مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الاقتصادية والقانونية المجلد (39) العدد (3) 2017
Tishreen University Journal for Research and Scientific Studies -Economic and Legal Sciences Series Vol. (39) No. (3) 2017

Evaluating The Efficiency of The banking Accounting Information Systems in Protecting The Data And Information

Dr. Soha GH. Sankary*
Dr. Nazeer M. Mohammad*

(Received 15 / 2 / 2017. Accepted 3 / 5 / 2017)

□ 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.

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.

Keywords: Accounting Information System, Information Security, Efficiency of system.

***Assistant Professor - faculty of Economics- Tishreen University- Lattakia- Syria.**
****Work Supervisor- faculty of Economics- Tishreen University- Lattakia- Syria.**

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الاقتصادية والقانونية المجلد (39) العدد (3) 2017
Tishreen University Journal for Research and Scientific Studies -Economic and Legal Sciences Series Vol. (39) No. (3) 2017

تقييم مدى قدرة نظام المعلومات المحاسبي المصرفي على حماية البيانات والمعلومات (دراسة مقارنة)

الدكتورة سهى شفيق سنكري*

الدكتور نذير محمد محمد**

(تاريخ الإيداع 15 / 2 / 2017. قُبِل للنشر في 3 / 5 / 2017)

□ ملخّص □

هدف البحث إلى التعرف على المخاطر والمشاكل الناتجة عن استخدام البنوك والمصارف للتقنيات الحديثة وما هي إجراءات الحماية المتبعة متمثلة بالسياسات والإجراءات الإدارية والفنية والرقابية المطبقة في المصارف والتي تعزز من كفاءة نظم المعلومات.

تم بلوغ هدف البحث من خلال عرض واقع بيئة العمل الالكتروني بالمصارف السورية والخدمات التي تقدمها المصارف لعملائها، كما قام الباحثان أيضاً، ببيان المخاطر والمهددات التي تجابه استخدامات التقنية بصورة عامة وبالبنوك بصفة خاصة وذلك في ظل استخدام الشبكات العالمية:(الإنترنت) فتفتح بذلك نافذة على مخاطر لا يمكن التغلب عليها إلا باتخاذ إجراءات وسياسات وتطبيق معايير محددة، حيث تمَّ التركيز هنا على معيار الكوبيت والآيزو (27001) و(27002).

اتخذ الباحثان المصرف العقاري ومصرف عودة عينة لدراستها لمعرفة مدى تأثرها باستخدامات تقنية المعلومات والمخاطر التي تتعرض لها، ولمعرفة الاجراءات الإدارية والأمنية والفنية المتخذة للحد من مخاطر استخدامات التقنية، وذلك من خلال تحليل وتقييم 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 أُجريت بعض الاختبارات التجريبية كاختبار Acunetix Website Audit لمعرفة عدد الاختراقات والثغرات التي يمكن حدوثها والتي يمكن من خلالها تحديد مستوى الحماية في بعض العمليات المصرفية الإلكترونية.

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

الكلمات المفتاحية:نظم المعلومات المحاسبية – أمن المعلومات – كفاءة.

* **مدرّس – المعهد التقاني للعلوم المالية والمصرفية– جامعة تشرين–اللاذقية–سورية.**

** **مشرف على الأعمال – قسم المحاسبة– كلية الاقتصاد– جامعة تشرين –اللاذقية–سورية.**

مقدمة:

احتل القطاع المصرفي منذ بدايات القرن العشرين موقعاً متميزاً، وبات يلعب دوراً هاماً في الحياة الاقتصاديَة، وقد طرأت عليه تطورات كبيرة؛ فقد خلقت حدة المنافسة في هذا القطاع ضرورات متنوعة لتطويره وكان منها حالات الاندماج المصرفية التي هدفت إلى السيطرة على الأسواق العالمية. ثم ظهرت الأنظمة المصرفية العصرية، الإدارية، المحاسبية والفنية، نتيجة للتطور التكنولوجي السريع وتقدم وسائل الاتصال بسرعة لا متناهية.

وقد كان للتطور التكنولوجي في معالجة البيانات ونقلها أثراً بالغاً في عمل المصارف؛ فظهرت تغيرات جوهرية في بيئة نظم المعلومات المحاسبية واستخدمت الشبكات الداخلية والخارجية لربط جميع أقسام وإدارات وفروع المصارف، وربط المصارف بالأطراف الخارجية من عملاء وموردين وحكومة وغيرهم. فشهدت الصناعة المصرفية تطوراً نوعياً في مجال السماح للعملاء بتنفيذ العديد من العمليات المصرفية عبر شبكات الاتصالات الالكترونية.

غير أن نظم المعلومات المحاسبية المتقدمة، وخاصة المرتبطة بالشبكات، تحتاج إلى إجراءات رقابية أكثر دقة من غيرها من الأنظمة. والهدف من ذلك توفير الحماية الكافية لبيانات النظام ومعلوماته، الأمر الذي يوفر الطمأنينة لمستخدمي المعلومات عند الاعتماد على مخرجاته لاتخاذ القرارات، وإن عدم توفر الحماية للبيانات والمعلومات يهدد التقدم الذي حققته نظم المعلومات المحاسبية المصرفية في الوقت الحاضر.

