دور المدقق الخارجي في تقييم امن انظمة تكنولوجيا المعلومات في ضوء المواصفة القياسية (ISO/IEC٢٧٠٠١) (بحث تطبيقي على عينة من المصارف الخاصة)

The role of the external auditor in assessing the security of information technology systems in light of (ISO/IEC 27001) (Applied research on a sample of private banks)

راغب فخري عطية جامعة بغداد /المعهد العالي للدراسات المحاسبية والمالية raghib.fakhri@gmail.com
أ. م.د محمود اسماعيل محمد جامعة بغداد /المعهد العالي للدراسات المحاسبية والمالية t.planner@gmail.com

المستخلص :

يهدف هذا البحث الى تسليط الضوء على ضرورة انشاء نظام ادارة لأمن المعلومات تدار من خلاله المخاطر الامنية المصرفية في ضوء معيار الايزو (ISO/IEC ٢٧٠٠١) والذي من خلاله تسعى ادارات المصارف الى اثبات ادارة انظمتها الامنية وضوابطها وفق توصيفات المعيار للحصول على شهادة امن معترف بها دولياً، وحاجة الادارة العليا في المصارف الى شخص مستقل ذو تأهيل علمي وعملي وحاصل على شهادات معتمدة في مجال تكنولوجيا المعلومات لغرض مساعدتها في التأكد من مستوى التوافق بين السياسات والاجراءات المطبقة والسياسات الموصوفة في المعيار (ISO/IEC ٢٧٠٠١)، وقد تم إعتماد (قائمة فحص) مستندة الى المواصفات القياسية والاجراءات الواردة في المعيار كأداة رئيسية لجمع وتحليل البيانات والمعلومات لعينة من المصارف الخاصة، وفي ضوء عملية التطبيق تم الوصول الى عدد من الاستنتاجات كان ابرزها، عدم تحقيق المصارف عينة البحث لجميع متطلبات وشروط المواصفة القياسية (ISO/IEC٢٧٠٠١)، ووجود نقاط ضعف وخلل في آمنية الانظمة المستخدمة لمعالجة البيانات والمعلومات مما يتطلب الوقوف عليها ودراستها، وقدم الباحثان عدد من التوصيات ابرزها، على ادارات المصارف عينة البحث زيادة الاهتمام بتلبية متطلبات الجودة فيما يتعلق بأمن معلوماتها من خلال تلبية متطلبات الاعتمادية لأمن تكنولوجيا المعلومات والواردة في المواصفة القياسية (ISO/IEC 27001)، مع ضرورة الاستعانة بمستشارين ومدققين خارجيين متخصصين في مجال آمن المعلومات لغرض فحص امنية الأنظمة المطبقة في المصرف.

الكلمات المفتاحية: المصارف الخاصة، المدقق الخارجي، تكنولوجيا آمن المعلومات المصرفية، المواصفة القياسية (ISO/IEC 27001).

Abstract:

This research aims to shed light on the necessity of establishing an information security management system through which banking security risks are managed in the light of the ISO (IEC 27001) standard, through which bank departments seek to demonstrate the management of their security systems and their controls in accordance with the specifications of the standard to obtain an internationally recognized security certificate And the need for senior management in banks to an independent person with scientific and practical qualification and who has accredited certificates in the field of information technology for the purpose of helping them to verify the level of compatibility between the policies and procedures applied and the policies described in the standard (ISO / IEC 27001), has been approved (checklist) Based on the standard specifications and procedures mentioned in the standard as a main tool for collecting and analyzing data and information for a sample of private banks, and in the light of the application process a number of conclusions were reached, the most prominent of which is the failure of banks to fulfill the research sample for all the requirements and conditions of the standard (ISO / IEC) 27001. Weaknesses and imbalances in the security of the systems used to process data and information, which requires standing on them and studying them, and the researchers made a number of recommendations, the most prominent of which are on the banks 'departments. To discuss increasing interest in meeting quality requirements in relation to the security of its information by meeting the reliability requirements of information technology security contained in the standard

(ISO/IEC 27001), with the need to seek external consultants and auditors specialized in the field of information security for the purpose of security checks of the systems applied in the bank..

Keywords: private banks, external auditor, ISO (IEC 27001), banking information security technology.

المقدمة :

في ظل التحولات العديدة التي حصلت في شتى المجالات ومنها الثورة الحاصلة في انظمة تكنولوجيا المعلومات وتطبيقاتها والتي اصبحت العنصر الاساس في اداء معظم الانشطة لمختلف المنظمات ومنها القطاع المصرفي، وتزايد استخدام التكنولوجيا المصرفية في تقديم الخدمات والمنتجات المصرفية، حيث اصبحت التكنولوجيا عامل تمكين رئيسي وميزة تنافسية للمصارف تتميز بها ووسيلة لجذب العملاء وزيادة الحصة السوقية. ان ادخال تكنولوجيا المعلومات في القطاع المصرفي والتي مكنت من إعادة تصميم هياكلها وتحولها من الهياكل التقليدية الى هياكل اوسع تلائم متطلبات التكنولوجيا، وتوسيع نطاق العمل وتدفق المعلومات، وتغيير في اساليب اداء الانشطة وتقديم الخدمات والمنتجات المصرفية، كل هذا ادى الى الحاجة الى تدقيق وتقييم امن سياسات واجراءات انظمة تكنولوجيا المعلومات المتبعة في المصرف من قبل شخص مستقل مؤهل علميا وعملياً من اجل رفع تقارير الرقابة وتقييم الاداء عن مدى مطابقة سياسات واجراءات امن تكنولوجيا المعلومات المتبعة مع المواصفة القياسية (ISO/IEC 27001)، من اجل تحديد نقاط الضعف والخلل في سياسات واجراءات امن المعلومات وتقديم التوصيات بتحسينها ومعالجتها. مما تقدم، ولأجل مناقشة هذه الموضوعات المهمة والحساسة، فقد إشتمل البحث على أربعة محاور، خصص المحور الأول لعرض منهجية البحث وبعض الدراسات السابقة، فيما كرَّس المبحث الثاني للإحاطة بالإطار النظري للمدقق الخارجي وتكنولوجيا المعلومات المصرفية والمواصفة القياسية (ISO/IEC 27001)، بينما خصص المبحث الثالث لعرض الجانب التطبيقي، اما المبحث الرابع فقد ضم مجموعة من الإستنتاجات والتوصيات.

المحور الاول/منهجية البحث والدراسات السابقة

١- منهجية البحث:

١-١- مشكلة البحث Research Problem:

تتمثل مشكلة البحث في ضرورة فحص وتقييم الأدارات العليا في المصارف لآمن انظمة البيانات والمعلومات بشكل دوري ومدى تطبيقها لأجراءات وسياسات آمن المعلومات في ضوء المواصفة القياسية (ISO/IEC 27001) .

١-٢- أهمية البحث Research Significance:

تكمن أهمية البحث من كونه يسلط الضوء على ضرورة تطبيق المصارف لمعايير الجودة المعتمدة عالمياً في قطاع تكنولوجيا المعلومات ومنها معيار الايزو (ISO/IEC٢٧٠٠١) والذي يوصف الاحتياجات الى انشاء وتشغيل ومراقبة وصيانة وتحسين نظام ادارة امن المعلومات والمخاطر المصرفية لما لها من تأثير مباشر على ثقة العملاء بالمصارف وزيادة جودة الخدمات والمنتجات المصرفية المقدمة، اضافة الى حاجة المصرف الى مدقق خارجي معتمد في مجال انظمة المعلومات، لغرض مساعدتها في التأكد من مستوى التوافق بين السياسات والاجراءات والضوابط المتبعة في المصرف وبين الاجراءات والسياسات الموصوفة في المعيار (ISO/IEC ٢٧٠٠١) .

١-٣- أهداف البحث Research Objectives:

يسعى البحث إلى تحقيق الأهداف الآتية:

أ- التعريف بتكنولوجيا المعلومات، وتسليط الضوء على تكنولوجيا المعلومات والانظمة المصرفية المستخدمة.

ب- توضيح التطور في مهام ومسؤوليات المدقق الخارجي.

ج- التعريف بالمنظمة الدولية للتوحيد القياسي (ISO/IEC) والمعايير والمواصفات التي تصدرها ومن ضمنها المواصفة (ISO/IEC 27001) .

