تقويم نظام ادارة امن المعلومات في دائرة تكنولوجيا المعلومات وفق المواصفة ISO_27001

حاتم ناهي محيسن عواد كاظم حمود
وزارة العلوم والتكنولوجيا / دائرة تكنولوجيا المعلومات
بغداد - العراق

الخلاصة

يتزايد اهتمام المنظمات على اختلاف انواعها بتطبيق المتطلبات القياسية الدولية لنظام ادارة امن المعلومات وفق متطلبات المواصفة القياسية الدولية ISO_27001 . نفذ البحث في وزارة العلوم والتكنولوجيا/ دائرة تكنولوجيا المعلومات لغرض قياس استعداد الدائرة في امكانية تطبيق نظام ادارة امن المعلومات في اقسامها ومراكزها. اعدت استمارة استبانة وزعت على الفئات المستهدفة (الأقسام والمراكز)، اذ تضمنت مجموعة اسئلة حول الواقع المتبع الحالي في ادارة امن المعلومات. جمعت الأستمارات وبوبت ، واظهرت النتائج ان نسب الهجمات والمخاطر التي تتعرض لها الفعاليات والانشطة التي تقوم بها الدائرة كانت بمستويات مختلفة ، الأمر الذي يحتم تطبيق نظام ادارة امن المعلومات وفق المواصفة ISO_27001 في الدائرة المستهدفة.

الكلمات المفتاحية: تقويم ، نظام ، امن العلومات والمواصفة الدولية 27001.

Evaluation the Information Security Management System in the Directorate of IT Using ISO_27001

Hatem Nahi Mohaisen Awad Kadhim Hammoud
Ministry of Science and Technology/Information Technology Directorate
Baghdad-Iraq
E-mail : ha19652010@yahoo.com

Abstract

All organizations are increased draw attention about applying the requirements of specifications of ISO_27001 in their Information Security Management System,(ISMS). The research has been done in the Ministry of Science and Technology/ IT Directorate to measure the readiness of capability to apply the information security management system in the directorate. This is carried out through a questioner form prepared for this purpose and distributed for all the centers and departments in the directorate, this form include specific questions about the information security management system applied in the directorate. The results show that the ratio of attacks and risks which attacking all programs and activities in the directorate varying in different levels that enforce to implement Information Security Management System in the target directorate.

Key Words: Evaluation, System, Information Security and ISO_27001

المقدمة

يتبوأ موضوع الجودة أهمية كبيرة في مجال الإنتاج الصناعي والخدمي على حد سواء، إذ لايمكن لأي منتج أن ينافس المنتجات الأخرى مالم يكن بالمستوى والجودة التي يفوق بها المنتجات المنافسة أو البديلة.

فلم تعد الجودة مجرد معايير تميز المنتوج ، ولا أسلوباً يتم من خلاله التعرف على مدى مطابقة المنتوج النهائي لهذه المعايير فحسب ، وإنما ذهبت إلى أبعد من ذلك لتشمل الاستخدام الأمثل للموارد المادية والبشرية واستبعاد كل معيب من أول خطوة في الإنتاج. كما إن تحقيق الجودة هو مسؤولية الجميع بدءاً من الإدارة العليا وأفراد المنظمة والمجهز وإن تحسين الجودة يؤدي إلى رفع مستوى الإنتاجية والتخلص من التكاليف الناجمة من إعادة تصنيع المنتجات المتضررة والتالفة لكي تصبح جاهزة ، وبالتالي الحصول على أقصى الأرباح والحصة السوقية الأكبر وعليه فإن الجودة تعد بمثابة السور الواقي الذي لا يمكن اختراقه. (بريسمان 2004).

