتم مراجعة وتحديث إجراءات استمرار العمل بصفة دورية ؟ نعم – احيانا – لا
السؤال رقم (٣٤) هل يقوم البنك بعمل نسخ احتياطية للمعلومات بصفة دورية ويومية، لضمان أمن المعلومات وسلامتها ؟ نعم – لا – احيانا

السؤال رقم (٣٥) أين يحتفظ البنك بالنسخ الاحتياطية للسجلات وكافة المعلومات المهمة ؟ في مكان آمن داخل البنك – في مكان آمن خارج البنك – داخل غرفة الحاسوب
السؤال رقم (٣٦) هل الموظفون على دراية بأهمية أمن المعلومات وحمايتها ؟ نعم – لا
السؤال رقم (٣٧) ما الوسائل المستخدمة لتحفيز الموظفين العاملين التقنيين ؟ التحفيز المالي – التقدير الشخصي – حوافز أخرى
السؤال رقم (٣٨) هل تتوفر لدى البنك دورات تدريبية أو مجلات دورية عن أمن ونظم المعلومات ؟ نعم – لا – نوعا ما
السؤال رقم (٣٩) ما الإجراءات المتبعة عند الاستغناء عن موظفي الحاسوب أو استقالتهم؟ تغيير كافة الاجراءات التي كانوا يقومون بها – أخذ تعهدات منهم بعدم تسريب المعلومات – تقديم مكافأة مالية لهم على فترات – إجراءات اخرى
السؤال رقم (٤٠) هل توجد إجراءات إدارية وقانونية ضد الأفراد الذين يسربون المعلومات لجهات أخرى ؟ نعم – لا
السؤال رقم (٤١) ما الإجراءات التي يتبعها البنك حيال نظم المعلومات بعد نهاية ساعات العمل الرسمي؟تحديد المصرح لهم –إيقاف النظم والشبكات –مراقبة الشبكات والنظم– إجراءات أخرى

الملحق رقم (٣)

FREQUENCIES VARIABLES=q1 q2 q3 q4 q5 q9 q10 q11 q12 q34 q35 q36 q37 q38 q39 q40 /ORDER=ANALYSIS.

Frequencies

Notes		
Output Created		08-٢٠١٣ حزيران IDT 21:42:36
Comments		
Input	Data	F:\سهى سنكري\سهى سنكري.sav
	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	10
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on all cases with valid data.
Syntax		FREQUENCIES VARIABLES=q1 q2 q3 q4 q5 q9 q10 q11 q12 q34 q35 q36 q37 q38 q39 q40 /ORDER=ANALYSIS.
Resources	Processor Time	0:00:00.000
	Elapsed Time	0:00:00.000

[DataSet1] F:\سهى سنكري\سهى سنكري.sav

Statistics																	
		q1	q2	q3	q4	q5	q9	q10	q11	q12	q34	q35	q36	q37	q38	q39	q40
N	Valid	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
	Missing	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Frequency Table

q1					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	نعم	10	100.0	100.0	100.0

q2					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	نعم	10	100.0	100.0	100.0

q3					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	لا	5	50.0	50.0	50.0
	أحيانا	5	50.0	50.0	100.0
	Total	10	100.0	100.0	

q4					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	لا	6	60.0	60.0	60.0
	نعم	4	40.0	40.0	100.0
	Total	10	100.0	100.0	

q5					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	لا	1	10.0	10.0	10.0
	نعم	9	90.0	90.0	100.0
	Total	10	100.0	100.0	

q9					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	نعم	10	100.0	100.0	100.0

q10					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	نوعا ما	7	70.0	70.0	70.0
	اهتمام كبير	3	30.0	30.0	100.0
	Total	10	100.0	100.0	

q11					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	نعم	10	100.0	100.0	100.0

q12					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	لا	10	100.0	100.0	100.0

q34					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أحيانا	10	100.0	100.0	100.0

q35					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	في مكان آمن داخل البنك	3	30.0	30.0	30.0
	في مكان آمن خارج البنك	7	70.0	70.0	100.0
	Total	10	100.0	100.0	

q36					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	نعم	10	100.0	100.0	100.0

q37					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	التحفيز المالي	6	60.0	60.0	60.0
	التقدير الشخصي	1	10.0	10.0	70.0
	حوافز أخرى	3	30.0	30.0	100.0
	Total	10	100.0	100.0	

q38					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	لا	3	30.0	30.0	30.0
	نوعاً ما	5	50.0	50.0	80.0
	نعم	2	20.0	20.0	100.0
	Total	10	100.0	100.0	

q39					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	تغيير كافة الاجراءات التي كانوا يقومون بها	3	30.0	30.0	30.0
	إجراءات اخرى	7	70.0	70.0	100.0
	Total	10	100.0	100.0	

q40					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	نعم	10	100.0	100.0	100.0

```
FREQUENCIES VARIABLES=q6 q8 q21 q22 q23 q24 q28 q29
  /ORDER=ANALYSIS.
```

Frequencies

Notes		
Output Created		08-٢٠١٣ حزيران IDT 21:43:04
Comments		
Input	Data	F:\سهى سنكري\سهى سنكري.sav
	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	10
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on all cases with valid data.
Syntax		FREQUENCIES VARIABLES=q6 q8 q21 q22 q23 q24 q28 q29 /ORDER=ANALYSIS.
Resources	Processor Time	0:00:00.000
	Elapsed Time	0:00:00.015

