تقييم نظام أدارة امن المعلومات في الهيئة العراقية للحاسبات والمعلوماتية على وفق المواصفة الدولية (ISO/IEC 27001:2013)

أ.د. إيثار عبد الهادي آل فيحان/كلية الادارة والاقتصاد /جامعة بغداد
الباحث/ عامر حمدي عبد غريب/ معاون رئيس مهندسين/ وزارة التجارة

المستخلص:

تضمّن البحث الحالي (تقييم نظام ادارة امن المعلومات على وفق المواصفة الدولية (ISO/IEC 27001:2013) في الهيئة العراقية للحواسيب والمعلوماتية) , اذ يعد وضع نظام اداري لامن المعلومات من الأولويات في الوقت الحاضر, وفي ظل اعتماد المنظمات على الحواسيب وتقانة المعلومات في العمل والتواصل مع الاخرين , تبقى الشرعية الدولية (والمتمثلة بمنظمة التقييس الدولية (ISO)) اساساً للمطابقة والالتزام, وتتجلى اهمية تطبيق نظام ادارة امن المعلومات على وفق المواصفة الدولية (ISO/IEC 27001:2013) في حماية موجودات المنظمات وبخاصة المعلومات وقواعد البيانات بشكل منهجي ومستمر.

هدف البحث اجراء تقييم ما بين نظام ادارة امن المعلومات القائم حالياً في الهيئة العراقية للحواسيب والمعلوماتية (موقع اجراء البحث) وبين نظام ادارة امن المعلومات على وفق المواصفة الدولية (ISO/IEC 27001:2013) وباستعمال قوائم فحص تدقيقية من اجل تشخيص فجوات عدم المطابقة مع المواصفة الدولية.

وتوصل البحث الى استنتاج مهم الا وهو (ان النظام الإداري لأمن المعلومات والمتبع في الهيئة العراقية للحواسيب والمعلوماتية وعلى الرغم من اعتماده التقانة الحديثة والملاك الكفوء الا انه يفتقر الى حسن التوثيق والتطبيق لكثير من المتطلبات التي جاءت بها المواصفة الدولية (ISO/IEC 27001:2013) , وبحاجة الى اعادة بناء هيكل تنظيمي ووظائف تنسجم مع ما جاءت به المواصفة الداعمة (ISO/IEC 27003:2010).

واختتم البحث بأهم توصية (تشكيل فريق عمل يتبنى تهيئة مستلزمات تطبيق المواصفة (ISO/IEC 27001:2013), ويعمل على تلبية متطلباتها ومتطلبات نظم الادارة الاخرى (نظام ادارة الجودة وغير ذلك) , وترتبط بالادارة العليا لتيسير الدعم بالموارد والصلاحيات .

المصطلحات الرئيسة للبحث/ امن المعلومات- نظام ادارة امن المعلومات – الهيئة العراقية للحواسيب والمعلوماتية- مقياس ليكرت – NIST -ISO 27001.

مجلة العلوم الاقتصادية والإدارية
المجلد 21 العدد 86
الصفحات 1-26

*البحث مستل من رسالة ماجستير

المقدمة :

يعد نظام إدارة امن المعلومات من أهم القضايا في مجتمع اليوم والاعتماد المتزايد من قبل المنظمات والأفراد على تقانة الحاسوب وصناعة البرمجيات دفع الكثير من المنظمات إلى تبنّي أساليب مختلفة لحماية معلوماتها الخاصة وقواعد البيانات التي تمتلكها كما إن وجود تقانة لأمن المعلومات لا تؤدي الغرض المطلوب إن لم تُدعم بالجوانب التشريعية والتطبيقية , ومن هنا تظهر الحاجة إلى وجود منهجية لبناء نظام إداري لأمن المعلومات يوفر الحماية المرجوّة للمعلومات على جميع مستوياتها وبجميع طرائق حفظها أو تناقلها, وهذا ما توفره المواصفة الدولية (ISO/IEC27001:2013). تضمن هذا البحث اربع محاور انصرف المحور الاول للمنهجية والدراسات السابقة والمحور الثاني الجانب النظري والمحور الثالث الجانب العملي والمحور الرابع الاستنتاجات والتوصيات.

المحور الاول / منهجية البحث والدراسات السابقة:

أ- منهجية البحث:

اولاً: مشكلة البحث: أدى التطور الهائل في نظم المعلومات الرقمية وتطبيقاتها, والانتشار الواسع لإستراتيجية الاعتماد على الشبكات الحاسوبية في أعمال الأتمتة والإدارة , الى اعتماد تقانة المعلومات ضرورة من ضرورات عصرنا الحالي وأداة من أدوات العمل الرئيسة , ونتيجة للطفرة الكبيرة التي حدثت في وسائل الاتصالات وشبكات المعلومات والدخول في عصر العولمة والانترنت , ظهرت مخاطر وتهديدات جديدة في ساحة الأعمال , وهو ما يستدعي اخذ كافة الوسائل المتاحة والممكنة لتعزيز امن نظم المعلومات وحمايتها, وفي ظل غياب نظام إداري امني دولي معترف به يرفع من مستوى وكفاءة الهيئة العراقية للحواسيب والمعلوماتية في حفظ وإدارة امن معلوماتها تتجسد مشكلة البحث في الاجابة عن التساؤل الآتي: (ماهو حجم الفجوة بين الواقع الفعلي لنظام ادارة امن المعلومات في الهيئة العراقية للحواسيب والمعلوماتية ونظام ادارة امن المعلومات على وفق المواصفة الدولية (ISO/IEC 27001:2013)).

ثانياً: اهمية البحث: تظهر أهمية هذا البحث بوصفها محاولة للربط بين واقع نظم ادارة امن المعلومات في الهيئة العراقية للحواسيب والمعلوماتية مع المواصفة الدولية (ISO/IEC 27001:2013), وابراز الجوانب الاتية:

1- التمهيد لوضع منهج وخطة عمل لتطبيق المواصفة (ISO/IEC 27001:2013) في الهيئة العراقية للحواسيب والمعلوماتية, ومن ثم الحصول على شهادة المطابقة من الجهات المانحة.

2- السعي لرفع مستوى الدورات المقامة حالياً (امن الحواسيب والشبكات) والدورات الخاصة بنظام ادارة امن المعلومات مستقبلاً, مع استحداث دورة تدريبية لتاهيل الملاكات المختصة على تدقيق نظام ادارة امن المعلومات على وفق المواصفة الداعمة (ISO/IEC 27007:2011).

ثالثاً: المنهج وطريقة البحث: تمكن الباحث وباسلوب البحث التطبيقي ومن خلال المعايشة الميدانية والملاحظة وعمل المقابلات والاطلاع على الوثائق والمعلومات, ومن خلال المعلومات المستقاة من السجلات والوثائق من تحديد مقدار الفجوة الحاصلة مابين نظام ادارة امن معلومات الهيئة والنظام الذي جاءت به المواصفة واسبابها, ولغرض تحليل البيانات فقد استعمل مقياس ليكرت السباعي في قوائم الفحص لقياس مدى مطابقة التنفيذ والتوثيق الفعلي لمتطلبات المواصفة القياسية (ISO/IEC 27001:2013) في الهيئة العراقية للحواسيب والمعلوماتية ، ومع تحديد أوزان لإجابات الأسئلة الواردة في قوائم الفحص عن طريق تخصيص وزن محدد لكل فقرة من فقرات المقياس والموضح في الجدول رقم (1) , وبعد الاستعانة بآراء الأساتذة الإحصائيين عمد البحث الى تمثيل الرقم (7) اعلى وزن في المقياس بينما يمثل الرقم (1) اوطا وزن في المقياس , وكما مستخدم في احدث الدراسات .

جدول رقم (1)

المقياس السباعي لمدى المطابقة مع المواصفة القياسية

ت	فقرة القياس	وزن الفقرة (درجة)
1	مطبق كلياً وموثق كلياً	7
2	مطبق كلياً وموثق جزئياً	6
3	مطبق كلياً وغير موثق	5
4	مطبق جزئياً وموثق كلياً	4
5	مطبق جزئياً وموثق جزئياً	3
6	مطبق جزئياً وغير موثق	2
7	غير مطبق وغير موثق	1

المصدر :عمر، ماهر محمود (1988). سيكولوجية العلاقات الأجتماعية. مصر، الأسكندرية : دار المعرفة الجامعية .259

وتحويل الاجابات الواردة في قوائم الفحص الى تعابير كمية بأعتماد المعدلات والنسب ألآتية:

(1) المعدل التقريبي لمدى توثيق وتطبيق متطلبات المواصفة (ISO/IEC 27001:2013) في الهيئة باستخدام الوسط الحسابي المرجح (Weighted Mean) من خلال احتساب قيم التكرارات لكل قائمة من قوائم الفحص، وبحسب المعادلة الآتية:

$$\bar{x} = \frac{\sum xifi}{\sum fi}$$

إذ أن :

$\bar{x}$:المعدل أو الوسط الحسابي المرجح

xi: تمثل الاوزان

fi : تمثل التكرارات

(2) النسبة المئوية لمدى مطابقة التنفيذ الفعلي للمتطلب من قبل الهيئة قياسا بالمواصفة القياسية وبحسب المعادلة الآتية:

$$\% = \frac{\sum xifi}{\sum fi \times 7}$$

رابعاً: **عينة البحث**: تم اختيار الهيئة العراقية للحواسيب والمعلوماتية كموقع لتطبيق البحث وعمل التحليلات لملاءمتها لمتطلبات البحث واعتماد عدد كبير من الجهات الحكومية وغير الحكومية على خدماتها الاستشارية وبرامجها التدريبية والنظم البرمجية المصنعة فيها وما لبيانات النظم المصنعة من اهمية وسريّة تعود بالضرر في حال كشفها على الجهات المستفيدة ومثالها نظام الاستمارة الالكترونية المعد في الهيئة لصالح وزارة التعليم العالي والمستخدم في نظام القبول المركزي للجامعات والمعاهد , كما ان الهيئة تعمل على اعداد بنك للمعلومات يضم جميع الملاكات العلمية المتقدمة والتخصصات الدقيقة لعموم المنظمات العلمية في بلدنا العزيز , لذا فالهيئة تمتلك كم هائل من المعلومات والواجب تامين الحماية لها من العبث فضلاً عن خصوصية بيانات طلبة معهد المعلوماتية للدراسات العليا والمنضوي ضمن مجالس الهيئة الاربعة.