ولاشك أن حماية البيانات والمعلومات تحتاج إلى توفر العديد من الإجراءات والسياسات والمعايير التي تعتمدها الإدارة لضمان تطبيق هذه الخاصية الهامة من خصائص المعلومات، ومن أهم المعايير المطبقة في المصارف هي الآيزو والكوبيت والخدمات الإئتمانية لأنها من أهم المعايير التي تهتم بأمن وسلامة المعلومات. وعليه إن تطبيق المصارف لهذه المعايير يجعل نظم المعلومات المحاسبية المطبقة لديها تتمتع بموثوقية عالية وقدرة وكفاءة على حماية بياناتها ومعلوماتها.

مشكلة البحث:

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

وهنا تتمثل مشكلة البحث في الإجابة عن السؤالين الآتيين:

- 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 ؟

أهمية البحث وأهدافه:

تنبع أهمية البحث بشكل رئيسي من أنه يتناول مشكلة معاصرة برزت في مرحلة حاسمة من مراحل تطور الخدمات المصرفية في سورية، خاصة عند ربط هذه الخدمات بشبكات محلية أو عالمية وتبادل البيانات الكترونياً؛ وفي مرحلة يتزايد فيها أعداد المصارف الخاصة وتتوسع خدماتها. وأصبح عنصر الحماية في الخدمات المصرفية، وبالتالي في نظم المعلومات المحاسبية لهذه المصارف، من أهم عناصر نجاح العمل المصرفي. وتزداد أهمية البحث من خلال تفرده في تناول مشكلة حماية البيانات والمعلومات للنظم المحاسبية في المصارف السورية في ظل التبادل الالكتروني للبيانات.

لقد باتت مشكلة حماية البيانات والمعلومات في نظام المعلومات المحاسبي ضمن هذه المتغيرات المستجدة على عمل المصارف الحكومية والخاصة من أهم المشكلات المعاصرة التي تسعى المصارف إلى تجاوزها؛ وبات من الضروري تقييم الواقع المتبدل والمتغير لأمن البيانات والمعلومات في أنظمة المصارف للتمكّن من تحديد كفاءة هذه الأنظمة وتطوير سياسات وإجراءات الأمان. وهذا ما يسعى البحث إلى تحيقيقه، الأمر الذي يعطيه أهمية خاصة.

ويهدف البحث الى:

1. حصر المستجدات والتطورات المحيطة بعمل المصارف في سورية، ورصد مدى تفاعل المصارف معها، ومعرفة احتماليات تأثيرها في أمن البيانات والمعلومات.
2. تقييم كفاءة نظم المعلومات المحاسبية للمصارف السورية في حماية البيانات والمعلومات المحاسبية.
3. تحديد العوامل المؤثرة في كفاءة نظام المعلومات المحاسبي على ضمان أمن بياناته ومعلوماته.
4. تقديم المساهمة العلمية المناسبة التي يمكن أن تساعد في زيادة حماية بيانات ومعلومات نظم المعلومات المحاسبية للمصارف السورية.

فرضيات البحث:

يمكن صياغة الفرضية الرئيسية الآتية:

تعتبر كفاءة نظام المعلومات المحاسبي للمصرف في سوريا، في البيئة التكنولوجية المعاصرة، ضعيفة نسبياً كونها غير قادرة على بلوغ أهدافها في ضمان أمن البيانات والمعلومات بالشكل المطلوب.

تتوزع هذه الفرضية إلى فرضيات ثلاثة فرعية تبيّن سبب عدم قدرة هذه النظم على بلوغ أهدافها في تحقيق الأمان لبياناتها ومعلوماتها، وهي:

الفرضية الفرعية الأولى: البيئة التشريعية والتنظيمية الحاضنة لعمل المصارف السورية لا تقدم الدعم الكافي لنظم معلوماتها المحاسبية لتحقيق الأمان المنشود للبيانات والمعلومات.

الفرضية الفرعية الثانية: عدم كفاية الموارد المخصصة لدعم إجراءات أمان البيانات والمعلومات يضعف بشكل مباشر قدرة نظام المعلومات المحاسبي للمصرف على بلوغ أهداف الأمان لبياناته ومعلوماته.

الفرضية الفرعية الثالثة: ضعف سياسات الأمان وكذلك إجراءاته في البيئة التكنولوجية المعاصرة للنظام المحاسبي للمصرف، يضعف قدرته على بلوغ اهداف الأمان التي يرسمها.