[DataSet1] F:\سهى سنكري\سهى سنكري.sav

Statistics									
		q6	q8	q21	q22	q23	q24	q28	q29
N	Valid	10	10	10	10	10	10	10	10
	Missing	0	0	0	0	0	0	0	0

Frequency Table

q6					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	المستخدمون	6	60.0	60.0	60.0
	المبرمجون	3	30.0	30.0	90.0
	آخرون	1	10.0	10.0	100.0
	Total	10	100.0	100.0	

q8					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	موظفو البنك	2	20.0	20.0	20.0
	جهات أخرى	8	80.0	80.0	100.0
	Total	10	100.0	100.0	

q21					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أحيانا	4	40.0	40.0	40.0
	نعم	6	60.0	60.0	100.0
	Total	10	100.0	100.0	

q22					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	نعم	10	100.0	100.0	100.0

q23					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	نعم	10	100.0	100.0	100.0

q24					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	لا	3	30.0	30.0	30.0
	نعم	7	70.0	70.0	100.0
	Total	10	100.0	100.0	

q28					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	مستخدمو النظم من الموظفين	7	70.0	70.0	70.0

	مستخدموا النظم من الاداريين	3	30.0	30.0	100.0
	Total	10	100.0	100.0	

q29					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	الاتلاف داخل البنك بإشراف لجنة	2	20.0	20.0	20.0
	عدم الاتلاف	8	80.0	80.0	100.0
	Total	10	100.0	100.0	

FREQUENCIES VARIABLES=q7 q13 q14 q15 q16 q17 q18 q19 q20 q25 q26 q27 q30 q31 q32 q33 q41 /ORDER=ANALYSIS.

Frequencies

Notes		
Output Created		08-حزيران-٢٠١٣ 21:43:20 IDT
Comments		
Input	Data	F:\سهى سنكري\سهى سنكري.sav
	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	10
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on all cases with valid data.
Syntax		FREQUENCIES VARIABLES=q7 q13 q14 q15 q16 q17 q18 q19 q20 q25 q26 q27 q30 q31 q32 q33 q41 /ORDER=ANALYSIS.
Resources	Processor Time	0:00:00.031
	Elapsed Time	0:00:00.032

[DataSet1] F:\سهى سنكري\سهى سنكري.sav

Statistics																		
		q7	q13	q14	q15	q16	q17	q18	q19	q20	q25	q26	q27	q30	q31	q32	q33	q41
N	Valid	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
	Missing	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Frequency Table

q7					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	مدخل البيانات	9	90.0	90.0	90.0
	المشرف	1	10.0	10.0	100.0
	Total	10	100.0	100.0	

q13					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	لا	5	50.0	50.0	50.0
	نعم	5	50.0	50.0	100.0
	Total	10	100.0	100.0	

q14					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	جزئياً	3	30.0	30.0	30.0
	نعم	7	70.0	70.0	100.0
	Total	10	100.0	100.0	

q15					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	لا	7	70.0	70.0	70.0
	جزئياً	3	30.0	30.0	100.0
	Total	10	100.0	100.0	

q16					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	لا	8	80.0	80.0	80.0

	نعم	2	20.0	20.0	100.0
	Total	10	100.0	100.0	

q17

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	الإدارة العليا	4	40.0	40.0	40.0
	إدارة نظم المعلومات	6	60.0	60.0	100.0
	Total	10	100.0	100.0	

q18

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	برامج	4	40.0	40.0	40.0
	إجراءات	5	50.0	50.0	90.0
	اخرى	1	10.0	10.0	100.0
	Total	10	100.0	100.0	

q19

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	تركيب طوق أمني	6	60.0	60.0	60.0
	تركيب برامج حماية الشبكات	2	20.0	20.0	80.0
	عزل الشبكات عن بعضها	2	20.0	20.0	100.0
	Total	10	100.0	100.0	

q20

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	كلمة السر	10	100.0	100.0	100.0

q25

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	وضع خطة لمراقبة الأجهزة	3	30.0	30.0	30.0
	ترك أجهزة الرقابة تقوم بها آلياً	7	70.0	70.0	100.0
	Total	10	100.0	100.0	

q26

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	الرقم السري	5	50.0	50.0	50.0
	نظم المفتاح العادي	5	50.0	50.0	100.0
	Total	10	100.0	100.0	

q27

	Frequency	Percent	Valid Percent	Cumulative Percent

Valid	لا	4	40.0	40.0	40.0
	نعم	6	60.0	60.0	100.0
	Total	10	100.0	100.0	

q30					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	نوعاً ما	10	100.0	100.0	100.0

q31					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	لا	7	70.0	70.0	70.0
	نوعاً ما	3	30.0	30.0	100.0
	Total	10	100.0	100.0	

q32					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	الانتظار حتى معالجة العطل	10	100.0	100.0	100.0

q33					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	لا	10	100.0	100.0	100.0

q41					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	تحديد المصرح لهم	3	30.0	30.0	30.0
	إجراءات أخرى	2	20.0	20.0	50.0
	5	5	50.0	50.0	100.0
	Total	10	100.0	100.0	

```
T-TEST   /TESTVAL=1.5   /MISSING=ANALYSIS
  /VARIABLES=q1 q2 q4 q5   /CRITERIA=CI(.95).
```

T-Test

Notes	
Output Created	08-٢٠١٣-حزيران IDT 21:44:22

Comments		
Input	Data	F:\سهى سنكري\سهى سنكري.sav
	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	10
Missing Value Handling	Definition of Missing	User defined missing values are treated as missing.
	Cases Used	Statistics for each analysis are based on the cases with no missing or out-of-range data for any variable in the analysis.
Syntax		T-TEST /TESTVAL=1.5 /MISSING=ANALYSIS /VARIABLES=q1 q2 q4 q5 /CRITERIA=CI(.95).
Resources	Processor Time	0:00:00.000
	Elapsed Time	0:00:00.031

[DataSet1] F:\سهى سنكري\سهى سنكري.sav

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
q1	10	2.00	.000[a]	.000
q2	10	2.00	.000[a]	.000
q4	10	1.40	.516	.163
q5	10	1.90	.316	.100

a. t cannot be computed because the standard deviation is 0.