ب-الدراسات السابقة:

1- **عرض بعض الجهود المعرفية العربية**:

ت	أسم الباحث وتاريخ البحث	عنوان البحث	مشكلة البحث	أهداف البحث	أهم الاستنتاجات
1	(القحطاني ,منصور بن سعيد,2008)	تهديدات الامن المعلوماتي وسبل مواجهتها.	مدى فاعلية استخدام التقانة الحديثة في مواجهة تهديدات الامن المعلوماتي بمركز الحاسوب الآلي في القوات البحرية.	- الكشف عن مصادر تهديد الامن المعلوماتي. - سبل تطوير قدرات مركز الحاسب الالي .	- يمثل عدم ضبط الاتصال بشبكة الانترنت, احد اهم التهديدات.
2	(تايه,علاء الدين محمد ,2008)	مدى فاعلية إدارة أمن المعلومات في منظمات تقانة المعلومات في فلسطين.	تحديد الية مراجعة دورية لسياسة امن المعلومات	مدى فاعلية ادارة امن المعلومات في منظمات تقانة المعلومات في الاراضي الفلسطينية.	- تتحقق فاعلية إدارة أمن نظم المعلومات بمقدار توفر سياسة أمن المعلومات. - يؤثر أمن الأفراد إلى حد ما في كفاءة إدارة أمن نظم المعلومات.

3	(جبـــــوري , نـــــدى اسماعيل,2011)	حماية امن نظم المعلومات.	ايجاد مؤشرات حقيقية لقياس امنية نظم المعلومات.	تحليل العلاقة فيما بين مؤشرات امن نظم المعلومات وطبيعة ارتباطها بالقياسات الامنية.	- لا يمكن حماية نظم المعلومات من دون قياس حقيقي وبطريقة علمية. - حماية المعلومات يساعد في الحد من المخاطر ومواجهتها.
4	(الحافظ والنعيمي ,2013)	دور (ISO27001:2005) في تعزيز مفهوم ادارة دورة حياة المعلومات.	هل لدى الشركات الصناعية إلمـــــام بالمواصـــــفة (ISO27001) الخاصة بنظم إدارة امن المعلومات و ما مدى التوافق بين (ISO27001) و إدارة دورة حياة المعلومات	- التأكيد على المفاهيم الحديثة في جودة حماية المعلومات، ذلك من خلال توظيف المواصفة ISO (27001) كمواصفة حديثة لحماية المعلومات.	- تعد المواصفة (ISO 27001:2005) قاعدة لتقييم إدارة حماية المعلومات. - ضـرورة التركيـز علـى كلـف الخزن والاسترجاع
5	(الصـاحب, محمـود حسـن ,2013)	سياسـة امـن المعلومـات فـي الجامعات	. تحديد مصادر التهديدات التي تواجهها نظم المعلومات في الجامعات.	وضع سياسة امن معلومات تلائم جامعة بوليتكنك – فلسطين-والاطراف المتعاملة معها.	- اهمية اصدار وثيقة لامن المعلومات متبوعة بمجموعة من التعليمات والقوانين التي تتوافق مع السياسات, ومراجعة السياسات بصورة دورية.

2-عرض بعض الجهود المعرفية الأجنبية:

ت	أسم الباحث وتاريخ البحث	عنوان البحث	مشكلة البحث	أهداف البحث	أهم الاستنتاجات
1	(Erkan, (Ahment: 2006	AN Automated Tool for Information Security Management System أداة مؤتمتة لنظام أدارة امن المعلومات	كيفيـة تحقيـق التوافـق بـين المنظمات باتجاه التعامل الصحيح مع تحديات امن المعلومات.	تقـديم مجموعـة مـن الأدوات للمنظمات التي تتطلـع للحصـول علـى (ISO27001:2005) والتـي تسـاعد علـى أتمتـة الأنشـطة المطلوبـة فـي توثيـق (ISMS).	تتطلب عملية الحصول على شهادة المطابقة للمعيار الدولي (ISO/IEC 27001 :2005) الى الكثير من الوقت والمال ,وتستطيع المنظمات باستخدام ادوات امن المعلومات من الحصول على شهادة المطابقة بسهولة اكبر.
3	(Nakrem, Are:2007)	Managing Information Security in Organizations ادارة امن المعلومات في المنظمات	تجد العديد من المنظمـات صـعوبة وكلفـة عاليـة فـي التعامل مع امن المعلومـات بالاتجـاه الصحيح.	توفير اطار عمل جديد لادارة امن المعلومات.	يحتوي اطار العمل الخاص بادارة امـن المعلومـات ثـلاث محاور:متطلبات العمل وموارد تقانة المعلومـات ومتطلبـات امـن المعلومات.

4	(Brewer, David & Nash, Michael: 2010)	Insights into the ISO/IEC 27001 Annex (A) نظرة ثاقبة على الملحق (A) للمواصفة (ISO/IEC27001)	تحديد فاعلية الملحق (A) في علاج مخاطر امن المعلومات.	وضع بيان قابلية التطبيق (SoA) لمختلف المنظمات.	-اهمية تعديل الملحق (A) في الاصدار ISO//27001:2005 لتتلائم الضوابط الامنية مع نظم الادارة الاخرى والمطبقة في ان واحد في المنظمة. - الضوابط الامنية للاصدار الحالي تحتاج الى تكيف وتعديل لتتلائم مع تقانة المعلومات الحديثة.
6	(Sharma&Dash :2012)	Effectiveeness of ISO 27001,AS an Information Security Management System فاعلية المواصفة (ISO 27001) كنظام ادارة امن معلومات.	تحديد العلاقة مابين المواصفة (ISO 27001) كنظام وقائي ضد حوادث امن المعلومات , والفوائد المالية المكتسبة للمنظمة.	-تشخص التحديات في تنفيذ المعيار (ISO27001). -دراسة الآثار المالية لما قبل وبعد تنفيذ (ISO27001).	-ان المنظمات التي تطبق المواصفة (ISO27001) كنظام اداري لامن المعلومات, تمتلك ضوابط داخلية فاعلة لادارة العمليات المالية. -الامتثال للمواصفة(ISO27001) يساعد في حفظ وحماية موجودات المنظمة ويزيد من ارباحها وسمعتها التجارية.

المحور الثاني /الجانب النظري للبحث:

اولا: **أهمية أمن المعلومات** -The importance of information security

يتميز امن المعلومات بوصفه استباقي، اي بمعنى ان تتوقع سياسة امن المعلومات المشكلات المستقبلية وتقوم بمحاولات للوقاية منها (AL-Kolaly,2005,59), ويلاحظ ان 75% من كبار المديرين في المملكة المتحدة يدعون الآن إلى اعتبار أمن المعلومات أولوية عليا وعلى نحو متزايد اذ ان متوسط أنفاق شركة بريطانية مايقارب (4-5٪) من الميزانية على أمن المعلومات (Calder&Watkins,2008,11). وتنبع أهمية أمن المعلومات من أنها تستخدم من لدن الجميع (افراد ومنظمات وحكومات) وفي بعض الأحيان تكون المعلومات هي الفاصل بين المكسب والخسارة للمنظمات, وقد تكلف الفرد ثروته وربما حياته في بعض الأحيان واصبحت المشكلة الان ليس الحصول على المعلومات , وانما كيفية حماية هذه المعلومات من الأخطار التي تهددها (داود ,2000 ,30) , ومن هنا اقتصر دور الكثير من مديرين ومشرفي أقسام وإدارات تقانة المعلومات على التعامل مع المنظمات الأمنية, لوضع البرامج المضادة للفيروسات وبرامج الاختراق والتسلل وبرامج الإغراق وغيرها, وتدور جميعها حول "وسائل الحماية".

ثانياً: **أهداف أمن المعلومات** : The objects of information security

تتضح أهداف إدارة أمن المعلومات في الدقة والسلامة والأمان لجميع العمليات ومصادر نظم المعلومات (O'Brien, 2003,401), ويتمثل الهدف الأساسي من أمن وسرية المعلومات في تحديد جميع الثغرات الامنية في المراقبة المحتملة التي قد تسمح للأفراد غير المصرح لهم بالوصول إلى النظام , وكذلك يجب على مدير المنظمة إن يكون على دراية باستخدام التقنيات المعروفة جميعها لأمن النظام للتغلب على الثغرات الامنية (Tipton& Krause, 2008,7) .

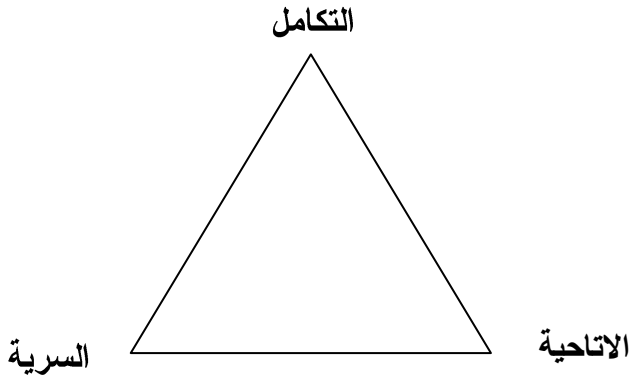
ويجمع الباحثون على ان امن نظم المعلومات يمتاز بثلاث اهداف رئيسة , وهي كل من الآتي: (الحمامي والعاني,21,2007 ; مكليود وشيل ,792,2009/2006 ; Whitson,2003,57 ; Arnason&Willett,2008,2)

(1) السّرية Confidentiality : وهي الحفاظ على المعلومات بعدم اظهارها لغير الافراد المخولين رسمياً, ويوفر هذا الهدف للمنظمة السرية التامة لكافة المعلومات، حتى لو كانت المعلومات صغيرة وبسيطة, ومنها (المعلومات الشخصية, والموقف المالي لمنظمة ما قبل اعلانه, والمعلومات العسكرية, وغير ذلك).

(2) التكامل Integrity : التاكد من ان المعلومات لم يتم تغييرها او حذف جزء منها من قبل وسائل غير معروفة او غير مخولة ومنها (تغيير اسماء المقبولين في قوائم التعيين عن طريق حذف وادراج اسماء بديلة مما يسبب الارباك للجهة المعنية , او تغيير مبلغ تحويل باضافة اصفار).

(3) الاتاحية Availability : وهي ان تكون المعلومات والحواسيب متاحة للافراد المخولين باستخدامها لان المعلومات تصبح غير ذات قيمة اذا كان من يحق له الاطلاع عليها لايمكنه الوصول اليها او ان الوصول اليها يحتاج الى وقت طويل, ويتخذ المهاجمون وسائل شتى لحرمان المستفيدين من الوصول الى المعلومات, ومن هذه الوسائل حذف المعلومات ذاتها او مهاجمة الاجهزة التي تخزن المعلومات فيها وشّلها عن العمل.

