تقييم نظام ادارة أمن المعلومات على وفق المواصفة (ISO27001) دراسة حالة الشركة العامة للأنظمة الالكترونية(*)

أ.م.د نداء صالح الشاهين الباحث زهور سعد عباس
الجامعة التقنية الوسطى الكلية التقنية الأدارية

مستخلص
يهدف البحث الحالي الى تقييم نظام ادارة امن المعلومات في الشركة العامة للأنظمة الالكترونية على وفق المواصفة (ISO 27001: 2013) من خلال قياس فجوة التطبيق وتحليلها.
انطلق البحث من مشكلة عبر عنها بعدد من التساؤلات كان اهمهما ما مدى توافر متطلبات نظام ادارة امن المعلومات وفق المواصفة(ISO 27001: 2013) في الشركة العامة للأنظمة الالكترونية
استعمل منهج دراسة الحالة للوصول الى اهدافه ووقع الاختيار على الشركة العامة للأنظمة الالكترونية ميدانا عمليا لاجراء البحث، واستعملت عدد من الادوات والاساليب الاحصائية منها قوائم الفحص لجمع البيانات والمعلومات وعدد من الاساليب الاحصائية لقياس وتحليل الفجوة (الوسط الحسابي المرجح والنسبة المئوية لمعدل المطابقة)
توصل البحث الى عدد من النتائج كان اهمها وجود فجوة بمقدار(٦٣%) لواقع تطبيق نظام إدارة امن المعلومات في الشركة.
الكلمات الدالة:- أمن المعلومات، نظام ادارة امن المعلومات، المواصفة الدولية (ISO 27001: 2013)

*** بحث مستل من رسالة ماجستير**

Abstract
The current research aims at evaluating the information security management system in the General Company for Electronic Systems according to the standard (ISO 27001: 2013) by measuring and analyzing the application gap.

The research started from a problem expressed by a number of questions, the most important of which was the availability of information security management system requirements according to the standard (ISO 27001: 2013) in the General Company for Electronic Systems.

Using a case study methodology to achieve its objectives, the General Company for Electronic Systems was chosen as a practical field for conducting the research. A number of statistical tools and methods were used, such as checklists to collect data and information and a number of statistical methods for measuring and analyzing the gap (weighted mean and percentage of the matching rate)

The research reached a number of results, the most important of which was a gap (63%) in the reality of the application of the information security management system in the company.

المقدمة

يعد نظام إدارة امن المعلومات من أهم القضايا في مجتمع اليوم الذي يعيش فيه الفرد عصر تقانة المعلومات والعولمة، وبازدياد حجم المعلومات وكثافتها ازدادت الحاجة الى تبادلها والى انتقالها من مكان الى اخر، سواء كان داخل المنظمة او من منظمة الى اخرى أو حتى بين الدول، لذلك يجب حماية المعلومات والمحافظة عليها من المخاطر التي قد تتعرض اليها خارجيا او داخليا، اذ ان هناك وسائل وادوات عديدة لحماية المعلومات من المخاطر التي قد تتعرض لها لكن هذا لايكفي رغم وجود عدد كبير من وسائل الحماية، اذ ان عالم الحاسوب وتكنولوجيا المعلومات يوجد فيه ثغرات يستطيع البعض اكتشاف هذه الثغرات واستغلالها، لذلك تظهر الحاجة الى وجود منهجية لبناء نظام اداري لأمن المعلومات لحماية المعلومات والحفاظ عليها من الاختراقات وتحديد المخاطر وتحليها، لذلك فأن نظام ادارة امن المعلومات (ISO 27001: 2013) يوفر الحماية للمعلومات، اذ انه (يقدم اطارا ومنهجية يمكن ان تستخدمها المنظمة لإدارة المخاطر والمحافظة على أصولها المعلوماتية. اما تميز الاعمال فيعبر عن قدرة المنظمة على التفوق في ادائها، وكفاءتها في حل مشاكلها وفعاليتها في اقتناص ما يلوح في البيئة المحيطة من فرص وتجنب المخاطر والتهديدات بالتنبؤ المسبق لها ومن هنا برزت مشكلة الدراسة الحالية التي صيغت على شكل تساؤلات وقد تمحورت حول الى بيان مدى توافر تطبيق متطلبات المواصفة ومتطلباتها **(ISO 27001:2013)** في الشركة العامة للأنظمة

الالكترونية، اذ يهدف البحث الى تقييم وتحليل مستويات التوثيق والتطبيق الفعلي لمتطلبات المواصفة القياسية وذلك بأستخدام قوائم الفحص (Checklist) وتحديد ألاسباب المؤدية للفجوات بأعتماد المقياس السباعي، وتتجلى أهميته بتشجيع الشركة العامة للأنظمة الالكترونية التي تمتلك انظمة معلومات دقيقة وتتعامل مع معلومات سرية ومهمة في تطبيق مواصفة أمن المعلومات (ISO 27001: 2013) واعتمد البحث منهج الحالة لكونه المنهج الانسب لتحقيق اهدافه، وجرى اختيار الشركة العامة للأنظمة الالكترونية بوصفها حدود مكانيا لأجراء البحث. خرج البحث بعدد من ألاستنتاجات كان اهمها الاهتمام بتطبيق نظام ادارة امن المعلومات وفق المواصفة (ISO 27001: 2013) مازال محدود لعدم توافر التخصيصات المالية والدعم اللازم من قبل الادارة العليا فضلا عن ذلك لاتوجد في الشركة سياسة خاصة بتطبيق نظام إدارة أمن المعلومات، وهذا ماجعل المسؤوليات موزعة على جميع المستويات إلادارية في الشركة فيما يخص نظام أدارة امن المعلومات. اما أهم التوصيات فهي قيام الشركة العامة للأنظمة الالكترونية بوضع خطة تحسين مناسبة بما يتناسب مع سياسة الجودة للمنظمة ومراقبة وقياس العملية للتحقق من النتائج، أي استخدام منهج ديمنغ (PDCA) مع التوثيق لكل خطوة للاستفادة من ذلك في المستقبل والاستمرار في البحث عن اجراءات ووسائل جديدة للتحسن الاداء ووضع سياسة خاصة بنظام ادارة امن المعلومات معلنة للعاملين والزبائن .

في ضوء ماتقدم انفا، سيتضمن البحث المباحث الأتية :-

المبحث الاول:- منهجية البحث

المبحث الثاني:- ألاطار النظري للبحث.

المبحث الثالث:- ألاطار العملي للبحث.

المبحث الرابع:- الاستنتاجات والتوصيات .

المبحث الأول :- منهجية البحث

أولا:- مشكلة البحث

يعد أمن المعلومات، واحدا من القضايا المهمة المقترنة بالاستخدام المتزايد للتقنيات الحديثة ومنها شبكة المعلومات، مما قد يشكل خطرا وتهديدا وفقدانا للثقة وعبئا على المنظمة في حال فشل اداء نظام المعلومات فيها بالمحافظة على سرية وسلامة المعلومات، لذلك فإن الحاجة قائمة الى تطبيق نظام إداري لأمن المعلومات يوافر الحماية المرجوة للمعلومات على مستوياتها المختلفة وبجميع طرائق حفظها، وهذا ماتوافره المواصفة الدولية**(ISO 27001: 2013)** وقد يلمس الباحثان اهمية تطبيق المواصفة المذكورة في الشركة العامة للأنظمة الالكترونية، نظرا لان الشركات تتعامل بشكل كبير مع الشركات العالمية بأستخدام تكنولوجيا المعلومات، وتقديم الدعم والاسناد الى القطاعات العامة والخاصة في مجال صناعة البرمجيات الحديثة والصناعة الالكترونية، لذا فقد أصبح من الضروري اعتماد نظام لأداره امن المعلومات وفق المواصفة العالمية

المذكورة لضمان المحافظة على سرية المعلومات وصيانتها ويمكن التعبير عن مشكلة البحث بأثارة التساؤلات الاتية:-

١- ما مدى توافر متطلبات نظام ادارة امن المعلومات وفق المواصفة **ISO (27001:2013)** في الشركة العامة للأنظمة الالكترونية؟

٢- ماهو حجم الفجوة بين الواقع الفعلي لنظام إدارة أمن المعلومات في الشركة العامة للأنظمة الالكترونية ونظام إدارة أمن المعلومات على وفق المواصفة **(ISO 27001: 2013)**

ثانيا:- أهداف البحث

يحاول البحث بلوغ الأهداف الاتية :-

١- قياس الفجوة بين الواقع الفعلي لإدارة أمن المعلومات في الشركة العامة للأنظمة الالكترونية ومتطلبات المواصفة (ISO 27001: 2013)

٢- تحليل الفجوة بين الواقع الفعلي لإدارة أمن المعلومات في الشركة العامة للأنظمة الالكترونية ومتطلبات المواصفة (ISO 27001: 2013) لتشخيص نقاط القوة والضعف من اجل تقديم توصيات في محاولة لردم الفجوة.

ثالثا:- أهمية البحث

١- تشجيع الشركة العامة للأنظمة الالكترونية التي تمتلك انظمة معلومات دقيقة وتتعامل مع معلومات سرية ومهمة في تطبيق مواصفة امن المعلومات **(ISO27001:2013)**

٢- سيقدم البحث أدلة واقعية رقمية مستوحاة من واقع التشخيص الفعلي وما ستسفر عنه نتائج قوائم الفحص لمتغير البحث.

رابعا: حدود البحث

١- **الحدود الزمانية :-** اعتمدت مدة اجراء البحث من (٢٥/ ١٢/ ٢٠١٨) لغاية (١٥/ ٣/٢٠١٨)

٢- **الحدود المكانية :-** اختيرت (الشركة العامة للأنظمة الالكترونية) موقعا لأجراء البحث.

خامسا:- مصادر جمع البيانات

١-الجانب النظري: أ- الكتب العربية والاجنبية.

ب- الرسائل والاطروحات العربية والاجنبية .

ج - البحوث والدوريات العربية والاجنبية.

د- اصدارات منظمة التقييس الدولية (ISO)

٢- الجانب العملي:

أ- استعمال قوائم الفحص(Checklist) لتشخيص حجم الفجوة بين الواقع الفعلي لنظام ادارة امن المعلومات في الشركة العامة للأنظمة الالكترونية ومتطلبات نظام ادارة امن المعلومات على وفق المواصفة القياسية الدولية (ISO 27001:2013)، وكذلك في

تشخيص حجم الفجوة بين الواقع الفعلي لاداء الشركة ومعايير النموذج الاوربي لتمييز الاعمال.

ب- الاطلاع على تقارير الشركة والوثائق والسجلات ذات الصلة

سادسا:- أدوات التحليل والمعالجة الإحصائية

جرى اعتماد مقياس(ليكرت) السباعي لتشخيص مستوى تطبيق متطلبات المواصفة الدولية (ISO27001: 2013) في الشركة العامة للأنظمة الالكترونية، وقد حددت أوزان المقياس، ومن ثم تحليل البيانات بشكل كمي وتفسير النتائج، **(ويوضح الجدول (١))** فقرات المقياس السباعي واوزانه

جدول (١)

المقياس السباعي لتحديد درجة المطابقة مع المواصفة القياسية

مـــدى المطابقـــــة						
موثق كليا مطبق كليا	موثق كليا مطبق جزئيا	موثق كليا غير مطبق	موثق جزئيا مطبق كليا	موثق جزئيا مطبق جزئيا	غير موثق مطبق جزئيا	غير موثق غير مطبق
٦	٥	٤	٣	٢	١	٠

وبعد تحديد درجة المطابقة لكل محور من محاور المواصفة (ISO 27001: 2013) في ضوء ما تضمنته نتائج قوائم الفحص، سيجري اعتماد المعادلات الآتية لاستخراج النسبة المئوية لمدى المطابقة وحجم الفجوة (الخطيب،2008 :327-326):

1 - الوسط الحسابي المرجح = $\frac{\text{(الأوزان} \times \text{تكراراتها)}}{\text{مجموع التكرارات}}$ **.....(١)**

2 - النسبة المئوية لمدى المطابقة = $\frac{\text{الوسط الحسابي المرجح}}{\text{اعلى درجة في المقياس} \times \text{مجموع التكرارات}}$ **.....(٢)**

3 - حجم الفجوة = 1 – النسبة المئوية لمدى المطابقة.....(٣)

المبحث الثاني :- الإطار النظري للبحث

اولا:- تعريف امن المعلومات Information Security Define

مع التطور السريع في جمع وحفظ المعلومات واستخدام التكنولوجيا الحديثة في التعامل بالمعلومات ومع دخول الحواسيب الإلكترونية في مختلف مراحل بناء المنظومة المعلوماتية ، فضلا عن التطورات المتسارعة من حيث الإمكانات والتقنيات المتقدمة فقد بات من الضروري الحفاظ على المعلومات ووضع الأسس والثوابت الكفيلة بالحفاظ عليها وتحديد الاجراءات الوقائية لمنع تسربها والسطو عليها (السالمي واخرون، ٢٠٠٦: 24)

تعرف المواصفة الدولية (ISO/IEC 27000: 2009) أمن المعلومات على انها" وقاية لسرية وسلامة وتكامل واتاحة للمعلومات، فضلاً عن التأصيل (توثيق المصدر) والمسؤولية وعدم الانكار والاعتمادية.

تعرف المواصفة الدولية (ISO/IEC 27002:2013) أمن المعلومات هو حماية المعلومات والحفاظ عليها ، اذ تتضمن هذه المعلومات السرية والنزاهة والاتاحة .

ويعرف أمن المعلومات بأنه "حماية نظم المعلومات والمعلومات من الوصول غير المصرح به أو الاستخدام أو الإفصاح أو التعطيل أو التعديل أو التدمير "ووفقا للقانون الأمريكي في جوهرها، فهذا يعني حماية البيانات والانظمة من أولئك الذين يسعون إلى إساءة استخدامها.(Andress,2011:1)

ثانيا:- أهمية أمن المعلومات واهدافها The importance & goal of information

تنبع أهمية أمن المعلومات من ان المعلومات تستخدم من قبل الجميع بلا استثناء، وهي هدف للاختراق من قبل الجميع ، وفي بعض الاحيان تكون المعلومات هي الفيصل بين المكسب والخسارة للمنظمات وقد تكلف الفرد ثروته وربما حياته في بعض الأحيان(Cakmak&Eroglu,2016:9) وتزداد أهميتها في المنظمات الأمنية والعسكرية والاقتصادية ذات الطابع الاستراتيجي، لذلك ارتبط عنصر السرية بالمعلومات ودرجة توافرها، في ضوء ما يترتب على فقدانها من خسائر وما يترتب على توافرها من مكاسب (القحطاني، ٢٠٠٨: ٢٠).

