مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (33) العدد (1) 2011
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (33) No. (1) 2011

تحليل الهوة القائمة بين الواقع والمعايير العالمية لأمن المعلومات في المؤسسات المالية في سورية

الدكتور غسان فلوح *
الدكتور نور بك باشا**
وسيم أحمد***

(تاريخ الإيداع 22 / 8 / 2010. قُبِل للنشر في 20/ 2 / 2011)

ملخّص

نظراً للحاجة الكبيرة لوجود نظام قياس كمي لمستوى السرية وأمن المعلومات في المؤسسات المالية والمصرفية بما يسهل تحليل الثغرات والتعرف إلى مستوى تطبيق المعايير الدولية في مجال أمن المعلومات بغية الوصول للتوافق التام مع المعايير الدولية بما يحقق استمرارية الأعمال على أفضل المستويات، تم الشروع بدراسة تفصيلية عن واقع أمن المعلومات في هذه المؤسسات في الجمهورية العربية السورية كجزء رئيسي من بحث أوسع يتم العمل عليه يهدف إلى الوصول لتقديم دراسة كمية لقياس مستوى أمن المعلومات في هذه المؤسسات مما يشكل ركيزة أساسية في تعريف متطلبات هذه المؤسسات والخطوات الواجب اتباعها في كل من مجالات العمل بما يخص أمن المعلومات، إذ توضح هذه الورقة العلمية نتائج الدراسة الإحصائية على أربع عينات[1] من مؤسسات مالية ومصرفية في سورية لمعرفة توافق هذه العينة مع معايير أمن وسرية المعلومات وإيجاد ترتيب لأولوية هذه المعايير ومدى تأثيرها في استمرارية الأعمال بشكل مستقر وآمن.

الكلمات المفتاحية: السياسة الأمنية، نظام إدارة أمن المعلومات، الأصول، ادارة الكوارث، خطط استمرارية العمل، الرقابة، أمن النواحي الفيزيائية، الاتصالات.

* أستاذ –قسم هندسة الحواسيب والأتمتة– كلية الهندسة الكهربائية والميكانيكية –جامعة دمشق –سورية.
** أستاذ –قسم أمن المعلومات– كلية الهندسة المعلوماتية–جامعة كولالمبور–ماليزيا.
***طالب دراسات عليا(دكتوراه)– قسم هندسة الحواسيب والأتمتة– كلية الهندسة الكهربائية والميكانيكية –جامعة دمشق–سورية.

[1] في كل مؤسسة تم إجراء استطلاع لكل من الإدارة العامة وفرع على حدة ، وبالتالي فالدراسة بُنيت على ثمانية استطلاعات.

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (33) العدد (1) 2011
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (33) No. (1) 2011

Analysis of the Gap between the existing situation of information security in financial institutions in Syria and international standards

Dr. Ghassan Fallouh [*]
Dr. Norbik Basha [**]
Wassim Ahmad [***]

(Received 22 / 8 / 2010. Accepted 20 / 2 / 2011)

□ ABSTRACT □

This research was written under the urgent need to find a quantitative measurement of the level of security that financial institutions in Syria already have, which facilitates the analysis of the gap between them and the international standards, especially ISO27K in the field of information security, in order to improve the level of security for those institutions, complying with international requirements in this filed and providing secure environment and services for both employees and customers. The paper includes statistical studies, in-site meetings, analyses of the existing situations of information security, comparisons with ISO27K for 4 main financial institutions[2] in Syria, and defines priorities for those standards and their effects on business continuity in a way that provides security and stability.

Keywords: security policy, ISMS (Information Security Management System), Assessment, Assets Management, physical security, telecommunications.

[*] **Prof - Department of Computer Engineering and Automation- Faculty of Mechanical and Electrical Engineering- Damascus University -Syria.**
[**] **Prof -Centre for Advanced Software Engineering, University Technology Malaysia, Kuala-Lampur, Malaysia.**
[***] **Postgraduate Student- Department of Computer Engineering and Automation- Faculty of Mechanical and Electrical Engineering- Damascus University -Syria.**
[2] **For each sample we have done 2 surveys, for the Headquarter, and branch.**

مقدمة:

يعتبر أمن المعلومات من أهم الموضوعات التي تولي لها جميع المؤسسات والهيئات العلمية في جميع أنحاء العالم اهتماماً خاصاً وموارد مالية كبيرة وذلك للحفاظ على سوية عالية من السرية والحماية للمعلومات والتي تعتبر لدى بعض المؤسسات – وخاصة المصارف والمؤسسات المالية – الأصول الأغلى Assets والأكثر خطورة، والتي يسعى الجميع للحفاظ عليها من التسرب أو الضياع أو التغيير.

ومع تعاظم دور الانترنت والخدمات الالكترونية، وخاصة المالية منها. والتزايد المخيف للبرامج الضارة والاختراقات للمواقع والحسابات المصرفية. ازدادت الحاجة لأبحاث ودراسات في مجال أمن الشبكات والمعلومات.

وعليه فقد دأبت الجهات العلمية المختصة بوضع معايير دولية لأمن المعلومات بحيث تسهل على المعنيين بالموضوع في كافة المؤسسات على اختلافها تطبيق سياسات أمنية محكمة ومراجعتها للوصول لحالة أمنية مستقرة وفي مستوى مقبول لتقديم الخدمات والتسهيلات للزبائن أو للحفاظ على سرية المعلومات والتحكم بالوصول إليها، نذكر منها: ISO 27K,COBIT,BASEL2 وغيرها.

أهمية البحث وأهدافه:

تهدف هذا الورقة إلى إعطاء رؤية موسعة للحالة الراهنة للمؤسسات المالية في سورية وتحليل الهوة الموجودة بين الواقع الراهن والمعايير العالمية وخاصة ISO27K وشرح الخطوات التطبيقية الهامة المطلوب القيام بها بصورة منهجية للوصول الى حالة أمنية عالية، وذلك على كامل الفقرات اللاحقة.

تقوم هذه الدراسة بتعريف الهوة الموجودة بين الوضع الراهن لأمن المعلومات والمعايير العالمية، وتوضيح أولوية وأهمية كل من هذه المعايير تبعاً لنتائج الاستطلاع الذي تم القيام به، والانتقال إلى الخطوات التطبيقية الهامة للوصول إلى الحالة المطلوبة اعتماداً على المفاصل الأساسية في المعيار ISO27K وعلى الاستطلاعات بما يتوافق مع واقع ومتطلبات أمن المعلومات في المؤسسات المالية والمصرفية في الجمهورية العربية السورية.