يوضح الشكل رقم (1) اهداف امن المعلومات الرئيسة وهي على درجة واحدة من الاهمية وهو ما دفع المتخصصين لوضعها في اركان مثلث متساوي الاضلاع , اذ تعد احجار الزاوية لأمن المعلومات وبخاصة امن الحواسيب .



شكل رقم (1): الاهداف الثلاثة لامن المعلومات

Source: Arnason , Sigurjon Thor & Willett, Keith D.(2008). How to Achieve 27001 Certification An Example of Applied Compliance Management. USA, New York : Taylor& Francis Group LLC. 3

ثالثاً: **تهديدات نظم المعلومات** - Threats of Information Systems

تختلف التهديدات الموجهة لنظم المعلومات فبعضها بنوايا خبيثة (منها اعمال التجسس والتخريب والابتزاز) واخرى من قوى الطبيعة الخارقة (ومنها الزلازل والفيضانات) (Caballero,2009,277) وتندرج معظم التهديدات من النوع الاول ضمن مصطلح جرائم الانترنت (Cybercrime) في معظم المصادر المتخصصة بامن المعلومات. وتتبع مخاطر وتهديدات امن المعلومات من داخل المنظمة ومن خارجها وتزداد الامور سوءاً كل عام , وتؤدي سرعة تطور اساليب الهجوم وانتشار المعرفة المتعلقة الى صعوبة وضع اجراء لكل تهديد محدد , الامر الذي يدفع الى تطبيق اسلوب شامل ومنتظم من اساليب الحماية لتحقيق مستوى امن معلومات تحتاجه اي منظمة مستقبلا" (Calder&Watkins,2008,9), وتصنف مصادر التهديدات لنظم المعلومات الى الآتي :

أ- **تخريب الموظفين** – Staff Sabotage : يعتمد امن نظم المعلومات على امانة الافراد المتعاملين معه , اذ لا يكفي التاكد من اخلاقيات واهلية الموظف عند التعيين , بل يجب ان تستمر مراقبته , اذ ان التغيير السلوكي متوقع, ويجب سحب صلاحيات اي موظف عند انتهاء خدماته وبمدة كافية , وتوجد عدة حوادث انتقام بدرت من موظفين انهيت خدماتهم (حاج علي,12,2006), ومن امثلة التخريب التي يحدثها الموظفين في المنظمة :(Geric & Hutinski,2007,53)

- تخريب اجهزة الحاسوب (Hard Ware Sabotage).
- زرع القنابل المنطقية (Logic Bombs) التي تدمر البرامج والبيانات.
- ادخال البيانات بشكل غير صحيح.
- عمل حذف او تغيير للبيانات.

تعد جميع تهديدات الافراد العاملين من التهديدات الداخلية والتي تشكل وفقا لوكالة (FBI) التابعة لحكومة الولايات المتحدة الامريكية, ما نسبته 60% الى 80% من التهديدات التي يتم الاخبار عنها (Cisco Systems,2001,20), اما التهديدات الخارجية التي تقدم من خارج المنظمة, تكمن الخطورة فيها بعدم او صعوبة معرفة المخترق, واهدافه من وراء الاختراق , ومدى اختراق النظام (الحميد ونينو,2007 , 38-40).

يقوم معهد امن الحاسوب (CSI–Computer Security Institute) في كل عام وبالتعاون مع مكتب التحقيقات الفيدرالي (FBI–Federal Bureau of Investigation) في الولايات المتحدة بدراسة امن وجرائم الحاسوب واصدار احدث التقارير على الموقع (gocsi.com) بخصوص جرائم سرقة المعلومات واطلاع غير المخولين عليها وما تحدثه من خسائر مادية للمنظمات, اذ يتبين من خلال الارقام حجم الزيادة السنوي لجرائم سرقة المعلومات وجرائم الدخول غير الشرعي, وبنسبة مئوية تفوق باضعاف ما يحدث من الخسائر من الجرائم الاخرى, (Turban, Leidner, Mclean& Wetherbe,2008,625)

ب- تهديد البرمجيات الخبيثة (Malware)

تُنتهك البنية التحتية لنظم المعلومات بعدة طرائق وآليات , ومن جملة تهديدات نظم امن المعلومات البرامج الضارة والتي تؤثر سلبا في اداء الحواسيب واهمها:

(اولا) الفيروسات– **Viruses** : تعّرف الفايروسات بانها برامج حاسوبية غريبة قد تلحق ضررا بنظام المعلومات او ما يحتويه من بيانات ولديها القدرة على التخفي والتوسع والانتشار , ويعمل الفايروس على اتلاف الملفات وهو مصمم على هذا الاساس وله قابلية على تجنب الاكتشاف ويقدم نفسه على انه برنامج شرعي (AL-Kolaly ,2005,65) ويأخذ الفايروس هيئات مختلفة من حيث طبيعة العمل , ويتميز الفايروس بخاصيتين : (Calder&Watkins ,2008, 181)

(1) برنامج قادر على تكرار ذاته (اي انتاج وظيفة من صورته الاصلية).

(2) يعتمد على ملف مضيف (وثيقة او ملف تنفيذي) لنقل كل نسخة.

(ثانياً) الديدان – **Worms** : وهي برامج حاسوبية لها القدرة على النسخ والانتشار عبر الشبكة (Bagad & Dhotre,2007,9), وكما تستطيع مضاعفة وتكرار ذاتها عن طريق وسيط ناقل مثل البريد الالكتروني والرسائل الفورية, والمحادثة التي تعتمد على الانترنت ووصلات الشبكات (Ziolkowski,2013 ,46) .

(ثالثاً) احصنة طروادة– **Trojans** : برامج عادية الا انها تحمل في جوانبها الخطر غير المتوقع بما تقدمه من ضرر خفي وهي شفرة عدائية تتخفى داخلياً (O, Brien,2003,384) وتقوم بالتسلل الى الحاسوب بشكل مخفي كجزء من برنامج ما يتم تنصيبه على الحاسوب من قبل المستخدم نفسه, وعلى خلاف الفيروسات وديدان الحاسوب فهي لا تستطيع نسخ ذاتها (Owen,2003,115) .

(رابعاً) القطّار– **Dropper**: هو برنامج يستخدم لتنصيب الفايروسات على الحاسوب (Cole et al. 2009,129,).

(خامساً) ادوات الجذر– **Rootkits** : ظهر عام (2005) , وهو عبارة عن برنامج يتألف من مجموعة برامج تخريبية, ينتقل الى الحاسوب دون معرفة المستخدم ويعمل على السيطرة على النظام من خلال اتخاذ هيئة نظام فرعي ضمن نظام التشغيل , وعادة ما يقوم باتخاذ مواقع نظم المكافحة والامن في النظام مقرا له (Russell & Gangemi,1991,87) .

(سادساً) الباب الخلفي **Backdoors** : يساعد هذا البرنامج المتسللين على الدخول الى الحاسوب من خلال استغلال الثغرات الموجودة فيه, والعمل على تعديل اعدادات تجهيزات الشبكة, ومن ثم السماح بالدخول للحاسوب عن طريق منافذ غير قانونية (الطريقة المعتادة التي تطالب المستخدم بتراخيص دخول) ' (O Brien,2003,384) .

(سابعاً) مسجلات ضربات المفاتيح– **Registered Keystrokes**: تمثل برمجيات صغيرة تقوم بتسجيل ضربات المفاتيح التي يقوم بها المستخدم وذلك سعيا لالتقاط كلمات المرور والمعلومات الخاصة كارقام بطاقات الائتمان ومن ثم تخزينها , وبعض هذه البرمجيات له اهداف حميدة ويقوم المستخدم بتثبيته من اجل الحماية الاسرية خاصة في حال استخدام الاطفال للانترنت وخوفا من استغلالهم من مواقع ذات اغراض سيئة (Janzeweski,2008,174).

(ثامناً) الرسائل الخادعة– Hoax Messages: تعتمد هذه الرسائل على جهل المستخدمين الذين لا يهتمون عادة بالفيروسات ومن ثم يرون انه من المفيد ان يعيدو توجيه مثل هذه الرسائل الى المسجلين في جميع العناوين, وهي معروفة لدى مستخدمي البريد الالكتروني (Calder&Watkins,2008, 183) .

ج – الاقتحام او التطفل – Intrusion : يعد من اكبر التهديدات الامنية خطورة وانتشارا, اذ يستطيع المتطفل بعد اقتحامه نظام المعلومات وتحديداً اجهزة الحاسوب او توابعه ,ان يستخدم هذا الجهاز كيفما يشاء وبكامل صلاحيات المستخدم الشرعي , كما يستطيع المقتحم عند نجاحه في اقتحام النظام من ارتكاب جميع انواع الانتهاك الاخرى كالتنصت او التزوير او اقتحام الرسائل, وهو على انواع نذكر منها : (Geric&Hutinski,2007,57)

(اولاً) التنصت – Eavesdropping: يُعرف التنصت بانه قيام المهاجم بمراقبة مايدور بالشبكة وما يتم تبادله فيها من رسائل وذلك بهدف الحصول على معلومات يرغب الآخرون بابقائها في طي الكتمان (داوود,2004,128) , والادوات المستخدمة لتنفيذ التنصت , تتضمن برامج تحليل الشبكات وبروتوكولاتها فضلاً عن ادوات التقاط الحزم على شبكات الحاسوب.

(ثانياً) منع تقديم الخدمة (Denial of Service-DoS) : يتيح وجود اخطاء برمجية او اعدادات خاطئة في مخدم الشبكة من امكانية الدخول عن بعد من قبل المستخدمين غير المخول لهم بذلك الى المعلومات الشخصية السريّة , اوالحصول على معلومات حول الجهاز المضيف , مما يسمح بحدوث اختراق للنظام , ويتمكن المهاجم من تنفيذ تعليمات على الجهاز المضيف وتعديل للنظام واطلاق هجمات اغراقية تؤدي الى التعطيل المؤقت للجهاز , ان هذه الهجمات تعمل على ابطاء او ايقاف حركة مرور البيانات عبر الشبكة .(Brown et al,2009,608 ; O, Brien,2003,384 ; Russell & Gangemi,1991,87)

د– مشاكل جودة النظام (البرامج والبيانات) : فضلاً عن الكوارث والفيروسات والخروقات الامنية لنظم المعلومات يسبب كذلكً تخلّف البرامجيات والبيانات الناقصة تهديداً مستمراً لنظم المعلومات مسبباً خسائر لامثيل لها في الانتاجية اذ يمكن ان ينتج عن الخطا غير المكتشف في برامجيات ائتمان المنظمة او البيانات المالية الخاطئة خسائر بملايين الدولارات (Laudon & Laudon,2005,529).