يشكل العدوان على البيئة المعلوماتية الوجه القبيح للتقنية الحديثة ، فالجرائم المتحققة عن هذا العدوان تتميز عن الجرائم العادية بسرعتها الفائقة وتأثيرها المدمر، وقدرة مرتكبيها على الإفلات من الملاحقة والعقاب في ظل افتقاد كثير من الدول أنظمة قانونية قادرة على التعامل مع هذا العدوان والجرائم الناجمة عنه، وتشير الإحصائيات الدولية إلى أن هناك أكثر من ملياري شخص مستخدم لأجهزة الحاسب الآلي، فضلاً عن وجود أكثر من 13 مليار صفحة على شبكة المعلومات الدولية (الانترنت) ونحو300 مليون موقع عليها. هكذا اتسعت البيئة المعلوماتية لتصبح ميداناً فسيحاً للعدوان عليها ولتشكل تحدياً كبيرا" لمختلف الأجهزة في مواجهة هذا العدوان وما ينجم عنه من جرائم ، حيث إن ما نسبته 24% إلى 42% من المنظمات في القطاعين الحكومي والخاص كانت ضحية لجرائم مرتبطة بالتقنية الحاسوبية، وأن 145 إلى 730 مليون دولار سنوياً خسارة 72 شركة بسبب جرائم الحاسب الآلي ، وبينت دراسة للأمم المتحدة عن مخاطر الحاسب الآلي وأن 73% من الجرائم داخلي، 23% منها يرجع إلى مصادر خارجية وقدرت الخسائر الاقتصادية لهذه الجرائم عام (1993) بنحو 2 مليار دولار، وفي دراسة عن حالات الاختراق كوجه من أوجه العدوان على أجهزة الحكومة الامريكية لعام 1995 وجد أن هناك 250000 حالة اختراق ، 64% منها ناجحة، وأن 1-4% منها تم اكتشافه (نجم، 2010). تهدف الدراسة الى السيطرة على التهديدات المكتشفة والمحتملة اعتماداً على سياستها واهدافها المعلنة في نظام ادارة امن المعلومات من خلال تطبيق اجراءات وسياسات عمل صارمة من شأنها توفير ممارسات فعالة وضمانات مقبولة لأمن المعلومات تزيد من فعالية تنفيذ الأعمال وتعزز رضا الزبون والجهات المستفيدة من التطبيقات والخدمات التي تقدمها دائرة تكنولوجيا المعلومات.

المواد وطرائق العمل

إن الفكرة الرئيسة للمواصفة القياسية ISO 27001تستند على مبادئ وفلسفة إدارة الجودة الشاملة ، إذ يسمى نموذج المواصفة بـ(PDCA) Plan-Do-Check-Act، وكما يأتي (الشركة العامة لنظم المعلومات، 2011) :

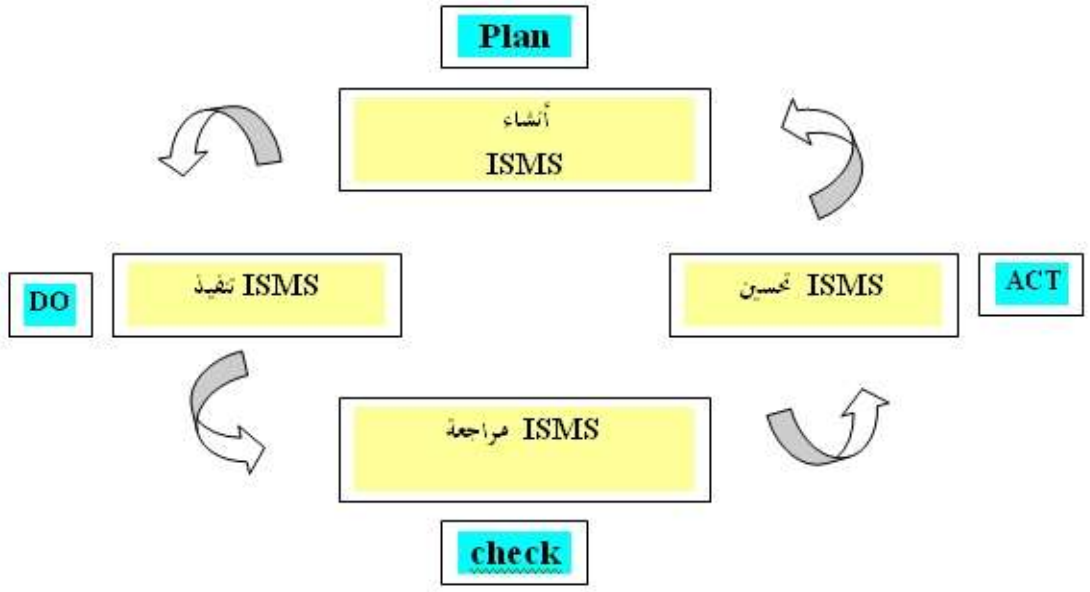
1- إنشاء نظام إدارة أمن المعلومات (ISMS) (Plan)

2- تنفيذ وتشغيل **ISMS** / **DO**

3- مراقبة ومراجعة **ISMS** / **Check**

4- المحافظة على ISMS والعمل على تحسينه Act.