طرائق البحث ومواده:

انطلاقاً من حصيلة الاستطلاع والاجتماعات والوثائق والجولات الميدانية التي تمت خلال السنوات الأربعة الماضية على أربع مؤسسات مالية كبرى في سورية (تم إجراء استطلاعين في كل مؤسسة واحد للإدارة العامة وآخر لأحد الفروع وذلك على اعتبار أن عمل ومتطلبات أمن المعلومات للفروع مختلف عن الإدارات) وشملت مصرفّين هامين ومؤسستين ماليتين (وكل منها يتكون من إدارة عامة وأكثر من 30 فرعاً) دون ذكر الأسماء حفاظاً على الخصوصية وسرية العمل حسب طلب هذه الجهات.

اتخذت الدراسة المنهج التالي:

1) اعتماد المعيار ISO27K كمعيار رئيسي لتقييم وضع أمن المعلومات في المؤسسات المالية في سوريا.
2) تحديد نقاط التقييم والاستطلاع انطلاقاً من المعايير ISO27K.
3) بالإضافة إلى ISO27K تم اعتماد إطار العملNIST SP 800-53 rev1:2010 كخطوات عملية للوصول إلى المعايير المطلوبة وتقييمها(Assessment).

4) اعتماد أجوبة الاستطلاع المتعلقة بالنقطة المدروسة، مع ملاحظة اختلاف بعض الأجوبة في المؤسسات الأربع المدروسة حيث تم اختيار الجواب الأكثر بعداً عن المعيار المقابل ووضع النسبة من الاستطلاع الموافقة لذلك.
5) تحليل الفجوة الذي يعكس موجز عن حصيلة الإجابات.
6) مفاتيح الممارسات العملية، التي صممت على الشكل التالي:
   a) تعريف الإشكالات العامة.
   b) توضيح الخطوات التطبيقية الواجب اتباعها لتجاوز تلك الإشكالات.

يبقى التذكير بأنه تم تضمين النقاط والإشكاليات التي حصلت على تصويت جهة واحدة على الأقل من العينات التي تم تطبيق الاستطلاع عليها مع ذكر نسبة الجهات التي قامت بتأكيد الإشكاليات وضرورة معالجتها من عدد العينات الكلية.

النتائج والمناقشة:

سنقوم بعرض النتائج والمناقشة لكل مجال مدروس كما يلي:

الإشكاليات: وتعني الفقرات من المعايير ISO 27001,27002 التي وجدنا فيها إشكالات (غير مطبقة أو ناقصة أو خاطئة...)	**نسبة العينات:** وتعني النسبة من الاستطلاعات التي وجدت فيها الإشكالية	**ملاحظات عامة:** توضيحات

الخطوات التطبيقية الهامة:[3]

وهي الخطوات الواجب اتخاذها من قبل المؤسسة المدروسة لتصحيح الإشكاليات الواردة في فقرة المعيار المناقش

1. نظام إدارة أمن المعلومات (ISMS)

الإشكاليات	نسبة العينات	ملاحظات عامة
العلاقة بين استراتيجية المؤسسة ومحددات تقييم المخاطر وسلوك الإدارة	%75	
وضوح وجلاء الأدوار والمسؤوليات	%100	تم الإجماع على ضرورة وجود إدارة عامة مدركة لأهمية أمن المعلومات وإدارة تقنية قادرة على تنفيذ كافة الخطط والاستراتيجيات المتعلقة بأمن المعلومات
عملية المراجعة والتغذية الراجعة	%50	

[3] تم اعتماد عدة مراجع لتوضيح الخطوات التطبيقية وخاصة NIST SP 800-53 rev1, المراجع

الخطوات التطبيقية الهامة:

على الإدارة بكافة مستوياتها دعم نظام أمن المعلومات بتوجيه واضح والتزام كامل ومعرفة جلية بالمسؤوليات المترتبة عند تطبيق أمن المعلومات.

تتجلى الخطوة الأولى في تغيير النظرة التقليدية في التعامل مع تكنولوجيا المعلومات على أنها أداة مساعدة في العمل لا علاقة لها بأهداف وغايات العمل. لقد أصبحت المعلومات من أهم العوامل التنافسية وجزءاً ثميناً من أصول المؤسسة ويجب حمايتها والحفاظ على أمنها

2. تقييم المخاطر ومعالجتها

الإشكاليات	نسبة العينات	ملاحظات عامة
الحاجة إلى ترتيب المخاطر على ضوء أهداف ومحددات المخاطر	%50	
عكس تقييم المخاطر على الاستراتيجيات والخطط المتعلقة بأمن المعلومات بما يشمل الميزانية المخصصة	%100	بين الاستطلاع وجود فجوة كبيرة بين قوائم تقييم المخاطر في العينات المدروسة وبين الخطط والموازنة المحجوزة لإدارة ومعالجة هذه المخاطر

الخطوات التطبيقية الهامة:[4]

تقييم المخاطر

يجب القيام بتقييم المخاطر وتحديثه خلال فواصل مناسبة لكافة المتعلقات المعلوماتية.

معالجة المخاطر

يجب أن تتضافر جهود معالجة المخاطر لصد المخاطر المعرفة عبر استخدام وسائل التحكم الأمنية الإدارية والفنية والفيزيائية المناسبة وعبر تخصيص موازنة خاصة لمعالجة هذه المخاطر.

3. السياسة الأمنية

الإشكاليات	نسبة العينات	ملاحظات عامة
عملية التخطيط وتحليل الهوة بين الواقع والمتطلبات الأمنية	%50	
تضييق الفجوة بين الواقع والمتطلبات الأمنية عبر الخطوات التنفيذية	%100	
عملية المتابعة والتقييم المستمر	%50	تم ذكر إشكالية تأثير تغيير الإدارات على عمليات المتابعة والتقييم المستمر بما ينعكس سلباً على وجود استمرارية في عمليات تضييق الهوة الأمنية

[4] ISO/IEC TR 13335-3 ، المراجع

القيام بخطوات وتعديلات تبعاً لعمليات التقييم المستمر	%50	

الخطوات التطبيقية الهامة:[5]

المجال

على هذه السياسات أن تؤمن في مجملها تحكماً جلياً بكافة البيانات المحصلة المتداولة أو المخزنة في وسائط معالجة البيانات والاتصالات أو أنظمة التخزين، وكذلك الأمر بالنسبة للبيانات المحصلة والمتداولة مع الأطراف الخارجية المتعاقدة مع المؤسسة المالية.

التصديق

على هذه السياسات أن تصدق رسمياً من قبل السلطات المخولة حسب الأصول.