ان 75% من كبار المديرين في المملكة المتحدة، على سبيل المثال يدعون الآن إلى عدّ أمن المعلومات أولوية عليا، اذ ان متوسط أنفاق شركة بريطانية ما يقارب (4-5٪) من الميزانية على أمن المعلومات، اذ اصبحت المشكلة الان ليس الحصول على المعلومات ، وانما كيفية حماية هذه المعلومات من الأخطار التي تهددها (Calder & Watkins, 2008: 11)

اما الهدف الأساسي لأمن المعلومات فهو الدقة وسلامة وأمان كل العمليات ومصادر نظام المعلومات، كما ان ادارة الأمن يمكن أن تقلل الأخطاء والاحتيال وخسائر في النظام الذي يربط كل من المنظمة وزبائنها واصحاب المصالح (عبد الكريم والربيعي ، ٢٩٨:2013)

فضلا عن ذلك فإن أمن وسرية المعلومات يتضمن تحديد جميع الثغرات الامنية في المراقبة المحتملة التي قد تسمح للأفراد غير المصرح لهم الوصول إلى النظام، لذلك يجب على ادارة المنظمة إن يكون على دراية باستعمال التقنيات المعروفة جميعها لأمن النظام للتغلب على الثغرات الامنية (Tipton& Krause, 2006: 7).

ثالثا:- مبادئ أمن المعلومات The Principles information security

ترتكز امن المعلومات على ثلاثة مبادئ اساس وهي (ISO/IEC27002, 2013: 10)(Arnason & Willett, 2008: 20)

١. **السّرية Confidentiality** : (بما في ذلك الخصوصية) - ضمان أن المعلومات (الحساسة أو الخاصة) يمكن الوصول إليها فقط لأولئك الافراد المخولين بالحصول عليها وعدم اظهارها لغير الافراد المخولين قانونا، ويوافر هذا المبدأ للمنظمة السرية التامة للمعلومات كافة، حتى لو كانت المعلومات صغيرة وبسيطة ومنها (المعلومات الشخصية والموقف المالي لمنظمة ما قبل اعلانه والمعلومات العسكرية وغير ذلك).

٢- **السلامة والكمال Integrity** : يجب التأكد من ان المعلومات لم تغير أو 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 بإضافة اصفار)، ان النظام الأمن يؤمن تكاملية البيانات المخزنة فيه، فالمقصود بالتكاملية حماية البيانات من عمليات الحذف والتخريب ،ويجري تأمين ذلك من خلال مجموعة من الاساليب توفرها نظم قواعد البيانات فضلا عن علاقات الترابط ما بين البيانات المخزونة فيها . عرفت المواصفة (ISO27002:2013) السلامة او النزاهة (بأنها صون دقة واكتمال المعلومات وطرائق المعالجة لها).

١- **الأتاحية Availability** : بمعنى ان تكون المعلومات والحواسيب متاحة للأفراد المخولين باستعمالها لان المعلومات تصبح غير ذات قيمة اذا كان من يحق له الاطلاع عليها لا يمكنه الوصول اليها أو أن الوصول اليها يحتاج الى وقت طويل، وقد يتخذ المهاجمون وسائل عده لحرمان المستفيدين من الوصول الى المعلومات، ومن هذه الوسائل حذف المعلومات ذاتها او مهاجمة الاجهزة التي تخزن المعلومات فيها وشّلها عن العمل، كذلك فإن النظام الأمن يؤمن استمرارية وصول المستخدمين الى المعلومات الخاصة بهم بلا تأخير.

يتضح مما تقدم ان مبادئ أمن المعلومات ذات أهمية متساوية ، مما دفع المختصين بوضعها في اركان مثلث متساوي الاضلاع الذي سمي(ثالوث أمن المعلومات)

رابعا:- مفهوم المواصفة القياسية (ISO 27001:2013)

تتعرض معظم المنظمات الى العدوان على معلوماتها ومحاولة سرقتها والعبث بها. وهذا مايشكل الجانب السلبي للتطور التكنولوجي لنظام المعلومات، فالجرائم المتحققة عن هذا العدوان تتميز عن الجرائم العادية بسرعتها الفائقة وتأثيرها المدمر، وقدرة مرتكبيها على الافلات من الملاحقة والعقاب في ظل افتقاد كثير من الدول نظم قانونية قادرة على التعامل مع هذا العدوان والجرائم الناجمة عنه، وتشير الاحصاءات الدولية الى ان هناك اكثر من مليار شخص مستخدم لأجهزة الحاسب الالي ، فضلا عن وجود أكثر من (١٣) مليار صفحة على شبكة المعلومات الدولية (الانترنيت) ونحو (٣٠٠) مليون موقع. وهكذا اتسعت البيئة المعلوماتية لتصبح ميدانا فسيحا للعدوان عليها ، وقد بينت دراسة للأمم المتحدة عن مخاطر الحاسب الالي ان (٧٣%) من الجرائم داخلي و(٢٣%) منها يرجع الى مصادر خارجية وقدرت الخسائر الاقتصادية لهذه الجرائم عام (١٩٩٣) بنحو (٢) مليار دولار، ومن أجل الوقوف بوجه هذا العدوان، أصدرت منظمة التقييس العالمية للمواصفات العالمية المواصفة القياسية (ISO27001). المختصة بإدارة امن المعلومات، وتأتي هذه المواصفة مقابل للمعيار البريطاني المعروف ببوليفيانو BS-7799 . (الطائي واخرون، ٢٠٠٩: ٤١٦)

خامسا:- سلسلة المواصفات (ISO 2700X)

قررت منظمة التقييس العالمية (ISO) واللجنة الفرعية المنبثقة لتوحيد مواصفات أمن المعلومات في سلسلة (ISO 2700X) لعدد من المواصفات التي نشر بعضها (ولا يزال

بعضها الاخر قيد التطوير)والتي تضم عددا من المكونات الهيكلية الهامة، اذ تركز هذه المكونات على المواصفات المرجعية الموحدة التي تصف متطلبات نظم ادارة امن المعلومات (ISO27001) ومتطلبات جهات منح الشهادات (ISO 27006) للتوافق مع المواصفة، بينما تقدم مواصفات اخرى ارشادات توجيهية في العديد من جوانب تطبيق مواصفات نظم ادارة امن المعلومات (ISO/IEC 27000:2009) ، وتتضمن عائلة المواصفات القياسية) (ISO2700Xالمواصفات الاتية (Sewuster, 2015: 7)

١. ISO / IEC 27000: 2009، نظم إدارة أمن المعلومات - نظرة عامة والمفردات
٢. ISO / IEC 27001: 2005، نظم إدارة أمن المعلومات – المتطلبات
٣. ISO / IEC 27002: 2005، مدونة قواعد الممارسة لإدارة أمن المعلومات
٤. ISO / IEC 27003: 2010، ارشادات تنفيذ نظام ادارة امن المعلومات
٥. ISO / IEC 27004: 2009، وإدارة أمن المعلومات – مقياس
٦. ISO / IEC 27005: 2011 أدارة مخاطر أمن المعلومات
٧. ISO / IEC 27006: 2011، متطلبات هيئات تقديم خدمات التدقيق ومنح الشهادات لنظم إدارة أمن المعلومات
٨. ISO / IEC 27007: 2011، مبادئ توجيهية لنظم إدارة التدقيق أمن المعلومات
٩. ISO / IEC 27008: 2011، مبادئ توجيهية للمدققين بشأن ضوابط أمن المعلومات
١٠. ISO/IEC27010: 2012، إدارة أمن المعلومات للاتصالات بين القطاعات وبين المنظمات.

سادسا:-:- فوائد تطبيق المواصفة (ISO 27001:2013)

يساعد تطبيق المواصفة (ISO27001) المنظمات في مقارنة نفسها مع المنافسين وتوفير المعلومات ذات الصلة بأمن تكنولوجيا المعلومات للزبائن، وتمكن الإدارة من إظهار العناية الواجبة وتعزز كفاءة إدارة التكاليف الأمنية والامتثال للقوانين واللوائح بسبب مجموعة مشتركة من المبادئ التوجيهية التي تتبعها المنظمة الشريكة. ويساعد الحصول على الشهادة في التركيز على التحسين المستمر لعمليات امن المعلومات في المنظمة، وتضمن الشهادة ايضاً المراجعة الخارجية الدورية والتي يعتمد عليها لاستمرار صلاحية الحصول على الشهادة، اذ يهييء اي نظام يلتزم بالمواصفة(ISO 27001) اسلوب منظم لتحديد المخاطر المحتملة وسبل مواجهتها، ويمكن ايجاز فوائد تطبيق المواصفة والحصول على الشهادة الاتي (:ISO27001) 2013 (Hinson, 2008: 3)

١. دمج أمن المعلومات في إدارة المنظمة
٢. الشهادة هي واحدة من العوامل الرئيسية التي تؤثر على منافسة الاعمال .
٣. العاملون مسؤولون عن تأمين معلومات مساحة العمل وبيانات عملائهم.
٤. تضمن متطلبات التحسين المستمر فاعلية إدارة الموارد على المدى الطويل.
٥. شفافية الحادث وتجنبه والكشف عن المخاطر والتناقضات والحوادث ذات التأثير غير المرغوب فيه.

٦. زيادة مصداقية الأعمال للمستثمرين والبنوك وشركات التأمين.
٧. وفورات ناتجة عن العقوبات المتعلقة بتسرب المعلومات.

سابعا:- نظام ادارة امن المعلومات على وفق المواصفة (ISO 27001: 2013)

ان التطور السريع في عالم جرائم الحاسوب والتغييرات البيئية المتسارعة، جعل المختصون يهتمون بتحديد جهة مختصة لإدارة هذه التغيرات ومواكبتها وسد الثغرات، لذا كان ضروريا أن تنشأ ادارة تعنى بإدارة الأمن ومهيأة بملاكات ذوو خبرة، على ان تتمتع هذه الإدارة باستقلالية تامة وان يكون موقعها في الهيكل التنظيمي في موضع يجعلها تعمل بفاعلية ودون مؤثرات وضغوط من الادارات الأخرى، وتستمد هذه الإدارة قوتها من قناعة ودعم الادارة العليا للمنظمة . (BSI ,2006)

لذا أصبح نظام إدارة أمن المعلومات (ISMS) ضروريا لمواجهة التهديدات الموجهة، نظرا لتوافر ونزاهة وسرية امن المعلومات التي أصبحت كبيرة ، وبذلك وضعت منظمة المعايير الدولية (ISO) وصفاً لنظام ادارة امن المعلومات (ISMS) بانه جزءاً من نظام الادارة الكلي، والذي يعمل داخل المنظمة على تطبيق قواعد الجودة، فضلاً عن وضع وتطبيق اجراءات وقواعد أمن المعلومات (Arnason & Willett,2008,14)، ووصفته بأنه ((الإطار والمنهجية التي تستخدمها الإدارة لإدارة المخاطر على أصولها المعلوماتية. و(ISMS) وهو عملية إدارة مستمرة تهدف إلى تحسين الضوابط الأمنية باستمرار .ويتمثل الهدف العام للنظام في ضمان تحديد المعلومات الأمنية بشكل صحيح، وإدارتها بفاعلية وكفاءة)) ,ISO/IEC 27002) (2013: 4)

ثامنا:- فوائد نظام ادارة امن المعلومات (ISMS)

هناك فوائد كثيرة يتوخى الحصول عليها من اقامة نظام لادارة امن المعلومات في المنظمات (Sojcik,2012:11)(Calder&Watkins ,2008:20)

١- يوافر فرصة لتحديد المخاطر وإدارتها بشكل منهجي
٢- يسمح بإجراء مراجعة مستقلة لممارسات أمن المعلومات
٣- يوافر نهج شامل قائم على المخاطر لتأمين المعلومات
٤- إثبات المصداقية لأصحاب المصلحة
٥- يوضح الحالة الأمنية وفقا للمعايير المقبولة دوليا
٦- يخلق ميزة تنافسية للمنظمة في السوق
٧- تعتمد مرة واحدة ويكون الاعتماد عالميا
٨- دمج أمن المعلومات في إدارة المنظمة
٩- الشهادة هي واحدة من العوامل الرئيسة التي تؤثر على منافسة الاعمال .

