
المحور
الإداري

أستحداث أدارة مخاطرة رقمية لمواجهة مخاطر أستخدام تكنولوجيا المعلومات

دراسة ميدانية في عينة من المصارف العراقية

أ.م. سلمان عبود زيار المعهد التقني المسيب – أدارة أعمال – نظم معلومات إدارية

المستخلص :

تناولت هذه الدراسة التعرف على خطوات أستحدات أدارة مخاطرة رقمية لمواجهة النتائج العرضية التي ترافق استخدام تكنولوجيا المعلومات مما يتطلب وجود منهجية متكاملة قائمة على أدارة المخاطر أستنادآ إلى عدد من معايير المنظمة الدولية (ISO) الخاصة بأمن وخصوصية المعلومات ومن أشهرها المعيار 27005 لعام 2011 ، كما هدفت الدراسة التعرف على مدى توافر سياسات وأجراءات أمن المعلومات في مجالاتها (الادارية ، الفنية وأدارة المخاطرة) في نظام المعلومات تم تطبيقها في المصارف العراقية (مجتمع الدراسة) على عينة قوامها (٤٠) فردآ ، أعتمدت الدراسة على منهج الاستطلاعي أضف إلى ذلك المنهج الوصفي في عرض البيانات وتحليلها، وقد توصلت الدراسة إلى الأتي :

١- أتفقت عينة الدراسة إلى عدم وجود أدارة متخصصة بأمن المخاطر وأدارتها في المصارف العراقية (مجتمع الدراسة) وبمستوى أقل من المتوسط .
٢- أتفقت عينة الدراسة إلى أن المصارف تطبق سياسات حماية أدارية في نظام أمن المعلومات بمستوى أعلى من المتوسط .
٣- أتفقت عينة الدراسة إلى أن المصارف تتبع العديد من سياسات و أجراءات الحماية الفنية في نظام معلوماتها بمستوى عالي .
٤- أتفقت عينة الدراسة إلى حدوث مخاطر في نظام أمن المعلومات بشكل متكرر نتيجة قلة الخبرة والوعي والتدريب قد تحدث أكثر من مرة أسبوعيآ إلى مرة شهريآ .
٥- أتفقت عينة الدراسة إلى وجود بعض المخاطر التي قد تتكرر مرة على الاقل يوميآ مثل العبث بالبيانات أو أتلافها ، الوصول غير المرخص من خارج المنظمة ، دخول فيروسات في نظام أمن المعلومات .
٦- توصلت الدراسة إلى مجموعة من التوصيات لعل أبرزها أستحدث أدارة متخصصة في أدارة المخاطر الرقمية لتحقيق التكامل والداعم بين جميع الوحدات المرتبطة بها حيث أن المصارف العراقية (مجتمع الدراسة) الا انها على الرغم من النجاحات في السياسات (الادارية والفنية) الا انها تواجه مخاطر وتهديدات في نظام أمن معلوماتها (سياسة أدارة المخاطر) .

Abstract

This study dealt with identify the steps the creating of adigidital risk management to counteract the incidental findings that a company the use of inFormation technology , which requires an in tegreted a pproach to risk management based on anumber of international standards organization (ISO) For security and privacy of information and best known standard 27005 For 2011 , also the aim of the study identify the

policies Availability and procedures For information security (administrative discpling , technical and risk management) in the inFormation security system was applied in Iraqi banks (study population) on as ample of (40) persons , the study had reached for the following .

1 – The study sample agreed to lack of specialized management with security risk management in Iraqi banks (study community) and to alesser extent than the average level .

2 –The study sample agreed that blanks apply management protection policies of management information security system higher than the average level .

3- The study sample agreed that banks follow mang of the policies and procedures techrical protection in the information security system .

4- The study sample agreed to occurrence risk information security system frequently as a result of lock experience , aware ness and training more than once may a week to once month .

5- The study sample agreed to the presence of some risks that maybe at least once day , such as tampering with or destruction of data , unauthorized access from outside the organization and entry of viruses in the system information security .