كما موضح في الشكل (1).



شكل (1) منهج العملية

متطلبات تطبيق المواصفة القياسية

إن عملية تبني لنظام ادارة امن المعلومات (ISMS) معتمدا" على المواصفة القياسية - ISO 27001 تعد خطوة مثالية لبناء أمن فاعل لإدارة المعلومات في المنظمة، وهذه العملية قد تتسم بالتعقيد إن لم تكن هناك خطوات محددة من خلالها تتم عملية التبني بسهولة، لذلك جاء الدليل الإرشادي للمواصفة القياسية ISO 27001 ليوضح أهم متطلبات تطبيقها، والتي حددها بما يأتي(Hinson,2008)

1) **التعريف بحدود ونطاق الـ(ISMS):** يجب أن يحدد في ضوء المواصفات الخاصة بأنظمة معلومات المنظمة من ناحية الحجم والمصادر والأنواع ، مع الأخذ بنظر الاعتبار لاحتياجات التنظيمية والتشريعية للمنظمة .
2) **وضع إستراتيجية لـ(ISMS):** تتمثل بمجموعة من الإجراءات والخطوات اللازمة لتطبيق الـ(ISMS) ويعد العامل الرئيس للنجاح في هذه المرحلة هو دعم الإدارة العليا لإستراتيجية النظام,(Niclson,2008) .
3) **تحديد المخاطر واكتشافها:** يجب أن تحدد طريقة منهجية (Methodology) ومدخل مناسب لاكتشاف المخاطر .
4) **التمييز بين المخاطر:** العمل على التمييز بين الأنواع المختلفة للمخاطر التي تهدد أمن المعلومات.
5) **فهم وتقييم المخاطر:** تقييم المخاطر الحالية والمحتملة من أجل ضمان الاستخدام الأكثر فعالية للموارد المتاحة.
6) **تقييم خيارات معالجة المخاطر.**
7) **اختيار أهداف الرقابة المناسبة.**
8) **الحصول على موافقة الإدارة فيما يخص المخاطر المثبتة.**
9) **الحصول على موافقة الإدارة في تنفيذ النظام.**
10) **البدء بالتطبيق :** تنطوي هذه المرحلة على أعداد بيان التطبيق . والذي يصف الوثائق المختارة ومراقبة الأهداف وضوابط وأسباب الاختيار أو الاستبعاد .

نتيجة لدراسة اجريت على مراكز واقسام الدائرة حول انواع المخاطر التي تتعرض لها مختلف النظم الحاسوبية واليدوية في الدائرة. تم تصميم استمارة استبانة ، كما في الشكل (2) حول ادارة امن المعلومات في الدائرة تضمنت المحاور التالية:

1- البرنامج ، الفعالية او الخدمة.
2- وصف ملخص للخطر.
3- تحديد الأثر.
4- درجة الأهمية.

استمارة استبيان لادارة امن المعلومات في دائرة تكنولوجيا المعلومات
استمارة تحديد وتقييم المخاطر

القسم او المركز.....

ت	البرنامج ، الفعالية او الخدمة	وصف ملخص للخطر(المخاطر)	تحديد الأثر(الأثار)	درجة الأهمية
١				
٢				
٣				
٤				
٥				
٦				
٧				

اسم و توقيع رئيس القسم او المركز .....

شكل (2) استمارة استبانة

خطوات العمل:

1- وزعت الأستمارارات على جميع مراكز واقسام الدائرة .
2- جمع المعلومات الواردة في الأستمارات و تحليلها.
3- تم اعداد جدول استنادا" الى المعلومات الواردة في نتائج الأستبيان ، وتضمن الجدول الحقول التالية:
   1- المخاطر
   2- الأولويات
   3- السياسة
   4- الأجراء
   5- الجدار الناري
   6- حماية ضد الفايروسات

وكما موضح في الجدول (1).