تاسعا:- بنود المواصفة (ISO27001: 2013) لإصدار بين (٢٠٠٥ و٢٠١٣)

الجدول (٢) يوضح بنود المواصفة (ISO27001: 2013) لإصدارين (٢٠٠٥ و٢٠١٣)

جدول (٢)
بنود المواصفة (ISO/IEC 27001) لإصداريين (2005 و2013)

ISO 27001: 2013	ISO 27001:2005
4- سياق المنظمة	4 - نظام ادارة امن المعلومات
4.1- فهم المنظمة وسياقها	4.1 - متطلبات عامة
4.2- فهم حاجات وتوقعات الاطراف المهمة	4.2 - انشاء وادارة ISMS
4.3 تحديد مجال نظام ادارة امن المعلومات	4.2.1 - انشاء ISMS
4.4 نظام ادارة امن المعلومات	4.2.2 - تنفيذ وتشغيل ISMS
	4.2.3- مراقبة ومراجعة ISMS
	4.2.4- صيانة وتحسين SMS
	4.3- متطلبات التوثيق
	4.3.1 – عام
	4.3.2 - ضبط الوثائق
	4.3.3 - ضبط السجلات
5- القيادة	5 - مسؤولية الادارة
٥.١ القيادة والالتزام	5.1 - التزام الادارة
٥.٢ السياسة	5.2 - ادارة الموارد
٥.٣ الادوار المنظمية، المسؤوليات والسلطات	5.2.1 - توفير الموارد
	5.2.2 - التدريب والتوعية والكفاءة
6- التخطي	6 - التدقيق الداخلي ISMS
6.1 – اجراءات تناول المخاطر والفرص	
6.1.1- عام	
6.1.2- تقييم مخاطر امن المعلومات	
6.1.3- معالجة مخاطر امن المعلومات	
6.2- اهداف امن المعلومات والتخطيط لتحقيقها	
7- الدعم	7 - مراجعة الادارة ISMS
7.1- الموارد	7.1 – عام
7.2- الكفاءة	7.2 - مدخلات المراجعة
7.3- الوعي	7.3 - مخرجات المراجعة
7.4- الاتصالات	
7.5- المعل مات الموثقة	
7.5.1- عام	
7.5.2- انشاء وتحديث	
7.5.3- رقابة المعلومات الموثقة	
8- العملية	8 - تحسين ISMS
8.1- التخطيط العملياتي والرقابة	8.1 - التحسين المستمر
8.2- تقييم مخاطر امن المعلومات	8.2 - الاجراء التصحيحي
8.3-معالجة مخاطر امن المعلومات	
9.1- المراقبة والقياس والتحليل والتقويم	
9.2- التدقيق الداخلي	
9.3– المراجعة الادارية	
10- التحسين	
10.1- اللاتطابق والاجراء التصحيحي	
10.2- التحسين المستمر	

المبحث الثالث: الاطار العملي

لغرض الاجابة عن التساؤل الاول للبحث وتحقيق الهدف الاول منها، سيجري ضمن هذا المبحث تقييم واقع توافر متطلبات نظام ادارة امن المعلومات على وفق المواصفة (ISO 27001: 2013) في الشركة العامة للأنظمة الالكترونية/ مركز البيانات باعتماد قوائم الفحص التي تتضمن عددا من المتطلبات الرئيسة والفرعية والتي سيجرى تحليلها ومناقشتها كما يأتي :

أولا:- عرض نتائج قائمة فحص بنود المواصفة المبحوثة في الشركة العامة للأنظمة الالكترونية/ مركز البيانات

سيجري ضمن هذه الفقرة قياس مدى توافر متطلبات المواصفة (ISO 27001: 2013) في الشركة بإعتماد قوائم الفحص لقياس فجوة التطبيق، وتحليلها على وفق المواصفة، وابتداءا من البند الرابع نظرا لكون البنود الثلاثة الأول عامة.

4- سياق المنظمة :

1.4: فهم المنظمة وسياقها

على المنظمة ان تقرر القضايا الخارجية والداخلية ذات الصلة بغرضها والتي تؤثر في قابليتها على تحقيق النتائج المرجوة لنظام ادارتها لامن المعلومات [ISO/IEC27001:2013(E) 1] ، اذ يعد تحديد متطلبات امن المعلومات المحور الاساس لفهم سياق عمل المنظمة ، والتي تندرج في احتياجات امن المعلومات والتوقعات، ولتاخذ بنظر الاعتبار القضايا الداخلية والخارجية ، والتي من شانها ان تؤثر في تنفيذ نظام ادارة امن المعلومات (ISMS) في المنظمة ، وتشمل القضايا الخارجية مثلاً : مقدمي سحابة الحوسبة (Cloud Computing Providers) ، في حين ان القضايا الداخلية قد تدور بشان التغييرات في الادارة ومتطلبات الاعمال

تظهر قائمة الفحص في الجدول (٣) مدى تنفيذ متطلبات سياق المنظمة / البند (١.٤) وتوثيقها في الشركة العامة للأنظمة الالكترونية / مركز البيانات مقارنة بالمواصفة الدولية (ISO 27001: 2013)

جدول (٣)

قائمة فحص متطلب فهم المنظمة وسياقها

١.٤: فهم المنظمة وسياقها تقوم المنظمة بتقرير القضايا الخارجية والداخلية ذات الصلة بغايتها	٦	٥	٤	٣	٢	١	٠
١.تجري تحديد القضايا الداخلية والخارجية في نظام إدارة أمن المعلومات.				□			
٢. تعيين القضايا الداخلية والخارجية ذات الصلة بغاية الهياة وقدرتها لتحقيق النتائج المرتقبة لنظام ادارة امن المعلومات (ISMS).				□			
التكرارات				٢			
النتيجة				٦			
الوسط الحسابي المرجح	٣						
النسبة المئوية لمدى المطابقة	٥٠%						
حجم الفجوة (%)	٥٠%						

يتضح من خلال نتائج قائمة الفحص في الجدول (٣) مستوى التوثيق والتطبيق الفعلي لبند (١.٤) فقد حققت الشركة وسطا حسابيا قدرة (٣) من اصل (٦) درجات، وبنسبة مطابقة (٥٠%)، مما يشير الى وجود فجوة أساس لعدم المطابقة بنسبة (٥٠%) تعود الى :

١- أن التوثيق للقضايا الداخلية متوفر في الشركة مثل منتجات الشركة والمراكز الوظيفية للموظفين وميزانية الشركة والجرد السنوي، إلا أنه غير مكتمل لعدم اعتماد مبدأ المعلومات الموثقة الذي استند عليه الاصدار الجديد من المواصفة (ISO/IEC 27001:2013) .

٢- ضعف في توثيق جميع خدمات سحابة الحوسبة، اذ تعد من القضايا الخارجية، التي تشتمل على الخدمات المرتبطة بالأنترنت جميعها.

٢.٤: فهم حاجات وتوقعات الاطراف المهتمة

على المنظمة تحديد: [ISO/IEC27001:2013(E)1]

أ) الاطراف المهتمة ذات الصلة بنظام ادارة امن المعلومات .

ب) متطلبات هذه الاطراف المهتمة ، ذات الصلة بامن المعلومات.

يعكس البند الحالي من المعيار اهمية التعامل مع الاطراف الخارجية ذات الصلة بنظام إدارة امن المعلومات وبما يتطلب من ضوابط تمنح الزبائن حق الوصول الى معلومات المنظمة.

تظهر قائمة الفحص في الجدول (٤) مدى توافر متطلب فهم حاجات وتوقعات الاطراف المهتمة/البند (٢.٤) وتوثيقها في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013)

جدول (٤)

قائمة فحص متطلب فهم حاجات وتوقعات الاطراف المهتمة

٢.٤: فهم حاجات وتوقعات الاطراف المهتمة	٦	٥	٤	٣	٢	١	٠
٣. تحدد المنظمة الاطراف المهتمة ذات الصلة بنظام ادارة امن المعلومات	□						
٤. تحدد المنظمة متطلبات الاطراف المهتمة .	□						
التكرارات	٢						
النتيجة	١٢						
الوسط الحسابي المرجح	٦						
النسبة المئوية لمدى المطابقة	١٠٠%						
حجكم الفجوة(%)	٠%						

يتضح من خلال نتائج قائمة الفحص في الجدول (٤) مستوى توثيق وتطبيق بند (٢.٤)، اذ حققت الشركة وسطا حسابيا قدره (٦) من اصل (٦) درجات، وبنسبة مطابقة (١٠٠%)، مما يشير الى عدم وجود فجوة (٠%) بين البنود وواقع التطبيق وذلك ناجم عن التطبيق والتوثيق الكلي للبند وهو يعود الى:-

١- تحديد متطلبات الجهات المستفيدة ،اذ تتعامل الشركة مع طيف واسع من الزبائن (مثل الجهات الطالبة للأنظمة البرمجية) و(الجهات التي تقوم بتخزين بيانتها في مركز البيانات) والمستشارين
(مثل : منظمة CISCO وMicrosoft) والطلاب الراغبين بتطبيق بحوثهم في مختبرات الشركة، وفي الشركة مختبرات تخصصية مجهزة من شركات عالمية تختص هذه المختبرات بتدريب وتأهيل ملاكات الشركة وملاكات الوزارات والشركات الاخرى من خلال اعداد جدول بالدورات التدريبية مستمرة على طول السنة، والتعاون مع طلبة الدراسات العليا. وأهم هذه المختبرات :

, Seimens Lab, Schneider Lab ,Allen- Bradely Lab)
Honeywell Lab, Microsoft Lab, Mikro Tik Lab, Cisco Lab)

٣.٤: تحديد مجال نظام ادارة امن المعلومات

على المنظمة تحديد حدود وامكانية تطبيق نظام ادارة امن المعلومات لانشاء مجالها، وعند تحديد مجالها ، ينبغي على المنظمة مراعاة كل من الآتي: [ISO/IEC27001:2013 (E)2]

أ) القضايا الخارجية والداخلية المشار اليها في البند(4.1).

ب) المتطلبات المشار اليها في البند(4.2).

ج) التداخل بين الانشطة التي تؤديها المنظمة ، وتلك التي تؤديها منظمات اخرى ، وينبغي توافر واتاحة المجال كمعلومات موثّقة .

يمثل مجال نظام ادارة امن المعلومات (ISMS) امراً بالغ الاهمية، ويشير الى اي مدى يتم تطبيق (ISMS) في المنظمة. تظهر قائمة الفحص في الجدول (٥) مدى توافر متطلب تحديد مجال نظام ادارة أمن المعلومات/البند(٣.٤) وتوثيقها في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013) .

جدول (٥)

قائمة فحص متطلب تحديد مجال نظام ادارة امن المعلومات

٣.٤: تحديد مجال نظام ادارة امن المعلومات	٦	٥	٤	٣	٢	١	٠
٥. تحدد المنظمة امكانيتها في تطبيق نظام ادارة امن المعلومات.				□			
٦. تحدد المنظمة المجال مع الاخذ بنظر الاعتبار القضايا الداخلية والخارجية.				□			
٧. تعين المنظمة دليل لنظام ادارة امن المعلومات متضمناً مجال ISMS .						□	
التكرارات				٢		١	
النتيجة				٦		١	
الوسط الحسابي المرجح	٢.٣٣						
النسبة المئوية لمدى المطابقة	%٣٨						
حجم الفجوة (%)	%٦٢						

يتضح خلال نتائج قائمة الفحص في الجدول (٥) مستوى التوثيق والتطبيق لبند (٣.٤)، فقد حققت وسطا حسابيا قدرة (٢.٣) من أصل (٦) درجات، وبنسبة مطابقة (٣٨%)، مما يشير الى وجود فجوة اساس لعدم المطابقة بنسبة (٦٢%) ويعود ذلك الى:

- تحدد الشركة امكانية تطبيق نظام إدارة أمن المعلومات وتحدد المجال في (مركز البيانات Data Center)، وهو عبارة عن وحدة مركزية تجميعية للبيانات والمعلومات لكافة المؤسسات العراقية الراغبة في خزن بيانتها وإدارتها من خلال التطبيقات الالكترونية المستعملة، ويعد من المشروعات الرائدة في بناء القواعد الأساس لمشروع الحكومة الالكترونية التي تسهم في تحقيق السرعة والدقة والامان وحماية المعلومات والبيانات، الا انها لاتوثق ذلك بشكل كامل ولايوجد امر اداري بتطبيق النظام على وفق متطلبات المواصفة (ISO 27001: 2013).

٤.٤.: نظام ادارة امن المعلومات (ISMS)

ينبغي للمنظمة انشاء وتنفيذ وصيانة وتحسين مستمر لنظام ادارة امن المعلومات، وبالتوافق مع متطلبات المواصفة الدولية [ISO/IEC27001:2013(E)2].

تظهر قائمة الفحص في الجدول (٦) مدى توافر متطلب نظام ادارة امن المعلومات / البند(٤.٤) وتوثيقه في الشركة مقارنة بالمواصفة الدولية (ISO27001:2013)

جدول(٦)

4.4: نظام ادارة امن المعلومات (ISMS) ينبغي للمنظمة انشاء وتنفيذ وصيانة نظام ادارة امن المعلومات ، بالتوافق مع متطلبات هذا المعيار الدولي ويجب ان تقوم بما يلي :	٦	٥	٤	٣	٢	١	٠
٨. انشاء وتنفيذ (ISMS) على وفق متطلبات(ISO/IEC27001:2013) .						□	
٩.تحدد المنظمة طريقة لانشاء نظام ادارة امن المعلومات .						□	
١٠.تحدد المنظمة طريقة لصيانة نظام ادارة امن المعلومات (ISMS) في المنظمة.						□	
١١.تعمل على تحقيق التحسين المستمر في نظام ادارة امن المعلومات وفقاً للمعيار (ISO/IEC27001:2013) .							□
التكرارات						3	1
النتيجة						3	0
الوسط الحسابي المرجح	0.75						
النسبة المئوية لمدى المطابقة	%١٢						
حجم الفجوة (%)	%٨٨						

قائمة فحص متطلب نظام ادارة امن المعلومات

يتضح من خلال نتائج قائمة الفحص في الجدول (٦) مستوى التوثيق والتطبيق لبند (٤.٤)، اذ حققت وسطا حسابيا قدره (٠.٧٥) من اصل (٦) درجات، وبنسبة مطابقة (١٢%)، مما يشير وجود فجوة اساسية لعدم المطابقة بنسبة (٨٨%) ويعود ذلك الى

١- لايوجد توثيق لآلية انشاء نظام إدارة أمن المعلومات على وفق المواصفة (ISO/IEC27001:2013)، أما التطبيق فهو جزئي .

٢- لاتوجد خطوات عملية لأنشاء وتنفيذ نظام ادارة امن المعلومات على وفق المواصفة (ISO/IEC27001:2013)، بالرغم من مواكبة الشركة لعملية التطور المتسارعة في مجال حماية المعلومات وادارة امنها.

٥ـ القيادة

٥.١: القيادة والالتزام

على الادارة العليا اثبات القيادة والالتزام فيما يخص نظام ادارة امن المعلومات عن طريق [ISO/IEC 27001:2013(E)2] :

أـ ضمان سياسة لامن المعلومات وضمان ترسيخ اهداف امن المعلومات وانسجامها مع الاتجاه الإستراتيجي للمنظمة.

بـ ضمان دمج متطلبات نظام ادارة امن المعلومات في عمليات المنظمة .

جـ ضمان توافر واتاحة الموارد المطلوبة لنظام ادارة امن المعلومات.

دـ ايصال اهمية ادارة امن معلوماتي فاعل وتطابقها مع متطلبات نظام ادارة امن المعلومات.