One-Sample Test

	Test Value = 1.5					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
q4	-.612-	9	.555	-.100-	-.47-	.27
q5	4.000	9	.003	.400	.17	.63

T-TEST /TESTVAL=1.5 /MISSING=ANALYSIS
/VARIABLES=q1 q2 q4 q5 q9 q11 q12 q36 q40 /CRITERIA=CI(.95).

T-Test

Notes		
Output Created		08-٢٠١٣ حزيران IDT 21:46:46
Comments		
Input	Data	F:\سهى سنكري\سهى سنكري.sav
	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	10
Missing Value Handling	Definition of Missing	User defined missing values are treated as missing.
	Cases Used	Statistics for each analysis are based on the cases with no missing or out-of-range data for any variable in the analysis.
Syntax		T-TEST /TESTVAL=1.5 /MISSING=ANALYSIS /VARIABLES=q1 q2 q4 q5 q9 q11 q12 q36 q40 /CRITERIA=CI(.95).
Resources	Processor Time	0:00:00.016
	Elapsed Time	0:00:00.016

[DataSet1] F:\سهى سنكري\سهى سنكري.sav

One-Sample Statistics				
	N	Mean	Std. Deviation	Std. Error Mean
q1	10	2.00	.000[a]	.000
q2	10	2.00	.000[a]	.000
q4	10	1.40	.516	.163
q5	10	1.90	.316	.100
q9	10	2.00	.000[a]	.000
q11	10	2.00	.000[a]	.000
q12	10	1.00	.000[a]	.000
q36	10	2.00	.000[a]	.000
q40	10	2.00	.000[a]	.000
a. t cannot be computed because the standard deviation is 0.				

One-Sample Test						
	Test Value = 1.5					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
q4	-.612-	9	.555	-.100-	-.47-	.27
q5	4.000	9	.003	.400	.17	.63

المراجع

المصادر والمراجع العربية:

الكتب:

١. إبراهيم, الحبيتي، قاسم، يحى السقا، "زياد: الإطار العلمي للمحاسبة كنظام للمعلومات"، جامعة الحدباء، الموصل، ٢٠٠٣.

٢. حماد، عبد العال، طارق، "التطورات العالمية وإنعكاساتها على أعمال البنوك الاسكندرية"،الدار الجامعية، ١٩٩٩.

٣. الحميد، محمد عباس, ونينو وماركو، ابراهيم, "حماية أنظمة المعلومات"، دار الحامد للنشر، عمان، ٢٠٠٧

٤. حنان، رضوان حلوة,و الحارث، أسامة, وأبو جاموس, فوز الدين, "أسس المحاسبة المالية"، دار الحامد للنشر والتوزيع، ٢٠٠٤.

٥. راضي،عبد المنعم، وعزت،فرج، "اقتصاديات النقود والبنوك"، البيان للطباعة والنشر، الاسكندرية، ٢٠٠١،

٦. ستيفن أ.موسكوف، مارك & سيمكن، "نظم المعلومات المحاسبية لاتخاذ القرارات، مفاهيم وتطبيقات"، دار المريخ، الرياض ٢٠٠٥.

٧. عبد المطلب, عبد الحميد، "البنوك الشاملة –عملياتها إداراتها"، الاسكندرية، الدارالجامعية، ٢٠٠٠

٨. الغثبر, سليمان، خالد، ومهندس, القحطاني, عبدالله،محمد "أمن المعلومات"، مكتبة الملك فهد الوطنية، ٢٠٠٩،

٩. القاسم، عبد الرزاق، "تحليل وتصميم نظم المعلومات المحاسبية"، عمان، مكتبة دار الثقافة للنشر والتوزيع، ٢٠٠٤.

١٠. القاسم، عبد الرزاق، والمصري، تيسير، والطويل، ليلى، "نظم المعلومات المحاسبية"، منشورات جامعة دمشق، ٢٠٠٥.

١١. القاضي, حسين، قريط عصام، "مراجعة الحسابات(إجراءات) "،منشورات جامعة دمشق، ٢٠٠٥.