ه– الخطا والسهو– Error and Omission : يعد من التهديدات الامنية الكبيرة, والتي عادة مايتم التقليل من شانها ويكون المسبب الرئيس لها الموظفين والمتعاقدين داخل المنظمة, اذ قدمت منظمة (R.Conorteny) في الولايات المتحدة الامريكية دراسة اثبتت ان (65%) من التهديدات ترجع الى الخطا والسهو ,سواء كانت متعمدة او عرضية (Geric & Hutinski,2007,52).

رابعاً: وسائل حماية نظم المعلومات- Methods of protect information systems

تسعى الكثير من المنظمات لايجاد السبل والوسائل الوقائية والاجرائية التي تمكنها من مواجهة التهديدات الامنية لكي تتمكن من القيام بوظائف امن المعلومات , ويتزايد الاهتمام بحماية نظم المعلومات سعيا لتقليل الكلف ولضمان استمرارية العمل وجودة المعلومات المقدمة, ويلاحظ ان بعض المنظمات ولاسيما منظمات الاعمال الصغيرة, والتي عندها نقص بالموارد والخبرة في توفير الامن تستعين بمصادر تقديم الخدمات الامنية الخارجية لسد حاجتها (Laudon& Laudon,2009,255) , وفيما يأتي وسائل الحماية البرمجية لنظم المعلومات :

أ- التشفير- Encryption : تشفير البيانات اصبح اسلوب مهم لحماية البيانات ومكونات شبكة الحاسوب ولا سيما الانترنت والانترانيت والاكسترانيت (O'Brien,2003,402) . ويعد التشفير او "الرموز السرية" من ادوات امن المعلومات الاساسية والحيوية, اذ يُمكن المنظمة من حماية المعلومات الحساسة او المهمة (Stamp,2006,4). وهناك نوعان من انواع التشفير: (Calder&Watkins,2008, 277)

(اولاً) التشفير المتماثل : يستخدم المفتاح نفسه أو الرمز لتشفير البيانات وفك شفرتها.

(ثانياً) التشفير غير المتماثل: بموجب هذه الطريقة يكون لدى اي منظمة مفتاحين احدهما مفتاح خاص والآخر مفتاح عام ويستطيع اي شخص استخدام المفتاح العام لتشفير اي رسالة موجهة من المنظمة , وهو على يقين ان معالج المفتاح الخاص فقط هو الذي يستطيع فك شفرتها, مما تقدم يتضح ان للتشفير منافع كثيرة ، الا انه توجد بعض الثغرات فيه ومنها : (حاج علي , 2006 , 14 -12)

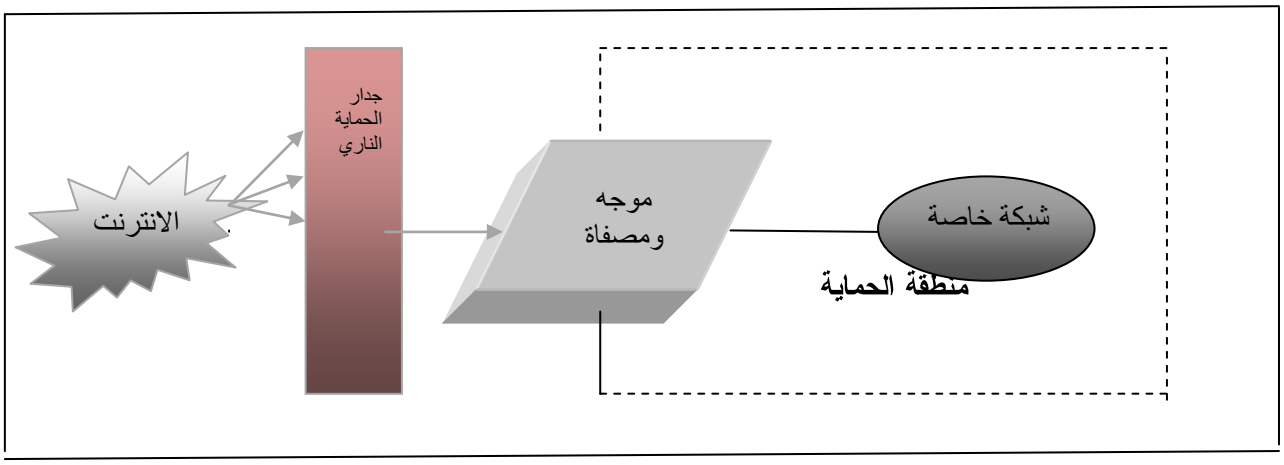
(1) يساعد اعتماد معظم التطبيقات على طريقة تشفير واحدة لمدة زمنية طويلة في تركيز المخترق على هذه الطريقة فقط الى ان يتمكن من معرفة المفتاح أو تصميم آلية لمعرفة المفتاح في كل مرة يتم تغييره.

(2) تعد عملية تغيير المفتاح عملية معقدة نظراً لتداخل عوامل إدارة وتوزيع المفاتيح ولاسيما عندما يزداد عدد المشتركين, ومع استمرار بعض الإدارات باستخدام المفتاح لمدة طويلة فانه يمكن المخترق من كشفه.

(3) يؤدي توزيع المفتاح ضمن شبكات الاتصال إلى إعتراضه من قبل المتطفلين .

(4) يزداد ضعف جميع نظم التشفير مع مرور الزمن لتكاثر الهجمات عليها, وثبت من التجارب أن طرائق التشفير والتي تكون قوية في مدة معينة تتحول الى ضعيفة في مدد لاحقة , وقد كان يعول على الطرائق الكلاسيكية في تشفير المعلومات الا ان التقدم في معالجة إستخدام الحواسيب أدى إلى التقليل من مكانتها في حماية البيانات.

ب- جدار حماية ناري- Firewall : يمثل مجموعة متكاملة من التدابير الأمنية التقانية والمصممة لمنع الوصول إلالكتروني غير المصرح به إلى نظام حاسوب متصل بالشبكة (Practical ,2009,9 Handbook), ويعمل (Firewall) كنظام "حارس البوابة" يحمي انترانت المنظمة وشبكات الحاسوب الاخرى من المتطفلين (O'Brien,2003,402) , ويمثل جدار الحماية كاداة مصفاة لمرور البيانات بين الشبكة الداخلية المحمية والشبكة الخارجية التي نخشى منها, كما موضح بالشكل رقم (2) والذي يمثل مخططاً مبسطاً لمنظومة الحماية والعائدة للهيئة العراقية للحواسيب والمعلوماتية , ويهدف النظام الامني الى حجز المستخدم في حيز سياسة أمنية معينة.



شكل رقم (2) وحدات حماية الشبكة الداخلية للهيئة العراقية

المصدر بتصرف من:

Source: Bagad, Vilas.S. & Dhotre ,Iresh A. (2007*).Information Security* ,India:Technical Publications Pune.5

ج- نسخ احتياطية Backup : تعالج النسخ الاحتياطية مشكلة فقد البيانات الرقمية غير المكتوبة , والتي تكون اكثر عرضة من غيرها للتلف او العطب او الفقد (العامري , 2010 , 59) , وينص (البند A-10-5) من المواصفة (ISO/IEC 17799:2005) على ضرورة ان تعمل المنظمة نسخاً من المعلومات والبرامج الخاصة بالاعمال المهمة, ويعد هذا البند من اهم البنود الاساسية, لانه يمكن المنظمة من استعادة المعلومات عقب حدوث طارىء او عطل في الوسائط التي تحملها, ويُمكن الافراد المستخدمين من استرجاع المعلومات نتيجة اخطاء غير مقصودة , وقد يستحيل التعافي من تاثيرات اي كارثة عندما لايتم عمل نسخ احتياطية .

د-العلامة المائية الرقمية (Digital Watermarking)

ادى التطور السريع في الاتصالات وتقنيات الوسائط المتعددة الى الحاجة الى استخدام تقنيات لحماية حقوق الملكية ومراقبة النسخ غير الشرعي لتلك الوسائط ومن اهم هذه التقنيات هي العلامة المائية الرقمية (طه وعبد الرحيم, 87,2007) .

وتعد وسائل حماية نظم المعلومات في تطور مستمر ولا يسعنا حصرها في هذا البحث ومنها على سبيل المثال مبدا اختصار المعلومات .

خامساً: الهيكل التنظيمي لنظام ادارة امن المعلومات: يحدد المعيار (ISO/IEC 27002:2005) في المادتين(6.1.1) و(6.1.2) ماهية افضل التطبيقات العملية في هيكل الادارة , وينبغي ان يتضمن الهيكل التنظيمي لنظام ادارة امن المعلومات الفرق الاتية :

(اولاً) فريق ادارة المنظمة: يتكون هذا الفريق من الادارة العليا واللجنة التوجيهية لنظام ادارة امن المعلومات (ISMS).

(ثانياً) فريق قيادة (ISMS).

(ثالثاً) فريق تنفيذ (ISMS).

ينبغي ان يقوم بتصميم وتنفيذ نظام ادارة امن المعلومات فريق يتم اختياره من ادارات المنظمة التي قد تتاثر اكثر من غيرها بتنفيذه فضلاً عن عدد من خبراء الادارة , ويجب ان يضم الفريق مدير للمشروع ذو خبرة كبيرة ويكون مسؤولاً عن متابعة مدى تقدم العمل طبقاً للاهداف الموضوعة واعداد تقارير بشان ذلك, وتوفير الموارد يعد الخطوة الاولى للتنفيذ, ولضمان تنفيذ (ISMS) فاعل وناجح ، ينبغي للمنظمات النظر في كل من الآتي: (ISMS Implemention Guideline,2013,3)

(اولا) ضمان الحصول على التزام ودعم الإدارة العليا قبل التنفيذ وبشكل متواصل طوال مدة التنفيذ.

(ثانياً) ينبغي ان يكون تنفيذ (ISMS) متسق مع ستراتيجية واهداف المنظمة ، وجزء" لا يتجزأ من الإدارة العامة للمنظمة والتي تعكس نهج المنظمة في إدارة مخاطر أمن المعلومات.