هـ ضمان ان يحقق نظام ادارة امن المعلومات نتائجه المرجوة .

وـ توجيه ودعم الافراد للمساهمة في فاعلية نظام ادارة امن المعلومات.

زـ تعزيز التحسن المستمر.

تظهر قائمة الفحص في الجدول (٧) مدى توافر متطلب القيادة والالتزام / البند(٥.١) وتوثيقه في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013)

جدول (٧) قائمة فحص متطلب القيادة والالتزام

٥.١: القيادة والالتزام على الادارة العليا اثبات القيادة والالتزام فيما يخص نظام ادارة امن المعلومات عن طريق	٦	٥	٤	٣	٢	١	٠
١٢.وضع سياسة لنظام ادارة امن المعلومات والمصادقة عليها من قبل الادارة العليا.							□
١٣. تحدد المنظمة اهداف (ISMS) المتوافقة مع الاتجاه الاستراتيجي للمنظمة والمصادقة عليها.						□	
١٤.ضمان دمج متطلبات نظام ادارة امن المعلومات في عمليات المنظمة.					□		
١٥.ضمان توافر الموارد المطلوبة لنظام ادارة امن المعلومات.					□		
١٦.ايصال اهمية ادارة امن المعلومات وتطابقها مع متطلبات نظام ادارة امن المعلومات الى جميع العاملين لضمان نتائج مرجوة .					□		
١٧.ضمان ان يحقق نظام ادارة امن المعلومات نتائجه المرجوة.					□		
١٨.توجيه ودعم الافراد للمساهمة في فاعلية نظام ادارة امن المعلومات .				□			
١٩. تعزيز التحسين المستمر.				□			
٢٠. دعم ادوار الدوائر الاخرى ذات الصلة.					□		
التكرارات				٢	٥	١	١
النتيجة				٦	١٠	١	٠
الوسط الحسابي المرجح	١.٨٨						
النسبة المئوية لمدى المطابقة	%٣١						
حجم الفجوة (%)	%٦٩						

يتضح من خلال نتائج قائمة الفحص في الجدول (٧) مستوى التوثيق والتطبيق لبند (٥.١)، اذ حققت وسطا حسابيا قدره (١.٨٨) من اصل (٦) درجات، وبنسبة مطابقة (٣١%)، مما يشير الى وجود فجوة اساسية لعدم المطابقة بنسبة (٦٩%) ويعود ذلك الى:

١- لاتوجد اهداف خاصة بأمن المعلومات معلنة في دليل الشركة، وعدم وجود سياسة لأمن المعلومات مكتوبة ومصادق عليها من الادارة العليا على وفق المواصفة (ISO 27001)

2- ضعف التخصيص المالي لأنشاء نظام ادارة امن المعلومات بالمعنى المستقل على وفق متطلبات المواصفة، ولكن كل قسم في الشركة يقدم حاجته من الموارد المالية من ميزانية الشركة على وفق الابواب المعروفة ولا يوجد باب خاص بإدارة امن المعلومات.

2.5: السياسة:

ينبغي على الادارة العليا انشاء سياسة لامن المعلومات تكون :[ISO/IEC27001:2013(E)2]

أ- ملائمة لغرض المنظمة .

ب- تشمل اهدافًا لامن المعلومات (البند-6.2) او توفر اطاراً لوضع اهدافٍ لامن المعلومات.

ج- تتضمن التزاماً بتلبية المتطلبات المطبقة ذات الصلة بامن المعلومات.

د- تتضمن التزاماً بالتحسين المستمر لنظام ادارة امن المعلومات.

ينبغي ان تكون سياسة امن المعلومات:

ه- متوافرة ومتاحة كمعلومات موثقة.

و- متناقلة داخل المنظمة.

ز- إتاحتها للأطراف المهتمة ، كلما كان ذلك مناسباً.

تظهر قائمة الفحص في الجدول (٨) مدى توافر متطلب السياسة / البند(٢.٥) وتوثيقه في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013) .

جدول (٨) قائمة فحص متطلب السياسة

٢.٥ :السياسة ينبغي على الادارة العليا انشاء سياسة لأمن المعلومات تكون:	٦	٥	٤	٣	٢	١	٠
٢١. ملائمة السياسة لأغراض المنظمة .							□
٢٢. تتضمن السياسة اهداف امن المعلومات او اطار لتحديد اهداف امن المعلومات.							□
٢٣. تتضمن التزاماً بتلبية المتطلبات ذات الصلة بأمن المعلومات.							□
٢٤. تتضمن التزاما بالتحسين المستمر لنظام ادارة امن المعلومات.							□
٢٥. متوفرة ومتاحة كمعلومات موثقة.							□
٢٦. مبلغة ومفهومة للأفراد داخل المنظمة.							□
٢٧.تكون متاحة للأطراف المهتمة .							□
التكرارات							7
النتيجة							0
الوسط الحسابي المرجح	0						
النسبة المئوية لمدى المطابقة	%0						
حجم الفجوة(%)	%100						

يتضح من خلال نتائج قائمة الفحص في الجدول (٨) مستوى التوثيق والتطبيق لبند (٢.٥)، فقد حققت وسطا حسابيا قدره (0) من اصل (٦) درجات، وبنسبة مطابقة

(0%)، مما يشير الى وجود فجوة اساسية لعدم المطابقة بنسبة (100%) ويعود ذلك الى :

١- عدم وجود سياسة موثقة خاصة بنظام أدارة أمن المعلومات ومعلنة للجميع لنظام ادارة امن المعلومات.

٢- الاعتماد على السياسات والتعليمات التي تصاحب البرامج والمعدات في التنصيب والتشغيل والادامة وهي مقتصرة على عدد محدود من المختصين.

3.5:الادوار المنظمية والمسؤوليات والسلطات

ينبغي على الادارة العليا ضمان ان تحدد المسؤوليات والسلطات عن الادوار ذات الصلة بامن المعلومات وان يتم تناقلها، وينبغي على الادارة العليا تعيين المسؤولية والسلطة عن طريق :][ISO/IEC27001:2013(E)3

أ) ضمان ان يتطابق نظام ادارة امن المعلومات مع متطلبات المواصفة الدولية .

ب) رفع تقارير بشان اداء نظام ادارة امن المعلومات الى الادارة العليا

تظهر قائمة الفحص في الجدول (9) مدى توافر متطلب الادوار المنظمية والمسؤوليات والسلطات / البند(٣.٥) وتنفيذه في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013) .

جدول (9)

قائمة فحص متطلب الادوار المنظمية والمسؤوليات والسلطات

٣.٥:الادوار المنظمية والمسؤوليات والسلطات: ينبغي ان تضمن الادارة العليا :	٦	٥	٤	٣	٢	١	٠
٢٨. تطابق نظام ادارة امن المعلومات مع متطلبات المعيار (ISO/IEC27001:2013).						□	
٢٩. توثيق الوصف الوظيفي متضمناً المسؤوليات والسلطات للأدوار ذات الصلة بأمن المعلومات.					□		
٣٠. رفع تقارير بخصوص اداء نظام ادارة امن المعلومات الى الادارة العليا.					□		
التكرارات					٢	١	
النتيجة					٤	١	
الوسط الحسابي المرجح	١.٦٦						
النسبة المئوية لمدى المطابقة	٢٨%						
حجم الفجوة (%)	٧٢%						

يتضح من خلال نتائج قائمة الفحص في الجدول (9) مستوى التوثيق والتطبيق لبند (٣.٥)، فقد حققت وسطا حسابيا قدره (١.٦٦) من اصل (٦) درجات، وبنسبة مطابقة (٢٨%)، مما يشير الى وجود فجوة اساسية لعدم المطابقة بنسبة (٧٢%) ويعود ذلك الى :

١- لا يوجد فصل للمهام والمسؤوليات والصلاحيات بشكل دقيق ووفقا للمواصفة (ISO 27001: 2013) .

٢- اعتمد الوصف الوظيفي الحالي في المركز الذي وضع استناداً للأمر الاداري المرقم (998)

ذي العدد (4952) في (21-8-2011) مبدا الشخص المناسب في المكان المناسب ولكن لا يتضمن الوظائف ذات الصلة بأمن المعلومات بشكل كامل .

٦- التخطيط

١.٦:اجراءات تناول المخاطر والفرص

عند التخطيط لنظام ادارة امن المعلومات ، ينبغي على المنظمة مراعاة القضايا المشار اليها في (البند- 4.1 والبند-4.2) وتحديد المخاطر والفرص ودراستها لتحقيق كل من الآتي : (ISO/IEC27001:2013(E)3)

أ) ضمان ان يحقق نظام ادارة امن المعلومات نتائجه المرجوة.

ب) منع ، اوتقليل الاثار غير المرغوبة.

ج) تحقيق التحسن المستمر.

وينبغي على المنظمة تخطيط الاجراءات لتناول هذه المخاطر والفرص وكيفية دمج وتنفيذ الاجراءات في عمليات نظام ادارتها لامن المعلومات ، وتقويم فاعلية هذه الاجراءات

تظهر قائمة الفحص في الجدول (10) مدى توافر متطلب اجراءات تناول المخاطر والفرص/ البند(١.٦) وتوثيقه في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013) .

جدول (10)

قائمة فحص متطلب اجراءات تناول المخاطر والفرص

1.6: اجراءات تناول المخاطر والفرص	٦	٥	٤	٣	٢	١	٠
31. ضمان ان يحقق ISMS نتائجه المرجوة.					□		
32. منع او تقليل الاثار غير المرغوبة .				□			
33. تحقيق التحسين المستمر.					□		
وينبغي على المنظمة التخطيط لكل من الاتي:							
34.اجراءات لتناول المخاطر والفرص.				□			
35. القيام بدمج وتنفيذ الاجراءات في عمليات ISMS.					□		
36. تقويم فاعلية الاجراءات.				□			
التكرارات				٣	٣		
النتيجة				٩	٦		
الوسط الحسابي المرجح	٢.٥						
النسبة المئوية لمدى المطابقة	٤٢%						
حجم الفجوة (%)	٥٨%						

يتضح من خلال نتائج قائمة الفحص في الجدول (10) مستوى التوثيق والتطبيق بند (١.٦)، فقد حققت وسطا حسابيا قدره (٢.٥) من اصل (٦) درجات، وبنسبة مطابقة (٤٢%)، مما يشير الى وجود فجوة اساسية لعدم المطابقة بنسبة (٥٨%) ويعود ذلك الى :

- عدم وضع استراتيجية او خطة موثقة من الشركة لتحديد المخاطر واستثمار الفرص، لكن يوجد هناك مجموعة من الاجراءات الموضوعة من الشركة مثلا (وضع جدار

الحماية، عمل نسخ احتياطية للمعلومات المخزنة، ترحيل البيانات الى (الحاسبة الام) التي تكون خارج موقع الشركة، تجديد كلمة السر، لكن هذه الاجراءات غير موثقة، يجب ان توضع خطة لمواجهة المخاطر التي تتعرض لها المعلومات وتنفيذ هذه الخطة بصورة دقيقة لكي تحقق الشركة النتائج المرغوبة وهي حماية المعلومات ومن ثم تحقيق ميزة تنافسية للشركة .

٢.١.٦ :تقييم مخاطر امن المعلومات

ينبغي على المنظمة تحديد وتطبيق عملية تقييم مخاطر امن المعلومات: (ISO/IEC27001:2013(E)4)

أ) التي تتبنى وتحافظ على معايير مخاطر امن المعلومات والتي تشمل:

معايير قبول المخاطر.-اولاً

معايير اداء تقييمات مخاطر امن المعلومات.-ثانياً

ب) تضمن ان تولّد تقييمات مخاطر امن المعلومات المتكررة ، نتائج ثابتة ، وصالحة ومقارنة.

ج) تحدد مخاطر امن المعلومات

د) تُحلِّل مخاطر امن المعلومات

هـ) تقويم مخاطر امن المعلومات تظهر قائمة الفحص في الجدول (١١) مدى توافر متطلب تقييم مخاطر امن المعلومات /المتطلب (١.٦.٢) وتوثيقه في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013)

جدول (١١) قائمة فحص متطلب تقييم مخاطر امن المعلومات

٢.١.٦: تقييم مخاطر امن المعلومات	٦	٥	٤	٣	٢	١	٠
٣٧. ينبغي على المنظمة تحديد عملية تقييم مخاطر امن المعلومات: .أ تحديد عملية تقييم لمخاطر امن المعلومات.				□			
ب. تحديد معيار لأداء تقييمات مخاطر امن المعلومات.							□
٣٨.ضمان ان تولّد تقييمات مخاطر امن المعلومات المتكررة نتائج متماثلة وصالحة.				□			
٣٩. تحديد مخاطر امن المعلومات: أ. عملية تقييم مخاطر امن المعلومات لتحديد المخاطر المرتبطة بفقدان السريّة ودمج وتوفر المعلومات ضمن مجال نظام ادارة امن المعلومات.						□	
ب. تحديد اصحاب المخاطر.						□	
٤٠.تحليل مخاطر امن المعلومات: أ. تقييم العواقب المحتملة و التي تنتج اذا المخاطر حددت وجسدت.						□	
ب. تقييم الاحتمالات الواقعية لحدوث المخاطر المحددة.						□	
ج. تحديد مستويات الخطر .						□	
٤١. تقويم مخاطر امن المعلومات. أ. مقارنة نتائج تحليل المخاطر مع معيار الخطر الموضوع.						□	
ب. وضع اولوية للمخاطر المحللة لمعالجة المخاطر.						□	
التكرارات				٢		٨	
النتيجة				٦		٨	
الوسط الحسابي المرجح	١.٤						
النسبة المئوية لمدى المطابقة	%٢٣						
حجم الفجوة (%)	%٧٧						

يتضح من خلال نتائج قائمة الفحص في الجدول (11) مستوى التوثيق والتطبيق لبند (٢.١.٦)، فقد حققت وسطا حسابيا قدره (١.٤) من أصل (٦) درجات، وبنسبة مطابقة (٢٣%)، مما يشير الى وجود فجوة اساس لعدم المطابقة بنسبة (٧٧%) ويعود ذلك الى :

١- عملية تحديد المخاطر غير موثقة بالكامل (ومنها: عدم وجود توثيق لحالات الاختراق لنظم لمعلومات او اساءة استعمال كلمات السر، أو اعطال الشبكة والحواسيب)، ويجري الاكتفاء فقط بكتابة مذكرات طلب المعالجة للجهات الفنية ويعود سبب ذلك لمنع الاخرين من معرفة الثغرات الامنية على وفق المقابلة مع مدير الخدمات الفنية .