د- اعداد قائمة فحص للتأكد من مستوى التوافق بين السياسات والاجراءات والضوابط المتبعة في المصرف وبين الاجراءات والسياسات الموصوفة في المعيار (ISO/IEC٢٧٠٠١) وتطبيقها على المصارف عينة البحث .

١-٤- فرضية البحث Research Hypothesis :

ان استعانة الادارة العليا في المصارف بالمدقق الخارجي المؤهل علمياً وعملياً عند تقييم امن انظمة تكنولوجيا المعلومات ومدى تطبيقها المواصفة القياسية الدولية (ISO/IEC 27001) يساعد في تحسين جودة آمن المعلومات .

١-٥- منهج البحث Research Tool:

أ- **المنهج الوصفي:** تم الإعتماد على المنهج الوصفي التحليلي لدراسة مشكلة البحث وإثبات الفرضية من خلال تحليل البيانات للوصول الى النتائج وتحديد التوصيات الملائمة .

ب- **الجانب التطبيقي** : اعتمد الباحثين على دراسة البيانات وتحليلها من خلال تطبيق قائمة الفحص على المصارف عينة البحث (الوطني الاسلامي، الشرق الاوسط، الخليج التجاري) .

١-٦- الدراسات السابقة Previous studies:

ومن بين أهم تلك الدراسات ما يأتي:-

اولاً- دراسة الزهرة واخرون (٢٠١٦): فعالية التدقيق في ظل تطور تكنولوجيا المعلومات

حيث بينت هذه الدراسة الى ضرورة الاهتمام بعملية التدقيق وتطويرها بأستخدام الاساليب الحديثة ومحاولة وابراز التطوير في تكنولوجيا المعلومات ومدى تأثيره على التطور في مهام ومسؤوليات المدقق وخلصت الدراسة الى عدد من النقاط المهمة ابرزها :

(١) ان تطور تكنولوجيا المعلومات في المؤسسة قد فرض واقعاً جديداً على عملية التدقيق والمدققين، الامر الذي ادى الى تطور أساليب التدقيق وضرورة الاعتماد على برامج الكترونية متخصصة تسهل من انجاز مهام التدقيق بأقل وقت ممكن واقل التكاليف .

(٢) لا بد ان يكون لدى المدقق مهارات متخصصة وكفاءة عالية في مجال تكنولوجيا المعلومات للتحكم في كافة المخاطر المحتملة والغير محتملة .

ثانياً- الحافظ والنعيمي (٢٠١٣) : دور المواصفة (ISO/IEC ٢٧٠٠١) في تعزيز مفهوم ادارة دورة حياة المعلومات .

حيث تطرقت الدراسة الى مدى المام الشركات الصناعية بالمواصفة القياسية (ISO/IEC 27001) وما مدى التوافق بينها وبين ادارة دروة حياة المعلومات وتوصلت الدراسة الى عدد من النقاط ابرزها :-

(١) التأكيد على المفاهيم الحديثة في جودة حماية المعلومات وذلك من خلال تطبيق المواصفة (ISO/IEC 27001) كمواصفة حديثة لحماية المعلومات .

(٢) اهمية اصدار وثيقة لأمن تكنولوجيا المعلومات متبوعة بمجموعة من التعليمات والسياسات التي تتوافق مع المواصفات الامنية (ISO/IEC 27001) ومراجعة تلك السياسات بصورة دورية.

المحور الثاني/ التدقيق الخارجي وآمن تكنولوجيا المعلومات والمواصفة القياسية ISO/IEC 27001

٢-١- التدقيق الخارجي

٢-١-١- مفهوم واهمية التدقيق الخارجي :

ان الغرض الرئيسي للتدقيق الخارجي هو ابداء الرأي في سلامة وصحة التقارير المالية الناتجة عن النظام المحاسبي حيث انه يلعب دورا مهما في الاوساط المالية والاوساط الحكومية الاقتصادية، والمعلومات المالية التي نعتمد عليها ونثق بها ضرورية لأي مجتمع والمستثمر يتخذ قرارات الشراء والبيع لأستثماراته، البنوك تتخذ قرارات اعطاء القروض والسلطات الضريبية تقوم بأحتساب

الدخل الخاضع للضريبة كل هذه الامور وغيرها تعتمد على معلومات جهزت او قدمت من قبل الاخرين ولهذا نشأت الحاجة الى وجود خدمة المدقق المستقل والمحايد وهذا الشخص المستقل والمحايد سيقوم بأعلام الاطراف الاخرى، ان كانت هذه المعلومات المالية تمثل بأعتدال او بوضوح ومن جميع جوانبها المادية المركز المالي كما هو بتاريخ معين والنشاط للسنة او الفترة المنتهية لذلك.(عبدالله:٢٠٠٤،١٥)

ويعرف بأنه (تجميع وتقييم الادلة المرتبطة بالمعلومات بغية التحديد والابلاغ عن درجة التوافق بين المعلومات والمعايير الموضوعة ، وينبغي أن يتم من قبل شخص كفوء ومستقل). (Arens,2008:24)

وتناولت ادبيات التدقيق أهميتة فضلا عن اللجنة الدولية للممارسة مهنة التدقيق المنبثقة عن الاتحاد الدولي للمحاسبين (IFAC)، والآتي عرض أهمية التدقيق : (المطارنة :٢٠٠٩،١٩)

أ- تعتمد ادارة المنشأة اعتماداً كلياً على البيانات المالية المدققة من قبل مدقق خارجي مستقل، في التخطيط ومراقبة الاداء وبالتالي فان توكيد المدقق على قوائمها المالية سيمنحها درجة كبيرة من الثقة

ب- تعتمد المؤسسات المالية والمصارف التجارية على القوائم المالية المدققة من قبل مدقق خارجي مستقل عند فحصها للمراكز المالية للمشروعات التي تتقدم بطلب قرض وتسهيلات ائتمانية منها.

ج- تعتمد الهيئات الحكومية واجهزة الدولة على القوائم المالية المدققة لاغراض (التخطيط والرقابة وفرض الضرائب وتحديد الأسعار وتقرير الاعانات لبعض الصناعات).

د- أهمية التدقيق في تخصيص الموارد المتاحة بأفضل كفاءة ممكنة لانتاج السلع والخدمات التي يزيد الطلب عليها، فالموارد النادرة تجتذبها الوحدات الاقتصادية القادرة على أستخدامها بأفضل كفاءة والتي تظهرها البيانات المالية المدققة الظاهرة في القوائم المالية.

٢-١-٢- التطور في خدمات المدقق الخارجي

لقد تطورت الخدمات المهنية التي يقدمها المدقق الخارجي المستقل، عاكسة بذلك تأثرها بعدة عوامل مختلفة كالعولمة والمنافسة ومتطلبات سوق العمل والتي كانت سبباً جوهرياً في توسيع تلك الخدمات وعدم اقتصارها على ابداء الرأي بالأمور المالية انما توسعت لتقديم خدمات غير مالية تساعد الادارة في تحقيق اهدافها، متمثلة بخدمات الاستشارات الادارية والضريبية وخدمات التقييم واصدار معايير مستقلة خاصة بتقديم كل نوع من هذه الخدمات، والتي تمثل اضافة نوعية للخدمات التي يقدمها المدقق الخارجي المستقل، ولقد ظهر هناك اختلاف بين الباحثين والمفكرين في تحديد وتبويب الخدمات تلك الخدمات **(تعليق الباحث)**، وكما يأتي :

جدول رقم (١) التطور في الخدمات التي يقدمها المدقق الخارجي

المصدر	الخدمات المقدمة
Boynton & et al. 2001 (:900-976)	• خدمات متنوعة مثل التقارير الخاصة، فحص عناصر خاصة، تدقيق القوائم المالية. • عمليات ابداء الرأي. • خدمات المحاسبة والفحص. • الخدمات التأكيدية.
(Pickett,2005:115-117)	• حدد الكاتب (٦٦) نوع من الخدمات المهنية لمراقب الحسابات الخارجي وبشكل متسلسل
(lowers, et al 2008:3-9)	• خدمات التأكيد . • خدمات التدقيق. • عمليات ابداء الرأي غير التدقيقية . • الخدمات الضريبية. • الخدمات الاستشارية .
(Grawford,2009:1-2)	خدمات التأكيد منها ما يرتبط بـــ: • ما يرتبط بالقوائم المالية التاريخية (خدمات التدقيق والفحص والاعداد) • ما يرتبط بالمعلومات المالية وغير المالية خدمات التصديق وأخرى .