التوثيق

يجب أن توثق السياسات الأمنية بطريقة مناسبة للمؤسسة.

التواصل والتدريب والتوعية

يجب تبادل سياسات أمن المعلومات ضمن المؤسسة المالية، ومع الأطراف الخارجية المتعلقة أيضاً، من خلال برنامج تدريب وتوعية مناسب.

المراجعة الدورية

يجب مراجعة هذه السياسات على فترات محددة وحين حدوث تغييرات مؤثرة في البيئة الخارجية لضمان استمرارية فعاليتها وملاءمتها ومناسبتها.

4. تنظيم أمن المعلومات

الإشكاليات

يعكس هذا القسم نفس المشاكل التي تم طرحها في القسم السابق.

الخطوات التطبيقية الهامة:[6]

التزام الإدارة

اهتمام واضح ودعم عملي لمبادرات أمن المعلومات متضمناً تخصيص الموارد المناسبة لوسائل التحكم الخاصة بأمن المعلومات.

تنسيق الجهود

يجب تنسيق الأنشطة المتعلقة بأمن المعلومات عن طريق تمثيل الجهات المختلفة في المؤسسات المالية بالأدوار الأمنية والوظائفية المتعلقة.

توزيع المسؤوليات

يجب تعريف كافة المسؤوليات المتعلقة بأمن المعلومات بشكل واضح.

[5] ISO/IEC 13335-1:2004. ، المراجع.
[6] ISO/IEC 13335-1:2004. ، المراجع.

عمليات التفويض

على عملية التفويض المتعلقة بوسائل وقابليات معالجة المعلومات الجديدة أو المتعلقة بالتغيرات المؤثرة في الوسائل والقابليات الموجودة أن تكون معرفة ومنفذة.

اتفاقات السرية وعدم الإفصاح

على اتفاقات السرية وعدم الإفصاح أن تعكس حاجات المؤسسات المالية لحماية معلوماتها، ويجب مراجعة هذه الاتفاقات دورياً.

الاتصال مع السلطات الخارجية

يجب الحفاظ على آليات الاتصال مع السلطات الخارجية.

الاتصال مع المجموعات ذات الاهتمام الخاص

يجب الحفاظ على اتصال مناسب مع المجموعات ذات الاهتمام الخاص أو المنتديات الأخرى المهتمة بأمن المعلومات والجمعيات المختصة.

الاتصال والعقود مع الطرف العقدي الثالث (غير المباشر)

على الاتفاقات مع الطرف الثالث المنخرط في الدخول إلى معلومات المؤسسة أومعالجتها أو إدارتها أو وسائل معالجتها أن تغطي كافة المتطلبات الأمنية المطلوبة.

الاتصال والعقود مع المستخدمين

يجب مواجهة كل المتطلبات الأمنية المعرفة قبل إعطاء المستخدم حق الدخول إلى معلومات أو أصول المؤسسة المالية. تتشابه الخطوات المتبعة هنا مع تلك المذكورة سابقاً والمتعلقة بالأطراف الخارجية.

المراجعة المستقلة لأمن المعلومات

على المؤسسات المالية خلال عمليات إدارة وتنفيذ أمن المعلومات أن تتبع أسلوب المراجعة المستقلة والمجدولة سلفاً أو الطارئة حين حدوث متغيرات مؤثرة في البنية الداخلية أو البيئة الخارجية.

5. إدارة الأصول المعلوماتية

الإشكاليات	نسبة العينات	ملاحظات عامة
إعادة تعريف الأصول المعلوماتية	%50	
تسجيل الأصول المعلوماتية	%25	
التوثيق ووضع اللصاقات المناسبة	%75	إن توثيق وأرشفة كافة المعلومات والتجهيزات والإجرائيات حسب المعايير يعتبر الركيزة التي تعتمد عليها كافة المؤسسات لمتابعة تطبيق المعايير المتعلقة بأمن المعلومات

الخطوات التطبيقية الهامة:[7]

مخزون الأصول

يجب حصر كافة الأصول المعلوماتية بدقة على شكل قوائم، بحيث تحتوي هذه القوائم على أسماء مالكي الأصول والمتحكمين بها والمسؤولين عن حمايتها.

ملكية الأصول (التحكم بها)

يجب أن تدار جميع الأصول بوساطة شخص أو مجموعة مكلفة من المؤسسة المالية، ممن لديهم مسؤوليات محددة وواضحة لإدارة الأصل المعني.

تصنيف الأصول

يجب تصنيف الأصول انطلاقاً من قيمتها وحساسيتها وحراجتها بالنسبة للمؤسسة، وكذلك متطلباتها القانونية.

العنونة والمعاملة

يجب إعداد مجموعة من الإجراءات المتعلقة بعنونة ومعاملة الأصول وتنفيذها بالتوافق مع جداول التصنيف التي تتبناها المؤسسة المالية.

العنونة دون الوقوع في المتاعب

1. تحديد المعلومات المرغوب استخلاصها من لصاقة العنونة مباشرةً.
2. تحديد جدول ترميز وترقيم مناسب.
3. التجميع ضمن كتلة حين توفر الإمكانية (مثلاً، إعطاء ترميز للشبكات المحلية الافتراضية، المخدمات، أو التجهيزات).

الاستخدام المقبول للمعلومات

يجب تعريف وتوثيق وتطبيق قواعد الاستخدام المقبول للآصول المعلوماتية المرتبطة بوسائل معالجة المعلومات.

6. الأمن والموارد البشرية

الإشكاليات	نسبة العينات	ملاحظات عامة
قانون التوظيف وإجرائياته	%75	إن وجود قانون تفصيلي يوضح حقوق وواجبات الموارد البشرية فيما يتعلق بأمن المعلومات كان المتطلب الرئيسي لمعظم العينات المدروسة في الجمهورية العربية السورية
تأثير طبيعة العلاقات الاجتماعية بالعلاقات المهنية على أمن المعلومات	%75	

[7] ISO/IEC TR 13335-3، المراجع.

الخطوات التطبيقية الهامة:

المجال

يجب أن تشمل سياسات المؤسسات المالية المتعلقة بالموارد البشرية إجمالاً جميع الأفراد خارج وداخل المؤسسات المالية الذين يستخدمون المعلومات ووسائل معالجتها.

الأدوار والمسؤوليات

يجب تعريف وتوثيق أدوار ومسؤوليات الموظفين والمتعاقدين والأطراف العقدية الثالثة من الناحية الأمنية، بما يتماشى مع سياسات الخصوصية وأمن المعلومات في المؤسسة المالية.