النتائج والمناقشة

تم دراسة وتحليل البيانات التي جمعت من مراكز وأقسام الدائرة ، وتم تصنيفها الى نشاطات وبرامج حيث وضعت في مصفوفة صممت لهذا الغرض والتي اوضحها Thmson(2005) و بموجب ذلك تم تحديد مايلي :

1- نوع النشاط او البرنامج
2- الهجمات والمخاطر
3- درجة الأهمية
4- السياسة
5- الجدار الناري
6- الأجراء
7- الحماية من الفايروسات.

وكما في الجدول (1).

جدول (1) الخطة المقترحة في معالجة الهجمات/المخاطر في الدائرة

ت	البرنامج	الهجمات/ المخاطر	درجة الاهمية	السياسة	الجدار الناري	الأجراء	الحماية من الفايروسات
1	البريد الالكتروني بين مدراء المراكز في الدائرة	1. تمرير البريد الإلكتروني من قبل اشخاص غير مخولين 2. التوقيع الالكتروني على البريد الخاطئ	عالي	√	√	√	
2	المكتبة الالكترونية	1. تعرض البرنامج الى فايروسات 2. تعرص صفحات الويب الخاصة الى الاختراق	عالي	√	√	√	√
3	البرامج الالكترونية	1. تعرض البرنامج الى فايروسات 2. تعرص صفحات الويب الخاصة الى الاختراق	عالي	√	√	√	√
4	نظام اتمتة اعمال قسم العمليات المادية	1. خطئ في البيانات الواردة 2. ادخال البيانات بصورة خاطئة	عالي	√		√	
5	برنامج الموقف اليومي لحضور المنتسبين (الاجازات الانقطاعات التفرغ الدراسات التاخير)	تعرضه الى الاختراق والدخول الى قاعدة البيانات من غير المخولين	عالي	√		√	√
6	ادارة مخزن الدائرة (ورقي)	السرقة والحوادث العرضية (الحريق)	عالي			√	
7	ادارة مخزن المستهلكات والمواد المشطوبة	الحريق والتماس الكهربائي	متوسط			√	
8	جهاز البصمة	تلاعب في بيانات ومعلومات	عالي				√
9	الاجازات بكافة انواعها	تلاعب بكارتات الاجازة	متوسط	√			

10	اعمال صيانه كهربائية	صعقة كهربائية	عالي	√		√		
11	اعمال انشائية خدمية	التلاعب في الفحوصات المختبرية والمواصفات الفنية لتلك الاعمال	عالي	√		√		
12	الاضابير الشخصية الفرعية	1 تعرضها للتلف	متوسط			√		
13	برنامج حفظ الاضابيرالشخصية	اصابتها بفايروس	عالي		√			√
14	برنامج نظام الافراد	اصابتها بفايروس	عالي		√			√
15	برنامج العلاوات	اصابتها بفايروس	عالي		√			√
16	خدمة التحكم في الوصول	الوصول لغير المخولين	عالي	√	√	√		
17	ادارة مستوى الخدمة	التعرض الخدمة الى الهجمات والمخاطر	عالي		√			√
18	النظام وسلامه البيانات	فقدان البيانات وعدم استمرارية عمل النظام بشكل طبيعي	عالي	√	√	√	√	√
19	الشبكة المستخدمة لخدمة الانترنت	تسبب الاختراق وتدمير المعلومات	عالي	√	√	√	√	√
20	تداول وتناقل المعلومات بين الحاسبات بأستخدام الفلاش داخل المركز	خطر تسريب المعلومات والوثائق	عالي	√	√	√	√	√
21	الانظمة التشغيلية والبرامج	اختراق تلك البرامج تؤدي الى المشاكل في تشغيل البرامج	عالي	√	√	√	√	√
22	عميات بحث علمي عبر النفاذ من شبكة الانترنت	1- ايقاف الخدمة	1 متوسط			√		
		2- مشاكل الفايروسات	2 عالي		√	√	√	√
		3 - انقطاع الكهرباء	3 متوسط					
23	بحوث ودراسات في مجالت تقنات المعلومات المستخدمة في المجتمعات الرقمية	مخاطر الفايروسات	متوسطة		√			√
24	حفظ الملفات الورقية	تلف الاضابير	متوسط			√		
25	الحفظ الالكتروني	تلف الاقراص المدمجة	عالي	√	√	√	√	√
26	فحص الحاسبات الدوري	1 تعرضها للاختراق من اشخاص غير مخولين	عالي	√		√		