	• الخدمات غير التأكيدية (لخدمات الاستشارية، الخدمات الضريبية، خدمات التقييم ، التخطيط) .
(Arens,et al,2014-13)	خدمات تأكيدية • خدمات التصديق ▪ تدقيق البيانات المالية . ▪ تدقيق الرقابة الداخلية . ▪ الاطلاع او المراجعة . ▪ خدمات تصديق اخرى . ▪ خدمات التصديق التي تتعلق بتكنولوجيا المعلومات . • خدمات التأكيد اخرى . ▪ خدمات تقييم مخاطر الغش والتصرفات غير القانونية . ▪ المخاطر الخاصة بالاستثمارات والادوات المالية . خدمات غير تاكيدية ▪ خدمات تقييم الاداء . ▪ الخدمات الاستشارية . ▪ خدمات التخطيط المالي.

المصدر : من اعداد الباحث بالاعتماد على المصادر اعلاه .

حيث نلاحظ من الجدول اختلاف الباحثين في تحديد الخدمات التي يقدمها مراقب الحسابات وعدم تحديد اسس معتمدة في عملية تحديد الخدمات المقدمة بالأضافة الى توسع الخدمات وتطورها وشمولها لأنظمة تكنولوجيا المعلومات والتي سوف يتم التركيز عليها في دراستنا في هذا البحث .

٢-٢- آمن تكنولوجيا المعلومات (Information Technology)

٢-٢-١- مفهوم تكنولوجيا المعلومات (Information Technology)

لقد عرفت التكنولوجيا بتسميات عديدة بحيث وصفت في أول ظهور لها على انها Modern information and communication technology (NTIC) ثم حذفت كلمة الحديثة من التسمية لتصبح Information and Communication Technology (TIC)، ثم مع بداية استخدام الانترنت في التسعينات ظهرت بعض الأدبيات التي استخدم مؤلفوها التسمية المختصرة Information Technology (IT). (محاجبية،٢٠١٤: ١٧١)

ويقوم مفهوم تكنولوجيا المعلومات على فكرة أستخدام الحاسب الآلي في معالجة المعلومات من حيث تخزينها واسترجاعها وطباعتها وقد استخدم مصطلح تكنولوجيا المعلومات (IT) لتشمل ثورة القرن الحالي في مجال أتمتة نظم المعلومات، ويمكن تعريف تكنولوجيا المعلومات بأنه (كل اشكال التكنولوجيا المستخدمة لجمع ومعالجة وتخزين والتعامل مع المعلومات، بحيث يمكن تمثيلها بمجموعة من المكونات المترابطة التي تجمع وتعالج وتخزن وتنشر البيانات والمعلومات وتوفر وسيلة للتغذية العكسية لغرض تحقيق هدف معين). (Pearlson&saunders,2006:14)

٢-٢-٢-اهمية امن المعلومات

مع تطور وسائل التكنولوجيا والتخزين وتبادلها بطرق مختلفة أو ما يسمى بنقل البيانات من موقع الى أخر عبر الشبكة العنكبوتية، حيث اصبح ينظر الى آمن المعلومات بأهمية بالغة ويتميز آمن المعلومات بوصفه بمجموعة من الوسائل والادوات التي يتوجب توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية ويتميز امن المعلومات بأنه استباقي، بمعنى انه يجب ان تتوقع سياسة امن المعلومات الحوادث والمشكلات المستقبلية ووضع الاجراءات المناسبة للوقاية والحد منها (AL-Kolaly,2005:59)، وتتبع اهمية دراسة امن المعلومات من كونها تستخدم من قبل الجميع سواء اكانوا (اشخاص او منظمات او حكومات) وفي بعض الاحيان تكون حماية امن المعلومات هي الفاصل بين الربح والخسارة للمنظمات، وقد تكلف الفرد ثروته حيث ان تعزيز ثقة العملاء بالمنظمة تأتي من خلال حماية المنظمة لمواردها، وبالتالي اصبحت المشكلة الان ليس في الحصول على المعلومات، وانما

كيفية حماية هذه المعلومات من الاخطار التي تهددها سواء اكانت الاخطر داخلية ام خارجية (داوود، ٢٠٠٤: ٣٠)، وهنا كان لا على مدراء تكنولوجيا المعلومات وضع الجدران النارية وبرامج مكافحة الفايروسات والاختراق والتسلل وغيرها من اجل ضمان امن وحماية البيانات والمعلومات .

٢-٣- المواصفات القياسية لتكنولوجيا المعلومات ومعيار الايزو ISO / IEC 27001

وفقًا لمعايير الجودة العالمية الصادرة عن المنظمة العالمية للتوحيد القياسي[١] (ISO/IEC) المعنية بوضع المعايير لكافة الوحدات والمؤسسات الراغبة في الحصول على شهادات الجودة العالمية المتعارف عليها في كافة الأوساط والمجالات، حيث يقدم المستشارون العالميون خدمات استشارية ذات قيمة مضافة لتأهيل الشركات والمؤسسات والهيئات للتوافق مع متطلبات مواصفات الجودة، وان مطابقتها للمواصفات يعمل على رفع كفاءة الأداء والفاعلية والتميز بإرضاء عملائها وتحقيق اهدافها .

ومن ضمن المعايير التي تصدرها المنظمة العالمية للتوحيد القياسي (ISO/IEC)، هي المعايير الخاصة بتكنولوجيا المعلومات وأهمها معيار الايزو **ISO/IEC 27001** الخاص بأمنية المعلومات والذي يعتبر احد معايير او مداخل الجودة لتكنولوجيا المعلومات المطبقة في المصارف، تم إعداد هذه المواصفة القياسية الدولية لتوفير متطلبات إنشاء وتنفيذ وصيانة نظام إدارة أمن المعلومات باستمرار. واعتماد نظام إدارة أمن المعلومات هو قرار استراتيجي للمؤسسة، ويتأثر تطبيق نظام إدارة أمن المعلومات في المنظمة باحتياجات المنظمة وأهدافها ومتطلبات الأمن والعمليات التنظيمية المستخدمة وحجم وهيكل المؤسسة. ويحافظ نظام إدارة أمن المعلومات على سرية وسلامة وتوافر المعلومات من خلال تطبيق عملية إدارة المخاطر ويعطي الثقة للأطراف المعنية بأن المخاطر تدار بشكل مناسب، **(ISO / IEC 27001,2013:10-22)**.

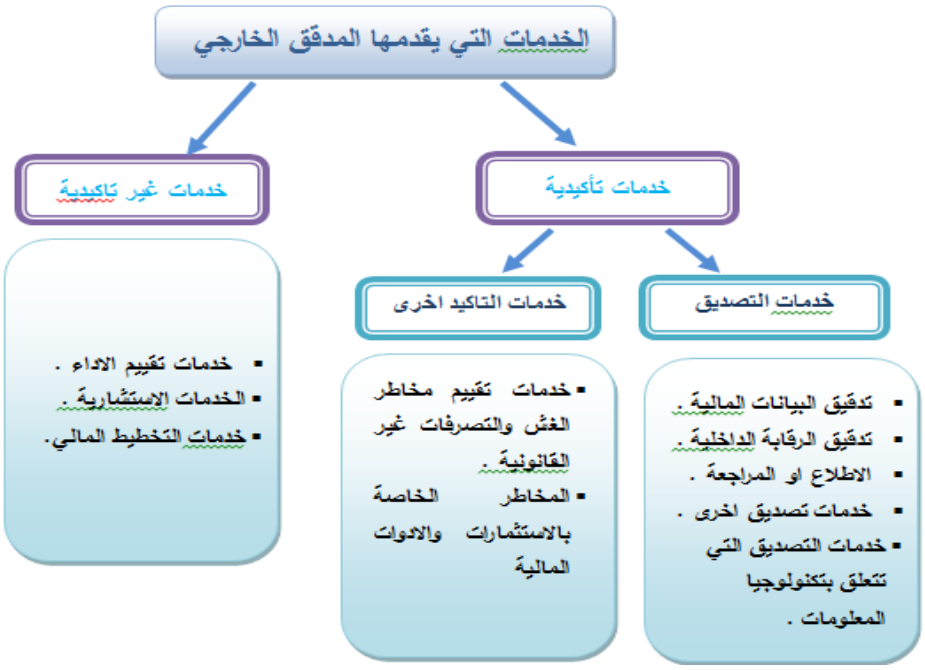
٢-٤- دور المدقق الخارجي في تقييم آمن انظمة تكنولوجيا المعلومات