ما قبل التوظيف

يجب أن تقوم المؤسسات المالية أو طرف ثالث مناسب بعمليات التحقق من خلفية المرشحين للوظيفة ووضع المتعاقدين والأطراف العقدية الثالثة.

شروط وبنود التوظيف

على الموظفين والمتعاقدين والأطراف العقدية الثالثة الاتفاق والتوقيع على تصريح الحقوق والمسؤوليات الناجمة عن ارتباطهم مع المؤسسة المالية، بما في ذلك ما هو متعلق منها بخصوصية المعلومات وسريتها.

اتفاقات إضافية لمرحلة ما قبل التوظيف

على الموظفين والمتعاقدين والأطراف العقدية الثالثة توقيع اتفاقات أخرى عند اللزوم، قبل إعطائهم أذن الدخول والسماحيات الأخرى إلى المعلومات ووسائل معالجتها.

مسؤوليات الإدارة

على الإدارة أن تلزم الموظفين والمتعاقدين والأطراف العقدية الثالثة بتطبيق وسائل التحكم الأمنية المنسجمة مع السياسات والإجراءات المتبعة في المؤسسة المالية.

التوعية والتعليم والتدريب

يجب القيام بحملة توعية وتدريب حول التحديثات في سياسات المؤسسات المالية وفي الإجراءات الوظيفية المتعلقة لكل من الموظفين والمتعاقدين والأطراف العقدية الثالثة.

عملية التأديب

يجب أن يتعرض الموظفون الذين يقومون بالمخالفة إلى عملية تأديبية رسمية.

مسؤوليات نهاية الخدمة

يجب التعريف والتكليف الواضح لمسؤوليات وممارسات أداء نهاية الخدمة أو تغيير الوظيفة.

استرجاع الأصول

على جميع الموظفين والمتعاقدين والأطراف العقدية الثالثة إعادة كافة الأصول المعلوماتية والفيزيائية التي في ذممهم إلى المؤسسات المالية حال نهاية علاقتهم الوظيفية أو عقدهم.

إلغاء حقوق الدخول

يجب إلغاء كافة حقوق الدخول إلى المعلومات ووسائل معالجتها حال انتهاء العلاقة الوظيفية أو العقدية.

7. الأمن من الناحية الفيزيائية والبيئية

الإشكاليات	نسبة العينات	ملاحظات عامة
تطبيق وصيانة وتغيير وفحص واختبار العديد من الحمايات الفيزيائية الموجودة	%100	تم الإجماع على ضرورة متابعة عمليات الصيانة وخصوصاً التي تتم من قبل شركات خارجية إذ تعتبر هذه العمليات سبباً رئيسياً لتسرب وفقدان المعلومات والتجهيزات

الخطوات التطبيقية الهامة:

الطوق الأمني الفيزيائي

يجب أن يستخدم الطوق الأمني الفيزيائي من أجل حماية المناطق الحساسة التي تحتوي المعلومات ووسائل معالجتها. يجب تصميم وتنفيذ الحماية الفيزيائية للمكاتب والغرف والمنشآت الأخرى بحيث تتناسب مع المخاطر المُعرَّفة وقيمة الأصول المحتملة الإصابة في كل موضع.

وسائل التحكم بالمدخل الفيزيائي

يجب أن تتم حماية مناطق وجود وسائل معالجة المعلومات الحساسة عن طريق وسائل التحكم على المداخل للتأكد من عدم تمكن غير المصرح لهم بالدخول اليها. كما يجب تصميم وتنفيذ الحماية الفيزيائية للمكاتب والغرف والمنشآت الأخرى بحيث تتناسب مع المخاطر المُعرَّفة وقيمة الأصول المحتملة الإصابة في كل موضع.

الحماية من التهديدات البيئية الخارجية

يجب تصميم وتنفيذ وسائل الحماية الفيزيائية ضد أخطار النيران والطوفان والعواصف والزلازل والانفجارات والعصيان المدني وكل أشكال المخاطر الأخرى الطبيعية منها وتلك ذات المنشأ البشري.

العمل في المناطق الحساسة

يجب تصميم وتنفيذ أدوات وإرشادات الحماية الخاصة بالعمل في المناطق الحساسة.

معابر الدخول والتسليم والتحميل العامة

يجب التحكم في نقاط العبور مثل مناطق التسليم والتحميل أو أية نقاط أخرى قد يلج من خلالها أشخاص غير مصرح لهم بالدخول إلى هذه المناطق.

وضع وحماية المعدات

يجب أن يتم وضع وحماية المعدات بشكل يقلل التهديدات والأخطار البيئية، وكذلك التهديدات البشرية بواسطة الدخول غير المصرح له.

الأدوات الداعمة

يجب أن تتم حماية الأجهزة من انقطاع التيار الكهربائي والاتصالات وغيرها من الأعطال الناجمة عن انقطاع التزويد بالأدوات الداعمة مثل المياه والصرف الصحي.

أمن الكبلات

يجب حماية كبلات الكهرباء والاتصالات التي تنقل بيانات حساسة أو خدمات المعلومات الداعمة من التدخل أو الضرر.

صيانة المعدات

يجب أن يُحافَظ على التجهيزات بصورة سليمة لضمان استمرارية إتاحيتها وصحتها.

ترحيل الأملاك إلى خارج المنشأة

لا يجوز إخراج أية تجهيزات أو معلومات أو برامج دون تصريح مسبق ومقيد.

أمن الأملاك خارج المنشأة

يجب تطبيق معايير أمنية ملائمة على المعدات خارج مرافق المؤسسات المالية مع الانتباه إلى اختلاف المخاطر داخل المنشأة عن خارجها.

أمن المعدات المنسقة أو المعاد استخدامها

يجب فحص كافة المعدات ذات وسائط التخزين وتجهيزات وسائط التخزين المستقلة للتأكد من خلوها من أية بيانات حساسة أو برامج مرخصة.

8. إدارة عمليات التشغيل والاتصالات

الإشكاليات	نسبة العينات	ملاحظات عامة
استراتيجية الحوادث والكوارث	%100	رغم وجود تصورات عن آليات العمل في حالات الحوادث والكوارث لم يتم تطبيق هذه التصورات وفق خطط تنفيذية بما يشمل مقرات العمل الاحتياطية وخصوصاً فيما يتعلق بالتجهيزات
استراتيجية المتغيرات	%75	
استراتيجية التوثيق والتقارير	%50	
النسخ الاحتياطي والأرشفة	%25	

<u>الخطوات التطبيقية الهامة:</u>

توثيق الإجراءات التشغيلية

يجب توثيق وصيانة وضمان إتاحة الإجراءات التشغيلية لكل من يحتاجها.