٢- لا يوجد معيار لأداء تقييمات مخاطر أمن المعلومات.

٣- تحليل مخاطر امن المعلومات وفقا لمتطلبات المواصفة ليس بالمستوى المطلوب، فضلا عن ذلك تقييم الاحتمالات لوقوع المخاطر وكذلك تحديد الاولويات .

٣.١.٦:معالجة مخاطر امن المعلومات

ينبغي على المنظمة تحديد وتطبيق عملية معالجة مخاطر امن المعلومات وذلك من خلال: ISO/IEC27001:2013)(

أ) انتقاء خيارات معالجة مخاطر امن المعلومات.

ب) تحديد انواع الضوابط الضرورية لتنفيذ خيارات معالجة مخاطر امن المعلومات المنتخبة جميعاً.

ج) مقارنة انواع الضوابط المحددة في (البند - 6.1.3 ب) مع تلك التي في الملحق(A) والتحقق من عدم حذف اية ضوابط امنية غير ضرورية.
د) انشاء قائمة بامكانية التطبيق تحوي على انواع الضوابط الضرورية في (البند - 6.1.3 ب ، ج) وتبرير انواع الضوابط من الملحق (A) سواء طبقت ام لم تطبق.
ه) صياغة خطة لمعالجة مخاطر امن المعلومات.
ز) الحصول على موافقة اصحاب المخاطر على خطة معالجة مخاطر امن المعلومات وقبول مخاطر امن المعلومات المتبقية.

تظهر قائمة الفحص في الجدول (١٢) مدى توافر متطلب معالجة مخاطر امن المعلومات /المتطلب (٣.١.٦) وتوثيقه في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013) .

جدول رقم (١٢)
قائمة فحص متطلب معالجة مخاطر امن المعلومات

٣.١.٦معالجة مخاطر امن المعلومات ينبغي على المنظمة تحديد وتطبيق عملية معالجة مخاطر امن المعلومات:	٦	٥	٤	٣	٢	١	٠
٤٢. تحديد خيارات معالجة مخاطر امن المعلومات.				□			
٤٣. تحديد انواع الرقابة الضرورية لتنفيذ خيارات معالجة مخاطر امن المعلومات.			□				
٤٤. وضع بيان قابلية التطبيق					□		
٤٥. صياغة خطة لمعالجة مخاطر امن المعلومات.					□		
٤٦.الحصول على موافقة اصحاب المخاطر على خطة معالجة المخاطر.					□		
التكرارات	7	6	١	١	3	2	1
النتيجة			٤	٣	٦		
الوسط الحسابي المرجح	٢.٦						
النسبة المئوية لمدى المطابقة	٤٣%						
حجم الفجوة (%)	٥٧%						

يتضح من خلال نتائج قائمة الفحص في الجدول (١٢) مستوى التوثيق والتطبيق لبند (٣.١.٦)، فقد حققت وسطا حسابيا قدره (٢.٦) من اصل (٦) درجات، وبنسبة مطابقة (٤٣%)، مما يشير الى وجود فجوة اساسية لعدم المطابقة بنسبة (٥٧%) ويعود ذلك الى :

١- لا يوجد توثيق لحالات معالجة المخاطر التي تؤدي الى حدوث اضرار بشكل كلي وفقا للمواصفة(ISO/IEC27001:2013) .
٢- لم تضع الشركة استراتيجية واضحة لمعالجة المخاطر أو بيان قابلية التطبيق (SOA) كما ورد بالمواصفة (ISO/IEC27001:2013).
٣- لم تضع الشركة خطة موثقة لمعالجة مخاطر امن المعلومات، لكن هناك اجراءات تتخذها الشركة لحماية بيانتها وتقوم بهذه الاجراءات تلقائيا وبصورة مستمرة، مثل وضع جدران حماية (Fair well) عمل (Bake- up) نسخ احتياطية للبيانات والمعلومات والملفات المخزونة وترحل هذه البيانات بصورة مشفرة الى (الحاسبة الام) خارج موقع

الشركة تبعد ٥٠ مترا ولا أحد يستطيع الوصول الى هذه الحاسبة سوى أشخاص محددين، إلا أن هذه الاجراءات لم توثق وهذا ما سبب هذه الفجوة.

٢.٦: اهداف امن المعلومات والتخطيط لتحقيقها:

ينبغي على المنظمة انشاء اهداف لامن المعلومات عند وظائف ومستويات ذات صلة، وينبغي لاهداف امن المعلومات ان تكون : [ISO/IEC27001:2013(E) 5]

أ) متسقة مع سياسة امن المعلومات.

ب) قابلة للقياس (ان كانت عملية).

ج) الاخذ بالحسبان متطلبات امن المعلومات القابلة للتطبيق ،والنتائج المتحصلة من تقييم ومعالجة المخاطر.

د) متناقلة.

ه) محّدثة بالشكل الملائم: وينبغي على المنظمة الاحتفاظ بالمعلومات الموثّقة عن اهداف امن المعلومات عند التخطيط لكيفية تحقيق اهدافها لامن المعلومات ،و ينبغي للمنظمة تحديد (مالذي سيتم القيام به و ماهي الموارد المطلوبة ومن سيكون مسؤولاً ومتى سيتم اكمالها وكيف سيتم تقويم النتائج)

تظهر قائمة الفحص في الجدول (١٣) مدى توافر متطلب اهداف امن /المتطلب (٢.٦) وتوثيقه في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013) .

جدول (١٣)

قائمة فحص متطلب اهداف امن المعلومات والتخطيط لتحقيقها

6: التخطيط	6	5	4	3	2	1	0
٢.٦: اهداف امن المعلومات والتخطيط لتحقيقها							
٤٧.تحدد المنظمة الاهداف المتعلقة بالوظائف والمستويات متفقة مع سياسة امن المعلومات.							□
٤٨.تضع المنظمة اهداف امن معلومات قابلة للقياس.					□		
٤٩.المتطلبات الخاصة بأمن المعلومات قابلة للتطبيق.				□			
٥٠. تبليغ اهداف امن المعلومات العائدة للمنظمة	□						
٥١. تحديث اهداف امن المعلومات باستمرار.	□						
٥٢.تحتفظ المنظمة بالمعلومات الموثقة عن اهداف امن المعلومات متطلبات تخطيط الاهداف.				□			
٥٣.تحدد الموارد اللازمة للتخطيط	□						
٥٤.تحديد المسؤول عن تخطيط الاهداف.						□	
٥٥.تحديد وقت اكمال التخطيط.	□						
٥٦. تعمل المنظمة على تقويم النتائج .					□		
التكرارات	٤			٢	٢	١	١
النتيجة	٢٤			٦	٤	١	٠
الوسط الحسابي المرجح	٣.٥						
النسبة المئوية لمدى المطابقة	%٥٨						
حجم الفجوة(%)	%٤٢						

يتضح من خلال نتائج قائمة الفحص في الجدول (13) مستوى التوثيق والتطبيق لبند (٢.٦)،
فقد حققت وسطا حسابيا قدره (٣.٥) من اصل (٦) درجات، وبنسبة مطابقة (٥٨%) ، مما يشير الى وجود فجوة اساس لعدم المطابقة بنسبة (٤٢%) ويعود ذلك الى:
١- الاهداف التي تضعها الشركة لا تتفق مع سياسة امن المعلومات، لعدم وجود سياسة امن معلومات اصلا .
٢- لا تحدد مسؤول للتخطيط، وذلك بسبب تغيير المسؤولين عن تخطيط امن المعلومات باستمرار، الا أن الاهداف معروفة لدى العاملين في مجال امن المعلومات، وتحدد لها جميع الموارد المطلوبة لإنجاز صافي الوقت المحدد.

٧- الدعم

١.٧: الموارد

ينبغي على المنظمة تحديد وتوفير الموارد المطلوبة لانشاء وتنفيذ وصيانة وتحسين مستمر لنظام ادارة امن المعلومات (ISO/IEC 27001:2013(E)5) .

تظهر قائمة الفحص في الجدول (14) مدى توافر ارشادات ادارة امن المعلومات / المتطلب (١.٧) وتوثيقه في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013)

جدول (14)

قائمة فحص متطلب الموارد

١.٧: الموارد	6	٥	٤	٣	٢	١	٠
٥٧. تحديد وتوفر الموارد المطلوبة لأنشاء وتنفيذ وصيانة التحسين المستمر لنظام ادارة امن المعلومات.				□			
التكرارات				١			
النتيجة				٣			
الوسط الحسابي المرجح	٣						
النسبة المئوية لمدى المطابقة	٥٠%						
حجم الفجوة (%)	٥٠%						

يتضح من خلال نتائج قائمة الفحص في الجدول (١٤) مستوى التوثيق والتطبيق لبند (١.٧)، فقد حققت وسطا حسابيا قدرة (٣) من اصل (٦) درجات، وبنسبة مطابقة (٥٠%)، مما يشير الى وجود فجوة اساس لعدم المطابقة بنسبة (٥٠%) ويعود ذلك الى :
١- لا تتوافر تخصيصات مالية كافية لتوفير الموارد المطلوبة لنظام امن المعلومات الا بشكل يسير، فضلا عن انه لا توثق كل المعلومات المطلوبة لذلك.
٢- هناك تطبيق كامل لتوفير الموارد الضرورية لإدارة امن المعلومات واهمها العنصر البشري، اذ قامت الشركة بتدريب المسؤولين عن إدارة مركز البيانات، من خلال ايفادهم الى خارج البلد لتطوير امكانيتهم بما يتناسب مع التغيير والتطور الجديد الذي طرأ على الشركة بتأسيس (Data Center) وللحصول على الشهادة، اذ تمنح هذه الشهادة من شركة (برومترك) المسؤولة عن اجراء امتحان شركة (مايكروسوفت)، هذه الشهادة صالحة لمدة (٣) سنوات وتجدد بعد ذلك. اما من الناحية المادية فقد لوحظ من خلال المعايشة الميدانية والمقابلة مع مدير الخدمات الفنية و ومسؤولي (مركز البيانات)

التي اجرت معهم بتاريخ (١٨-١-٢٠١٨). والمقابلات بأن المركز متوافرة فيه البيئة المادية مناسبة من حيث الارضية، إذ أن ارضية الغرف التي توجد فيها الخوادم (Servers) مصممة لتحمل الاهتزازات والتي تسمى (بالأرضية الكاذبة) ومرتفعة بما يقرب (٥٠سم) عن الارضية، وسقوف ثانوية ذات مواصفات محددة وموضوعة وفقاً لما تتطلبه الخوادم، من حيث منظومات الحرائق واجهزة التبريد وغيرها .

٢.٧: الكفاءة (الاهلية)

ينبغي على المنظمة العمل بكل من الآتي : (ISO/IEC27001:2013(E)5)

أ) تحديد الكفاءة الضرورية للافراد القائمين بالعمل تحت رقابتها التي تؤثر في ادائها لأمن المعلومات.

ب) ضمان ان يكون هؤلاء الافراد أكفاء على اساس التعليم الملائم ، والتدريب او الخبرة.

ج) عندالاقتضاء، عمل اجراءات لاكتساب الكفاءة الضرورية، وتقييم فاعلية الاجراءات المتخذة.

د) الاحتفاظ بمعلومات موثقة ملائمة كدليل على الكفاءة.

تظهر قائمة الفحص في الجدول (١٥) مدى توافر متطلب الكفاءة / المتطلب (٢.٧) وتوثيقه في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013) .

جدول (١٥)

قائمة فحص متطلب الكفاءة

٢.٧: الكفاءة (الاهلية)	٦	٥	٤	٣	٢	١	٠
٥٨. تعين المنظمة الكفاءات الضرورية للافراد المؤثرين في اداء انشطة (ISMS).	□						
٥٩.توافر المنظمة التدريب لتحقيق الكفاءة اللازمة.	□						
٦٠.تحفظ المنظمة المعلومات الخاصة بالتعليم والتدريب والمهارات والخبرات بوصفها دليل على الكفاءة المناسبة.	□						
التكرارات	٣						
النتيجة	٨						
الوسط الحسابي المرجح	٦						
النسبة المئوية لمدى المطابقة	١٠٠%						
حجم الفجوة (%)	٠%						

يتضح من خلال نتائج قائمة الفحص في الجدول (١٥) مستوى التوثيق والتطبيق لبند (٢.٧)، اذ حققت وسطا حسابيا قدره (٦) من اصل (٦) درجات، وبنسبة مطابقة (١٠٠%)، وبذلك لا تكون هناك فجوة ويعود ذلك الى التطبيق والتوثيق التام وعلى النحو الاتي :

١- اذ تعين المنظمة الكفاءات الضرورية للأفراد الذين لهم تأثير على اداء انشطة المنظمة، فكما نلاحظ في جدول توزيع الافراد، نجد أن عدد المهندسين في الشركة كبير ، فهو يبلغ (١٧٧) مهندسا

٢- تقوم المنظمة بتطوير عامليها من خلال زجهم في دورات تدريبية على مدار السنة لتطوير امكانيتهم لان ذلك سيعود بالفائدة الكبيرة للمنظمة، اذ يعد التدريب للعنصر البشري هو استثمار للشركة .

٣- تحتفظ المنظمة بالمعلومات الخاصة بالتعليم والتدريب والمهارات والخبرات بوصفها دليل على الكفاءة المناسبة. كذلك تقوم الشركة بإعداد استمارة تقييم لدورات التدريب يقوم بها قسم التدريب مثبتة في الملحق (٩) .

٣.٧: الوعي

ينبغي ان يكون الافراد الذين يقومون بالعمل تحت رقابة المنظمة على وعي تام بالآتي: (ISO/IEC27001:2013(E)5)

أ) سياسة امن المعلومات.