(ثالثاً) يجري تبليغ سياسات واجراءات أمن المعلومات على وجه السرعة لجميع مستويات الموظفين، من الإدارة العليا إلى المكتب الامامي لضمان عدم سوء الفهم ونقص المعلومات بين الموظفين.

(رابعاً) التصميم الفاعل لنظام ادارة امن المعلومات مدعوم بمختلف الآليات الإبداعية لكي تكون الرغبة في التغيير مرئية ومقبولة من قبل جميع المستويات.

(خامساً) ينبغي ان تمتلك طواقم الافراد المشاركين في تنفيذ(ISMS) المؤهلات والمهارات اللازمة .

(سادساً) تقام برامج التوعية لجميع الأفراد والكيانات وبشكل متواصل لخلق ثقافة امنية شاملة لفهم الأدوار والمسؤوليات الأمنية.

(سابعاً) يسهم كل من المراقبة الفاعلة والتحسين المستمر في ضمان سرعة التعامل مع المخاطر والحوادث.

يتاثر تصميم وتنفيذ نظام ادارة امن المعلومات باحتياجات المنظمة واهدافها, وتسهم المبادىء الاساسية الآتية في التنفيذ الناجح لنظام ادارة امن المعلومات (ISMS) : (البند– 3.2.1 - (ISO27000:2009(E)):

(اولاً) الوعي بالحاجة لامن المعلومات.

(ثانياً) تحديد المسؤولية عن امن المعلومات.

(ثالثاً) تضمين وشمول التزام الادارة واهتمامات اصحاب المصلحة.

(رابعاً) تعزيز القيم المجتمعية.

(خامساً) تقييم المخاطر يحدد الضوابط المناسبة للوصول الى مستويات مقبولة من المخاطر.

(سادساً) عد الامن عنصراً اساسيا في شبكات المعلومات والنظم.

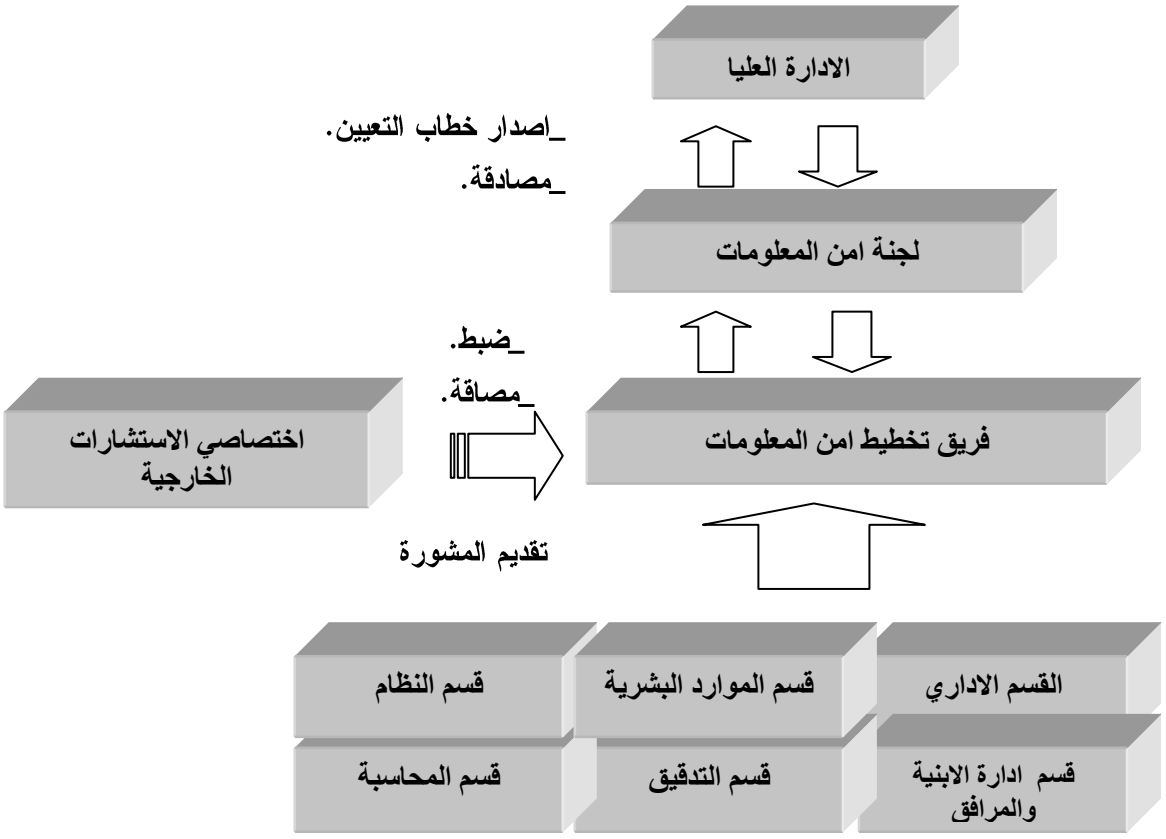
(سابعاً) الوقاية الفاعلة والكشف عن حوادث امن المعلومات.

(ثامناً) ضمان اتباع منهج شامل لادارة امن المعلومات.

(تاسعاً) اعادة التقييم المستمر لامن المعلومات, واجراء التعديلات تبعا لذلك.

ويمثل الشكل رقم (3) الهيكل التنظيمي لانشاء نظام ادارة امن المعلومات , اذ يعمل بهيئة هرم يبدأ بالإدارة العليا, اذ لايمكن ان يتحقق انشاء وتطبيق نظام ادارة امن المعلومات في المنظمة دون موافقة ودعم الادارة العليا, ومن مهامه الاساسية اصدار خطابات التعيين للملاكات المطلوبة والمصادقة على قرارات لجنة امن المعلومات. كما تسهم جميع الاطراف في حماية موجودات المنظمة كل بحسب مسؤوليته ودوره بالعمل, ويعد فريق تخطيط امن المعلومات بمثابة فريق القيادة, اذ يتلقى المشورة والنصح من اختصاصي الاستشارات الخارجية, ويحتاج باستمرار الى ضبط الاجراءات والعمليات والمصادقة عليها من قبل لجنة امن المعلومات, كذلك يسهم الاستعانة بالافراد ذوي الخبرة بعمل المنظمة والبيئة بشكل فاعل في دقة وسرعة انجاز العمل, والذين يشكلون عادةً طيف واسع من المراكز الوظيفية يشمل كل من: (ISO/IEC 27003:2010(E)52)

- الادارة العليا : مثلاً الرئيس التنفيذي للعمليات (COO- Chief Operating Officer) ,ومن مسؤولياتها وضع الرؤية والقرارات الاستراتيجية.
- اعضاء لجنة امن المعلومات , ومن مسؤولياتهم معالجة الاصول المعلوماتية.
- اعضاء فريق تخطيط امن المعلومات , ومن مسؤلياتهم اعمال التخطيط في الاقسام وفض الصراع حتى الانتهاء من وضع نظام ادارة امن المعلومات.
- مديروا الخط : مثلاً رؤساء الوحدات التنظيمية, يمتلكوا المسؤوليات العليا لوظائف المنظمة.
- اصحاب العملية (اي ذوي المجالات التشغيلية المهمة), اذ يقوم بهذه الوظيفة افراد متخصصون بمعالجة البيانات ومسؤوليتهم على سبيل المثال : تفويض المهام ومعالجة البيانات في عمليات المنظمة .
- اختصاصي الاستشارات الخارجية, يعطوا النصح من خلال معاينة عمليات المنظمة وكذلك من واقع الخبرة الصناعية او التجارية.



الشكل رقم (3) نموذج لهيكل تنظيمي ينشى (ISMS)

SOURCE:ISO/IEC27003:2010(E),*Information technology- Security techniques- Information security management system implementation guidance*, Geneva: ISO Copyright Office.52

وصف الاصدار الجديد للمواصفة (ISO/IEC 27001:2013) :

يتضمن الاصدار الجديد (ISO/IEC 27001:2013) عشرة بنود رئيسة , وتشمل (14) مركز سيطرة و (114) موقع للسيطرة والمتمثلة بالملحق (A) والمتوافقة مع المواصفة (ISO/IEC27002:2013) , ومن ابرز التغييرات التي اجريت على المواصفة (ISO/IEC27002:2013) كل من الآتي : (www.dnv ba.co.uk_)

(اولاً) الغاء الفقرة (4.2.1 –d) والتي تتضمن تحديد المخاطر, و تقرر إزالة التفاصيل بشان الكيفية التي ينبغي أن يتم تقييم المخاطر بها وبذلك الغيت متطلبات تحديد الموجودات والتهديدات والثغرات الامنية, وغير ذلك , والسبب يعود الى ان تلك المتطلبات مقيدة ، كما تم وصف كيف ينبغي للمنظمات إدارة المخاطر بدلا من وصف الأهداف.

(ثانياً) لا تتم الإشارة إلى نموذج (PDCA) صراحة في الاصدار الجديد , ولكن اطوارها موجودة ضمنياً في بنود الاصدار الجديد وكما موضح في الجدول رقم (3) .

جدول رقم (3) ترتيب بنود المواصفة (ISO/IEC 27001:2013) على وفق حلقة ديمنغ

PDCA	ISO/ IEC 27001:2013
PLAN- خطط	البند (6):التخطيط – Planning
DO- اعمل	البند (8):العملية – Operation
CHECK- راجع	البند (9):تقويم الاداء- Performance Evaluation
ACT- نفذ	البند (10):التحسين - Improvement

Source:*ISO 27001:2013 An Overview of the Changes* (2013). DNV Business Assurance.27

(ثالثاً) تتطلب المواصفة الجديدة "معلومات موثقة" بدلا من "وثائق" , ويمثل البند (7.5) المتطلبات العامة على إنشاء وتحديث والسيطرة على المعلومات الموثقة وتبقى الحاجة الى التوثيق في كثير من المواضع مطلوبة ومنها سياسة امن المعلومات ومجال (ISMS) , وغيرذلك .

ادخل الاصدار الجديد لسنة (2013) تعديلات على الاصدار السابق لسنة(2005) ,اذ ادخل تحسينات على الضوابط الامنية المدرجة في الملحق (A) ضمن المواصفة (ISO/IEC27001:2013) لضمان ان تبقى المواصفة فاعلة وقادرة على التعامل مع اخطار اليوم , ويعرض الجدول رقم (4) , مقارنة البنود بين الاصدارين بحسب الاتجاه الذي يرمي له كل بند (www.bsigroup.com/27kmapping).