منهجية البحث:

للتحقق من فرضيات الدراسة تم رسم مجموعة الخطوات والمراحل الواجب إنجازها لبلوغ غاية البحث مع مراعاة طبيعة الدراسة وهدفها والأدوات المناسبة لبلوغ الأهداف. فالدراسة وصفية الهدف وتحليلية الأداة، تحاول توصيف واقع أمن البيانات وتحليله لكشف ثغراته، مستندة إلى عمليات المقارنة المرجعية مع معايير عالمية رائدة في مجال رقابة العمليات الإلكترونية لتوليد المعلومات ونقلها. هذه الخطوات والمراحل تم رسمها حسب التلسلسل الآتي: جمع المعارف العلمية والمعلومات الضرورية، لتكوين معارف كافية لإنجاز الدراسة، خاصة ما يتعلق بنظم المعلومات المحاسبية وتكنولوجيا المعلومات، وبمفاهيم أمن المعلومات وتقييم الكفاءة؛ وذلك بالعودة إلى الدراسات السابقة والأدبيات العلمية ذات الصلة.

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 والأكثر قرباً من مشكلة البحث، وفيما يأتي أهمها:

1) دراسة شاهين 2012 (العوامل المؤثرة في كفاءة وفاعلية نظم المعلومات المحاسبية المحوسبة في المصارف التجارية العاملة في فلسطين):[1]

تهدف هذه الدراسة إلى تحليل ومناقشة العوامل المؤثرة في مستوى كفاءة وفاعلية نظم المعلومات المحاسبية المحوسبة، 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 (10) استبانات لكل مصرف وبعدد 120 استبانة واسترد منها 103 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.

2) دراسة قرم 2012 (أنظمة الدفع الإلكتروني وتطبيقها في سورية):[2]

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. وأهم النتائج التي خلصت إليها الدراسة: أنّ هناك تحول كبير في أنظمة الدفع التقليدية باتجاه أنظمة الدفع الإلكترونية. والسبب الرئيس لذلك هو خفض التكاليف وضمان خدمة العملاء (24/24) ساعة يومياً وعلى مدار أيام الأسبوع، ويمثل هذا التطور الربح للجميع (win–win)، حيث العميل يحفظ وقته وجهده والمصرف يخفض الكلفة. بالإضافة إلى 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 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.

3) دراسة Bagher Shamszadeh & Abolfazl Azizi Sharif 2012 (مواجهة نظم المعلومات المحاسبية المحوسبة للتهديدات الأمنية):[3]

هدفت هذه الدراسة الى تحديد التهديدات الأمنية الكبيرة التي تواجه النظم المحاسبية المحوسبة والعلاقة بين أمن هذه الأنظمة و مستوى التعليم والخبرة لمستخدمي النظام، وجودة تصميم النظام ونوع الصناعة في شركات مختلفة. وقامت هذه الدراسة بإجراء دراسة مسحية وصفية ومن ثمَّ تحديد العلاقة بين المتغيرات، أما طريقة جمع البيانات فقد تم استخدام (الاستبيانات)، على أنظمة المحاسبة المحوسبة لـ Hamadan للأوراق المالية في الفترة الزمنية من 2006 حتى 2011 وتشير النتائج إلى أن التهديدات الأمنية في شركات مختلفة في كثير من الأحيان تعود لأسباب مختلفة حسب طبيعة ونوعية التصميم وليس لها تأثير يذكر على أمن النظام لأن معظم التهديدات أصلها 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.

4) دراسة الساكني وعواودة 2011(مخاطر استخدام تكنولوجيا المعلومات وأثرها على أداء نظم المعلومات المحاسبية):[4]

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. حيث تم اختيار عينة عشوائية بلغت 100 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، وأظهرت الدراسة أن هناك علاقة تأثير بين مخاطر استخدام تكنولوجيا المعلومات وأداء نظم المعلومات المحاسبية وبالتحديد مخاطر التشغيل ومخاطر عدم تحديد الصلاحيات.

5) دراسة القاسم و ردايده 2010 (أمن البيانات ونظم المعلومات المحاسبية في بيئة تكنولوجيا المعلومات في البنوك الأردنية–دراسة ميدانية):[5]

هدف 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، والأجهزة 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 (87.33%)، كما بلغت نسبة الاهتمام بأمن الأفراد (91.73%)، ونسبة الاهتمام بأمن النظم والتطبيقات والبرمجيات (90.68%)، ونسبة الاهتمام بأمن الأجهزة والمعدات (90.94%)، ونسبة الاهتمام بأمن طرق الحفظ السليمة وتبادل المعلومات وتخزينها (92.53%)، وهذا يدل على أن الإجراءات المتبعة 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 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 2010 (أثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية في زيادة موثوقية المعلومات المحاسبية):[6]

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.

7) دراسة زيدان وحمو 2010 (متطلبات أمن المعلومات المصرفية في بيئة الإنترنت):[7]

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.

8) دراسة معهد الرقابة على نظم المعلومات،2009 (الضوابط الرقابية وفق معايير الكوبيت (COBIT) دراسة حالة شركة تشارلز سكوب للائتمان):[8]

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.

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.

الدراسة الميدانية:

لبلوغ هدف البحث قام الباحثان بتحديد مرجعية أساسية للمقارنة تمثلت في معايير الجودة ومعايير Cobit. ثم قاما بزيارات ميدانية متكررة إلى المصرف العقاري ومصرف عودة وجمعا خلالها البيانات والمعلومات اللازمة لعمليات المقارنة والتحليل. وقد اعتُمدَ في سبيل ذلك مجموعة وسائل منها:[9]

1.الملاحظة المباشرة لكيفية إنجاز الأعمال من قبل العاملين في الأقسام ذات الصلة.