١٢. المصري، تيسير، ويوسف، علي، "نظم المعلومات المحاسبية"، منشورات جامعة دمشق، ٢٠١١.
١٣. ياسين، فؤاد توفيق، درويش، أحمد عبد الله، "المحاسبية المصرفية في البنوك التجارية الإسلامية"، دار اليازوري العلمية، عمان، ١٩٩٦م

ب-الدوريات والمؤتمرات العربية:

١. القاسم ، عبد الرزاق و ردايده ، مراد " أمن نظم المعلومات المحاسبية في البنوك الأردنية"- دراسة ميدانية، المجلة العربية للعلوم الادارية والاقتصادية ، لبنان ، ٢٠١٠
٢. أبو سعد، وليد " أمن المعلومات"، الموسوعة العربية للكمبيوتر، سلسلة الدورات التعليمية الإلكترونية، ٢٠٠٥.
٣. اتحاد المصارف العربية، المبادئ العشرة للممارسات السليمة في مجال الرقابة على، وإدارة، مخاطر التشغيل، مديرية البحوث، مجلة اتحاد المصارف العربية، إبريل ٢٠٠٣.
٤. البحيصي، محمد عصام وشعبان،حرية "مخاطر نظم المعلومات المحاسبية الألكترونية: دراسة تطبيقية على المصارف العاملة في غزة", ٢٠٠٧.
٥. بختي, إبراهيم, "الإنترنت في الجزائر" مجلة الباحث، مجلة فصلية نصف سنوية تصدر عن كلية ا لحقوق والعلوم الاقتصادية جامعة ورقلة، ٢٠٠٢ عدد1
٦. بشنق، زهير "العمليات المصرفية الإلكترونية، اتحاد المصارف العربية، ٢٠٠٦،ص٣٤٤
٧. حسن, شحادة الحسين، "العمليات المصرفية الالكترونية- الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية"- مداخلة مقدمة إلى المؤتمر العلمي السنوي لكلية الحقوق، جامعة بيروت العربية، ٢٠٠٢.
٨. حمادة، رشا, "أثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الالكترونية في زيادة موثوقية المعلومات المحاسبية(دراسة ميدانية). ٢٠١٠
٩. زيدان، محمد, وحمو، محمد "متطلبات أمن المعلومات المصرفية في بيئة الانترنت"، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، الرياض، ٢٠١٠
١٠. زيدان، محمد, وحمو، محمد "متطلبات أمن المعلومات المصرفية في بيئة الانترنت، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية " الرياض, ٢٠١٠
١١. الساكني، عبد الكريم، سعد والعواودة، علي، حنان "مخاطر استخدام تكنولوجيا المعلومات وأثرها على أداء نظم المعلومات المحاسبية" جامعة الاسراء, ٢٠١١.

١٢. الشحادة ,عبد الرزاق, "دراسة العوامل المؤثرة في كفاءة نظم المعلومات المحاسبية في المصارف التجارية السورية",مجلة بحوث جامعة حلب، العدد ٣٤، ٢٠٠٣.
١٣. الشيخ، عاصم، "الاستخدامات الإلكترونية في القطاع المصرفي"، مجلة الدراسات المالية والمصرفية، المجلد ١٠، العدد ٢، يونيو ٢٠٠٢.
١٤. صيام، وليد زكريا، "كفاءة نظم المعلومات في القطاع المصرفي في ظل تكنولوجيا المعلومات"، مجلة البنوك في الأردن، المجلد ٢١، العدد ٩، ٢٠٠٢.
١٥. عبد الصادق، أسامة سعيد, "التقييم المحاسبي لكفاءة وفعالية نظم المعلومات الاستراتيجية في ظل عولمة النشاط الاقتصادي بالتطبيق على البيئة المصرية"، مجلة الدرسات المالية والتجارية، جامعة القاهرة، كلية تجارة بني سويف، السنة الثانية عشر، العدد الثاني، يوليو، ٢٠٠٢.
١٦. عبد الله، خالد أمين, وقطناني، خالد بعنوان "البيئة المصرفية وأثرها على كفاءة وفاعلية نظم المعلومات المحاسبية: دراسة تحليلية على المصارف التجارية في الأردن"، الأكاديمية العربية للعلوم المالية والمصرفية، جامعة عمان الأهلية ,٢٠٠٧.
١٧. عبد اللطيف, رشدي وادي," أهمية ومزايا البنوك الإلكترونية في قطاع غزة بفلسطين ومعوقات انتشارها"، الجامعة الاسلامية، غزة، ٢٠١٠
١٨. العنزي, سامية "مدى التزام البنوك التجارية الأردنية بمتطلبات الرقابة الداخلية على أنشطة التجارة الالكترونية من وجهة نظر المدقق الخارجي"، مجلة العلوم الانسانية، جامعة آل البيت– الاردن، ٢٠٠٨.
١٩. قاسم الشحادة, عبد الرزاق, والعاصي سعد محمد, "إطار متكامل لتقييم كفاءة نظم المعلومات المحاسبية في المؤسسات المصرفية في ظل الأزمة المالية العالمية"، المؤتمر العلمي الثاني.
٢٠. القطاونة، عادل، "أثر استخدام تكنولوجيا المعلومات على فاعلية نظم المعلومات المحاسبية "دراسة على منشآت المصارف والتأمين المدرجة أسهمها في بورصة عمان ضمن السوق الأول", ٢٠٠٥
٢١. الكرسانة, إبراهيم، "أطر أساسية ومعاصرة في الرقابة على البنوك وإدارة المخاطر"، صندوق النقد العربي، أبوظبي، مارس ٢٠٠٦.
٢٢. الكري، طاهر, "تكلفة الاستثمار في أنظمة المعلومات وعلاقتها بأداء المنظمات"، مجلة الجندول، ليبيا، ٢٠٠٥