جدول رقم (4) مقارنة وجه الشبه بين بنود اصداري المواصفة (ISO/IEC27001:2013)

ISO/IEC27001:2013	ISO/IEC27001:2005
4.1- فهم المنظمة وسياقها	8.3- الاجراء الوقائي
4.2- فهم حاجات وتوقعات الاطراف المهتمة	5.2.1(C)- تحديد ومعالجة المتطلبات القانونية والتنظيمية والالتزامات الأمنية التعاقدية
4.3 تحديد مجال نظام ادارة امن المعلومات	4.2.1(a)- تحديد المجال و حدوده. 4.2.3(f)- ضمان أن يبقى النطاق كافي
4.4 نظام ادارة امن المعلومات	4.1- المتطلبات العامة
5.1- القيادة والالتزام	5.1- التزام الإدارة
5.2- السياسة	4.2.1(b)- تحديد سياسة ISMS
5.3- الادوار المنظمية, المسؤوليات والسلطات	5.1(c)- وضع الأدوار والمسؤوليات لأمن المعلومات
6.1- اجراءات تناول المخاطر والفرص	8.3-الاجراء الوقائي
6.1.2- تقييم مخاطر امن المعلومات	4.2.1(c)- تعريف نهج تقييم المخاطر. 4.2.1(d)- تحديد المخاطر. 4.2.1(e)-تحليل وتقييم المخاطر
6.1.3- معالجة مخاطر امن المعلومات	4.2.1(f)-تحديد وتقييم خيارات معالجة المخاطر. 4.2.1(g)-اختيار اهداف الرقابة والتحكم لمعالجة المخاطر. 4.2.1(h)-الحصول على تقييم الادارة للمخاطر المتبقية المقترحة. 4.2.1(j)-تهيئة بيان قابلية التطبيق. 4.2.2(a)-صياغة خطة معالجة المخاطر.

6.2- اهداف امن المعلومات والتخطيط لتحقيقها	5.1(b)-ضمان ان اهداف وخطط ISMS قد وضعت.
7.1- الموارد	4.2.2(G)-ادارة موارد ISMS. 5.2.1-توفير الموارد.
7.2- الكفاءة	5.2.2-التدريب والوعي والكفاءة.
7.3- الوعي	4.2.2(e)-تطبيق التدريب وبرامج التوعية. 5.2.2-التدريب والوعي والكفاءة.
7.4- الاتصالات	4.2.4(c)-التواصل مع الاجراءات والتحسينات. 5.1(d)- التواصل مع المنظمة.
7.5- المعلومات الموثقة	4.3-توثيق المتطلبات.
8.1- التخطيط العملياتي والرقابة	4.2.2(f)-ادارة عمليات ISMS.
8.2- تقييم مخاطر امن المعلومات	4.2.3(d)-مراجعة تقييم المخاطر لفترات مخطط لها.
8.3-معالجة مخاطر امن المعلومات	4.2.2(b)-تنفيذ خطة معالجة المخاطر. 4.2.2(c)- تطبيق الضوابط
9.1- المراقبة والقياس والتحليل والتقويم	4.2.2(d)-تحديد كيفية قياس الفاعلية. 4.2.3(b)-اجراء مراجعة منتظمة لفاعلية ISMS. 4.2.3(C)-قياس فاعلية الرقابات.
9.2- التدقيق الداخلي	4.2.3(e)-تدقيق السلوك الداخلي لنظام ادارة امن المعلومات. 6-التدقيق الداخلي ISMS.
9.3– المراجعة الادارية	4.2.3(f)-اجراء مراجعة ادارية ISMS. 7- مراجعة الادارة لنظام ادارة امن المعلومات.
10.1- اللاتطابق والاجراء التصحيحي	4.2.4 صيانة وتحسين ISMS. 8.2- الاجراء التصحيحي
10.2- التحسين المستمر	4.2.4 صيانة وتحسين ISMS. 8.1-التحسين المستمر.

Source:*ISO/IEC27001Mapping Guid*.(2013). UK, Milton Keynes: MK58PP.8

يلاحظ في ترتيب بنود المواصفة (ISO/IEC 27001:2005) اعتماد الاصدار السابق على مبادىء وفلسفة الجودة الشاملة (TQM) , اذ انها تعتمد بشكل اساسي على حلقة (Deming) , ويشمل هذا النهج كلاً من المواصفة (ISO9001:2000) الخاصة بمتطلبات تطبيق نظام إدارة الجودة , والمواصفة (ISO 14001: 2004) الخاصة بنظام الادارة البيئية , وان غاية منظمة الايزو التنسيق بين تلك المعايير لتناسب الهيكل الجديد رفيع المستوى المستخدم في جميع مواصفات نظم الادارة , ويساعد هذا التغيير المنظمات التي تنفذ اكثر من مواصفة لنظام ادارة في وقت واحد, وسيكون ذو فائدة للمدققين الذين يمنحون شهادة للمنظمات التي تستخدم اكثر من مواصفة (عفيفي, 2014, 22) .

هيكلية المواصفة وخطوط عملها العريضة

تمثل مراكز السيطرة الاربعة عشر خطوط عمل المواصفة العريضة, اذ تستعين المنظمات بالضوابط المدرجة فيها في تطبيق العمليات والاجراءات اللازمة لانشاء نظام ادارة امن المعلومات على وفق المواصفة (ISO/IEC 27001:2013), والجدول رقم (5) يوضح مراكز السيطرة الرئيسة والمتوافقة مع المواصفة (ISO/IEC 27002:2013).

الجدول رقم (5) مراكز سيطرة لحماية المعلومات

A5	سياسات امن المعلومات
A6	تنظيم امن المعلومات
A7	امن الموارد البشرية
A8	ادارة الموجودات
A9	التحكم بالوصول الى المعلومات
A10	تعمية (التشفير)
A11	الامن المادي والبيئة المحيطة بالمعلومات
A12	امن العمليات
A13	امن الاتصالات
A14	نظام تحقيق التطوير والصيانة
A15	العلاقات مع الموردين
A16	ادارة حوادث امن المعلومات
A17	الجوانب الامنية لادارة استمرارية الاعمال
A18	الاذعان

المصدر: اعداد الباحث استناداً

Source:Annex (A)-ISO/IEC27001:2013(E),*Information technology- Security techniques-Information security management system -Requirements* ,Geneva: ISO Copyright Office.10

المحور الثالث /الجانب العملي :

يهدف هذا المبحث الى تقييم نظام ادارة امن المعلومات في الهيئة العراقية للحواسيب والمعلوماتية على وفق المواصفة (ISO/IEC27001:2013) , إذ يتضمن عرضاً وتحليلاً للبيانات التي جمعت من واقع الهيئة العراقية للحواسيب والمعلوماتية من خلال المعايشة الميدانية للباحث لتحديد مستوى المطابقة والتوثيق لكل متطلب من متطلبات المواصفة (ISO/IEC27001:2013) , وكذلك وضع الحلول والمقترحات لكل فجوة بما ينسجم ومتطلبات المواصفة الرئيسة (ISO/IEC27001:2013) والمواصفة الداعمة (ISO/IEC27003:2010) والتي تتضمن دليلا تنفيذيا لنظام ادارة امن المعلومات , ويمكن الاستفادة من المعيار(NIST) في وضع مقترحات لمعالجة الفجوات في كل بند من بنود المواصفة وتعني (NIST) اختصاراً المعهد الوطني للمعايير والتقانة ويقوم باصدار معايير تخص امن المعلومات ومقره في الولايات المتحدة الامريكية , اذ ان معايير (NIST) متوافقة مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهروتقنية الدولية (IEC) برؤية مشتركة لنظام إدارة أمن المعلومات (NIST SP 800-53A , 2010 VI), وقدا عتمدت قوائم فحص (Checklists) والخاصة بالمواصفة (ISO/IEC27001:2013), والمعدّة من قبل منظمة التقييس الدولية والمتضمنة (113) سؤالاً موزعة على (10) متطلبات رئيسة تتضمن (28) متطلباً فرعياً, ولغرض تحليل البيانات فقد استعمل مقياس ليكرت السباعي لقوائم الفحص, ويقدم المبحث قوائم الفحص والتحليل لجميع متطلبات المواصفة , ويلخص الجدول رقم (6) نتائج مستوى التنفيذ الفعلي والنسبة المؤية لمستوى المطابقة والتوثيق لمتطلبات المواصفة القياسية (ISO/IEC27001:2013) في الهيئة العراقية للحواسيب والمعلوماتية .

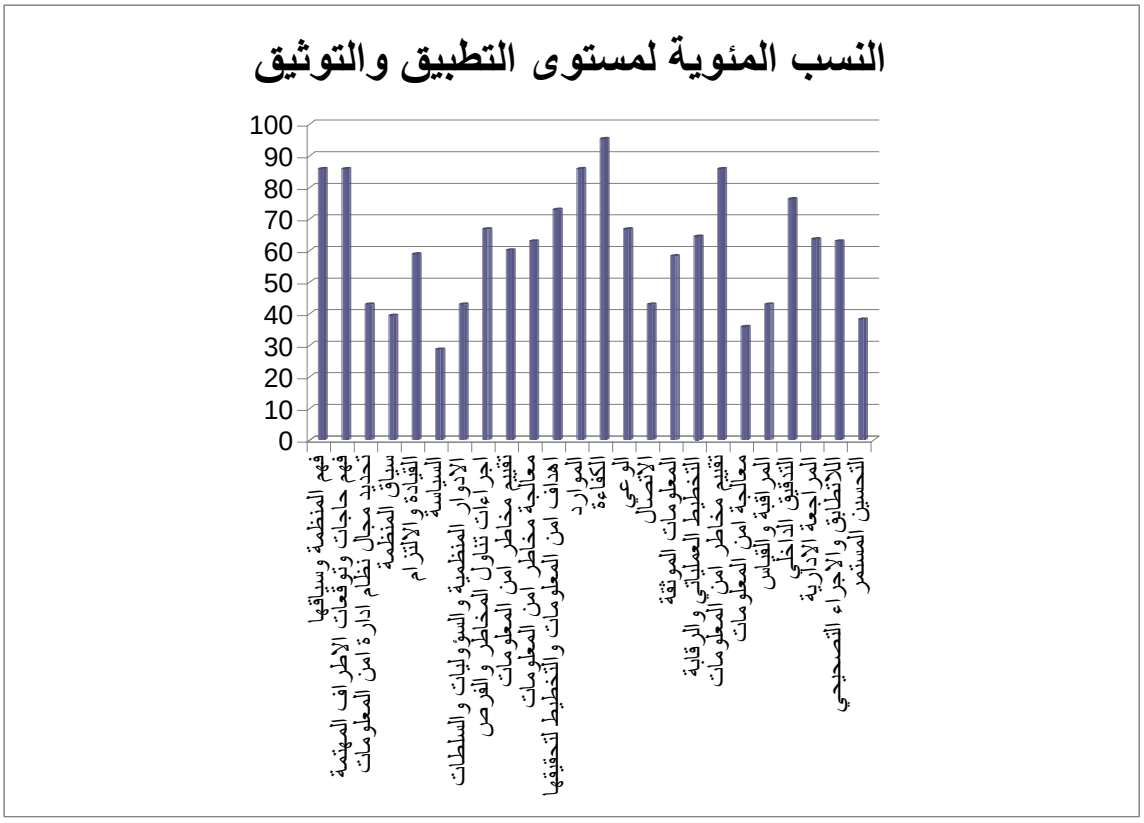
جدول رقم (6) ملخص نتائج مستوى مطابقة وتوثيق متطلبات المواصفة القياسية (ISO/IEC 27001:2013) في الهيئة العراقية للحواسيب والمعلوماتية