2.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).

3.المقابلات الشخصية مع رئيس قسم نظم المعلومات والعاملين في القسم للمصرفيين وتوجيه الأسئلة لاستخدامها في اختبار الفرضيات حول:

a. الإجراءات الإدارية في البنوك عينة الدراسة والتي تشمل:

- 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.

b. الإجراءات الأمنية 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.

4.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. التي وقد استخدمت في هذا الاختبار أداة 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 واستخدام المتوسطات الحسابية والانحرافات المعيارية ،كما تم استخدام اختبار T ستودينيت لاختبار الفرضيات.

مجتمع الدراسة وعينتها:

مجتمع الدراسة هو المصارف العاملة في سورية التي يبلغ عددها: 23 مصرفا، منها 6 مصارف حكومية و17 مصارفاً خاصاً.

تكونت عينة الدراسة من مصرفين: المصرف العقاري باعتباره مصرفاً حكومياً، ومصرف "عودة" كمصرف خاص، حيث شملت هذه العينة جميع العاملين في قسم نظم المعلومات وقد تم اعتماد هذين المصرفيين دون غيرهما لسببين هما: 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. وثانياً نظراً لعدم تعاون المصارف الأخرى مع الباحثان لإنجاز العمل.

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:

1) الخدمات الإلكترونية للمصرف العقاري:

- خدمة الصراف الألي.
- بنك الإنترنت.
- خدمات نقاط البيع[3]
- سيريا كارد.
- بطاقات الائتمان.
- خدمة توطين الرواتب (التوطين المصرفي Salary File)
- خدمة الرسائل القصيرة
- تسديد الفواتير
- الحسابات والودائع
- القروض العقارية

2) الخدمات التي يقدمها مصرف عودة:

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

- الحسابات المصرفية، وبشكلٍ خاص حسابات التوفير، والحسابات الجارية، والودائع الزمنية، وحسابات الحوالات.
- القروض التجارية والتسهيلات المتنوّعة، بما فيها تمويل مشاريع طويلة ومتوسّطة الأجل، والاعتمادات المستندية والكفالات.
- 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.
- 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

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.

[3] **لا يمكن استخدام هذه الميزة على الموقع الجديد لبنك الإنترنت حالياً، وسيتم تفعيلها قريباً.**

إجراءات أمن البيانات والمعلومات المطبقة في المصارف:

تم تحليل نظام المعلومات المحاسبية لتحديد نقاط القوة والضعف الموجودة باستخدام تحليل "سووت" (SWOT analysis[4]) وهو تحليل "القوة، مواطن الضعف، الفرصة والتهديدات" (Strength, Weakness, Opportunities &Threats) " للأنظمة الإلكترونية. اعتمد التحليل على إطارين مرجعيين:

1) إطار COBIT.

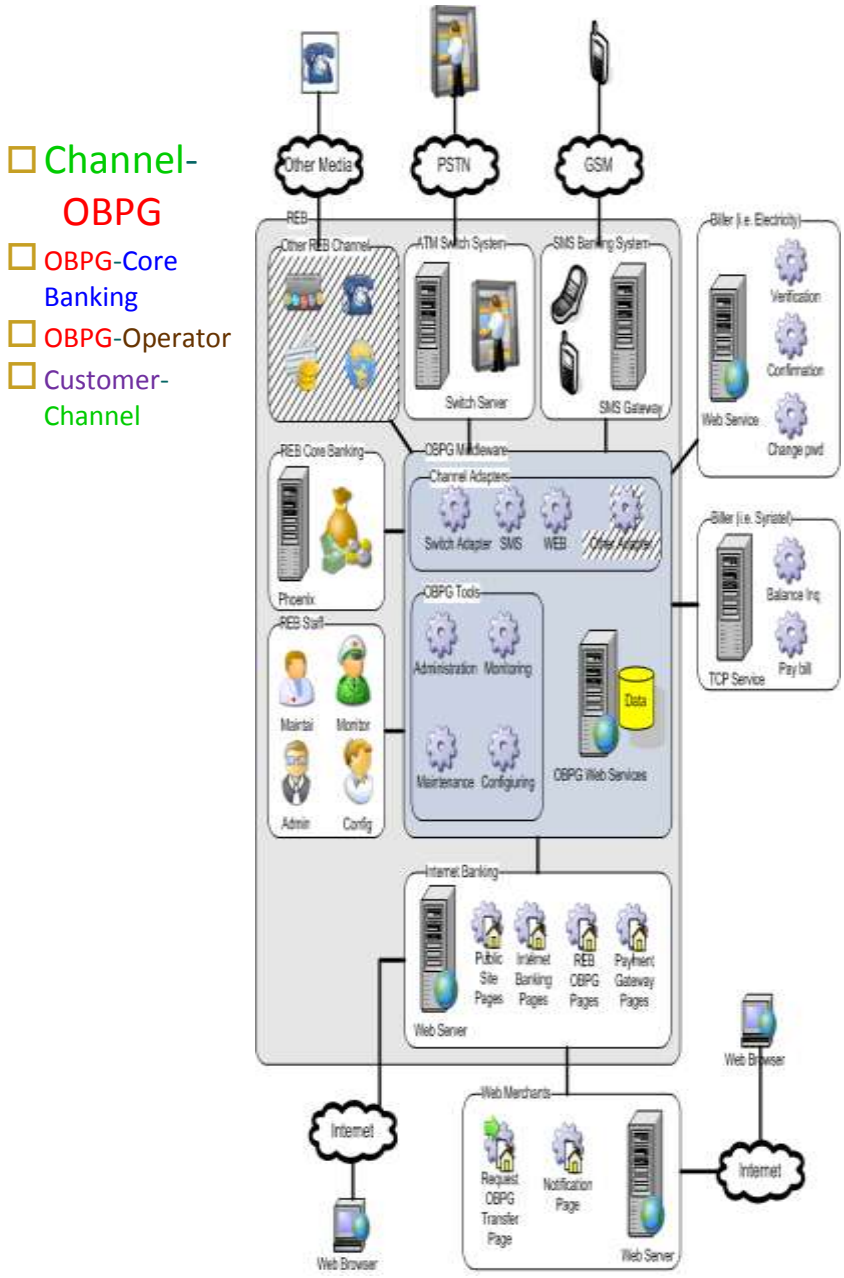
2) إطار الخدمات الائتمانية (خدمات الثقة) Trust Services.