٢٣. كنجو, عبود كنجو،"الأبعاد المفقودة في إصلاح النظام المصرفي في سوريا جامعة فيلادلفيا الاردن"،المؤتمر العلمي الرابع، الريادة والإبداع،2005 .
٢٤. محروس، حسن, "تغير الدور التقليدي للبنوك"، Kotobarabia.com، ٢٠٠٦.
٢٥. مصطفى, سمارة، "استيعاب استراتيجيات التجارة الإلكترونية المنطلق الأساسي نحو البنوك الإلكترونية"، مجلة انترنت، العدد الحادي والعشرون،تشرين الثاني، ٢٠٠٧.
٢٦. معروف، إبراهيم, " التجارة الإلكترونية والبنوك", مجلس الغرف التجارية والصناعية السعودية, ٢٠٠٢/٠١/٠٢
٢٧. منصوري, الزين، "وسائل وأنظمة الدفع والسداد الالكتروني عوامل الانتشار وشروط النجاح "– الملتقى العلمي الدولي الرابع،موسوعة الاقتصاد والتمويل الاسلامي، ٢٠١١.
٢٨. الموسوي, نوار, كحيط، عباس، "أهمية البنوك الالكترونية في تحسين جودة الخدمة المصرفية"، جامعة واسط – العراق، ٢٠٠٨.
٢٩. نبي، سيد عرفان، ميرزا عبد الرحمن، الغتبر خالد , "أمن المعلومات في المنظمات السعودية ",جامعة الملك سعود، ٢٠١٠
٣٠. نصولي, صالح, وشايختر اندريا، "تحديات المعاملات المصرفية الإلكترونية"،مجلة التمويل والتنمية، سبتمبر2002
٣١. الهادي, محمد محمد, "توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية" cybrarians journal يونيو ٢٠٠٦.
٣٢. يونس,عرب،"ورقة عمل مخاطر الانفتاح الالكتروني",الملتقى السابع لمجتمع الاعمال العربي – البحرين ١٨–٢٠ اكتوبر / تشرين اول ٢٠٠٣.

ج– رسائل الماجستير والدكتوراه:

١. احمد, عبد الله العموري،"أثر التجارة الالكترونية على المراجعة – دراسة ميدانية في اليمن"، رسالة ماجستير غير منشورة، جامعة دمشق – سوريا، ٢٠٠٦.
٢. طوايبية, أحمد، "المحاسبة التحليلية كأداة لتخطيط ومراقبة الإنتاج"، مذكرة لنيل شهادة الماجستير في العلوم الاقتصادية، جامعة الجزائر، ٢٠٠٢
٣. قرم، عباس، "أنظمة الدفع الالكتروني وتطبيقها في سورية"، الجامعة الافتراضية السورية، رسالة ماجستير، ٢٠١٢.
٤. بركات ، ليدا ، "ادارة المخاطر التشغيلية في بيئة الأعمال المصرفية الالكترونية في المصارف السورية"، رسالة ماجستير ،جامعة دمشق ،٢٠١٠ .

٥. شاهين، علي عبدالله، "العوامل المؤثرة في كفاءة وفاعلية نظم المعلومات المحاسبية المحوسبة في المصارف التجارية العاملة في فلسطين "،الجامعة الأسلامية غزة، ٢٠١٢
٦. محمد حامد، نورالدين١، " أمن نظم ومعلومات المصارف وحمايتها بإشارة خاصة للواقع السوداني" ، رسالة ماجستير ،جامعة النيلين ،٢٠٠٧

د) الوثائق الرسمية:

١- التقرير السنوي للمصرف العقاري ٢٠١٠..
٢-تقرير وزارة رئاسة مجلس الوزراء في السودان،المركز القومي للمعلومات، الإدارة الفنية، ٢٠١٠

المراجع الأجنبية

Books:

1. Abolfazl Azizi Sharif and Bagher Shamszadeh: Computerized Accounting Information Systems (Cais) Versus Security Threats ،Journal of Academic Research in Economics Spiru Haret University, Faculty of Accounting and Financial Management ،2012
2. AICPA &CICA, Trust Services, Principles,Criteria and Illustrations,Copy Rights، USA. -2007
3. Allsopp, William. Unauthorised access: Physical penetration testing for it security teams. Hoboken, NJ: Wiley, 2009.
4. Anderson, Ross J.. *Security engineering: a guide to building dependable distributed systems* (2nd ed.). Indianapolis, IN: Wiley. (2008)
5. Arnason, Sigurjon Thor & Willett, Keith D،., How to Achieve 27001 Certification: An Example of Applied Compliance Management, Taylor & Francis Group, LLC, USA. 2008
6. Avison ،D. and G،. Fifzgerald ،Information Systems Development ، Methodologies ،Techniques&Tools ،4th ،2006
7. Bank for international Settlement ,Basel Committee on Bank Supervision“ ,Risk management principles for electronic banking”,

8. Bondner George H&WilliamS. Hopwood, Optic "Accounting Information Systems" Prentice Hall International INC,New Jersey, USA, 2000,
9. Brian Carter, Ari Kassin, and Tanja Magoc. Advanced Encryption Standard. October 30, 2007.
10. Calder, A. and J. Van Bon, Information Security Based on ISO 27001/ISO 17799: A Management Guide.: The Stationery Office/Tso،2006.
11. Cary ,Hayward“ ,The Internet Protocol Security (IPSec) Standard: Clearing up the Confusion ,”Product Marketing Manager/RedCreek Communications.2008
12. Dave Burrows, "Introduction to becoming a Penetration Tester", SANS Institute, part of the Information Security Reading Room, June,2 2003.
13. E. H. Freeman, “Holistic Information Security: ISO 27001 and Due Care. ,” Information Systems Security, vol. 16, Sep. 2007
14. , Donald ;Kusel,JimOxner,Tom. Internal Auditing in the Banking Industry Bank Accounting & Finance, (Euromoney Publications PLC), Fall2001. vol 15 Issue 1.
15. Efraim Turban, PH.D., Electronic Commerce: Global Edition, Pearson Education, Limited, 2010,
16. Forouzan, Behrouz A. Cryptography and Network Security. s.l.: McGraw-Hill, 2007.
17. Garrison Ray H&Noreen, Eric E& Brewer, Peter C: "Managerial accounting" , 11 thed, McGraw – Hill Inc, New York, USA 2006 ،
18. Gary P. Schneider, Electronic Commerce, Cengage Learning, Edition 8,2008.