توفر عمليات تقييم آمن تكنولوجيا المعلومات لمجلس الادارة والادارة العليا تقييما موضوعياً مستقلاً لأدارة تكنولوجيا المعلومات، حيث يجب على المصرف انشاء هيكل تنظيمي وتقارير لعمليات تقييم آمن تكنولوجيا المعلومات بطريقة تحافظ على استقلالية وموضوعية عمليات التقييم لأمن تكنولوجيا المعلومات، وعلى مجلس الادارة رصد الموازنات الكافية وتخصيص الادوات اللازمة بما في ذلك العنصر البشري المؤهل والمتخصص بتكنولوجيا المعلومات وبالتنسيق مع المدقق الخارجي بهدف التأكد من كفاءة وفاعلية توظيف وادارة آمن موارد تكنولوجيا المعلومات، وعمليات المراجعة الفنية المتخصصة (IT Audit)، من خلال الاستعانة بكوادر خارجية مهنية مؤهلة وحاصلة على شهادات دولية معتمدة في هذا المجال ومن أمثلتها (CISM شهادة مدير امن المعلومات)، (شهادة ضبط انظمة المخاطر والمعلومات CRISC) (CISA مدقق نظم معلومات معتمد)،(COPIT-5,2012:20) لقد أدركت المنظمات أهمية وجود حواجز لحماية آمن معلوماتها وانظمتها خصوصًا عندما تكون هذه المعلومات ذات قيمة وتؤثر على ثقة الزبون بأدارة امن المعلومات للمصرف، ويعتبر معيار الايزو(ISO/IEC27001) والخاص بأمن تكنولوجيا المعلومات هو احد المعايير الذي يوفر مواصفات ومتطلبات نظام إدارة أمن المعلومات والذي يمكن للمدقق الخارجي الاستناد اليه عند تقييم آمن انظمة تكنولوجيا المعلومات لأدارات المصارف لما يوفره هذا المعيار من ضمان للجودة وتحسين لأدارة امن المعلومات. **(تعليق الباحث)**

حيث تقسم الخدمات التي يقدمها المدقق الخارجي الى خدمات تأكيدية وخدمات غير تأكيدية وكما يأتي:

[١] ISO/ هي منظمة دولية غير حكومية تتكون من هيئات المعايير أو المقاييس الوطنية وتضم ممثلين لـ (١٦٢) دولة ويقع مقرها في جنيف، سويسرا وتعمل على تطوير ونشر مجموعة واسعة من المعايير لمجموعة واسعة من المنتجات والمواد والعمليات لـ (٩٧) مجالاً ومن ضمنها تكنولوجيا المعلومات .

شكل رقم (١) الخدمات التي يقدمها المدقق الخارجي



المصدر :اعداد الباحث بالاعتماد على (Arens,et al,2014:8-13)

حيث نلاحظ من الشكل اعلاه ان من بين الخدمات التي يقدمها المدقق الخارجي هي:

خدمات التصديق الاخرى : وهي تتمثل بالخدمات المرتبطة بالتصديق على المعلومات المالية وغير المالية، حيث يقدم مراقب الحسابات شهادة تصديقية في المعلومات المالية وغير المالية التي تعدها الادارة (AICPA,2010:1016)، ان خدمات التصديق تتجه نحو بيان مدى دقة وموثوقية مزاعم معينة تم اعدادها من قبل شخص معين وتقديم تقرير مكتوب عنها (Knechcl,2001:4)، وتشمل خدمات التصديق التي تتعلق بتكنولوجيا المعلومات، حيث تم اجراء البحوث والدراسات بين المعهد الامريكي (AICPA) والكندي (CICA)، حول قيام مراقب الحسابات في الولايات المتحدة وكندا بمنح شهادة التصديق عن موثوقية نظام المعلومات (System Trust) اي تقرير التصديق، (Elder,et al:2010:801)، وان خدمة التأكيد على الثقة في موقع الشركة على شبكة الانترنت هي خدمة مهنية تصديقية غير تقليدية لمراقب الحسابات يبدي فيها رأيا على مدى صدق تأكيدات الإدارة بشأن استيفاء موقع الشركة على شبكة الانترنت لمعايير الثقة (الامن، توفر المعلومات، الخصوصية، السرية).(علي وشحاتة،٢٠١١، ٣٤)، حيث يتم التعاقد مع المحاسب القانوني للحصول على تأكيد معقول بان موقع الشركة على الشبكة العنكبوتية يحقق بعض المبادئ الاساسية لتحسين الثقة مع العميل، فهي خدمات تأكيدية تزود الادارة ومجلس الادارة والطرف الاخر بدرجة من المصداقية بان النظم تحقق متطلبات ومبادئ اساسية. (Arens,et al,2014:793).

المحور الثالث / مدى التزام المصارف بتطبيق المواصفة الدولية (ISO/IEC 27001)

٣-١- تقييم مدى التزام المصارف بمتطلبات امن المعلومات وفق المواصفة الدولية (ISO/IEC 27001)

سيقوم الباحث بتقييم نظام ادارة أمن المعلومات في المصارف عينة البحث (مصرف الشرق الاوسط، مصرف الخليج، مصرف الوطني الاسلامي)، من خلال قياس مدى التزام كل مصرف بالمتطلبات والمواصفات القياسية الواردة في معيار الايزو (ISO/IEC 27001)، والتي سيتم عرضها من خلال اعداد جدول يلخص متطلبات تطبيق المعيار وفحص مدى التزام المصارف عينة البحث بتلك المتطلبات وتحليل البيانات التي جمعت من واقع المصارف عينة البحث، من خلال اجراء المقابلات الشخصية الميدانية وتوثيق كل متطلب من المتطلبات الواردة في المواصفة (ISO/IEC 27001) ويتطلب مقياس تنفيذ الالتزام بكل بند ان

يتوفر هناك اكثر من جانب فمثلاً يعني تطبيق البند ان المصرف قد التزم بتوفير متطلبات البند من كافة جوانبه، اما الملتزم بشكل جزئي فيعني ان المصارف قد التزمت جزئياً بالمتطلب مثلاً (طبقت المتطلب بشكل عملي الا انه غير موثق بتقارير او اجراءات عمل مكتوبة)، اما بالنسبة لغير الملتزم فهذا يعني ان المصرف لم يتم الالتزام بتطبيق البند من كافة جوانبه وبأي شكل من الاشكال، وتوضح الجداول الاتية المواصفات والمتطلبات الواردة في المعيار ومدى التزام المصارف بها:-

جدول رقم (٢)المواصفات الواردة في معيار الايزو (ISO/IEC 27001) وتقييم التزام المصارف بها