فيما يلي مقارنة بين قنوات المصرف تتجلى فيها النقاط التالية:

الجدول رقم (1)مقارنة بين قنوات المصرف العقاري

	نظام المجيب الصوتي الآلي IVR	قناة SMS	الصراف ATM	بنك الإنترنت 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 جميعها عن الأنظمة الداخلية بالمصرف شبكيا وبرمجياً			

[4]- **تحليل الفرص والمخاطر SWOT وهو اختصار لـ Strength, Weakness, Opportunities &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 محاولة 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..**



(القنوات الواجب حمايتها)

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 (27001) [10] وذلك وفق نقاط قوة تتجلى بالجدول التالي:

الجدول رقم (2) جدول مقارنة وفق COBIT

	المصرف العقاري	مصرف عودة
1-الأمن والحماية	أ. حماية كافة الاتصالات الإلكترونية بين أجزاء البوابة والأنظمة الأخرى المختلفة. ب. التخطيط لسياسات أمنية معيارية والصرامة	أ. حماية كافة الاتصالات الإلكترونية بين أجزاء البوابة والأنظمة الأخرى المختلفة فجميع الاتصالات مشفرة بأحدث نظم التشفير العالمية وعن طريق تجهيزات نوعية

	المصرف العقاري	مصرف عودة
	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 و IPSEC. • ربط السماحيات بالأدوار Role-based Authorization. ث. التدقيق المستمر Real-time Auditing. ج. تنفيذ اختبارات الأمن والاختراق Vulnerability Tests بشكل دوري.	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: ت. 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 و IPSEC. • ربط السماحيات بالأدوار Role-base Authorization. ث. التدقيق المستمر Real-time Auditing. من قبل جهات خارجية معتمدة ومن قبل موظفي المصرف المعتمدين من المصرف المركزي ج. تنفيذ اختبارات الأمن والاختراق Vulnerability Tests بشكل دوري. سواء من داخل أم من خارج سوريا من خلال شركات عالمية ومحلية
2-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.	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.

	المصرف العقاري	مصرف عودة
	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.	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 سماحيته. ج.يمكن لموظفي المصرف أو المؤسسات المعنية توليد تقارير تقاص Reconciliation آلياً.
3-التكامل	ب. تدعم البوابة واجهات تخاطب معيارية، منها: • المعيار ISO 8583 (فيزا)، الخاص بالتخاطب مع محولة الصرافات. • قنياتSOAP وXML (خدمات الويب). • SSL (بروتوكول طبقة المنافذ الآمنة) لحماية قنوات الاتصال. ت. تدعم البوابة واجهات تخاطب خاصة، منها: • XAPI: واجهة التخاطب مع النظام المصرفي. • البروتوكول الخاص بدفع فواتير الخطوط لاحقة الدفع من سيرياتل. ث. تتكامل البوابة مع نظام إعلام Notification يتيح إرسال رسائل نصية أو بريد إلكتروني للمعنين في حالات المشاكل والحالات الطارئة وغيرها من الأحداث.	ب. 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. • 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.
4-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.

	المصرف العقاري	مصرف عودة
5-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: • سهولة إضافة قنوات جديدة. • سهولة إضافة خدمات جديدة. • سهولة تقديم الخدمات ذاتها لبنوك أخرى كما أشرنا سابقاً. • سهولة تقديم الخدمات ذاتها لمؤسسات جديدة.	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 تقديم الخدمات ذاتها لبنوك أخرى كما أشرنا سابقاً. • سهولة تقديم الخدمات ذاتها لمؤسسات جديدة.
6-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 السريعة24/24.