فصل المهام

يجب فصل الواجبات عن المسؤوليات إلى الحدود الممكنة، وذلك لتقليص فرص التعديل غير المتعمد(عن طريق الخطأ) أو غير المصرح به أو سوء استخدام أصول المؤسسة المالية.

فصل وسائل التطوير عن الاختبار عن التشغيل

يجب فصل أدوات التطوير عن الاختبار عن التشغيل إلى الحدود الممكنة، وذلك لتقليص مخاطر الدخول غير المصرح له أو التغيير الكلي لأنظمة التشغيل.

وسائل التحكم لحماية الموارد المركزية

يجب إدارة وضمان التحكم بوسائل معالجة المعلومات المركزية، مثل مخدمات التطبيقات ومعدات تخزين البيانات في "مراكز البيانات"، بصورة مناسبة قادرة على حمايتها من التهديدات والمحافظة على أمن الأنظمة والتطبيقات التي تستخدمها.

أمن الموارد المركزية

يجب تعريف كل المزايا الأمنية ومستوى الخدمة ومتطلبات الإدراة لكل الموارد والخدمات المركزية بالتفصيل، وإضافتها إلى اتفاقات الخدمات المقدمة ضمن المؤسسات المالية أو المحولة إلى طرف خارجي لتقديمها.

وسائل التحكم الشبكية

يجب إدارة وضمان التحكم بالشبكات بصورة مناسبة قادرة على حمايتها من التهديدات والمحافظة على أمن الأنظمة والتطبيقات التي تستخدمها، بما في ذلك المعلومات المنقولة عبرها.

أمن الخدمات الشبكية

يجب تعريف كل المزايا الأمنية ومستوى الخدمة ومتطلبات الإدراة لكل الخدمات الشبكية بالتفصيل، وإضافتها إلى اتفاقات الخدمات الشبكية المقدمة ضمن المؤسسات المالية أو المحولة إلى طرف خارجي لتقديمها.

التحكم بمحطات العمل

يجب إدارة وضمان التحكم بأجهزة محطات العمل بصورة مناسبة قادرة على حمايتها من التهديدات والمحافظة على الأمن عموماً، يتضمن ذلك معايير مشابهة للموارد المركزية والشبكية تطبق حين توافر الإمكانية التقنية والإدارية.

أمن تجهيزات محطات العمل

يجب تعريف كل المزايا الأمنية ومستوى الخدمة ومتطلبات الإدارة لكل خدمات محطات العمل بالتفصيل، وإضافتها إلى اتفاقات الخدمات المقدمة ضمن المؤسسات المالية أو المحولة إلى طرف خارجي لتقديمها، يتضمن ذلك معايير مشابهة للموارد المركزية والشبكية تطبق حين توفر الإمكانية التقنية والإدارية.

الترابط بين الأنظمة المعلوماتية

يجب إعداد وتنفيذ السياسات والإجراءات لحماية المعلومات المتعلقة الترابط بين أنظمة العمل.

الانترنت والرسائل الإلكترونية

يجب حماية المعلومات المتداولة عبر الرسائل الإلكترونية، مثل البريد الإلتروني، الرسائل البعيدة، الاجتماعات عبر الصوت والصورة، كل الاتصالات الشخصية فرد لفرد أو فرد لمجموعة أو مجموعة لمجموعة.

التجارة الإلكترونية

يجب حماية المعلومات المتداولة عبر التجارة الالكترونية والتي تستخدم الشبكات االعامة من أنشطة الاحتيال والكشف والتعديل غير المصرح له وكل نشاط آخر يؤدي إلى هجوم محتمل.

الخطوات التطبيقية للمعاملات المباشرة

يجب حماية المعلومات المتعلقة بالمعاملات المتداولة عبر الانترنت وخطواتها التطبيقية لمنع النقل الناقص أو التوجيه الخاطئ أو تبديل /كشف /مضاعفة الرسائل والرد غير المصرح له.

المعلومات المتاحة للعموم

يجب حماية صحة المعلومات المقدمة عبر حماية النظام الذي يؤمنها للعموم – مخدم الويب مثلاً– لمنع التعديل غير المصرح له.

إدارة التغيير والمشاريع

يجب التحكم بعمليات تغيير وسائل وأنظمة معالجة المعلومات عن طريق إجراءات إدارة التغيير والمشاريع المناسبة.

عوامل قبول النظام

يجب تأسيس عوامل قبول أنظمة المعاوماتية الجديدة والتحديثات والنسخ الجديدة والتأكد من نجاح اختبارها أثناء إعدادها وقبل اعتمادها.

إدارة الحوادث والمشاكل

يجب تسجيل الانحرافات عن عمليات التشغيل النظامية المتعلقة بوسائل معالجة المعلومات والتحقيق فيها باستخدام إجراءات إدارة الحوادث والمشاكل المناسبة.

إدارة التهيئة

يجب تسجيل وتحديث تهيئة أدوات معالجة المعلومات لكي تجاري التغييرات.

إدارة جودة واستيعاب الخدمة

يجب تحديد مستوى جودة الخدمة المتوقعة رسمياً لكامل مكونات الخدمة الأساسية، للواقع الحالي والمتطلبات المستقبلية أيضاً.

عقود خدمات الطرف العقدي الثالث

يجب أن تتضمن اتفاقات تسليم الخدمات على وسائل التحكم الأمنية وتعريف بالخدمات ومواصفات الخدمة المطلوبة.

9. التحكم بالوصول

الإشكاليات	نسبة العينات	ملاحظات عامة
متابعة ومراقبة تجهيزات وسياسات أمن الوصول وتغييرها في حال اقتضت الحاجة	%100	تم الإجماع على ضرورة تعريف سياسات تحكم بالوصول والدخول إذ تعتبر أي ثغرة في هذه السياسات سبباً مباشراً لمعظم عمليات الاختراق والتسريب

<u>الخطوات التطبيقية الهامة:</u>

سياسة التحكم بالوصول

يجب إرساء سياسة التحكم بالوصول وتوثيقها ومراجعتها دورياً على قاعدة حاجات العمل والمتطلبات الخارجية.

إدارة سياسة الدخول المستخدم

يجب أن تركز السياسات على ضمان دخول المستخدم المصرح له إلى المعلومات ووسائل معالجتها، ومنع دخول غير المصرح له.

تسجيل المستخدم

يجب تطبيق الإجراءات الرسمية لتسجيل المستخدم وإلغاء تسجيله، لضمان الدخول وعدم الدخول إلى كافة أنظمة وخدمات المعلومات. إضافةً إلى إعطاء هوية فريدة بكل مستخدم.