ب) مساهمتها بفاعلية نظام ادارة امن المعلومات ، بما في ذلك فوائد تحسين اداء امن المعلومات.

تظهر قائمة الفحص في الجدول (١٦) مدى توافر متطلب الوعي /المتطلب (٣.٧) وتوثيقه في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013) .

جدول (١٦)

قائمة فحص متطلب الوعي

٣.٧ الوعي	٦	٥	٤	٣	٢	١	٠
٦١.تضمن المنظمة ان عاملين المنظمة على بينة من سياسة امن المعلومات.							□
٦٢. تحدد المنظمة الاداء المستحسن لأمن المعلومات.						□	
٦٣. تحدد المنظمة الاثار المترتبة على عدم التطابق مع متطلبات ISMS.						□	
التكرارات						٢	١
النتيجة						٢	٠
الوسط الحسابي المرجح	٠.٦٦						
النسبة المئوية لمدى المطابقة	١١%						
حجم الفجوة (%)	٨٩%						

يتضح من خلال نتائج قائمة الفحص في الجدول (١٦) مستوى التوثيق والتطبيق لبند (٣.٧)، فقد حققت وسطا حسابيا قدره (٠.٦٦) من اصل (٦) درجات، وبنسبة مطابقة (١١%)، مما يشير الى وجود فجوة أساس لعدم المطابقة بنسبة (٨٩%) ويعود ذلك الى:

١- التوعية بمتطلبات نظام ادارة امن المعلومات وفق المواصفة (ISO 27001: 2013) وسياسية أمن المعلومات معدومة، مع توثيق ضعيف .

٢- تحديد وتوثيق الاثار التي تنتج عن عدم التطابق مع نظام ادارة امن المعلومات (ISMS) غير كافية بل تكاد تكون معدومة .

٤.٧: الاتصال

ينبغي على المنظمة تحديد الحاجة للاتصالات الداخلية والخارجية ذات الصلة بنظام ادارة امن المعلومات بما في ذلك : (ISO/IEC27001:2013(E)6)

أ) على ماذا ينبغي الاتصال و متى ينبغي الاتصال و مع مَن ينبغي الاتصال.

ب) العمليات التي بها ينبغي التاثر بالاتصال

تظهر قائمة الفحص في الجدول (١٧) مدى توافر متطلب الاتصال /المتطلب (٤.٧) وتوثيقه

في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013) .

جدول (١٧)

قائمة فحص متطلب الاتصال

٤.٧: الاتصال تحدد المنظمة الحاجة للاتصالات الداخلية والخارجية ذات الصلة بنظام ادارة امن المعلومات بما في ذلك:	٦	٥	٤	٣	٢	١	٠
٦٤.تحديد الاتصال المتعلق بنظام ادارة امن المعلومات.					□		
٦٥. وقت الاتصال.					□		
٦٦. تحديد الجهة التي ينبغي الاتصال بها.					□		
٦٧. تحديد الجهة الواجب عليها الاتصال.					□		
التكرارات					٤		
النتيجة					٨		
الوسط الحسابي المرجح	٢						
النسبة المئوية لمدى المطابقة	٣٣%						
حجم الفجوة (%)	٦٧%						

يتضح من خلال نتائج قائمة الفحص في الجدول (١٧) مستوى التوثيق والتطبيق لبند (٤.٧)، فقد حققت وسطا حسابيا قدره (٢) من اصل (٦) درجات، وبنسبة مطابقة (٣٣%)، مما يشير الى وجود فجوة اساس لعدم المطابقة بنسبة (٦٧%) ويعود ذلك الى:

١- التوثيق والتطبيق جزئي وضعيف لتحديد الاتصال ووقته والجهة التي ينبغي الاتصال بها، اذ تخلو الاجتماعات الدورية لإدارة من التوعية باتجاه تطبيق نظام إدارة أمن المعلومات على وفق المواصفة (ISO27001) .

٢- لا يوجد قسم خاص لإدارة امن المعلومات يتولى مهمة الاتصال داخليا أو خارجيا في حال حدوث خلل او اختراقات او اي حالة اخرى خارج حدود السيطرة .

٥.٧: المعلومات الموثقة

(ISO/IEC27001:2013(E)6) ينبغي لنظام ادارة امن معلومات المنظمة ان يشمل :

أ)المعلومات الموثقة المطلوبة بهذه المواصفة الدولية .

ب) المعلومات الموثقة المحددة من المنظمة بوصفها ضرورية لفاعلية نظام ادارة امن المعلومات

تظهر قائمة الفحص في الجدول (١٨) مدى توافر متطلب المعلومات الموثقة /المتطلب (٥.٧) ، وتوثيقه في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013)

جدول (١٨)
قائمة فحص متطلب المعلومات الموثقة

٥.٧: المعلومات الموثقة ١.٥.٧: عام	٦	٥	٤	٣	٢	١	٠
٦٨.تحدد المنظمة المعلومات الموثقة المطلوبة للمواصفة (ISO/IEC27001:2013).							□
٦٩. توثق المنظمة معلومات كفاءة الفرد.	□						
٧٠. توثق المنظمة السياسة الامنية والمجال.							□
٧١. توثق المنظمة تقرير تقييم ومعالجة المخاطر.						□	
٧٢. تحدد المنظمة سجل للاذعان لمتطلبات (ISO/IEC27001:2013).							□
٢.٥.٧: الابتكار والتحديث							
٧٣. تحديد ووصف ملائم (العنوان ، التاريخ ، المؤلف).						□	
٧٤. صنع فرمتة تتضمن تحديد (اللغة واصدار البرامج).						□	
٧٥. ضمان ان المعلومات الموثقة كافية وملائمة للغرض.						□	
٣.٥.٧: رقابة المعلومات الموثقة							
٧٦. تحديد المعلومات الموثقة.						□	
٧٧. ضمان اتاحة المعلومات الموثقة للاستعمال عند الحاجة اليها.					□		
٧٨. ضمان حماية المعلومات الموثقة على نحو ملائم (السرية او الاستعمال الصحيح او فقدان التكامل).					□		
٧٩.خزن السجلات والمحافظة عليها.				□			
٨٠. امكانية الوصول والاسترجاع والاستعمال للمعلومات الموثقة.					□		
٨١. ضمان الرقابة على التغيرات.				□			
٨٢. امكانية الاحتفاظ والتخلص.	□						
التكرارات	٢			٢	٣	٥	٣
النتيجة	١٢			٦	٦	٥	٠
الوسط الحسابي المرجح	١.٩٣						
النسبة المئوية لمدى المطابقة	%٣٢						
حجم الفجوة (%)	%٦٨						

يتضح من خلال نتائج قائمة الفحص في الجدول (١٨) مستوى التوثيق والتطبيق لبند (٥.٧)، فقد حققت وسطا حسابيا قدره (١.٩٣) من اصل (٦) درجات، وبنسبة مطابقة (٣٢%)، مما يشير الى وجود فجوة أساس لعدم المطابقة بنسبة (٦٨%) ويعود ذلك الى :

- لا يوجد دعم كاف من الادارات العليا لكي يطبق نظام ادارة امن المعلومات بكل متطلباته، على الرغم من وجود موارد بشرية كفوءة وتكنولوجيا حديثة مثال ذلك (تعمل الشركة بنظام الارشفة الالكتروني الذي يهدف الى انشاء بيئة مبسطة وذات أمنية عالية و سرعة ودقة عالية من أجل حفظ جميع الكتب والمخاطبات وتخزن هذه البيانات في مركز البيانات ثم تعمل لهم نسخ احتياطية (Backup)، اذ يجري حفظ ملفات العاملين وكذلك حفظ كافة الاوامر الادارية وكتب تسهيل المهمة والمذكرات والصادر والوارد وهذا ما

لاحظناه من خلال المقابلة مع مديرة قسم الشؤون الادارية في احدى المقابلات بتاريخ (١٩-١-٢٠١٨)، الا انه لا يستغل بشكل صحيح ووفق متطلبات محددة .

8- التشغيل

٨.١: التخطيط العملياتي والرقابة،(٨.٢) تقييم مخاطر امن المعلومات

ينبغي على المنظمة تخطيط، وتنفيذ ورقابة العمليات المطلوبة لتلبية متطلبات امن المعدات ،وتنفيذ الاجراءات المحددة في (البند- 6.1) ، وكذلك ينبغي للمنظمة تنفيذ الخطط لتحقيق اهداف امن المعلومات المحددة في (البند- 6.2) كما يجب على المنظمة الاحتفاظ بمعلومات موثقة الى الحد الذي يكون ضرورياً في الحصول على الثقة في ان العمليات قد نفذت كما خطط لها ، و ينبغي على المنظمة رقابة التغيرات المخطط لها ومراجعة عواقب التغيرات غير المقصودة، متخذة إجراء لتخفيف اية تاثيرات عكسية عند الضرورة، وينبغي على المنظمة ضمان تحديد ورقابة العمليات المموّلة من الخارج.(ISO/IEC27001:2013)

كذلك و ينبغي على المنظمة اجراء تقييمات لمخاطر امن المعلومات عند فواصل زمنية مخطط لها او عند حدوث تغييرات هامة، اخذةً بنظر الاعتبار المعايير المتبناة في (البند- أ 6.1.2) وعلى المنظمة الاحتفاظ بمعلومات موثّقة عن نتائج تقييمات مخاطر امن المعلومات.

تظهر قائمة الفحص في الجدول (١٩) مدى توافر متطلب التخطيط العملياتي والرقابة /المتطلب (١.٨)، ومتطلب تقييم مخاطر امن المعلومات (٢.٨)، في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013).

جدول (١٩)

قائمة فحص متطلب التخطيط العملياتي والرقابة وتقييم مخاطر امن المعلومات

8. العملية	٦	٥	٤	٣	٢	١	٠
١.٨: التخطيط العملياتي والرقابة							
٨٣. تعمل المنظمة على تخطيط وتنفيذ ورقابة العمليات المطلوبة لتلبية متطلبات امن المعلومات على وفق (ISO/IEC27001:2013) .						□	
٨٤. ضمان العمليات الخارجية مسيطر عليها.	□						
٢.٨: تقييم مخاطر امن المعلومات							
٨٥. تحتفظ المنظمة بمعلومات موثقة عن نتائج تقييم مخاطر امن المعلومات.				□			
التكرارات	١			١		١	
النتيجة	٦			٣		١	
الوسط الحسابي المرجح	٣.٣						
النسبة المئوية لمدى المطابقة	٥٥%						
الفجوة (%)	٤٥%						

يتضح من خلال عرض نتائج قائمة الفحص في الجدول (١٩) مستوى التوثيق والتطبيق لبند (١.٨) و (٢.٨)، فقد حققت وسطا حسابيا قدرة (٣.٣) من أصل (٦) درجات، وبنسبة مطابقة (٥٥%)، مما يشير الى وجود فجوة اساس لعدم المطابقة بنسبة (٤٥%) ويعود ذلك الى :

١- عدم وجود خطة موثقة بشكل تتفق مع متطلبات المواصفة والتي تعتمد على دورة ديمنغ (PDCA) اي خطط وحدد الاهداف ثم نفذ وراقب واجري التحسين المستمر.
٢- تجرى عملية تدقيق داخلي على كافة الاقسام من خلال وضع خطة تدقيق وفريق وتوقيتات التدقيق، اذ ان الخطة مثبتة في الملحق (١٣) إلا أنه لا يوجد تدقيق خاص بأمن المعلومات .
٣ - التوثيق الضعيف لمخاطر امن المعلومات، كذلك فإنه لا يوجد تحليل لمخاطر أمن المعلومات سواء كان كميا او نوعيا .

٣.٨:معالجة مخاطر امن المعلومات

ينبغي على المنظمة تنفيذ خطة لمعالجة مخاطر امن المعلومات، والاحتفاظ بمعلومات موثّقة عن نتائج معالجة مخاطر امن المعلومات

تظهر قائمة الفحص في الجدول (٢٠) مدى توافر متطلب معالجة مخاطر امن المعلومات /المتطلب (٣.٨) وتوثيقه في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013) .

جدول (٢٠) قائمة فحص متطلب معالجة مخاطر امن المعلومات

٣.٨:معالجة مخاطر امن المعلومات	٦	٥	٤	٣	٢	١	٠
٨٦. تنفيذ المنظمة خطة لمعالجة مخاطر امن المعلومات.					□		
٨٧. ينبغي على المنظمة الاحتفاظ بمعلومات موثقة عن نتائج معالجة مخاطر امن المعلومات.						□	
التكرارات					١	١	
النتيجة					٢	١	
الوسط الحسابي المرجح	١.٥						
النسبة المئوية لمدى المطابقة	٢٥%						
الفجوة (%)	٧٥%						

يتضح من خلال نتائج قائمة الفحص في الجدول (٢٠) مستوى التوثيق والتطبيق لبند (٣.٨)، فقد حققت وسطا حسابيا قدره (١.٥) من اصل (٦) درجات، وبنسبة مطابقة (٢٥%)، مما يشير الى وجود فجوة اساس لعدم المطابقة بنسبة (٧٥%) ويعود ذلك الى :

- لا توجد خطة موثقة لمعالجة المخاطر في الشركة، اذ يقوم المتخصصون في الشركة في مركز البيانات بالتصدي تلقائيا لمعالجة المخاطر من خلال مجموعة من الاجراءات التي يقومون بها في حال حصول خطر وهي (عمل نسخ احتياطية للبيانات في حال حصول اي حالة تخريب او حرائق او اي مشكلة طارئة، كذلك هناك حاسبة كبيرة تسمى (الحاسبة الام) ترسل اليها البيانات تبعد ٥٠ متر عن الشركة وموقعها سري فقط هناك اشخاص محددين لهم معرفة بموقع هذه الحاسبة للتخزين البيانات بحيث حتى وان حدثت مشكلة او خسارة للبيانات في المركز فجميع البيانات موجودة في هذه الحاسبة، كذلك هناك مجموعة من وسائل الحماية وهي البطاقة الذكية للدخول للمركز، وهذه البطاقة لا توجد الا عند أشخاص محددين والجدار الناري (Fair wall)، إذ أنه لم تسجل حتى الان

اي حالة اختراق او عبث، الا ان هذه الاجراءات يجب ان توثق لكي تكون مفهومة وواضحة للجميع .