	المصرف العقاري	مصرف عودة
7-مراقبة وقياس الأداء	1. 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.	1. 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.
8-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 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. أ. تعالج معظم الأخطاء والمشاكل بسيناريوهات آلية تقوم بها خدمة التدخل الأوتوماتيكي.	أ. تتكامل البوابة مع نظام إعلام Notification يتيح إعلام القائمين على البوابة في حالات المشاكل والحالات الطارئة وغيرها من الأحداث. وذلك على مدار 24/24 ب. تُظهر تطبيقات المراقبة معلومات دقيقة ومفصلة عن جميع الطلبات مما يمكن المعنيين من تحديد 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.
1- نوع الرقابة	الرقابة الوقائية والتصحيحية	الرقابة الوقائية والتصحيحية
تعتبر المواصفة (ISO 27001:2005) قاعدة لتقييم إدارة حماية المعلومات، باعتبارها وثيقة لتقييم النظام		

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، 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 وذلك بإجراء الآتي:

1- 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

وبمقارنة عدد الخروقات في هذا التقرير مع الستة أشهر السابقة كان عدد الخروقات كالتالي :

الجدول رقم (3) عدد الخروقات على موقع العقاري عن طرق اختبار Acunetix Website Audit

التاريخ	عدد الخروقات
2015-8-26	13 اختراق
2015-9-30	11 اختراق وستة اختراق منها مستوى الاختراق اعلام
2015-10-31	10 أغلبها مستوى الاختراق منخفض
2015-11-28	4 كما وردت سابقا
2015-12-30	5
2016-1-30	3

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 .

2- 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 (2)

تم معالجة البيانات التي تم الحصول عليها من خلال أحد أدوات الدراسة باستخدام البرنامج الإحصائي SPSS (Statistical Package for Social Sciences) الملحق رقم (3) 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 (4): 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 (5): 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 8.135 t 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 (6): 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 (7): 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 11.859 t 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 (8): 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 (9): 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 لا تعزز كفاءة نظم المعلومات.

نستنتج من تحليل النتائج التي حصل عليها الباحثان من المصرفيين ما يلي :

- **بالنسبة للإجراءات والسياسات الإدارية**

1- إن المصرفيين يستخدمان تقنية النظم في أداء الأعمال المصرفية .

2- جميع فروع المصرفيين مربوطة بشبكة معلومات .

3- إن المصرفيين لهما اتصال بالشبكة العالمية (الانترنت).

4- مصرف عودة به نسبة عالية من الوعي الأمني أكثر من المصرف العقاري.

5- إن المصرفيين لا يتبعان طريقة معينة لتحفيز الموظفيين العامليين وكسب انتمائهم .

6- إن اهتمام المصارف بشكل عام ضعيف في مجال التدريب وتوفير المجلات الدورية .

7- إن المصرفيين يقومان بتغيير كافة الإجراءات التي كانوا يقومون بها الموظفون عند تركهم العمل .

8- إن المصرفيين لديهم إجراءات إدارية وقانونية ضد الأفراد الذين يسربون المعلومات لجهات اخرى .

9- التهديد في المصرفيين يأتي من مستخدمي النظام من الموظفيين وأنهم الذين يقومون بإساءة استخدامه .

- **بالنسبة للإجراءات والسياسات الأمنية**

1- إن المصرفيين يرون أن اعتماد استخدام التقنية لا يشكل خطورة على أموال المودعيين .

2- إن المصرفيين يرون أن استخدام التقنية يساعد في السرقات المالية .

3- إن المصرفيين ليس لديهم إجراءات لاستمرار العمل عند حدوث خلل أو أعطال في النظم والشبكات .

4- إن المصارف لا تقوم بتلف الوسائط والمستندات والتقارير .

5- إن المصرفيين لديهم تجهيزات مكافحة الحريق .

6- إن المصرفيين ليس لديهم إجراءات لاستمرار و تحديث العمل بصفة دورية .

7- إن المصرفيين يقومان بحفظ النسخ الاحتياطية خارج غرفة الحاسوب في مكان آمن خارج المصرف .

8- إن موظفي المصرف من مستخدمي النظم ومبرمجيها هم فقط المصرح لهم بالدخول واستخدام النظم .

9- إن المصرفيين يعتمدان كلياً على الجهات الاخرى في تركيب وصيانة الشبكات .

10- إن المصرفيين يستخدمان برامج ونظم حماية المعلومات يتركون جزء منها لموظفي التقنية والمستخدمين ويقومون بوضع خطط للمراقبة .

11- إن تستخدم مضادات الفيروسات الأصلية المرخصة ولا تواكب تحديثها .

12- إن المصارف حريصة على تطوير إستراتيجية لمكافحة الفيروسات ولكن مصرف عودة مهتم أكثر بهذا الموضوع

13- إن المصرفيين يستخدمان برامج أصلية ومرخصة .

14- إن الموظفيين يعتمدون على كلمة السر للدخول في نظم الحاسوب .