ت	عناوين المتطلبات بحسب المواصفة: (ISO/IEC 27001:2013)		درجات التقويم للتطبيق والتوثيق الفعلي	
	رقم المتطلب	اسم المتطلب	الوسط الحسابي المرجح (المعدل)	النسبة المئوية للمطابقة
1	4-1	فهم المنظمة وسياقها	6	85.71
2	4-2	فهم حاجات وتوقعات الاطراف المهتمة	6	85.71
3	4-3	تحديد مجال نظام ادارة امن المعلومات	3	42.85
4	4-4	نظام ادارة امن المعلومات	2.75	39.28
5	5-1	القيادة والالتزام	4.11	58.73
6	5-2	السياسة	2	28.57
7	5-3	الادوار المنظمية والمسؤوليات والسلطات	3	42.85
8	6-1	اجراءات تناول المخاطر والفرص	4.66	66.67
9	6-1-2	تقييم مخاطر امن المعلومات	4.2	60
10	6-1-3	معالجة مخاطر امن المعلومات	4.4	62.85
11	6-2	اهداف امن المعلومات والتخطيط لتحقيقها	5.1	72.85
12	7-1	الموارد	6	85.71
13	7-2	الكفاءة	6.66	95.24
14	7-3	الوعي	4.66	66.66
15	7-4	الاتصال	3	42.85
16	7-5	المعلومات الموثقة	4.07	58.16
17	8-1	التخطيط العملياتي والرقابة	4.5	64.28
18	8-2	تقييم مخاطر امن المعلومات	6	85.71
19	8-3	معالجة مخاطر امن المعلومات	2.5	35.71
20	9-1	المراقبة والقياس والتحليل والتقويم	3	42.85
21	9-2	التدقيق الداخلي	5.33	76.19
22	9-3	المراجعة الادارية	4.44	63.49
23	10-1	اللاتطابق والاجراء التصحيحي	4.4	62.85
24	10-2	التحسين المستمر	2.66	38.09
25	المجموع الاجمالي لنتائج التقويم		102.44	1463.86
26	الحد الأعلى للتطبيق والتوثيق التام للمتطلب		7	100
27	المجموع الاجمالي المفترض للتطبيق والتوثيق التام		168	2400
28	مقدار الفجوة في تطبيق وتوثيق إجمالي المتطلبات		65.56	936.14
29	نسبة النتائج الفعلية الاجمالية الى النتائج المفترضة الاجمالية		39.02	39.02

المصدر : استناداً الى تحليل بيانات الجانب العملي

يوضح لنا الشكل رقم (4) الرسم البياني لمستوى تطبيق وتوثيق متطلبات المواصفة (ISO/IEC27001:2013) في الهيئة العراقية للحواسيب والمعلوماتية , اذ يؤشر انخفاض مستوى التطبيق والتوثيق في المتطلبات: (تحديد المجال , ونظام ادارة امن المعلومات , والسياسة , والادوار المنظمية والمسؤوليات والسلطات , والاتصال , ومعالجة مخاطر امن المعلومات , وفي المراقبة والقياس , وكذلك التحسين المستمر), ويعود السبب الى عدم وجود قرار من الادارة العليا بتطبيق المواصفة (ISO/IEC27001:2013) في الهيئة او احد اقسامها او انشطتها , لذا نجد ان كثير من المستلزمات والاجراءات ليست متوفرة او ضعيفة ولاسيما بما يخص التوثيق , وفي مقابل ذلك نلحض ارتفاع مستوى التطبيق والتوثيق بشكل كبير في المتطلبات: (فهم المنظمة وسياقها , وفهم حاجات وتوقعات الاطراف المهتمة , وكذلك في توفير الموارد , والكفاءة) , ويعود ذلك الى وجود ملاكات متخصصة بالحواسيب والمعلوماتية , وذات خبرة في تطوير وتدريب الموظفين في الهيئة والجهات االمستفيدة الاخرى , وملاك الهيئة متخصص في التعامل مع التهديدات والمخاطر التي تعترض نظم المعلومات وذوي خبرة طويلة في سبل معالجتها والوقاية من ضررها, كما ان معهد المعلوماتية للدراسات العليا والتابع للهيئة متخصص بتاهيل الملاكات المتقدمة (دبلوم , وماجستير , ودكتوراه) في مجال الحواسيب , وتقانة المعلومات والاتصالات , ويعمل على رفد الهيئة باحدث البحوث في هذا المجال .

شكل رقم (4) أجمالي مستوى التطبيق والتوثيق لمتطلبات نظام إدارة امن المعلومات على وفق المواصفة (ISO/IEC27001:2013) في الهيئة العراقية للحواسيب والمعلوماتية



المصدر: استناداً الى تحليل بيانات الجانب العملي.

المحور الرابع/ الاستنتاجات والتوصيات

الاستنتاجات

تمخضت نتائج البحث الحالي عن مجموعة من الاستنتاجات , وقد تم تناولها بشكل متتابع وبما ينسجم مع تسلسل فصول البحث الحالي , وهي كل من الآتي :

1- تفتقر الهيئة (موقع اجراء البحث) لاي تصنيف موثق خاص بالمعلومات , ونظام التوثيق الالكتروني لم يتم العمل به بعد .

2- يعد الخطا والسهو عند الموظفين من ابرز التهديدات التي تواجه نظم المعلومات لجميع المنظمات , ويمثل التدريب الجيد والمستمر افضل اساليب الوقاية والعلاج , وهو ما يعزى اليه عدم تسجيل خرق امني لنظام ادارة امن المعلومات في الهيئة او النظم البرمجية المصممة فيها (كنظام الاستمارة الالكترونية والمعد للتقديم للجامعات والمعاهد) اذ اثبت حصانة امنية من الاختراق في الانترنت ولمدة ثلاث سنوات .

3- مهما بلغت نظم ادارة امن المعلومات من الرقي والحداثة والتحصين, فهي بحاجة الى تشريع عالمي يؤسس لنظام اداري شامل مبني على نهج التعامل مع المخاطر , وينسجم مع نظم الادارة الاخرى (كنظام ادارة الجودة ISO9001 , ونظام ادارة البيئة ISO14001), وهذا ما توفره المواصفة الدولية (ISO/IEC 27001:2013) .

4- يسهم تقييم موجودات الهيئة وبخاصة المعلومات وقواعد البيانات وتصنيفها بحسب اهميتها في ضمان حسن استخدامها من قبل المخولين والقدرة على ربط الهيئة بنظام الحكومة الالكترونية بشكل صحيح وآمن.

التوصيات :

- تصنيف المعلومات على وفق اهميتها ودرجة سريتها , وتصنيف الجهات المخولة للوصول اليها , وعلى وفق قواعد واجراءات التشفير , وينسب افراد للعمل عليها, وتحديد من له حق امتلاك المفاتيح العامة او الخاصة .

- تشكيل فريق عمل يتبنى تهيئة مستلزمات تطبيق المواصفة (ISO/IEC 27001:2013), وتعمل على تلبية متطلباتها ومتطلبات نظم الادارة الاخرى (نظام ادارة الجودة وغير ذلك) , وترتبط بالادارة العليا لتييسير الدعم بالموارد والصلاحيات .

- استحداث ادارة للمخاطر وحوادث امن المعلومات , تعمل على تحديد وتحليل وتقييم المخاطر والتهديدات وتقدم النتائج بشكل دوري للمسؤولين في الهيئة.

- اعتماد مبدا التوثيق الدقيق لجميع المعلومات والعمل على تصنيفها بنظام التوثيق الالكتروني وعدم اغفال توثيق الاخطاء وحالات الاختراق للافادة منها في تحليل المخاطر مستقبلاً.

- اعتماد مجموعة عمل متخصصة في صياغة السياسات الامنية للهيئة والجهات المستفيدة تعتمد المواصفة (ISO/IEC 27001:2013) والمواصفة الداعمة (ISO/IEC 27003:2010) , على ان تكون السياسة الموضوعة مفهومة ومبلغة لجميع الموظفين.

- اتخاذ الهيئة لبناية مستقلة , يراعى في تصميمها قواعد واجراءات الامن المادي العالمية.
- انشاء برنامج تدريبي لتوعية ملاك الهيئة والجهات المستفيدة باهمية المواصفة (ISO/IEC 27001:2013) واسلوبها الخاص في بناء نظام ادارة امن المعلومات , لتهيئة تطبيق المواصفة في الهيئة والمنظمات العراقية.
- وضع قواعد واجراءات للمساعدة في التخلص من الوثائق التالفة ووسائط حفظ المعلومات البالية العائدة للهيئة وتحديد جهة استشارية للفحص والتاكد في هذا المضمار.
- وضع استراتيجية لمعالجة المخاطر يراعى فيها الخيارات الاربعة (تجنب ونقل وتخفيف واستمرار المخاطر) وبموافقة واشراف الادارة العليا.
- اعتماد التدريب الجيد لملاك الهيئة لتقليل اخطاء الموظفين ما امكن .
- تكليف السيطرة النوعية والعائدة للهيئة باعمال الاستطلاع والتقويم لمنتجات الهيئة فضلاً عن تطبيق اختبارات قياس النظام الامني للهيئة وبالاعتماد على الضوابط الامنية الواردة في الملحق (A) ضمن المواصفة (ISO/IEC 27001:2013).
- توثيق جميع المعلومات الخاصة بتحسين وتطوير نظام ادارة امن المعلومات وحفظها كمعلومات موثقة وصيانتها وتحديثها دورياً.