19. Greenstein, M. &Vasarhelyi,M., Accounting Information Technology,and Business Soluution,2nd Edition,MC. Graw-Hill, NewYork, USA2000

20. Hinson,Gary, ,ISO27001 Security: The Financial Implications of Implementing ISO/IEC27002, Ageneric Cost Benefit Model, ISECT Ltd , www.ISO27001 security. Com، 2008.

21. I. T. L. Education Solutions Limited; Itl (). *Introduction to Information Technology*. Pearson Education India. 2009.

22. Information Security Awareness", Information Management and Computer Security, Bradford, (Vol. 8, Iss. 8), 2000.

23. ITGovernanceInstitute. COBIT® 4. 1. 2008 ٤٠-CSIA, 2007, ISO 27001: Get The Facts, www. csialliance. org

24. J. M. Hagen, E. Albrechtsen, and J. Hovden, "Implementation and effectiveness of organizational information security measures," Information Management & Computer Security, vol. 16, 2008 .

25. K. Hong, Y. Chi, L. R. Chao, and J. Tang, "An integrated system theory of information security management," Information Management & Computer Security, vol. 11, 2003.

26. Kenneth C. Laudon and Carol GuercioTraver, E-commerce business, technology, society. Security + Guide to Network Security Fundamentals,2009.

27. Kenneth C. Laudon, Carol Guercio Traver, E-Commerce , Prentice Hall,2011.

28. Kerem, K.. Adoption of electronic banking: underlying consumerbehavior and critical success factors. Case study of Estonia, paperpresented at the conference of the technology and everyday life network, London, U. K. retrieved from .2003

29. Khalid, k. &Abdallah, R. &Elrafe, E. Elbaset, E. "customer satisfaction with internet banking web Site (Case study onthearab Bank)". The Arab Academy for Banking and FinancialSciences, Jordan.

30. Kiso ،Donald E. and Wgeyganadt ،Jerry J ،Interbmediate Accounting ،NewYork: John Wiley and Sons Inc ،2002

31. Laudon, K.,&Laudon, J.. Management information systems: Managing the digital firm. (11th ed.). Upper Saddle River, NJ: Pearson Prentice Hall ،2010

32. Laudon, Kenneth C.; Laudon, Jane P.. *Management Information Systems: Managing the Digital Firm* (11 ed.). Prentice Hall/CourseSmart. 2009.

33. M. Alnatheer and K. Nelson, "A proposed framework for understanding information security culture and practices in the Saudi context," Proceedings of the 7th Australian Information Security Management Conference, Perth, Australia: SECAU – Edith Cowan University, Australia, 2009,.

34. M. Dlamini, J. Eloff, and M. Eloff, "Information security: The moving target," Computers & Security, vol. 28, May. 2009 .

35. M. E. Whitman, "Enemy at the gate: threats to information security," Communications of the ACM, vol. 46, 2003 .

36. M. Siponen, S. Pahnila, and M. Mahmood, "Compliance with Information Security Policies: An Empirical Investigation," Computer, vol. 43, 2010

37. M. T. Siponen and H. Oinas-Kukkonen, "A review of information security issues and respective research contributions," SIGMIS Database, vol. 38, 2007 .

38. Mark Ciampa, Second Edition, Thomson Course Technology, 2005 chapter#
39. Marshall B. Romney, Paul John Steinbart, Accounting Information Systems, Prentice Hall 2009
40. Mitnick, K: "The Art of Deception", Wiley Publishing Ltd: Indianapolis, Indiana; United States of America. 2002 ,
41. Montgomery Daniel D. ;MarkS. Beasly;SusanL. Menelaides, Auditors: New Procedures for delecting fraud, Jornal of Accontancy, NewYork, May
42. Moscove, Stepher," E- Business and Controls" The CPA Journal, 2003
43. Moscove. S. A,Simkin,MG. ,Bagranoff,N. A,: Core Concepts of Accounting Information System,7th ed ،John&SonsLtd,England, UK, 2002
44. P. Puhakainen and M. T. Siponen, “Improving employees’ compliance through information systems security training: An action research study,” MIS Quarterly, vol. 34, Dec. 2010 .
45. Peter Rob; Carlos Coronel. *Database systems: design, implementation, and management*. Cengage Learning،2009.
46. Romeny K M. and P. Steinbart, Accounting Information System, 3th،. ed, Prenticehall ،2006
47. Romney, Marshall B. &Steinbart, Paul John, Accounting Information Systems, 9th Edition, USA: Prentice Hall, 2003 .
48. Ross Anderson, Eli Biham, Lars Knudsen. Serpent: A Proposal for the Advanced Encryption Standard,2007.
49. Sallé, M. , IT Service Management and IT Governance: review, comparative analysis and their impact on utility computing. Trusted Systems Laboratory: HP Laboratories Palo Alto, 2004 .