٩- تقويم الاداء

٩.١: المراقبة والقياس والتحليل والتقويم:

ينبغي على المنظمة تقييم اداء امن المعلومات وفاعلية نظام ادارة امن المعلومات.

تحديد كل من الاتي: (ISO/IEC 27001:2013(E)7)

أ) ماالذي يحتاج الى المراقبة والقياس ، بما في ذلك عمليات امن المعلومات والرقابة عليها.

ب) طرائق المراقبة والقياس والتحليل والتقييم ، كلما امكن ذلك ، لضمان الحصول على نتائج صالحة وصحيحة

تظهر قائمة الفحص في الجدول (٢١) مدى توافر متطلب المراقبة والقياس والتحليل والتقويم /المتطلب (٩.١) وتوثيقه في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013)

جدول (٢١)

قائمة فحص متطلب المراقبة والقياس والتحليل والتقويم

9. تقويم الاداء							
٩.١: المراقبة والقياس والتحليل والتقويم: ينبغي على المنظمة تقويم اداء امن المعلومات وفاعلية نظام ادارة امن المعلومات.	٦	٥	٤	٣	٢	١	٠
٨٨. تراقب المنظمة وتقيس عمليات امن المعلومات.					□		
٨٩. ضمان ان النتائج هي من المراقبة والقياس.					□		
٩٠.حفظ ادلة مراقبة وقياس النتائج.					□		
التكرارات					٣		
النتيجة	٦						
الوسط الحسابي المرجح	٢						
النسبة المئوية لمدى المطابقة	%٣٣						
حجم الفجوة (%)	%٦٧						

يتضح من خلال نتائج قائمة الفحص في الجدول (٢١) مستوى التوثيق والتطبيق لبند (٩.١)، فقد حققت وسطا حسابيا قدره (٢) من اصل (٦) درجات، وبنسبة مطابقة (٣٣%)، مما يشير الى وجود فجوة اساسية لعدم المطابقة بنسبة (٦٧%) ويعود ذلك الى:

١- التوثيق والتطبيق الجزئي : مثلا في مركز البيانات تجري عملية مراقبة امن البيانات والمعلومات وتوفير كافة وسائل الحماية للبيانات والمعلومات إلا أنه لا يوجد توثيق لتلك الاجراءات، اما في قسم انتاج النظم فيجري انتاج النظم البرمجية وفقا لخطة يضعها الفريق وذلك بعد مقابلة الزبون او الجهة الطالبة للنظم، ويجري الاتفاق على المواصفات والمتطلبات التي يرغب بها الزبون، هذا ما لاحظته من خلال المناقشة مع مديرة القسم في إحدى المقابلات الشخصية بتاريخ (١٠- ١- ٢٠١٨.)

٢.٩: التدقيق الداخلي

ينبغي على المنظمة اجراء التدقيقات الداخلية عند فواصل زمنية مخطط لها لتوفير المعلومات فيما اذا كان نظام ادارة امن المعلومات: (ISO/IEC (E)7 (27001:2013)

أ) يتطابق مع المتطلبات الخاصة بنظام ادارة امن معلومات المنظمة ومتطلبات هذا المعيار الدولي

ب) قد نفّذ وتمت صيانته بفاعلية.

ينبغي على المنظمة ان:

ج) تخطط، وتنشىء وتنفذ وتحافظ على برامج التدقيق ، بما في ذلك التكرار ،الطرائق، المسؤوليات ،متطلبات التخطيط ورفع التقارير.وستاخذ برامج التدقيق في الاعتبار اهمية العمليات المعنية ونتائج التدقيقات السابقة.

د) تحدد معايير التدقيق ونطاق كل تدقيق.

ه) اختيار المدققين واجراء التدقيقات التي تضمن الموضوعية ونزاهة عملية التدقيق.

و) ضمان ان ترفع نتائج التدقيقات الى الادارة ذات الصلة

تظهر قائمة الفحص في الجدول (٢٢) مدى توافر متطلب التدقيق الداخلي/المتطلب (٢.٩)، وتوثيقه في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013) .

جدول (٢٢) قائمة فحص متطلب تقويم الاداء

٢.٩: التدقيق الداخلي. ينبغي على المنظمة اجراء التدقيقات الداخلية عند فواصل زمنية مخطط لها لتوفير المعلومات حول ان كان نظام ادارة امن المعلومات:	٦	٥	٤	٣	٢	١	٠
٩١.تطابق المتطلبات الخاصة للمنظمة مع نظامها لإدارة امن المعلومات.					□		
٩٢. تجري المنظمة تدقيق داخلي لضمان تنفيذ متطلبات ( ) ISO/IEC 27001:2013 بفاعلية.					□		
٩٣. تحدد المنظمة معايير التدقيق ومجال التدقيق الداخلي.				□			
٩٤. ضمان اختيار المدققون واجراء التدقيقات التي تضمن الموضوعية ونزاهة عملية التدقيق.	□						
٩٥.ضمان ان ترفع نتائج التدقيقات الى الادارة المسؤولة.	□						
٩٦.الاحتفاظ بمعلومات موثقة بوصفها دليل لبرامج التدقيق.					□		
التكرارات	٢			١	٣		
النتيجة	١٢			٣	٦		
الوسط الحسابي المرجح	٣						
النسبة المئوية لمدى المطابقة	%٥٠						
حجم الفجوة(%)	%٥٠						

يتضح من خلال عرض نتائج قائمة الفحص في الجدول (٢٢) مستوى التوثيق والتطبيق لبند (٢.٩) فقد حققت وسطا حسابيا قدره (٣) من اصل (٦) درجات، وبنسبة مطابقة (٥٠%)، مما يشير الى وجود فجوة اساس لعدم المطابقة بنسبة (٥٠%) ويعود ذلك الى:

١- لا يوجد تدقيق خاص بنظام إدارة أمن المعلومات، بل هناك تدقيق داخلي دوري موثق (الكترونياً وورقياً) لكافة اقسام الشركة يخص الاوامر الادارية ، ويوجد تدقيق سنوي يشتمل على المعلومات جميعها الخاصة بنتائج عمل الشركة والمراكز من الناحية الاحصائية على وفق المقابلة مع السيد رئيس المدققين بتاريخ (٢٣- ١- ٢٠١٨) ومشرف الجودة ، والخطة مثبتة بالمحلق (١٣) .

٢- يخضع التدقيق للجهات الخارجية (شركة VEXIL النيوزيلندية الهندية المانحة للشهادة الايزو ٩٠٠١) والجهات الادارية والمالية الحكومية (ديوان الرقابة المالية وهيأة النزاهة) ولا توجد جهة تدقيق خارجية على نظام ادارة امن المعلومات الايزو ٢٧٠٠١ تقانياً وادارياً.

٣.٩: المراجعة الادارية

ينبغي على الادارة العليا مراجعة نظام ادارة امن المعلومات للمنظمة عند فواصل زمنية مخطط لها لضمان ملاءمته وكفاءته وفاعليته ، وينبغي ان تنطوي المراجعة الادارية على مراعاة كل من الآتي: (8(E)ISO/IEC27001:2013)

أ) حالة الاجراءات من المراجعات الادارية السابقة.

ب) التغييرات في القضايا الداخلية والخارجية ذات الصلة بنظام ادارة امن المعلومات.

ج)التغذية العكسية على اداء امن المعلومات

تظهر قائمة الفحص في الجدول (٢٣) مدى توافر متطلب المراجعة الادارية /المتطلب (٣.٩)، وتوثيقه في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013) .

جدول (٢٣) قائمة فحص متطلب المراجعة الادارية

٣.٩: المراجعة الادارية ينبغي على الادارة العليا مراجعة نظام ادارة امن المعلومات للمنظمة عند فواصل زمنية مخطط لها لضمان ملائمتها وكفايتها وفاعليتها:	٦	٥	٤	٣	٢	١	٠
٩٧. وضع اجراءات لمراجعة نظام ادارة امن المعلومات .				□			
٩٨. ضمان التغيرات في القضايا الداخلية والخارجية ذات صلة بنظام ادارة امن المعلومات.					□		
٩٩. التغذية الراجعة على اداء امن المعلومات بما في ذلك الاتجاهات في : أ. اللا تطابق والاجراءات التصحيحية.					□		
ب. نتائج المراقبة والقياس .					□		
ج. نتائج التدقيق.							□
ه. تحقيق اهداف امن المعلومات.				□			
د. التغذية الراجعة من اطراف مهتمة.					□		
١٠٠. وضع خطة لعلاج المخاطر وتنفيذها وصيانتها في تقييم المخاطر.					□		
١٠١. تتضمن المراجعة الادارية فرص للتحسين المستمر.				□			
التكرارات				٣	٥		١
النتيجة				٩	٠		٠
الوسط الحسابي المرجح	٢.١١						
النسبة المئوية لمدى المطابقة	%٣٥						
حجم الفجوة (%)	%٦٥						

يتضح من خلال نتائج قائمة الفحص في الجدول (٢٣) مستوى التوثيق والتطبيق لبند (٣.٩)، فقد حققت وسطا حسابيا قدره (٢.١١) من اصل (٦) درجات، وبنسبة مطابقة (٣٥%)، مما يشير الى وجود فجوة أساس لعدم المطابقة بنسبة (٦٥%) ويعود ذلك الى:

١- ضعف عملية مراجعة وتوثيق لنظام ادارة امن المعلومات في الشركة .

٢- لا توجد خطة موثقة لعلاج مخاطر امن المعلومات في الشركة

١٠- التحسين

١.١٠: اللا تطابق والاجراء التصحيحي

حين يحدث اللاتطابق ، ينبغي على المنظمة اجراء كل من الآتي: (ISO/IEC27001:2013(E) 9)

أ) رد الفعل على اللاتطابق ، كلما امكن ذلك و اخذ اجراء للسيطرة عليه وتصحيحه و التعامل مع العواقب.

ب) تقويم الحاجة الى اجراء للقضاء على اسباب اللاتطابق ، من اجل ان لايتكرر او يحدث في مكان آخر، ومراجعة اللاتطابق ، وتحديد اسباب اللاتطابق، وتحديد ان كانت هناك حالات لاتطابق مماثلة موجودة ، او قد تحدث مستقبلاً.

ج) تنفيذ اي اجراء مطلوب.

د) مراجعة فاعلية اي اجراء تصحيحي متخّذ.

هـ) عمل تغييرات على نظام ادارة امن المعلومات ، عند الضرورة

تظهر قائمة الفحص في الجدول (٢٤) مدى توافر متطلب اللا تطابق والاجراء التصحيحي /المتطلب (١.١٠)، وتوثيقه في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013) .

جدول (٢٤)

قائمة فحص متطلب اللا تطابق والاجراء التصحيحي

10.1: اللا تطابق والاجراء التصحيحي. حين يحدث اللا تطابق ، ينبغي على المنظمة :	٦	٥	٤	٣	٢	١	٠
١٠٢. رد الفعل على اللا تطابق أ. اخذ اجراء للسيطرة عليه وتصحيحه.				□			
١٠٣. تحديد اجراء للقضاء على اسباب اللا تطابق. أ. مراجعة اللا تطابق.					□		
ب. تحدد المنظمة اسباب اللا تطابق.					□		
١٠٤. تنفيذ أي اجراء مطلوب.					□		
١٠٥. مراجعة فاعلية أي اجراء تصحيحي متخذ.					□		
١٠٦.عمل تغييرات على نظام ادارة امن المعلومات عند الضرورة.					□		
١٠٧.تحدد المنظمة طبيعة اللا تطابق.					□		
١٠٨.تحدد المنظمة نتائج أي اجراء تصحيحي				□			
التكرارات				٢	٦		
النتيجة				٦	١٢		
الوسط الحسابي المرجح	١.٥						
النسبة المئوية لمدى المطابقة	٢٥%						
حجم الفجوة (%)	٧٥%						

يتضح من خلال نتائج قائمة الفحص في الجدول (٢٤) مستوى التوثيق والتطبيق لبند (١.١٠)، فقد حققت وسطا حسابيا قدره (١.٥) من اصل (٦) درجات، وبنسبة مطابقة (٢٥%)، مما يشير الى وجود فجوة أساس لعدم المطابقة بنسبة (٧٥%) ويعود ذلك الى:
لا توضع خطط للإجراءات الوقائية لإزالة او التخفيف من الحالات غير المرغوب فيها و/او المتوقع حدوثها، ولذلك فعند حدوث حالات عدم التطابق فإنها تشخص عن طريق المتابعة الشخصية للمسؤولين عن المركز فقط، ومن ثم يجري العمل على اجراءات بسيطة للحد من هذه الحالات غير المطابقة .

٢.١٠: التحسين المستمر

ينبغي على المنظمة التحسين المستمر لملاءمة وكفاية وفاعلية نظام ادارة امن المعلومات.(ISO/IEC27001:2013(E) 10).

تظهر قائمة الفحص في الجدول (٢٥) مدى توافر متطلب التحسين المستمر/المتطلب (٢.١٠)، وتوثيقه في الشركة مقارنة بالمواصفة الدولية (ISO 27001: 2013) .

جدول (٢٥)

قائمة فحص متطلب التحسين المستمر

٢.١٠: التحسين المستمر ينبغي على المنظمة التحسين المستمر لملائمة واهلية وفاعلية نظام ادارة امن المعلومات.	٦	٥	٤	٣	٢	١	٠
١٠٩. ضمان ان المعلومات الموثقة تكون مناسبة وكافية لعملية التحسين .					□		
١١٠. صيانة المعلومات الموثقة.						□	
١١١. تحديد معلومات لفحص فاعلية (ISMS) .				□			
التكرارات				١	١	١	
النتيجة				٣	٢	١	
الوسط الحسابي المرجح	٢						
النسبة المئوية لمدى المطابقة	%٣٣						
حجم الفجوة (%)	%٦٧						

يتضح من خلال نتائج قائمة الفحص في الجدول (٢٥) مستوى التوثيق والتطبيق لبند (٢.١٠)، اذ حققت وسطا حسابيا قدره (٢) من اصل (٦) درجات، وبنسبة مطابقة (٣٣%)، مما يشير الى وجود فجوة اساسية لعدم المطابقة بنسبة (٦٧%) ويعود ذلك الى:
١- المعلومات الموثقة غير مكتملة ، وتوثيق ضعيف لعمليات التحسين.
٢- ضعف في صيانة المعلومات الموثقة.
٣- لا يستفاد من المعلومات الموثقة المتعلقة بنظام ادارة امن المعلومات بشكل كاف من تحليل البيانات واجراءات التحسينات المستمرة .
٤- ضعف دعم الادارة العليا لعملية التحسين .