ت	المتطلبات والمواصفات الواردة في معيار الايزو(ISO/IEC 27001)	مصرف الشرق الاوسط			مصرف الخليج			مصرف الوطني الاسلامي		
		التزام كامل	التزام جزئي	غير ملتزم	التزام كامل	التزام جزئي	غير ملتزم	التزام كامل	التزام جزئي	غير ملتزم
A- سياسات أمن المعلومات										
A.1	يتم تحديد واعتماد مجموعة من سياسات أمن المعلومات من قبل الإدارة، ونشرها وإبلاغ الموظفين والأطراف الخارجية ذات الصلة.		✓			✓			✓	
A.٢	يجب مراجعة سياسات أمن المعلومات كل فترة أو إذا حدثت تغييرات كبيرة لضمان استمرارية ملاءمتها وكفائتها .			✓	✓					✓
A.3	اعداد تقارير مراجعة لسياسات آمن المعلومات بأنتظام بصورة دورية ورفعها الى الادارة العليا.			✓	✓				✓	
B- تنظيم أمن المعلومات										
B.1	يجب تحديد وتخصيص جميع مسؤوليات أمن المعلومات من خلال خرائط المسؤولية (التوصيف الوظيفي).	✓			✓			✓		
B.2	الحفاظ على التواصل المناسب مع المستشارين المتخصصين في مجال تكنولوجيا المعلومات والجمعيات المهنية لغرض تطوير وتنظم العمل.	✓				✓			✓	
B.3	التأكد من وجود توافق بين هيكلية تكنولوجيا المعلومات ومتطلبات بيئة العمل المصرفي.			✓			✓			✓
C- إدارة الأصول										
C.1	يجب على جميع الموظفين والمستخدمين الخارجيين إعادة جميع الأصول التنظيمية التي بحوزتهم عند إنهاء عملهم أو عقدهم أو اتفاقهم.	✓			✓			✓		
C.٢	تحديد الأصول المرتبطة بمعالجة البيانات والمعلومات ووضع قائمة جرد لهذه الأصول وصيانتها بشكل دوري .	✓			✓				✓	
C.٣	تحديد وتوثيق وتنفيذ قواعد الاستخدام المقبول للأصول وموارد تكنولوجيا المعلومات والمرتبطة بمعالجة البيانات والمعلومات .			✓			✓			✓
D - آمن الموارد البشرية										
D.١	يجب أن تتم عمليات التحقق من جميع المرشحين للعمل وفقًا للقوانين واللوائح والأخلاقيات ذات الصلة وتتناسب مع متطلبات العمل وامن المعلومات المطلوب .	✓			✓			✓		
D. 2	يجب أن توضح الاتفاقيات التعاقدية مع الموظفين والمقاولين مسؤولياتهم تجاه أمن المعلومات.			✓			✓			✓
D. 3	يجب على الإدارة مطالبة جميع الموظفين والمقاولين بتطبيق أمن المعلومات وفقًا للسياسات والإجراءات المعمول بها في المصرف.		✓				✓			✓
D. 4	يجب أن يتلقى جميع موظفي المنظمة، وعند الاقتضاء، التثقيف والتدريب المناسبين في مجال التوعية والتحديثات المنتظمة في السياسات والإجراءات الامنية .	✓					✓		✓	
D. 5	يجب أن تكون هناك اجراءات رادعة رسمية ومبلغ بها لاتخاذ إجراءات ضد الموظفين الذين ارتكبوا انتهاكًا لأمن المعلومات.	✓				✓			✓	
D. 6	يجب تحديد مسؤوليات وواجبات أمن المعلومات التي تبقى سارية بعد إنهاء العمل أو تغييره للموظف أو المورد.			✓			✓			✓
E - آمنية وسائط التخزين										
E.1	تنفيذ الإجراءات الخاصة بإدارة الوسائط القابلة للإزالة وفقًا لنظام التصنيف الذي يتبناه المصرف			✓			✓			✓
E.2	يجب التخلص من الوسائط بأمان عند عدم الحاجة إليها ، باستخدام الإجراءات الرسمية، وضمان عدم الاضرار بالبيئة.			✓			✓			✓
E.3	يجب حماية الوسائط التي تحتوي على معلومات من الوصول غير المصرح به أو سوء الاستخدام أو الفساد أثناء النقل .		✓			✓			✓	
E.4	وجود اجراءات وتعليمات مبلغ بها جميع العاملين بضرورة عدم استخدام وسائط النقل (USP,CD, PORT...etc) وبما يضمن امن وحماية المعلومات من البرامج والاختراقات.		✓			✓				✓
E.5	وجود اجراءات للنسخ الاحتياطي من الملفات والبيانات الخاصة بالعملاء والتأكد من اجراء عملية النسخ اولاً بأول وان وسائط الخزن محمية ضد اعمال التخريب .	✓				✓			✓	
F. ادارة نقاط الضعف في الانظمة										
F.1	الحصول على معلومات حول نقاط الضعف التقنية لنظم المعلومات ومعالجتها في الوقت المناسب، وتقييم تعرض المصرف لهذه الثغرات الأمنية والتدابير المتخذة لمعالجتها.		✓			✓			✓	
F.2	يجب وضع وتنفيذ القواعد التي تحكم تثبيت البرنامج والانظمة من قبل المستخدمين .		✓			✓			✓	
F.3	وجود سجل لتوثيق نقاط الضعف المكتشفة والاجراءات المتخذة لمعالجتها وتصنيف نقاط الضعف بحسب خطورتها.	✓				✓				✓
G. الأمن المادي والبيئي										
G.1	تحديد محيط الأمان واستخدامه لحماية المناطق التي تحتوي على مرافق حساسة أو حرجة للمعلومات ومعالجة المعلومات.	✓					✓			✓
G.2	حماية المناطق الآمنة بواسطة ضوابط دخول مناسبة لضمان السماح فقط للأفراد المخولين والمصرح لهم بالدخول.	✓				✓			✓	
G.3	يجب تصميم وتطبيق الأمن المادي للمكاتب والغرف والمرافق، ضد الكوارث الطبيعية أو الهجمات الضارة أو الحوادث.	✓			✓			✓		
G.4	يجب أن تكون أنظمة إدارة كلمة المرور تفاعلية وتضمن جودة كلمات المرور.		✓			✓			✓	
G.5	يجب إزالة حقوق الوصول لجميع الموظفين والمستخدمين الخارجيين إلى مرافق معالجة المعلومات والمعلومات عند إنهاء عملهم أو عقدهم أو اتفاقهم أو تعديلها عند التغيير.	✓			✓			✓		
G.5	وضع سياسة لمراقبة الدخول وتوثيقها ومراجعتها بناءاً على متطلبات أمن المعلومات .	✓					✓			✓
H. أمن الاتصالات										
H.1	تزويد المستخدمين فقط بالوصول إلى خدمات الشبكة والمخولين في الشبكة الذين لديهم تصاريح استخدامها على وجه التحديد .	✓			✓			✓		
H.2	استخدام انظمة لحماية وإدارة الشبكات والتحكم فيها وحماية البيانات والمعلومات في الأنظمة والتطبيقات.	✓			✓				✓	

H.3	تحديد آليات الأمان ومستويات الخدمة ومتطلبات الإدارة لجميع خدمات الشبكة وإدراجها في اتفاقيات خدمات الشبكة، سواء كانت هذه الخدمات مقدمة داخليا أم خارجيا.	✓				✓				✓
H.4	يتم الفصل بين مجموعات خدمات المستخدمين والمعلومات وأنظمة المعلومات على الشبكات لضمان الحماية الكاملة .	✓			✓			✓		
I. إدارة حوادث أمن المعلومات										
I.1	تحديد المسؤوليات والإجراءات الإدارية لضمان الاستجابة السريعة والفعالة والمنظمة لحوادث أمن المعلومات.	✓				✓				✓
I.2	الإبلاغ عن حوادث أمن المعلومات من خلال قنوات الإدارة المناسبة في أسرع وقت ممكن.	✓				✓			✓	
I.3	على الموظفين والمقاولين الذين يستخدمون أنظمة وخدمات معلومات المنظمة أن يلاحظوا ويبلغوا عن أي مواطن ضعف ملحوظة أو مشتبه في أمن المعلومات في الأنظمة أو الخدمات.		✓		✓			✓	✓	
I.4	يجب تقييم أحداث أمن المعلومات وتصنيفها بحسب اهميتها واعداد تقارير عنها ورفعها الى الادارة العليا .	✓				✓				✓
I.5	يجب الرد على حوادث أمن المعلومات وفقًا للإجراءات الموثقة.	✓				✓			✓	
I.6	تحدد المصارف وتطبق إجراءات تحديد المعلومات وجمعها واقتنائها وحفظها، والتي يمكن أن تكون بمثابة دليل عن الحوادث .	✓			✓					✓
J . الامتثال للمتطلبات القانونية والتعاقدية										
J.1	تنفيذ الإجراءات المناسبة لضمان الامتثال للمتطلبات التشريعية والتنظيمية والتعاقدية المتعلقة بحقوق الملكية الفكرية واستخدام منتجات البرمجيات المسجلة الملكية.	✓				✓		✓		
J.2	حماية السجلات من الفقد والتدمير والتزوير والوصول غير المصرح به والإفراج غير المصرح به، وفقًا للمتطلبات التشريعية والتنظيمية والتعاقدية والتجارية .		✓			✓				✓
J.3	ضمان ادراج التعهد بخصوصية وحماية المعلومات الشخصية للزبائن كما هو مطلوب في التشريعات واللوائح ذات الصلة عند تقديم الخدمات .			✓	✓					✓
J.4	يجب استخدام ضوابط التشفير عند تقديم الخدمات الالكترونية وفقًا لجميع الشروط ذات الصلة بالاتفاقات والتشريعات واللوائح.			✓	✓					✓
K. مراجعة أمن المعلومات										
K.1	يجب مراجعة نهج المصرف في إدارة أمن المعلومات وتنفيذه (أهداف المراقبة والضوابط والسياسات والعمليات والإجراءات الخاصة بأمن المعلومات) بشكل مستقل على فترات مخطط لها أو عند حدوث تغييرات كبيرة.	✓			✓			✓		
K.2	يجب مراجعة أنظمة المعلومات بانتظام للامتثال لسياسات ومعايير أمن المعلومات الخاصة بالمصرف .		✓			✓				✓
K.3	مراجعة وادارة خطط الطوارئ وتقييمها كل فترة والمتعلقة بضمان استمرارية تقديم الخدمة وتوفرها .			✓			✓			✓