إدارة الامتيازات

يجب أن تكون أماكن توطين امتيازات الدخول مقيدة ومراقبة.

إدارة كلمة عبور المستخدم

يجب التحكم بأماكن توطين كلمات العبور من خلال عملية إدارة رسمية.

إدارة شارة دخول المستخدم

يجب التحكم بأماكن توطين الشارات، مثل الكروت الالكترونية، من خلال عملية إدارة رسمية.

مراجعة حقوق دخول المستخدم

يجب مراجعة حقوق دخول كل مستخدم دورياً من خلال عملية رسمية.

سياسة استخدام خدمات الشبكة

يجب أن يعطى المستخدمون حق الدخول إلى الخدمات الشبكية المصرح باستخدامها فقط.

التصريح للاتصال الخارجي

يجب اعتماد طرائق التصريح للتحكم بالدخول البعيد إلى الشبكة عندما يكون ذلك مناسباً ومجدياً من الناحية الفنية.

تعريف المعدات/ المواقع في الشبكة

يجب اقتصار الدخول إلى الشبكة على المعدات والمواقع المعرفة عندما يكون ذلك مناسباً ومجدياً من الناحية الفنية.

حماية منفذ التشخيص والتهيئة عن بعد

يجب التحكم منطقياً وفيزيائياً بالوصول إلى منافذ التشخيص والتهيئة.

فصل الشبكات

يجب فصل مجموعات المستخدمين والخدمات في الشبكات.

التحكم بالاتصال الشبكي

يجب تقييد حرية الاتصال بالشبكة بصورة مناسبة مدعمة بسياسات التحكم بالوصول ومتطلبات مختلف التطبيقات.

التحكم بالتوجيه الشبكي

يجب تطبيق وسائل التحكم بالتوجيه لضمان عدم مخالفة الاتصالات وجريان المعلومات لسياسات التحكم بالوصول من وإلى التطبيقات الموجودة على الشبكة.

التحكم باستخدام الأنظمة

يجب تنفيذ وسائل التحكم لتقييد الدخول إلى أنظمة التشغيل للمصرح لهم فقط عن طريق طلب التصريح من المستخدمين بما يتناسب مع سياسات التحكم بالوصول.

إجراءات الدخول الأمنية

وينبغي التحكم بالوصول إلى الأنظمة عن طريق إجراءات أمنية لتسجيل الدخول.

هوية وتصريح المستخدم

يجب أن يمتلك جميع المستخدمين وعلى كل الأنظمة اسم مستخدم وحيد لاستخدامهم الشخصي. ويجب اختيار آليات تصريح مناسبة مثل المبنية على المعرفة أو الشارة أو الثنائية للسماح بالاستخدام.

نظام إدارة كلمات العبور

على أنظمة إدارة كلمات العبور أن تتحقق من جودة طريقة التصريح بالدخول.

استخدام أدوات النظام التي تتجاوز وسائل التحكم

يجب أن يكون استخدام أدوات النظام التي تتجاوز زسائل التحكم مقيداً، ومراقباً بصورة مناسبة حين استخدامه (عن طريق عملية تسجيل أحداث مناسبة مثلاً).

انتهاء الجلسة

على الجلسات التفاعلية أن تغلق وتدع المستخدم خارجها بعد مدة زمنية معرفة. يجب إعادة التصريح من أجل معاودة الجلسة التفاعلية.

الحد من مدة ومكان الاتصال المسموح به

يجب أن يعطي تقييد زمن الاتصال أمناً إضافياً للتطبيقات عالية المخاطر أو لقابليات الاتصال البعيد.

تقييد الوصول إلى المعلومات

يجب تقييد الوصول إلى المعلومات ووظائف التطبيقات بما يتلاءم مع سياسات التحكم بالوصول المعرفة والمنسجمة بدورها مع سياسات المؤسسات المالية ككل، ويتضمن ذلك كل وسائل التحكم التي ذكرت في هذه الدراسة.

عزل الأنظمة الحساسة

يجب عزل الأنظمة الحساسة وتخصيصها ببيئة حاسوبية مستقلة.

10. اكتساب وتطوير وصيانة أنظمة المعلومات

الإشكاليات	نسبة العينات	ملاحظات عامة
المواصفات المطلوبة لوسائل التحكم الأمنية المرتبطة بالعروض المتعلقة بحاجة العمل لأنظمة معلومات جديدة	%100	ضرورة وجود هيئة مركزية لوضع المواصفات والمقاييس التي تحكم عمليات العروض والشراء الخاصة بأنظمة المعلومات

<u>الخطوات التطبيقية الهامة:</u>

متطلبات التحليل والتحديد

يجب أن تتضمن العروض المتعلقة بحاجة العمل لأنظمة معلومات جديدة، أو تعزيز تلك القائمة منها، على المواصفات المطلوبة لوسائل التحكم الأمنية.

عملية تصحيح التطبيقات

يجب ان يتم التحقق من سلامة معالجة الأنظمة للبيانات المدخلة التي يتعاملون معها من عدة أوجه كالمعالجة الداخلية والرسائل ومخرجات البيانات بين العمليات والضياعات والتعديل غير المصرح به أو إساءة استخدام المعلومات.

استخدام وسائل التحكم بالتشفير

يجب تطوير وتطبيق وسائل التحكم بالتشفير المناسبة لحماية سرية وصحة ووثوقية المعلومات.

إدارة مفاتيح التشفير

يجب تنفيذ سياسات وعمليات إدارة المفاتيح لدعم استخدام تقنيات التشفير في المؤسسة المالية.

أمن برامج التشغيل

يجب تطبيق الإجراءات من أجل التحكم في تنصيب البرامج على أنظمة التشغيل والحد من مخاطر انقطاع أو تشوه الخدمات المعلوماتية.

ترميز أمن البرامج وبيانات الاختبار

يجب تقييد الدخول ترميز أمن البرامج.

وسائل التحكم في مواجهة الترميز الخبيث

يجب تطبيق وسائل حماية لمنع وكشف ومعالجة الترميزات الخبيثة.

إجراءات التحكم بالتغيير

يجب توثيق ومراقبة تنفيذ التغيرات عبر استخدام إجراءات رسمية لمراقبة التغيرات.

البرامج المطورة خارج المؤسسة المالية

يجب القيام بعمليات الإشراف والمراقبة من قبل المؤسسات المالية على البرامج المطورة خارجه باستخدام وسائل تحكم مشابهة لتلك المستخدمة في عمليات التطوير الداخلي.

تسرب المعلومات

يجب منع أو الحد من فرص تسرب المعلومات.