		2 الفايروسات	عالي				√
27	خطة تأهيل وتدقيق متطلبات ادارة الجودة	1 تأخير في تنفيذ الخطة	1 واطئ				
		2 ارباك لعملية تدقيق وضياع لأدلة التدقيق	2 عالي	√		√	
		3 فشل التدقيق في اداء مهامه	3متوسط			√	
28	نظام الافراد	خطرانهيار النظام	عالي	√	√	√	√

من خلال النتائج اعلاه تباينت نسبة الهجمات والمخاطر بالنسبة للفعاليات والأنشطة والبرامج التي تقوم بها الدائرة من مستوى واطيء الى مستوى عالي وكما يلي :

1. اذا كان مجموع الوقت المستغرق لاكتشاف الخطر (D) ورد الفعل اتجاه هذا الخطر (R) اقل من الوقت المستغرق في منع تعطيل المنظومة(P)، اذن نحن في الحالة السليمة وكما في المعادلة (1) (Sans,2012) :

$$D + R < P \quad \ldots\ldots\ldots (1)$$

2. اذا كان مجموع الوقت المستغرق لاكتشاف الخطر (D) ورد الفعل اتجاه هذا الخطر (R) اكبر من الوقت المستغرق في منع تعطيل المنظومة(P)، اذن نحن في الحالة السيئة وكما في المعادلة (2)(Sans,2012) :

$$D + R > P \ldots\ldots\ldots (2)$$

الاستنتاجات والتوصيات

1- ان تطبيق نظام ادارة امن المعلومات في الدائرة يجب ان يكون قراراً استراتيجيا من قبل الأدارة العليا في المؤسسة ويكون العمل به ملزماً لكل قسم من اقسام الدائرة.

2- المواصفة الدولية القياسية ISO_27001 تحث على تبني منهج عملية معرفة لدى كافة اقسام الدائرة . ولكي يكون اداء الدائرة فاعلاً فأنه يجب تحديد وادارة انشطة عديدة ومرتبطة. فلنشاط ما أو مجموعة انشطة التي تستخدم موارد وتدار بأسلوب يسمح بتحويل المدخلات الى مخرجات يمكن اعتباره عملية. وغالباً مايكون مخرج عملية ما مدخلاً لعملية تالية.

3- وجود ضعف في التأكيد على العمل بنظام ادارة امن المعلومات وفق المواصفة الدولية اعلاه.

4- نوصي بوضع سياسات واجراءات تبعا" لنوع الهجمات والمخاطر الذي يتعرض له النشاط في الدائرة في ضوء النتائج التي حصلنا عليها في الجدول (1).

Data Warehousing. (www.dmreview.com)

المصادر

الشـــركـة العامة لنظم المعلومات،(2011). الدورة التعريفية بنظام ادارة امن المعلومات وفق متطلبات المواصفة القياسية ISO 27001، اربيل–العراق.

بريسمان ، روجر،(2004) .هندسة البرامجيات ، الدار العربية للعلوم.بيروت-لبنان.الطبعة الأولى.

نجم ، نجم عبود،(2010) .ادارة الجودة الشاملة في عصر الأنترنت . دار صفاء للنشر والتوزيع.عمان-الأردن. الطبعة الأولى.

CSIA, (2007). ISO 27001: Get The Facts, www.csialliance.org .

Herve,S.,(2007),ISO 27001Certification, Eurose Forum. (Paris, www.hsc.fr.)

Hinson,G. , (2008). ISO27001 Security: The Financial Implications of Implementing ISO/IEC 27001&27002, a generic Cost Benefit Model, Isect. Ltd. (www.iso27001security.com)

Nicolson, R. ,(2006). Information Life Cycle Management in the Upstream Oil Gas Industry, Fristbreak (24). (www.fristbreack.org)

Sans,(2012). 27000 Implementation and Management, ISO 27000 Implementation, Beirut-Lebenon.

Sans,(2012). 27000 Implementation and Management Introduction to ISO/IEC 27000: Policy, ISMS, and Awareness, Beirut-Lebenon.

Thompson, R. ,(2005). Information Life Cycle Management (ILM) for