ثانيا : خلاصة النتائج النهائية لقياس فجوة تطبيق نظام ادارة امن المعلومات في الشركة على وفق المواصفة(ISO 27001: 2013)

يوضح الجدول (٢٦) الخلاصة النهائية لنتائج قياس الفجوة بين واقع نظام ادارة امن المعلومات في الشركة العامة للأنظمة الالكترونية / مركز البيانات و بنود المواصفة (ISO27001:٢٠١٣) .

جدول (٢٦)خلاصة نتائج مستوى التوثيق والمطابقة لمتطلبات المواصفة في الشركة العامة للأنظمة الالكترونية/ مركز البيانات :ISO 27001) (2013

ت	عناوين المتطلبات على وفق المواصفة: (ISO/IEC 27001:2013)		درجات التقويم للتطبيق والتوثيق الفعلي		
	رقم المتطلب	اسم المتطلب	الوسط الحسابي المرجح (المعدل)	النسبة المئوية للمطابقة	حجم الفجوة (%)
1	١.٤	فهم المنظمة وسياقها	٣	%٥٠	%٥٠
2	٢.٤	فهم حاجات وتوقعات الاطراف المهتمة	٦	%١٠٠	%٠
3	٣.٤	تحديد مجال نظام ادارة امن المعلومات	٢.٣٣	%٣٨	%٦٢
4	٤.٤	نظام ادارة امن المعلومات	750.	%١٢	%٨٨
٥	٤	المجموع الكلي لبنود متطلب سياق المنظمة	٢.٠١	%٣٤	٦٦
٦	١.٥	القيادة والالتزام	١.٦٨	%٣١	%٦٩
٧	٢.٥	السياسة	٠	%٠	%١٠٠
٨	٣.٥	الادوار المنظمية والمسؤوليات والسلطات	١.٦٦	%٢٨	%٧٢
٩	٥	المجموع الكلي لبنود متطلب القيادة	١.٦٧	%٢٨	%٧٢
١٠	١.٦	اجراءات تناول المخاطر والفرص	٢.٥	%٤٢	%٥٨
١١	١.٢.٦	تقييم مخاطر امن المعلومات	١.٤	%٢٣	%٧٧
١٢	١.٣.٦	معالجة مخاطر امن المعلومات	٢.٦	%٤٣	%٥٧
١٣	٢.٦	اهداف امن المعلومات والتخطيط لتحقيقها	٣.٥	%٥٨	%٤٢
١٤	٦	المجموع الكلي لبنود متطلب التخطيط	٢.٥	%٤٢	%٥٨
٥1	١.٧	الموارد	٣	%٥٠	%٥٠
٦1	٢.٧	الكفاءة	٦	%١٠٠	%٠
٧1	٣.٧	الوعي	٠.٦٦	%١١	%٨٩
٨1	٤.٧	الاتصال	٢	%٣٣	%٦٧
٩1	٥.٧	المعلومات الموثقة	١.٩٣	%٣٢	%٦٨
٢٠	٧	المجموع الكلي لبنود متطلب الكفاءة	٢.٧	%٤٥	%٥٥
٢١	١.٨	التخطيط العملياتي والرقابة وتقييم مخاطر امن المعلومات	٣.٣	%٥٥	%٤٥
٢٢	٢.٨	معالجة مخاطر امن المعلومات	١.٥	%٢٥	%٧٥
٢٣	٨	المجموع الكلي لبنود متطلب التخطيط العملياتي والرقابة	٢.٤	%٤٠	%٦٠
٢٤	١.٩	المراقبة والقياس والتحليل والتقويم	٢	%٣٣	%٦٧
٥2	٢.٩	التدقيق الداخلي	٣	%٥٠	%٥٠
٦2	٣.٩	المراجعة الادارية	٢.١١	%٣٥	%٦٥
٢٧	٩	المجموع الكلي لبنود متطلب القياس والتحليل والتقويم	٢.٤	%٤٠	%٦٠
٨2	١.١٠	اللا تطابق والاجراء التصحيحي	١.٥	%٢٥	%٧٥
٩2	٢.١٠	التحسين المستمر	٣	%٣٣	%٦٧
٣٠	١٠	المجموع الكلي لبنود متطلب التحسين المستمر	٢.٢٥	%٣٨	%٦٢
٣١	المجموع الاجمالي لنتائج التقويم		٢.٢٧	%٣٧	%٦٣

المصدر : اعداد الباحثة

استنادا الى نتائج تحليل فجوة التوثيق والتطبيق وفقا للمواصفة (:ISO27001 2013) تشير النتائج الظاهرة في الجدول (٢٦) الى وجود فجوة بين الواقع الفعلي للتوثيق والتطبيق في الشركة العامة للأنظمة الالكترونية/ مركز البيانات و بنود

المواصفة، التي كانت بنسبة اجمالية قدرها (٦٣%)، وبلغت نسبة التوثيق والتطبيق الكلي في الشركة (٣٧%) مقارنة بالمواصفة الدولية كما موضح في الشكل(٢١)، اذ سجل البند (٢.٤ فهم حاجات وتوقعات الاطراف المهتمة) والبند (٢.٧ الكفاءة) اعلى نسبة مطابقة وبلغت (١٠٠%)، فيما سجل البند (٢.٥ السياسة) ادنى نسبة مطابقة والبالغة (٠%)، وتراوحت بقية نسب التوثيق والتطبيق بين اعلى نسبة وبلغت (٥٨%) للبند (٢.٦ اهداف امن المعلومات والتخطيط لتحقيقها)، واقل نسبة وبلغت (١١%) للبند (٣.٧ الوعي)، وبذلك يتطلب من الشركة تعزيز الجوانب الايجابية لديها والسعي لإزالة الجوانب السلبية.

المبحث الرابع:- ألاستنتاجات والتوصيات

الاستنتاجات

١- على الرغم من اهتمام الشركة بتطبيق ادارة الجودة الشاملة ونظمها وحصولها على مواصفة نظام ادارة الجودة وفق المواصفة (ISO 9001: 2008) الا ان اهتمامها بتطبيق نظام ادارة امن المعلومات وفق المواصفة (ISO 27001: 2013) ما زال محدود لعدم توافر التخصيصات المالية والدعم اللازم من قبل الادارة العليا بتبينه.

٢- ضعف التخصيص المالي لأنشاء وتنفيذ نظام ادارة امن المعلومات على وفق المواصفة (ISO 27001: 2013) بالرغم من مواكبة الشركة لعملية التطور المتسارعة في مجال حماية المعلومات وادارة امنها، بسبب ضعف التخصيص المالي لأنشاء نظام ادارة امن معلومات بالمعنى المستقل ولا يوجد قسم خاص بإدارة امن المعلومات .

٣- لا توجد في الشركة سياسة خاصة بتطبيق نظام ادارة امن المعلومات، وهذا ما جعل دون جعل المسؤوليات موزعة على جميع المستويات الادارية في الشركة فيما يخص ادارة امن المعلومات، اذ تتحدد المسؤولية بمدير قسم الخدمات الفنية ومدير مركز البيانات

٤- تحقق ما يطلق عليه بالفجوة الصفرية في توثيق وتطبيق بعض بنود المواصفة وتطبيقها في الشركة العامة للأنظمة الالكترونية / مركز البيانات وهو ما برز في البنود الاتية :

أ- البند **(٢.٤ فهم حاجات وتوقعات الاطراف المهتمة)** وذلك لان الشركة تحدد متطلباتهم

ب- البند **(٢.٧ الكفاءة)**، اذ حقق هذا البند الفجوة الصفرية، اي ان الشركة تقوم بتعيين الكفاءات الضرورية للأفراد المؤثرين في اداء العمل كذلك توفر الشركة التدريب للتحقيق الكفاءة المطلوبة.

٥- لاتوجد خطة موثقة لمعالجة المخاطر في الشركة، اذ يقوم المتخصصون في الشركة في مركز البيانات بالتصدي تلقائيا للمعالجة المخاطر، من خلال مجموعة من الاجراءات التي يقومون بها تلقائيا للتصدي للمخاطر .

٦- لم يحدد مجال خاص لأنشاء وتنفيذ وصيانة نظام للإدارة امن المعلومات وفقا للمواصفة(ISO 27001: 2013) بالرغم من توافر البيئة المناسبة وهي (مركز البيانات) الا انهم لا يوثقوا ذلك في دليل الشركة

٧- ان عملية الحصول على شهادة (ISO 27001: 2013) تضمن تحديد وتحليل وتقييم منتظم ومنهجي للمخاطر وتحقيق ميزة تنافسية للشركة في مجال امن المعلومات وحمايتها.

٨- تعتمد الشركة على السياسات والتعليمات التي تصاحب البرامج والمعدات في التنصيب والتشغيل والادامة وليس بالاعتماد على المواصفة الخاصة بأمن المعلومات (ISO 27001: 2013).

٩- هناك ولاء للزبون، فمن خلال المعايشة الميدانية للباحثان، لوحظ ان الزبائن يتوافدون الى الشركة لتجديد رخصة الانظمة، مما دليل على ان الزبون راضي على الخدمة المقدمة .

١٠- لا يوجد تدقيق خاص بنظام ادارة امن المعلومات وفقا للمواصفة (ISO 27007: 2011) الخاصة بتدقيق ومراقبة نظام ادارة امن المعلومات لعدم وجود نظام ادارة امن معلومات اصلا .

التوصيات

١-ضرورة توافر الدعم المالي اللازم لكي تسطيع الشركة بأنشاء نظام ادارة امن المعلومات وفقا المواصفة (ISO 27001: 2013) ويجب على الادارة العليا ان تعي وتدعم أنشاء وتنفيذ وصيانة نظام ادارة امن المعلومات

٢-ضرورة وضع خطة موثقة لمعالجة مخاطر امن المعلومات .

٣-وضع سياسة خاصة بنظام ادارة امن المعلومات ويجب ان تكون واضحة ومعلنة لدى جميع الافراد العاملين في المنظمة، فضلا عن زبائنها الخارجين.

٤-يجب ان تحدد الشركة مجال خاص لأنشاء وتنفيذ وصيانة نظام للإدارة امن المعلومات وفقا للمواصفة *(ISO 27001: 2013)* بالرغم من توافر البيئة المناسبة وهي (مركز البيانات)

٥- اعتماد مبدا العمل الوقائي من خلال وضع اجراء المتابعة والمراقبة والقياس والتحليل والقضاء على حالات عدم المطابقة ومنع حدوثها .

٥-ضرورة انشاء وتنفيذ وصيانة نظام ادارة امن المعلومات وفق المواصفة(ISO 27001: 2013)

٦-ضرورة الاعتماد على مواصفة(ISO 27007: 2011) الخاصة بتدقيق ومراقبة نظام ادارة امن المعلومات.

٧-ضرورة الحفاظ على وتعزيز البنود التي حققت الفجوة الصفرية وهما بند (فهم حاجات وتوقعات الاطراف المهتمة والكفاءة)

٨-ضرورة الاعتماد على المواصفة الخاصة بأمن المعلومات(ISO 27001: 2013) وليس بالاعتماد على السياسات والتعليمات التي تصاحب البرامج والمعدات في التنصيب والتشغيل والادامة.

المصادر

١- السالمي ، علاء ، الكيلاني ، عثمان ، البياتي ، هلال ، (٢٠١٢) ، **" اساسيات نظم المعلومات الإدارية "** ، دار المناهج للنشر والتوزيع ، الاردن .

٢- الطائي، يوسف حجيم ، العجيلي ،محمد عاصي والحكيم، ليث علي (2009) . **نظم ادارة الجودة: في المنظمات الانتاجية والخدمية.**: دار اليازوري العلمية للنشر والتوزيع، عمان- الاردن .

٣- القحطاني، منصور بن سعيد (٢٠٠٨)، **تهديدات الامن المعلوماتي وسبل مواجهتها: دراسة مسحية لمنسوبي مركز الحاسوب الالي بالقوات البحرية الملكية السعودية بالرياض**، جامعة نايف للعلوم الامنية، السعودية، الرياض .

٤- عبد الكريم، نهاد عبد اللطيف، الربيعي، خلود هادي، (٢٠١٣)، **" أمن وسرية المعلومات واثرهما على الاداء التنافسي: دراسة تطبيقية في شركتي التأمين العراقية العامة والحمراء للتأمين الاهلية"**، مجلة دراسات محاسبية ومالية، مجلد(٨)، العدد(٢٣).

5- Andress, Jason, (2011), **" The Basics of information security : Understanding the Fundamentals of inforsecu in theory and Practice"** , 1st .ed, Elsevier Inc .

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

7- Calder , Alan (2009).**Implementing Infoormation Security based on ISO 27001/ISO27002-Amanagement Guid**,(2nd ed) . London,England :Van Haren Publishing.

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

9- Sewuster, Pim, (2011), **" Information Security in Practice: the Practice of using ISO 27002 in the Public Sector,** Master Thesis .

10- Sojcik, Pavol, (2012), **" Tools for information Security Management",** Faculties informatice Master Thesis, Universities- Masarykiana.

11- Eroglu, Sahika & Cakmak, Tolga (2016), **" Enterprise information Systems within the Context of information Security : a risk assessment for organization in Turkey"** , Procedia Computer Science, PP(979- 986)

12- BSI- Standard 100- 1, (2008), **"Information Security Management Systems (ISMS)"**, Version 1.5, Bundeasamt Fursicherheit in der information stechnik, Godesberger Allee- Germany

13- ISO/IEC 27001:2013**, "International Standard – Information technology- Information security management systems- Requirements**"(2nd ed.) .Geneva: ISO Copyright Office.

14- ISO/IEC 27002:2013" **Information technology – Security techniques - Code of practice for information security controls"**