٣-٢- قياس مستوى الالتزام بمتطلبات المواصفات القياسية (ISO/IEC 27001) للمصارف عينة البحث :

من اجل تحديد مستوى التزام بمتطلبات معيار الايزو (ISO/IEC 27001) للمصارف عينة البحث والتي تم توضيحها في الجداول السابقة فقد استند الباحثان في عملية القياس الى مقياس من ثلاث درجات لأحتساب مستوى الالتزام، اذا تم اعطاء درجة (١) للمتطلب الذي لم يتم الالتزام به، و(٢) درجة للمتطلب الذي تم الالتزام به جزئياً، و (٣) درجات للمتطلب الذي تم الالتزام به كلياً، وقد تم وضع اساس للتمييز بين الدرجة الجيدة وغير الجديدة سميت بـ(درجة القطع) والتي بلغت (٨٣%) وتم احتسابها على اساس المعادلة الاتية:-

درجة القطع: وهي الدرجة التي تميز بين تحقيق الجيد وغير الجيد على وفق اسس تضعها الجهات المعنية

$$\frac{(٣+٢)}{(٣+٢+١)} = ٨٣\ \%$$

اما الالتزام الجزئي فسيكون أقل من درجة القطع لغاية (٥٠%) والتي تم احتسابها على اساس (١+٢÷٦)، اما الالتزام غير الكامل فسيكون اقل من (٥٠%).

وتوضح الجداول التالية قياس مستوى التزام المصارف عينة البحث بمتطلبات المواصفة القياسية (ISO/IEC 27001)

جدول رقم (٣)مدى التزام المصارف عينة البحث بمتطلبات المواصفة القياسية (ISO/IEC 27001)

متطلبات المواصفة القياسية (ISO/IEC 27001)	تقييم الالتزام	مصرف الشرق الاوسط	مصرف الخليج	مصرف الوطني الاسلامي
سياسة امن المعلومات	الدرجة	4	٨	٥
	نسبة الالتزام	44%	٨٩%	٥٦%
	تقييم الالتزام	غير ملتزم	ملتزم بشكل كامل	ملتزم جزئياً
تنظيم امن المعلومات	الدرجة	٧	٦	٦
	نسبة الالتزام	٧٨%	٦٧%	٦٧%
	تقييم الالتزام	ملتزم جزئياً	ملتزم جزئياً	ملتزم جزئياً
ادارة الاصول	الدرجة	٧	٧	٦
	نسبة الالتزام	٧٨%	٧٨%	٦٧%
	تقييم الالتزام	ملتزم جزئياً	ملتزم جزئياً	ملتزم جزئياً
امن الموارد البشرية	الدرجة	١٣	٩	١٠
	نسبة الالتزام	٧٢%	٥٠%	٥٦%
	تقييم الالتزام	ملتزم جزئياً	ملتزم جزئياً	ملتزم جزئياً
امنية وسائط التخزين	الدرجة	٩	٩	٨
	نسبة الالتزام	٦٠%	٦٠%	٥٣%
	تقييم الالتزام	ملتزم جزئياً	ملتزم جزئياً	ملتزم جزئياً
ادارة نقاط الضعف	الدرجة	٧	٦	7
	نسبة الالتزام	٧٨%	٦٧%	٧٨%
	تقييم الالتزام	ملتزم جزئياً	ملتزم جزئياً	ملتزم جزئياً
الامن المادي والبيئي	الدرجة	١٧	١٢	١٢
	نسبة الالتزام	٩٤%	٦٧%	٦٧%
	تقييم الالتزام	ملتزم بشكل كامل	ملتزم جزئياً	ملتزم جزئياً
امن الاتصالات	الدرجة	١٢	١١	٩
	نسبة الالتزام	١٠٠%	٩٢%	٧٥%
	تقييم الالتزام	ملتزم بشكل كامل	ملتزم بشكل كامل	ملتزم جزئياً
ادارة حوادث المعلومات	الدرجة	١٧	١١	٩
	نسبة الالتزام	٩٤%	٦١%	٥٠%
	تقييم الالتزام	ملتزم بشكل كامل	ملتزم جزئياً	ملتزم جزئياً
الامتثال للمتطلبات القانونية	الدرجة	٧	٧	٦
	نسبة الالتزام	٥٨%	٥٨%	٥٠%
	تقييم الالتزام	ملتزم جزئياً	ملتزم جزئياً	ملتزم جزئياً
مراجعة امن المعلومات	الدرجة	٦	٦	٥
	نسبة الالتزام	٦٧%	٦٧%	٥٦%
	تقييم الالتزام	ملتزم جزئياً	ملتزم جزئياً	ملتزم جزئياً

المصدر: من إعداد الباحثين.

من خلال الجدول اعلاه يتبين لنا اهم النقاط الاتية :-

أ- **سياسة آمن المعلومات:** نلاحظ حصول مصرف الخليج على (٨) نقاط من خلال التزامه بشكل كامل بأعداد سياسات خاصة بآمن المعلومات ونشرها وابلاغ كافة الموظفين بها ومراجعة تلك السياسات بفترات دورية واعداد تقارير عنها ورفعها للأدارة العليا، في حين التزم المصرف الوطني الاسلامي بشكل جزئي من خلال حصوله على (٥) نقاط، نتيجة تحديد واعتماد سياسات خاصة بأمن المعلومات الا انه لم يجر نشرها وابلاغ كافة الموظفين بضرورة الالتزام بها للمحافظة على آمن البيانات، فضلاً عن عدم مراجعة تلك السياسات بصورة دورية لغرض ضمان مدى ملائمتها وكفائتها، في حين لم يلتزم مصرف الشرق الاوسط بشكل كلي بمتطلبات سياسات آمن المعلومات والذي حقق فيه (٤) نقطة.

ب- **تنظيم آمن المعلومات:** حصل مصرف الشرق الاوسط على (٧) نقاط مقابل حصول مصرفي الخليج والوطني الاسلامي على (٦) نقاط، وتبين لدى الباحثين التزام المصارف عينة البحث بمتطلبات تنظيم آمن المعلومات بشكل جزئي، من خلال تحديد خرائط المسؤوليات والفصل الواضح بين المهام والواجبات لتقليل فرص التعديل او الاستخدام غير المصرح به، الا انه لم يجر التواصل مع الجمعيات والمستشارين المتخصصين في مجال تكنولوجيا المعلومات لغرض تطوير وتحسين انظمة الحماية.

ج- ادارة الاصول: نلاحظ حصول مصرفي الشرق الاوسط والخليج على (٧) نقاط مقابل (٦) نقاط لمصرف الوطني الاسلامي، ويلاحظ الباحثان من خلال نسب القياس التي تم التوصل لها ان المصارف عينة البحث التزمت بشكل جزئي بتطبيق آمن ادارة الاصول لتكنولوجيا المعلومات من خلال اعادة الموظفين للأصول المرتبطة بمعالجة البيانات والمعلومات عند انهاء عملهم او عقدهم، فضلاً عن السيطرة على هذه الاصول من خلال اعداد قوائم جرد بها وصيانتها بشكل دوري، وفي المقابل لم يجر تحديد قواعد وسياسات الاستخدام المقبول لموارد واصول تكنولوجيا المعلومات واقتصارها على الاعمال المصرفية.