50. Sheila, Frankel, “AN INTRODUCTION TO IPSec ,”Computer SecurityDivision/Information Technology Laboratory/National Institute of Standards andTechnology .
51. Slay ،J. andA. Koronios ،Security & Risk Management ،John Willy & Sons ،Australia ،ltd ٢٠٠٦ .
52. Stephen A. Moscove ،Mark. G ،Simkin ،Nancy. A ،Bagrannoff، Core Concepts of Accounting Information System ،John Wiley & Sons ،INC ، 2001 .
53. Van Bon, J. , Foundations of IT service management based on ITIL V3.: Van Haren2008
54. Whitman Michael E., "Enemy at the Gate: Threats to Information Security", Communication of the ACM, (Vol. 46, Iss. 8), 2003
55. Whitman Michael E.:Enemy at the Gate" Threats to Information Security", Communcation of the ACM,2006,
56. Wood, David J.. "Assessing IT Governance Maturity: The Case of San Marcos, Texas". Applied Research Projects, Texas State University-San Marcos،2010

Periodicals&Dissertations

1. Abu-Musa 2001“Evaluating The Security of Computerized Accounting Information System”: An Empirical Study on Egyptian Banking Industry
2. Abu-Musa2004 “Import Threats to Comptuerized Accounting Information Systems “:An Empirical Study on Saudi Organizations
3. An overview of information security standards بحث علمي لحكومة منطقة . هونغ كونغ الإدارية الخاصة
4. Angela Moscaritolo. http://www.scmagazineus.com/zeus-for-android-steals-one-time-banking-passwords/article/207286/. 2011-07-12

5. Cary ,Hayward“ ,The Internet Protocol Security (IPSec) Standard: Clearing up the Confusion ,”*Product Marketing Manager/RedCreek Communications*٢٠٠٨ .
6. Dominick Baier, "Improving Application Security through Penetration Testing", Conferences. Oct 2004
7. Geneva, "WHO Style Guide", World Health Organization. 2004.
8. GORDON, WHITSON. "Two-Factor Authentication: The Big List Of Everywhere You Should Enable It Right Now". *LifeHacker* (Australia) SEPTEMBER 2012)http://www.lifehacker.com.au/2012/09/two-factor-authentication-the-big-list-of-everywhere-you-should-enable-it-right-now/.
9. Kerem, K.. Adoption of electronic banking: underlying consumer behavior and critical success factors. Case study of Estonia, paper presented at the conference of the technology and everyday life network, London, U.K. retrieved from, 2003,
10. Nehad Aalhussban, AdmissibilityOf Electronic Signature in evidence and its legal effect,Comparative study in Jordanian laws,supervisor Fayyad alqudah ,Faculty of graduate studies,University of Jordan ,December 2005,
11. O.Sunday and E.arnold “Accessing E- banking Best on resilint transaction “Blekinge,Insitute of Tecnology Master Thesis , 2008
12. Pallab Dutta ,Benefits of Electronic Banking, 2011.
13. Perrin, Chad. "The CIA Triad". http://www.techrepublic.com/blog/security/the-cia-triad/488. 2012
14. Sheila, Frankel, “An Introduction To IP Sec ,”Computer Security Division/Information Technology Laboratory/National Institute of Standards and Technology. ،٢٠٠٦

15. Skillen, pater "Desktop Data Security n" International Journal of Information Rescues and Management, Vol 3, No 9, 2001 ,
16. Spagnoletti, Paolo; Resca A.. "The duality of Information Security Management: fighting against predictable and unpredictable threats". *Journal of Information System Security*. http://eprints.luiss.it/955/2008
17. Spencer, Kelly, Hackers outwit online banking identity security systems ,BBC News Technology , 10 February 2012.
18. Whitman 2003 "Enemy at the Gate: Threats to Information Security"

مراجع الانترنت:

١-E-Banking,http://www. arablaw. org/Download/E-Banking. doc, consulté le
٢-http://support. microsoft. com/kb/299357/ar
٣- Website: www. nans. gov. sy
٤-http://www. lse. ac. uk/collections/EMTEL/conference/papers/kerem. pdf
٥-www. intertek-semkocertification,se, 2007
6_http://www. isaca. org/Content/NavigationMenu/Members_and_Leaders/COBIT6/ObtaiOCOBIT/CobiT4. 1_Brochure. pdf٨-http://www. isaca. org/AMTemplate.
7-http://www. dralmarri. com/show. asp?field=res_a&id=205
10www. windowsecurity. com/whitepapers/Linux_Administrators_Security_Guide__IP_Security_IPSec. html-
8- www.microsoft.com/technet/prodtechnol/windows2000

9-E-Banking , http://www. arablaw. org/Download/E-Banking. doc
http://www. islam-online. net/iol-arabic/dowalia/murajaat. asp
10-http://www. arablaw. org/Download/E-banking_Infrastructure_Article. doc ,
11-http://en.wikipedia.org/wiki/payment_card
١2- http://en.wikipedia.org/wiki/Contactless_smart_card
13- Scribd. http://www.scribd.com/doc/62262162/HP-Pretexting-Scandal.
14- http://hespress.com/permalink/43431.html
15-www.bbc.co.uk/arabic/
16- com .sa/economy/newswww.alwatan
http://web.1asphost.com/attasaa/News...ject.asp?NO=80 21-
17-http://www.alwatan.com.sa/daily/2006-07-03/local/local10.htm
18-http://aljareema.com/newss/wmview.php?ArtID=2019
19. -http://www.ehow.com/facts_5172105_benefits-electronic-banking.html
٢٠.http://212.119.67.87/okazarchive/Data/2006/1/24/Art_310706.XML
٢١-http://www.lse.ac.uk/collections/EMTEL/conference/papers/kerem.pdf