التحكم بالثغرات الفنية

يجب تحديث المعلومات المتعلقة بثغرات الأنظمة المعلوماتية بانتظام، وتقييمها على أساس المخاطر والتعرض للكشف واتخاذ أدوات الصد المناسبة.

11. إدارة حوادث أمن المعلومات

الإشكاليات	نسبة العينات	ملاحظات عامة
إعادة النظر في كامل إدارة الحوادث في المؤسسات المالية السورية	%100	

<u>الخطوات التطبيقية الهامة:</u>

رفع الحوادث المعلوماتية الأمنية

على جميع الموظفين والمتعاقدين والأطراف العقدية الثالثة أن تبلغ وترفع تقريرها حول أي ملاحظات أو شكوك عن أحداث أمنية عبر قنوات مناسبة وباسرع ما يمكن.

رفع نقاط الضعف المعلوماتية الأمنية

على جميع الموظفين والمتعاقدين والأطراف العقدية الثالثة أن تبلغ وترفع تقريرها حول أي ملاحظات أو شكوك عن نقاط ضعف أمنية في الأنظمة أو الخدمات عبر قنوات مناسبة وباسرع ما يمكن.

مسؤوليات وإجراءات الاستجابة للحوادث الأمنية

يجب تاسيس إجراءات ومسؤوليات الإدارة بوضوح للتأكد من استجابة سريعة ومنظمة لحوادث المعلومات الأمنية.

التحقيق في الحوادث

قد يكون اتخاذ خطوات قانونية أو تأديبية جزءاً من متابعة حوادث أمن المعلومات، يجب أن تتبع مباشرة أو إدارة أية تحقيقات إجراءات وتأكيدات موثقة لقبول هذه الممارسات.

جمع الأدلة

عند مباشرة التحقيق كجزء من عملية قانونية أو تأديبية محتملة، يجب أن يتبع جمع وترتيب وعرض الأدلة إجراءات وتأكيدات موثقة لقبول هذه الممارسات.

التعلم من حوادث المعلومات الأمنية

ينبغي وجود آليات تمكن من تحديد كميات ومراقبة أنواع وأحجام والتكاليف التقديرية لحوادث أمن المعلومات.

12. إدارة استمرارية العمل

الإشكاليات	نسبة العينات	ملاحظات عامة
إعادة النظر في كامل سياسات استمرارية العمل	%75	

<u>الخطوات التطبيقية الهامة:</u>

تضمين أمن المعلومات في إدارة استمرارية العمل

ينبغي إدارة وتطوير وصيانة عملية الحفاظ على استمرارية العمل في جميع أنحاء المؤسسة المالية، وهذا يتضمن متطلبات أمن المعلومات اللازمة لاستمرارية عمل المؤسسة المالية.

استمرارية العمل وتقييم المخاطر

ينبغي تحديد الأحداث التي قد تسبب في حدوث انقطاع في العمليات المالي ة، مع تحديد احتمال وتأثير مثل هذه الانقطاعات وآثارها على أمن المعلومات.

تطوير وتنفيذ خطط الاستمرارية

يجب اعداد وتنفيذ خطط استمرارية العمل لصيانة أو استعادة عمليات التشغيل، وضمان توافر المعلومات على المستوى المطلوب وفي الوقت المطلوب، متابعة الانقطاعات أو الاخفاقات في العمليات المالية.

إطار تخطيط استمرارية العمل

ينبغي وضع إطار واحد لخطط استمرارية العمل، لضمان تناسق جميع الخطط واستمرارية تقييم متطلبات أمن المعلومات، وتحديد الأولويات للاختبار والصيانة.

اختبار وتطوير وإعادة تقييم الخطط

ينبغي اختبار وتحديث خطط استمرارية العمل بشكل منتظم لضمان حداثتها وفعاليتها.

13. الامتثال

الإشكاليات	نسبة العينات	ملاحظات عامة
الحاجة لتقييم مركزي من قبل المؤسسات المالية (المصرف المركزي على سبيل المثال)	%100	إن وجود هيئة مركزية للمراقبة وتطبيق المعايير يعتبر أحد العوامل المهمة لمتابعة تطبيق هذه المعايير وفق متطلبات القطر.

الخطوات التطبيقية الهامة:

تحديد المتطلبات الداخلية والخارجية

ينبغي تحديد جميع الاحتياجات التعاقدية الداخلية والخارجية المطبقة تحت أمن المعلومات.

التوثيق

أن يوثق ويحدث النهج المنظم للمؤسسة والمعد لتلبية هذه المتطلبات بوضوح.

التواصل والتدريب والتوعية

ينبغي تداول المتطلبات الداخلية والخارجية بين جميع الأشخاص العاملين مع المؤسسة المالية، بما فيهم الجهات الخارجية التي تتعامل مع البيانات باسم المؤسسة المالية، عبر التدريب الملائم وبرنامج التوعية.

المراجعة الدورية

يجب القيام بمراجعة دورية للبيانات ونظامها ووسائل التحكم بها داخل المناطق الخاضعة لمسؤوليتها لضمان الامتثال للمتطلبات الداخلية والخارجية المطبقة.

و بناءً على الدراسة تم التوصل للنقاط التالية:

1) يمكن اعتبار المعايير ISO 27K وملحقاتها (المذكورة في المراجع) الأكثر أهمية وأساساً لتحليل واقع أمن المعلومات في أي مؤسسة مالية كونها تشمل المعايير الأخرى (Basel 2, COBIT) –من ناحية أمن المعلومات–و كافية في حال تطبيقها للوصول الى حالة أمنية مستقرة وذلك وفق لما يلي:

أ- ISO/IEC 27001.

ب-ISO/IEC 27002.

ت-ISO/IEC 13335-1:2004.

ث-ISO/IEC TR 13335-3:2004.

ج-ISO/IEC 15408-1:1999.

ح- كما يمكن اعتماد اطار العمل NIST SP 800-53 rev1:2010 , كخطوات عملية لتطبيق السياسات الأمنية للمؤسسات الكبيرة وتقييمها.

2) اشتركت كافة المؤسسات التي أجريت عليها الدراسة بالتأكيد على ضرورة دعم وانخراط الإدارة، وبناء روابط قوية بين أمن المعلومات والعمل المالي، ليس من المنطلق التقني فحسب، وإنما بالتعامل مع المعلومات على أنها جزء من الأصول القيمة بحد ذاتها.