د- آمن الموارد البشرية: تبين لدى الباحثان حصول مصرف الشرق الاوسط على (١٣) نقطة مقابل حصول مصرفي الخليج والوطني الاسلامي على (٩)، (١٠) نقاط على التوالي، ونلاحظ من خلال النسب وآلية القياس ان المصارف عينة البحث التزمت بشكل جزئي بمتطلبات أمن الموارد البشرية لتكنولوجيا المعلومات، من خلال التأكد من ان جميع العاملين من ذوي التأهيل العلمي والعملي المناسب وان المهام المناطة بهم تتناسب مع طبيعة العمل ومتطلبات آمن البيانات، فضلاً عن وجود التدريب الكافي والمناسب في مجال التوعية والتحديثات المنتظمة للسياسات واجراءات آمن المعلومات، الا انه لم توضح اتفاقيات وشروط التوظيف المسؤوليات المترتبة على انتهاك آمن البيانات والمعلومات والتأكيد على المحافظة على سرية المعلومات بعد انهاء العمل للموظف او تغييره.

هـ- آمنية وسائط التخزين: تبين لنا حصول كل من مصرفي الشرق الاوسط والخليج على (٩) نقطة مقابل حصول مصرف الوطني الاسلامي على (٨) نقاط، ونلاحظ من خلال النسب وآلية القياس التي توصل اليها الباحثان، ان المصارف عينة البحث التزمت بشكل جزئي بمتطلبات أمنية وسائط التخزين لتكنولوجيا المعلومات، من خلال وجود اجراءات للنسخ الاحتياطي للملفات وقواعد البيانات وانها محمية ضد اعمال التخريب، فضلاً عن وجود اجراءات وتعليمات للعاملين بضرورة عدم استخدام وسائط النقل (USP,CD,...etc)، وفي المقابل عدم وجود اجراءات رسمية بشأن ادارة الوسائط القابلة للأزالة او التخلص من وسائط التخزين عند عدم الحاجة لها وبما يضمن المحافظة على السرية وعدم الاضرار بالبيئة.

و- ادارة نقاط الضعف: نلاحظ حصول مصرفي الشرق الاوسط والوطني الاسلامي على (٧) نقطة مقابل حصول مصرف الخليج على (٦) نقطة، ونلاحظ من خلال النسب وآلية القياس التي توصل اليها الباحثان ان المصارف عينة البحث التزمت جزئياً بمتطلبات أمنية وسائط التخزين لتكنولوجيا المعلومات، من خلال وجود سجل لتوثيق نقاط الضعف نقاط الضعف المكتشفة والاجراءات المتخذة لمعالجتها وتصنيفها بحسب خطورتها، وفي المقابل فأنه لا يتم معالجة نقاط الضعف في الانظمة بالوقت المناسب واجراء تقييم دوري للثغرات الامنية المكتشفة في الانظمة، فضلاً عن عدم وجود قواعد مكتوبة وموثقة حول الجهة التي تقوم بتثبيت الانظمة والبرامج والتدريب على استخدامها.

ز- الامن المادي والبيئي: نلاحظ حصول مصرف الشرق الاوسط على (١٧) نقطة مقابل حصول مصرف الخليج والوطني الاسلامي على (١٢) نقطة لكل منهما، ونلاحظ من خلال النسب وآلية القياس التي توصل اليها الباحثان، ان مصرف الشرق الاوسط قد حقق درجة الالتزام بشكل كامل فيما يتعلق بجانب الامن المادي والبيئي لتكنولوجيا المعلومات من خلال حماية المرافق الحساسة بواسط ضوابط دخول مناسبة لضمان السماح للأفراد المخولين والمصرح لهم بالدخول فضلاً عن تطبيق الامن المادي للمكاتب والمرافق الحيوية ضد الكوارث الطبيعية أو الحوادث، مقابل الالتزام الجزئي لمصرفي الخليج والوطني الاسلامي بتحقيق ذلك نتيجة عدم وضع سياسات لمراقبة الدخول وتوثيقها ومراجعتها بناءً على متطلبات آمن المعلومات بالاضافة الى عدم توثيق ووضع ضوابط أو تحديد محيط الامان للمناطق التي تحتوي على معالجات البيانات للزبائن.

ح- آمن الاتصالات : نلاحظ حصول مصرف الشرق الاوسط على (١٢) نقطة مقابل حصول مصرف الخليج على (١١) نقطة والوطني الاسلامي على (٩) نقاط، ونلاحظ من خلال النسب وآلية القياس التي توصل اليها الباحثان، ان مصرفي الشرق الاوسط والخليج قد حققا التزام كامل فيما يتعلق بأمن الاتصالات من خلال استخدام انظمة لحماية وادارة الشبكات والتحكم فيها وحماية البيانات والمعلومات في الانظمة والتطبيقات فضلاً عن تزويد المستخدمين فقط بصلاحية الوصول الى خدمات الشبكة

على خلاف المصرف الوطني الاسلامي الذي حقق التزام جزئياً بذلك نتيجة عدم تحديد وتوثيق مستويات خدمات الشبكة المقدمة وادراجها ضمن اتفاقيات خدمات الشبكة المزودة من جهات خارجية فضلاً عن الاستخدام الجزئي لأنظمة الحماية للشبكات.

ط- ادارة حوادث المعلومات: نلاحظ حصول مصرف الشرق الاوسط على (١٧) نقطة مقابل حصول مصرف الخليج على (١١) نقطة والوطني الاسلامي على (١٠) نقاط، ومن خلال النسب وآلية القياس التي توصل اليها الباحثان نلاحظ ان مصرف الشرق الاوسط قد حقق التزام كامل فيما يتعلق بكيفية ادارة حوادث المعلومات من خلال تحديد المسؤولية وتوثيق الاجراءات الادارية المتخذة لضمان الاستجابة السريعة والفعالة والمنظمة لحوادث آمن المعلومات فضلاً عن جمع البيانات ومعلومات عن الحوادث وتصنيفها بحسب اهميتها واعداد تقارير عنها ورفعها الى الادارة العليا، بينما حقق مصرفي الخليج والوطني الاسلامي التزاماً جزئياً بمتطلبات ادارة حوادث المعلومات نتيجة عدم وجود اجراءات موثقة ومحددة حول كيفية الاستجابة السريعة والفعالة لحوادث آمن المعلومات والابلاغ عنها من خلال قنوات الادارة المناسبة ومعالجتها بأسرع وقت ممكن.

ي- الامتثال للمتطلبات القانونية والتعاقدية: نلاحظ حصول مصرف الوطني الاسلامي على (٦) نقطة مقابل حصول مصرفي الشرق الاوسط والخليج على (٧) نقطة لكل منهما، ونلاحظ من خلال النسب وآلية القياس التي توصل اليها الباحثان، ان المصارف عينة البحث حققت التزام جزئياً بالامتثال للمتطلبات القانونية والتعاقدية نتيجة الالتزام بحقوق الملكية الفكرية واستخدام الانظمة والبرامج المرخصة وحماية السجلات والبيانات من الفقدان والتدمير او التزوير او الافراج غير المصرح عنها، وبالمقابل عدم تضمين الاتفاقيات التعاقدية شروط وضوابط التشفير الملائمة للحفاظ على امنية البيانات والمعلومات فضلا عن عدم ادراج تعهد المصارف بضمان خصوصية وحماية المعلومات الشخصية للزبائن عند فتح الحسابات الجارية او التوفير او غيرها من الخدمات المقدمة.

ك- مراجعة آمن المعلومات : نلاحظ حصول المصرف الوطني الاسلامي على (٥) نقطة مقابل حصول مصرفي الخليج والوطني الاسلامي على (٦) نقطة لكل منهما، ونلاحظ من خلال النسب وآلية القياس التي توصل اليها الباحثان، ان المصارف عينة البحث قد حققت التزاماً جزئياً فيما يتعلق بمراجعة آمن المعلومات، نتيجة الالتزام بمراجعة نهج ادارة امن المعلومات من حيث الضوابط والاجراءات والعمليات بصورة دورية او عند حدوث تغييرات كبيرة في انظمة العمل، وفي المقابل لاحظنا عدم مراجعة خطط الطوارئ وتقييمها كل فترة واعداد تقارير عنها ورفعها الى الادارة العليا والمتعلقة بضمان استمرارية تقديم الخدمة.