فهرس المصطلحات

المصطلح	الترجمة بالعربية
Automated Teller Machines(ATM)	آلات الصراف الآلية
Secure Sockets Layer(SSL)	بروتوكول(طبقة مآخذ التوصيل الآمنة) نقل المستندات بطريقة آمنة
Transport Layer security(TLS)	بروتوكول أمن طبقات النقل
Personal Communication (PCT) Technology	برتوكول تكنولوجيا الاتصالات الشخصية
International Accounting (IASB) Standards Board	مجلس معايير المحاسبة الدولية
Information technology (IT)	تكنولوجيا المعلومات
Control Objectives for Information (COBIT)and Related Technologies	أهداف الرقابة للمعلومات والتكنولوجيات
Sarbanes-Oxley Act(SOX)	قانون ساربانيس أوكسلي لأمن المعلومات
Committee Of Sponsoring (COSO) Organizations	لجنة المنظمة الراعية
The Health Insurance Portability (HIPAA)And Accountability Act	قانون قابلية التأمين الصحي وقانون المحاسبة
Federal Information Security (FISMA) Management Act	قانون إدارة أمن المعلومات الفيدرالي
International Standards (Iso) Organisation	المنظمة الدولية للتوحيد القياسي
The Information Technology Infrastructure Library (ITIL)	هو معيار إدارة خدمات تقنية المعلومات

Plan-Do-Check-Act. (PDCA)	قانون خطة –تنفيذ– تحقق–العمل
Cyber Security Industry Alliance(CSIA)	تحالف صناعة حماية شبكات الانترنيت
Federal Information Processing Standers(FIPS)	هيئة معايير معالجة البيانات الاتحادية
Generally Accepted Accounting Principles (GAAP)	مبادئ المحاسبة المقبولة عموماً
American Institute of Certified Public Accountants (AICPA)	المعهد الأمريكي للمحاسبين القانونيون
Personal Identification Numbers(PIN)	رقم التعريف الشخصي
Network Interface Card(NIC)	بطاقة تعريف الشبكة
Media Access Control(MAC)	التحكم بوصول الوسيط
Transmission Control Protocol (TCP/IP)/Internet Protocol	اتفاقية ضبط الإرسال والنقل / اتفاقية الاتصال بواسطة شبكة المعلومات الدولية
Intrustion Prevention Systems(IPS)	أنظمة منع الأختراق
Public Key Infrastructure(PKI)	البنية التحتية العامة للمفتاح
Computer Emergency (CERT) Response Team	فريق الاستجابة لطوارئ الكمبيوتر
Computer Incident Response (CIRT) Team	فريق الاستجابة لخروقات الكمبيوتر
Chief Information Security (CISO) Officer	ضابط أمن المعلومات الرئيسي
Point Of Sales(POS)	نقاط البيع
Unrestricted Supplementary Service Data (USSD)	خدمة نقل البيانات غير المقيد التكميلية
Online Bill Payment (OBPG) Gateway	النظام الوسيط لدفع الفواتير الآني

Assessing The Efficiency of Accounting Information Systems in Protecting The Data And Information in Syrian Banks.

(AComparative Study)

Abstract

This research aims to identify the risks and problems resulting from modern techniques used in banks, and to investigate the protection measures which are represented by administrative, technical, and monitoring procedures and policies applied in banks and which enhance the efficiency of information systems. Then it aims to assess the efficiency of these systems in Syrian banks in safeguarding their data and information, and to determine the factors affecting the efficiency of the accounting information system in ensuring the security of data and information. Thereafter, as a scientific contribution, it will provide solutions to the problems that Syrian banks are expected to face as a result of the use of modern techniques applications.

As a means to realize and achieve its objectives, the research presented the concept of information systems efficiency, and the factors influencing this efficiency, in addition to the actual status of the electronic work environment in Syrian banks and services offered by these banks to their clients. The researcher also demonstrated the risks and threats facing the uses of technology in general and in banks in particular in terms of using the global networks- Internet – thus shedding the light on risks that cannot be overcome unless by taking action, and applying some principles-the researcher focused here on COBIT and ISO standards (27001) and (27002).

The researcher has chosen the Real-Estate Bank and Audi Bank as a sample of her research. She studied the extent to which these banks were affected by the uses of information techniques, and the risks that they were exposed to, and also the administrative, security and technical procedures taken to reduce the risk of technology uses. This was done through analyzing and assessing the actual status of information and data security by comparing the data of practical reality with safety standards specified by the appropriate authorities.

Necessary data related to the accounting information systems used in the sample banks were collected from the managerial reports and statistics beside interviewing staff concerned in information and data security. In addition to that, some experimental trials were carried out, like Acunetix Website Audit, in oreder to know the number of penetrations and gaps that can occur and through which they can determine the level of protection in some electronic bank transactions.

The research concluded that the efficiency of accounting information systems to offer security for bankers is relatively limited, and that it could have been better. These systems were not able to reach an advanced level of safety objectives through their security policies and procedures.