المصادر العربية:

اولا: الكتب

1 - الحمامي,علاء حسين والعاني,سعد عبد العزيز (2007). *تكنولوجيا امنية المعلومات وانظمة الحماية*, عمان, الاردن : دار وائل للنشر.

2- الحميد , محمد دباس و نينو, ماركو ابراهيم (2007). *حماية أنظمة المعلومات*. الاردن , عمان: دار الحامد.

3-العامري , اسامة (2010).*اتجاهات ادارة المعلومات*. الأردن ,عمان , دار اسامة للنشر والتوزيع.

4- داود , حسن طاهر (2000) . *جرائم نظم المعلومات* , مركز الدراسات والبحوث ,المملكة العربية السعودية , الرياض.

5- داود , حسن طاهر (2004). *امن شبكات المعلومات* , المملكة العربية السعودية , الرياض : مركز الدراسات و البحوث .

6- عمر، ماهر محمود (1988). *سيكولوجية العلاقات الأجتماعية*. مصر، الأسكندرية : دار المعرفة الجامعية.

7- مكلود, رايموند وشيل , جورج (2009). *نظم المعلومات الادارية*(ط 3). (ترجمة: سرور علي ابراهيم).المملكة العربية السعودية , الرياض:دار المريخ للنشر.(سنة النشر الاصلية 2006).

ثانياً: البحوث والدراسات

8- الحافظ ,علي عبد الستار و النعيمي ,احمد هاني (2013). دور (ISO27001:2005) في تعزيز مفهوم ادارة دورة حياة المعلومات . زيارة 2 ايلول , 2013 , على شبكة الانترنت : www.kantakji.com .

9- الصاحب , محمود حسن (2013). سياسة امن المعلومات في الجامعات: حالة دراسية, CYBRARIANS JOURNAL, 2(33), 53-60 .

10- تايه , علاء الدين محمد (2008). مدى فعالية ادارة امن المعلومات في شركات تكنولوجيا المعلومات في فلسطين. الجامعة الاسلامية ,فلسطين , غزة .

11- جبوري , ندى اسماعيل (2011). حماية امن انظمة المعلومات:دراسة حالة في مصرف الرافدين/ فرع شارع فلسطين . مجلة تكريت للعلوم الادارية والاقتصادية, 7 (21), 72-91 , جامعة تكريت للعلوم الادارية والاقتصادية, تكريت , العراق .

12- حاج علي ، عوض (2006) .التعريف بتقنيات التشفير وأمنية المعلومات، جامعة النيلين ، زيارة 10 تشرين الاول , 2013 , على شبكة الانترنت :.http://www.profawad.info/7777

13- عفيفي , جمال (2014). المستهلك والجودة .(37) , (22) , الرياض , العربية السعودية.

14-طه, دجان بشير وعبد الرحيم, فرقد حامد (2007) , (5-30) . حماية حقوق الملكية للوثائق النصية. مجلة الرافدين لعلوم الحاسبات والرياضيات, العدد (2) , (87) .

ثالثاً: الرسائل والاطروحات الجامعية

15- القحطاني , منصور بن سعيد (2008). تهديدات الامن المعلوماتي وسبل مواجهتها:دراسة مسحية منسوبي مركز الحاسوب الالي بالقوات البحرية الملكية السعودية بالرياض . جامعة نايف العربية للعلوم الامنية , السعودية , الرياض

المصادر الاجنبية

First:Book

16- Al-Kolaly , M. (2005). Concepts of Information Technology (IT).UK : Cheltenham Courseware Ltd.

17-Arnason , Sigurjon Thor & Willett , Keith D. (2008) .How to Achieve 27001 Certification : An Example of Applied Compliance Management. USA:Taylor & Francis Group, LLC .

18-Bagad ,V.S., Dhotre I.A. (2009).Information Security, India :Technical Publications Pune.

19-Brown, Carol V.,De Hayes,Daniel W. ,Hoffer,Jeffrey A., Martin,E.Wainright & Perkins,William c. (2009). Managing Information Technology(6th ed).Amrican ,New Jersy: Pearson Prentic Hall.

20- Caballero ,Albert (2009). Information Security Essentials for IT Managers:Protecting Mission- Critical Systems.In John r. Vacca (Eds),Computer and Information Security (225-253).USA:Morgan Kaufmann.

21- Calder , Alan & Watkins , Steve (2008). IT Governance a Manager's Guide to Data Security and ISO27001/ISO 27002 (4th ed.). USA, Philadelphia : Replika Press,Pvt Ltd.

22-Cisco systems (2001). Cisco networking academy program guide (2nd ed.). Indiana: Cisco press.

23-Cole,Eric.,Krutz,Ronald.& Conley,James W.(2009).Network Security Bible (2nd ed).Indianapolis,Indiana:Wiley Publishing,Inc.

24-ISMS Impilementation Guideline:A Practical Approach. (2013).Malasia,Selangor Darul Ehsan : Cyber Security Malasia.

25-ISO 27001:2013 An Overview of the Changes.(2013). DNV Business Assurance.

26-Janzeweski , Lech (2008). Cyper crime and Cyper Terrorism, USA: IGI.

27-Laudon , K. C. & Laudon, J. P. (2009).Essential of Management Information systems(8th ed).USA, New Jersey ,Upper Saddle River :Pearson Education.

28-Laudon,k.c. & Laudon,J.P.(2005).Management Information System(6thed.).UAS,New Jersey :Prentic-Hill,International.

29-O'Brien , James A. (2003). Introduction to Information Systems(11th ed) . America,New York : Mc Graw Hill.

30-Owen ,Poole (2003).Computer Weekly Professional Series Network Security: A Practical Guid, Butter Worth Ltd.

31-Russell,D.& Gangemi Sr.(1991).Computer Security Basics,O'Reilly &Associates,Inc.

32-Stamp , Mark (2006). Information Securit Principles and Practice.USA,New Jersey: John Wiley & Sons.

33-The Basics of Information Security: Apractical Handbook (2009).Netherlands: Creative Commons Attribution

34-Tipton, Harold F. & Krause, Micki (2006) Information Security Management Handbook (5th ed.) , United States of America : Taylor & Francis Group .

35 Turban,Efraim, Leidner,Dorothy, Mclean,Ephraim & Wetherbe , James (2008).Information Technology for Management(6th ed.).USA :John Wiley & Sons.Inc.

36-Wright,Joe & Harmening,Jim(2009). Security Management System.In John r. Vacca (Eds),Computer and Information Security (255-258).USA:Morgan Kaufmann.

37-Ziolkowski , Katharina (2013).Peacetime Regime for State A Ctivities in Cyberspace.Tallin,Estonia:Cyber Defence Center of Excellence..

Second: Journals

38-Geric, Sandro &Hutinski, Zeijko (2007).Information System Security Threats Classifications. JOURNAL OF INFORMATION AND ORGANIZATIONAL SCIENCES , 31 (1),51-61.

39-Sharma,NK & Dash,Prabir kumar(2012).Effectiveness of ISO 27001,As an Information Security Management System:An Analytical Study of Financial Aspects.FAR EAST JOURNAL OF PSYCHOlLOGY AND BUSIN : An International Journal,9(3),42-55.
40-Whitson, G. (2003).Computer security: theory, process and management. The Journal of Computing in Small Colleges, 18(6) , 57 – 66.

Third:Thesis &Dissertations

41- Brewer, David & Nash, Michael(2010). Insights into the ISO/IEC 27001 Annex (A), Gamma Secure Systems Limited.
42- Erkan,Ahment (2006).An Automated Tool For Information Security Management System.Turkey.
43-Nakrem,Are(2007).Managing Information Security in Organizations:A Case Study.Agder University College.

Fourth :the International Standardization Organization(ISO) Versions &Other organizations

44 -ISO/IEC 27001:2013, "International Standard – Information technology- Information security management systems- Requirements"(2nd ed.) .Geneva: ISO Copyright Office.
45 -ISO/IEC 27002:2013, " Information technology — Security techniques — Code of practice for information security controls "(2nd ed.) .Geneva: ISO Copyright Office.
46-ISO/IEC 27000:2009,"Information technology-Security techniques-Information Security management Systems-Overview and Vocabulary".Geneva: ISO Copyright Office.
47-ISO/IEC27003:2013,Information technology- Security techniques-Information security management system implementation guidance.Geneva: ISO Copyright Office.
48 -(NIST800-53A)National Institute of Standard and Technology(2008). Information Security,U.S.Department of Commerce-Publication.

The Evaluation of Information Security Management System in the Iraqi Commission for Computers and Informatics according to the International Standard (ISO 27001: 2013)

Abstract

The current research included (the evaluation of Information Security Management System on according to international standard (ISO / IEC 27001: 2013) in Iraqi Commission for Computers and Informatics), for the development of an administrative system for information security is considered a priority in the present day, and in the light of the organizations dependence on computers and information technology in work and communication with others. The international legitimacy (represented by the International Organization for standardization (ISO)) remains the basis for matching and commitment and the importance of the application of information Security Management System according to the international standard (ISO / IEC 27001: 2013) is manifested in protecting the assets of the organizations especially information and databases systematically and continuously.

The aim of the research was evaluating between the Information Security Management System that currently exists in the Iraqi Commission for Computers and Informatics (site of conducting the research) and the Information Security Management System according to the International Standard (ISO / IEC 27001: 2013) by using examining checklists in order to diagnose nonconformity gaps with the international standard.

The research has come to an important conclusion, i.e. (the administrative system for information security followed by the Iraqi Commission for Computers and Informatics, despite its dependence on modern technology and the efficient staff , it lacks good documentation and application of many of the requirements International Standard (ISO / IEC 27001: 2013) came with needs to rebuild an organizational structure and functions consistent with the supporting International Standard (ISO / IEC 27003: 2010).

The research concluded with the most important recommendation (forming a work team that adopts preparing the prerequisites of Appling the standard (ISO / IEC 27001: 2013) works at meeting its requirements and the requirements of other management systems (quality management system and so on), and associated with the top management to facilitate the support with resources and powers.

Key Words: Information Security- Information Security Management System- Iraqi Commission for Computers and Informatics - Likert Scale - ISO 27001- NIST.