15- إن الموظفيين في المصرف العقاري يتهاونون في المحافظة على كلمة السر أكثر من مصرف عودة .

16- إن المصرفيين يستخدمون أكثر من وسيلة لحماية الشبكات .

- **بالنسبة للإجراءات والسياسات الرقابية**

1- إن المصرفيين لا يمنعون مدخلي البيانات من اجراء التعديلات .

2- إن نسبة إهتمام الإدارات العليا بأمن وحماية المعلومات مقبولة في المصرفيين .

3- لا توجد في المصرفيين دوائر مختصة بمراجعة وتدقيق نظم المعلومات .

4- إن المصرفيين لديها سياسات وإجراءات ومواصفات قياسية لأمن المعلومات ولكن هذه السياسات تضعها المصارف بنفسها .

5- المصرف العقاري لديه سياسات ومواصفات قياسية لتطوير وتشغيل نظم المعلومات أفضل من مصرف عودة.

6- لا يوجد في المصرفيين موظفون متخصصون بمراجعة وتدقيق نظم المعلومات .

7- إن الإدارة العليا لدى المصرفيين لا تشارك في تطبيق السياسات وتوكل مهام التطبيق لإدارة نظم المعلومات

8- إن المصرفيين لديهم إجراءات للمراقبة والتحكم في إدخال الأجهزة وإخراجها .

9- 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

النتائج والمناقشة:

أولاً: فيما يتعلق بالمخاطر المحيطة بعمل المصارف وعمل انظمة معلوماتها فقد تبين ان المخاطر تمثلت فيما يلي:

- وجود ثغرات بعدة مستويات ظهرت أثناء اختبار Acunetix Website Audit
- لا يوجد مستوى ثانٍ من الحماية لكلمات السر بالتوافق مع رقم المستخدم التعريفي للتأكد من أن الشخص نفسه هو صاحب الرقم
- حماية قناة المجيب الصوتي الآلي حيث 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
- الموارد المتوافرة لا تدعم النظم المحاسبية بشكل كافٍ لتحقيق الأمان للمعلومات والبيانات

ثانياً: فيما يتعلق بسياسات وإجراءات الأمان تبين ان هناك ثغرات تمثلت فيما يلي:

1. لم تلحظ سياسات المصرف ضرورة تطوير اجهزة الحاسب او تطوير انظمة التشغيل.
2. لم توفر الحماية الكافية لأنظمة الإلكترونية .
3. عدم كتابة السياسة الخاصة بالأدوار وادارة الموقع وعدم تحديثها وتطويرها.
4. يوجد عند باب الدخول لقسم نظم المعلومات في المصرف العقاري باب الكتروني يتم إدخال رقم سري على اللوحة التابعة له يسمح بالدخول الى القسم. مع العلم أن هذا الرقم معروف لكل موظفي المصرف وليس فقط لموظفي قسم نظم المعلومات
5. حدوث المخاطر في نظم المعلومات المحاسبية الالكترونية يرجع إلى أسباب تتعلق بموظفي المصرف، نتيجة ضعف الخبرة والوعي والتدريب
6. تعتمد الفروع على موظف واحد أو اثنين، مهمتهم تشغيل أنظمة الحاسوب. بينما الموظفون المتخصصون يكون مقر عملهم في المراكز الرئيسية للفروع. ولو حدث أن اضطر أحدهم للتغيب يؤدي إلى حدوث أزمة في العمل.
7. موارد شبكة (كابلات الشبكة الداخلية، الموجودة في بهو الادارة العامة للمصرف في الطابق الارضي) تحتاج الى حماية .

8. من الافضل عدم ادخال كلمة السر عن طريق لوحة المفاتيح أو استبدال اللوحة بلوحة أخرى تظهر على شاشة الحاسب حيث يتم النقر بالماوس على مفاتيحها واستخدام الماوس عن طريق اظهار لوحة المفاتيح على الشاشة وينقر عليها باستخدام الفأرة وهنا ايضا تظهر مشكلة الـ (Mouse Logger) وهو برنامج يسجل كل تحركات الفأرة.

9. عدم تخصيص المستخدمين الذين يتمتعون بمقدرات إدارية على كمبيوتر معين بحسابين أحدهما له مزايا إدارية والآخر له مزايا محدودة.

ثالثاً: فيما يتعلق بكفاءة النظام فقد تبينا أن كفاءة نظم المعلومات المحاسبية في تحقيق الأمان للمصرفين محدودة نسبياً، وكان من الممكن أن تكون أفضل. فهي لم تتمكن من بلوغ مستوى متقدم من أهداف الأمان من خلال سياساتها وإجراءاتها الأمنية التي كانت رسمتها

رابعاً: أما فيما يتعلق بالعوامل المؤثرة في كفاءة نظام المعلومات المحاسبي في بلوغ اهداف الامان فقد لوحظ من أن هناك مجموعة عوامل ساهمت في الحد من كفاءة نظام المعلومات في توفير الامان لبيناته ومعلوماته هذه العوامل هي:

<u>عوامل خارجية ساهمت في اضعاف قدرا النظام على بلوغ اهداف الامان منها:</u>

القوانين التشريعية والتنظيمية الناظمة لعمل المصارف والتي تحكم عمليات الدفع الإلكتروني غير كافية وغير واضحة

غياب السياسة الملزمة التي تصاغ للتأكيد من أن المصرف يطبق وينفذ المعايير التي تم كتابتها من قبل جهات محددة (المصرف المركزي)

<u>أما العوامل المرتبطة بالمصارف وأنظمتها والتي يمكن للمصرف أن يجد حلا لها، فكانت:</u>

1. تتمثل في تعدد القنوات مع المصرف وتعددها بين البنوك، فيصبح لدى العميل هويات كثيرة مما يؤدي الى ضياع الهويات مثل اسم المستخدم، كلمة المرور، الرمز السري، الرقم السري... الخ. وبما أن كل مصرف يعمل على حدة فالزبون مضطر للتعامل مع برمجيات كل مصرف بمفرده.
2. لا يوجد معايير اتصال وحماية موحدة لكل المصارف.
3. غياب الرقابة التي تقوم 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
4. عدم توفر القواعد والمعايير التي تحكم أداء العمل المصرفي.
5. عدم وجود وصف وظيفي مكتوب يحدد المهام والصلاحيات والإجراءات الواجب تطبيقها.

الاستنتاجات والتوصيات:

الاقتراحات:

أولاً: 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 لان يكون للمؤسسة اكثر 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.

ثانياً: إنشاء هذه البوابة وفق معايير اتصال موحدة ومعايير حماية موحدة، اي بالنسبة لهوية الزبون يجب أن يكون لديه هويتين، الهوية الافتراضية اي اسم المستخدم وكلمة المرور وهوية للصرافات اي البطاقات.

ملاحظة: من التوصية دمج كل مبدلات الصرافات في البنوك بمبدلة وطنية واحدة هي جزء من البوابة الموحدة.

ثالثاً: حماية هذه البوابة وذلك من خلال:

- إنشاء شهادة رقمية تصدر عن الهيئة الوطنية لخدمات الشبكة واعتماد التوقيع الرقمي كجزء أساسي بكل عمليات التحويل المالي في البوابة.
- 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)

التوصيات

1-ضرورة اهتمام المجتمع المالي بأمن البيانات والمعلومات وتطوير أنظمة الأمان في المصارف لتتأقلم مع التكنولوجيا المعاصرة .

2-تطوير القوانين والتشريعات بما يتلاءم مع التطورات الحديثة التي تحكم أنظمة الدفع الإلكتروني.

3-ضرورة ربط المصارف، فعليا، بين المعلومات والمواصفة (ISO 27001)، إذ أن هذا الربط سيوفر وسائل فاعلة وناجحة للتعامل مع المعلومات، فضلاً عن أن حصول المصارف على شهادة ISOفي هذا المجال سوف يمّكن المنظمات من الحصول على ميزة تنافسية، وإكسابها الطابع العالمي من خلال حصولها على شهادة دولية.

4-ضرورة وضع إجراءات تضمن استمرارية عمل وجاهزية نظم المعلومات للعمل في حالة الأزمات من خلال استخدام تجهيزات منيعة أو مرتبة بحيث تستطيع اكتشاف المخاطر قبل حدوثها والحد من وقوعها. وكذلك العمل على تعمية أو تشفير المعلومات عند الحفظ والنقل والتخزين على مختلف الوسائط كيلا يتمكن أحد من اختراقها.

5-بالإضافة إلى الرقابة الوقائية والتصحيحية 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.

المراجع:

1. شاهين، علي عبدالله. العوامل المؤثرة في كفاءة وفاعلية نظم المعلومات المحاسبية المحوسبة في المصارف التجارية العاملة في فلسطين، الجامعة الإسلامية، فلسطين، غزة، 2012.

2. قرم، عباس. أنظمة الدفع الالكتروني وتطبيقها في سورية، الجامعة الافتراضية السورية، رسالة ماجستير، 2012.

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)

4. الساكني. عبد الكريم، سعد والعواودة، علي، حنان. مخاطر استخدام تكنولوجيا المعلومات وأثرها على أداء نظم المعلومات المحاسبية، جامعة الإسراء، 2011.

5. القاسم ، عبد الرزاق و ردايده ، مراد. أمن نظم المعلومات المحاسبية في البنوك الأردنية– دراسة ميدانية، المجلة العربية للعلوم الإدارية والاقتصادية، لبنان، 2010.

6. حمادة، رشا، "أثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الالكترونية في زيادة موثوقية المعلومات المحاسبية (دراسة ميدانية). 2010.

7. زيدان، محمد، وحمو، محمد. متطلبات أمن المعلومات المصرفية في بيئة الإنترنت، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية للفترة 6–7 نيسان، الرياض، السعودية، 2010.

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

9. سنكري سهى، واقع استخدام تقنيات الدفع الالكتروني في المصارف السورية العامة، مجلة جامعه تشرين،2010.

10. Calder, A. and J. Van Bon, Information Security Based on ISO 27001/ISO 17799: A Management Guide.: The Stationery.