ومما تقدم واستناداً الى ما ورد اعلاه، يتبين لنا وجود التزام كلي أو جزئي أو عدم وجود التزام من قبل المصارف عينة البحث بمتطلبات أمن المعلومات والواردة في المواصفة القياسية (ISO/IEC 27001)، والتي تم تشخيصها من قبل المدقق الخارجي المؤهل علميا وعملياً، وان تحديد تلك المتطلبات سوف يساعد ادارات المصارف بتلبيتها وبما يؤدي الى تعزيز الجودة لأمن المعلومات ومعالجة نقاط الضعف وصولاً الى الاستيفاء الكامل لمتطلبات المواصفة، مما يؤكد صحة الفرضية التي وضعها الباحثان والمتضمنة:

(ان استعانة الادارة العليا في المصارف بالمدقق الخارجي المؤهل علمياً وعملياً عند تقييم امن انظمة تكنولوجيا المعلومات ومدى تطبيقها المواصفة القياسية الدولية (ISO/IEC 27001) يساعد في تحسين جودة امن المعلومات).

المحور الرابع / الاستنتاجات والتوصيات

٤-١ -الاستنتاجات:

أ. عدم تحقيق المصارف عينة البحث لجميع متطلبات وشروط المواصفة القياسية (ISO/IEC٢٧٠٠١)، ووجود نقاط ضعف وخلل في آمن تكنولوجيا المعلومات مما يتطلب الوقوف عليها ودراستها لغرض اتخاذ الاجراءات اللازمة المعالجتها.

ب. عدم تحديد واعتماد مجموعة من سياسات واجراءات آمن انظمة تكنولوجيا المعلومات من قبل الادارة العليا لغرض نشرها وابلاغ كافة العاملين بضرورة الالتزام بها واعداد تقارير امتثال ورفعها الى الادارة العليا لبيان مدى الالتزام بتلك السياسات.

ج. وجود ضعف في الاستجابة لحوادث آمن المعلومات الحاصلة وعدم تحليلها وتصنيفها بحسب الاهمية، بالأضافة الى عدم توثيق الاجراءات المتبعة لغرض ضمان الاستجابة الفعالة والمنظمة لحوادث آمن المعلومات ومعالجتها بأسرع وقت ممكن.

د. عدم وجود اجراءات رسمية وموثقة حول آلية التخلص من وسائط التخزين بأمان عند عدم الحاجة اليها وبما يضمن المحافظة على سرية البيانات والمعلومات للزبائن وعدم الاضرار بالبيئة.

هـ. ضرورة تحديد المسؤوليات والفصل بين المهام والواجبات تجاه آمن المعلومات وابلاغ جميع العاملين بها عند ارتكاب اي انتهاك لأمنية البيانات مع ضرورة المحافظة على السرية بعد انهاء العمل للموظف أو تغييره .

٤-٢- التوصيات:

أ. على ادارات المصارف عينة البحث زيادة الاهتمام بتلبية متطلبات الجودة فيما يتعلق بأمن معلوماتها من خلال تلبية متطلبات الاعتمادية لأمن تكنولوجيا المعلومات والواردة في المواصفة القياسية (ISO/IEC 27001)، مع ضرورة الاستعانة بمستشارين ومدققين خارجيين متخصصين في مجال آمن المعلومات لغرض فحص امنية الأنظمة المطبقة في المصرف.

ب. أهمية إعداد مجموعة من السياسات والاجراءات والضوابط الخاصة بمتطلبات آمن البيانات والمعلومات وإبلاغ جميع العاملين بها واعداد تقارير إمتثال دورية عن مدى الالتزام بها ورفعها الى الادارة العليا.

ج. التركيز على ايجاد ادارة كفؤة وفعالة لأدارة مخاطر آمن البيانات والمعلومات من خلال تحديد الاجراءات والضوابط المتبعة لمعالجة الحوادث المحتملة أو الحاصلة وتوثيقها وتقييم مخاطر آمن تكنولوجيا المعلومات بصورة مستمرة.

د. اعتماد الادارة العليا لمجموعة من الاجراءات الخاصة بكيفية التخلص من وسائط التخزين بما يضمن المحافظة على سرية البيانات للزبائن وعدم الاضرار بالبيئة.

هـ. ضرورة ادخال الملاكات البشرية المستخدمة لموارد تكنولوجيا المعلومات في دورات تدريبية وتثقيفية مستمرة لزيادة مستوى الوعي بمخاطر أمنية المعلومات وضرورة المحافظة سرية البيانات والمعلومات حتى بعد انتهاء عمل الموظف لدى المصرف.

٥- المصادر والمراجع:

٥-١-المصادر العربية

أ- الكتب

١. (IFAC) الاتحاد الدولي للمحاسبين القانونيين، اصدارات المعايير الدولية لممارسة اعمال التدقيق والتأكيد وقواعد واخلاقيات المهنة، ٢٠١١.
٢. (AICPA) اصدارات المعهد الامريكي للمحاسبين القانونيين، ٢٠١٠.
٣. داوود، حسن طاهر (٢٠٠٤)، امن شبكة المعلومات، المملكة العربية السعودية، الرياض، مراكز الدراسات والبحوث.
٤. محاجبية نصيرة، حمدي باشا نادية، دور تكنولوجيا المعلومات والاتصالات في في تفعيل التنمية المستدامة- التجربة الفرنسية نموذجاً" مجلة جامعة بغداد للعلوم الاقتصادية العدد الخاص بالمؤتمر العلمي المشترك،٢٠١٤.
٥. المطارنة، غسان فلاح، تدقيق الحسابات المعاصر من الناحية النظرية، دار المسيرة للطباعة والنشر، عمان، الاردن، ٢٠٠٩.

ب- الرسائل والاطاريح الجامعية

١. عبود عبد الله جابر،" اثر تكنولوجيا المعلومات في تحديد الخيار الاستراتيجي للمنظمة" رسالة ماجستير، كلية الادارة والاقتصاد، جامعة كربلاء، ٢٠٠٨.
٢. علي وشحاتة، إطار مقترح تطوير خدمات مراقبي الحسابات في بيئة التجارة الالكترونية"، ماجستير، جامعة الاسكندرية، مصر، ٢٠١١.

٥-٢- المصادر الاجنبية

1- Al-Kolaly , M. (2005). Concepts of Information Technology (IT).UK : Cheltenham Courseware Ltd.
2- Arens, Alven. Elder, Randal and Beasley, Mark "Auditing and assurance services: an integrated approach", 15th edition, Pearson Ltd, 2014.
3- Arens, Alvin a, randal j.elder, and, mark s.,Beasley,auditing and assurance services an integrated approach, 11th edition, new york, education, international, 2008
4- Boynton, willian c., Raymond n.johnson and walter g. kell, (2001), modern auditing, 7th edition, new york, john wiley & sons, inc.

5- COBIT introduction An ISACA framework 28 Feb 2012.
6- Elder , randal j., mark s. Beasley, and,Alvin A.arens ,(2010) auditing and assurance services an integrated approach,13th edition, new york, pearson eduation, inc.
7- Grawford, Michel a, attestation gide, cch a wolters business,2009 .
8- ISO/IEC 27001:2013, "International Standard – Information -04 technology- Information security management systems- Requirements"(2nd ed.) Geneva: ISO Copyright Office.
9- Knechcl,w. Robert, auditing assurance& risk, 2nd edition, ohio, south western college publishing,2001.
10- lowers, timothy j., Robert j. ramsay, david h .,sinason, and jerry r. strwser,(2008), aduting & assurance services, boston, mcgraw-hill lrwin .
11- Pearlson, Keri E. &Saunders, Carols. " Managing And Using Information Systems: A Strategic Approach ". 3rd edition. WILeY- Inc. USA. 2006.
12- Pickett, k.h. spencer,(2005), the essential handbook of internal auditing, jhon wiley & sons ltd.