3) وبالانتقال إلى المخاطر، لا بد من التركيز على ضرورة أن تتبنى المؤسسات المالية السورية أن أسلوباً منهجياً للمساعدة على المقارنة والتعديل والمراجعة والتغيير عند الحاجة أيضاً. تشير التجارب العالمية إلى كون

العمل في المؤسسة المالية واحداً من أكثر الأعمال حساسيةً تجاه السرية والخصوصية، حيث لا يسمح إلا بهامش ضئيل من الخطأ وإلا فسيواجه الفشل المحتوم.

4) لا يمكن الاستجابة بسياسات فعالة ومثمرة ما لم يتحقق الربط المناسب بين العمل المالي والمعلومات، ومن الضروري القيام بمراجعة عميقة وتفصيلية ووضع المؤشرات المناسبة من أجل ايصال هذه العملية إلى النجاح.

5) يعتمد تنظيم سرية المعلومات على التفاعل بين الأطراف المعنية الداخلية والخارجية، وبهذا هي أوسع من مجرد تشريعات والتزامات عامة، حيث أنها تضع الحدود التي لا يجوز تجاوزها منذ البداية وتظهر بجلاء مدى اهتمام المؤسسات المالية بأصولها المعلوماتية القيمة.

6) إن الانتقال من المفهوم التقليدي في التعامل مع تكنولوجيا المعلومات إلى المفهوم الحديث الذي يضمها إلى أصول الأعمال عملية شاقة، ليس بسبب الوسائل المعتمدة، ولكن بسبب علاقتها مع ثقافة المنظمة وبيئة العمل. وبكافة الأحوال، تعتبر هذه النقلة حركة إجبارية.

7) تشير الإحصائيات إلى أن أكثر من 80% من التهديدات التي تتعرض لها المعلومات ناتجة داخلياً من الكادر العامل، وأكثر من ذلك فإن 80% منها أيضاً غير مقصودة. يجب القيام بالعديد من الإجراءات تبدأ بمرحلة ما قبل التوظيف وحتى إنتهاء العلاقة الوظيفية لتقليص هكذا حوادث.

8) تلعب وسائل الحماية الفيزيائية دور حاجز الدفاع الأول مما يستدعي الاهتمام باختبارها وصيانتها.

9) يجب حماية العمليات التشغيلية اليومية كونها هي التي تضمن استمرار وازدهار العمل.

10) يعتبر التحكم بالوصول خلاصة الجهود المبذولة من أجل الحماية.

11) اكتساب وتطوير وصيانة المعلومات.

12) إدارة الحوادث، وأهمية وضع الخطط الفعالة للتعامل مع كل حدث والتخفيف ما أمكن من تأثيره.

13) إدارة استمرارية العمل بشكل جدي ومستمر وفعال لضمان عدم توقف الخدمات والعمليات.

14) ينبغي تحديد جميع الاحتياجات التعاقدية الداخلية والخارجية المطبقة تحت أمن المعلومات.

الاستنتاجات والتوصيات:

وجدنا في نهاية هذه الدراسة والتي اعطيت نتائجها للمؤسسات المعنية، بوجود هوة كبيرة – تتفاوت درجتها بين مؤسسة وأخرى– بين الواقع الملموس ومتطلبات أمن المعلومات العالمية، وأن المطلوب عمله كثير خصوصاً في غياب (أو قلة) المحددات والمعايير الوطنية من الجهات المختصة مثل المصرف المركزي ومجلس النقد والتسليف ووزارة الاتصالات والتقانة أو غيرهم من الجهات العليا ذات العلاقة[8].

كما وجدنا بأن الموضوعات الخاصة بأمن المعلومات والسياسات الأمنية تتعلق الى حد كبير بشخص وكفاءة رأس الهرم الإداري ومدير المعلوماتية –التقنية– في تلك المؤسسات.

[8] لابد من الإشارة إلى وجود تعليمات لمجلس النقد والتسليف، مصرف سورية المركزي فيما يخص المخاطر التشغيلية إلا أنه لا يوجد آليات لتطبيق هذه القرارات والرقابة عليها، المراجع.

مع الأخذ في الاعتبار أنه لا يمكن لأي استراتيجية معلوماتية أمنية أن تحقق مناعة تامة ضد أي هجوم، إلا أن اختيار الضوابط المناسبة وإعداد الاستجابة للحوادث والتخطيط بعناية لإدارة التغيير بصورة مسبقة وما إلى ذلك، يحمل معه المزيد من النجاح في مقاومة العاصفة الأمنية الكبيرة القادمة، وبالتالي في حماية العمل مما قد يحدث.

إن أمن المعلومات هو عملية مستمرة ، وينبغي إعادة النظر في كل بند بانتظام، وتصحيحه وربما تغييره بقدر ما تتطلب عوامل دفع العمل، تتلخص بعض التوصيات على النحو التالي :

1. لا يمكن تطبيق أمن المعلومات دون دعم الإدارة.
2. يجب معاملة أمن المعلومات في إطار حماية أصول العمل وليس كمسألة فنية فقط.
3. يعتبر توعية وتدريب الكادر من العوامل الحاسمة، وعليه فيجب على إدارة المؤسسات المالية السورية بذل كل الجهود من أجل نشر مفهوم أمن المعلومات وأهميته.
4. يتعلق نظام إدارة أمن المعلومات أساساً بتحديد نطاقه وتشخيص المفاهيم والمنهجيات وإجراءات التصحيح والتنظيم، بالإضافة إلى التوثيق والاستعراض والإشراف.
5. بدءاً من تعريف نطاق أمن المعلومات، ينبغي على المؤسسات المالية السورية المضي في خطوات صغيرة ولكن مستقرة ومستمرة. ونقترح القضايا الفنية البحتة كنقطة بداية.

المراجع:

[1] ISO/IEC 27001, Information technology- Security techniques - Information Security Management Systems (ISMS)- Requirements, 2005, 34.

[2] ISO/IEC 27002, or BS 17799, Information technology - Security techniques- Code of practice for information security management, 2005, 115.

[3] NIST SP 800-53 rev1, "Recommended Security Controls for Federal Information Systems", National Institute of Standards and Technology, USA, Department of Commerce, 2010, 422.
http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

[4] ISO/IEC TR 13335-3, (Guidelines for the Management of IT Security: Techniques for the Management of IT Security), 2005, 509.

[5] ISO/IEC 13335-1, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management, 2004, 301.

[6] ISO/IEC 15408-1, Information technology – Security techniques – Evaluation Criteria for IT security – Part 1: Introduction and general model, 1999, 342.

[7] قرارات مجلس النقد والتسليف، مصرف سورية المركزي،" المبادئ الأساسية لاستمرارية الأعمال" قرار 391م ن– ب4–2008، "التعليمات الخاصة بالمخاطر التشغيلية" قرار 106–م ن– ب4–2005.