6- The study reached aset of recommendations perhaps the most not able creating in digital risk management to achieve integration and support among all the associated management units , As Iraqi banks face risks and threats to security of its information system (risk management policy)

المقدمة :

تصدت هذه الدراسة إلى النتائج العرضية التي ترافق استخدام تكنولوجيا المعلومات ، ستستحدث الكثير من المنظمات في المستقبل منصب أداري هو منصب مدير المخاطر الرقمية (Digital Rick Manager (DRM أو ما يعادلها ، وذلك بسبب عجز فريق أمن تقنية المعلومات عن أدارة المخاطر الرقمية المرافقة للأستعانة بالتقنيات والأستخدامات الحديثة ، كما ستقوم تقنية المعلومات والتقنيات التشغيلية ، وأنترنيت الأشياء ، وتقنيات الأمن الحقيقية ، بالعمل وفق مفهوم الترابط والأعتماد المتبادل ، مما يتطلب وجود منهجية متكاملة قائمة على أدارة المخاطر من اجل الحوكمة والأدارة .(البوابة العربية لأخبار التقنية / 07 / 2014 / ait news . com (21

حيث أشارت دراسة أستقصائية في مؤسسة الأبحاث والدراسات العالمية (جارتنر) (Gartner) والخاصة بالرؤوساء التنفيذيين والأدارة التنفيذية العليا إلى أن أكثر من نصف الرؤوساء التنفيذيين سيعملون على أستحداث منصب أداري (رقمي) ضمن فرق عملهم نهاية العام 2015 أما بحلول العام 2020 فان 60 بالمئة من الشركات الرقمية ستعاني من حالات فشل شاملة وكبيرة في تقديم الخدمات بسبب عجز فريق عمل أمن تنقية المعلومات من أدارة المخاطر المرافقة لتكنولوجيا المعلومات الحديثة (جريدة الرياض ، 2014 : العدد 16834) .

وعليه ركزت الدراسة على المفاهيم المرتبطة بأدارة المخاطر الرقمية ، وأنشاء نظام لأدارة المخاطر الرقمية على وفق الأسس والمعايير الدولية (ISO) وخاصة المعيار 27005 لعام 2011 والذي يعطي المديريين العاملين في مراكز وإدارات تكنولوجيا المعلومات اطار عمل مفصل لتنفيذ وتطبيق مدخل متكامل لأدارة المخاطر والتهديدات التي تواجههم في أدارة نظم المعلومات . (الهادي ، ٢٠١٣ : ١٠ –١١)

أتجهت الدراسة لحسم أهم السياسات المتبعة (الأدارية ، الفنية ، أدارة مواجهة المخاطر) وفق نموذج دون باركر الخاص بأمن المعلومات ميدانياً على عينة في المصارف العراقية التي تتعامل مع تكنولوجيا المعلومات والبالغ عددهم (٤٠) فرداً ، بأعتبار ان تحقق ذلك يعد هدفا أساسيا للدراسة أنطلاقا من الفرضية الرئيسية (تستخدم المصارف العراقية مجتمع الدراسة مجموعة من السياسات والأجراءات المتبعة للحد من الأختراقات والتهديدات الأمنية) .

ولأختبار الفرضيات أستعملت أدوات التحليل والمعالجة الأحصائية فأعتمدت الأوساط الحسابية والأنحراف المعياري ومعامل الأختلاف فيما أعتمدت الدراسة على المنهج الاستطلاعي بالأضافة إلى المنهج الوصفي في عرض البيانات وتحليلها . وقد توصلت الدراسة إلى اتفقت عينة الدراسة إلى أن المصارف العراقية (مجتمع الدراسة) تطبق سياسات حماية إدارية بمستوى أعلى من المتوسط في حين إجابة عينة الدراسة إلى أن المصارف تطبق سياسات حماية فنية بمستوى عالي وأتفقت عينة الدراسة إلى وجود مخاطر تهدد أمن المعلومات تتكرر أسبوعياً وشهرياً وبعضها يتكرر يومياً .

وسيجري عرض متضمنات الدراسة من خلال أربعة مباحث كالاتي :

المبحث الأول : منهجية الدراسة

المبحث الثاني : الاطار النظري

المبحث الثالث : اختبار وتحليل فرضيات الدراسة

المبحث الرابع : الاستنتاجات والتوصيات

المبحث الأول : منهجية الدراسة

تناول هذا المبحث الاتي :

اولاً : مشكلة الدراسة : (study problem)

أدى تسارع التقنية وشعور كثير من الجهات الحكومية والخاصة بحاجتها إلى الأمان وأن التحول إلى (الحكومة الإلكترونية) أدى إلى زيادة أحتمال (خطر الاختراق) للمعلومات ، حيث تبرز الثغرات في بناء مشروعات عبر شركات غير مؤهلة ، وخوادم غير مؤمنة وتنتقص العمل في مجال امن المعلومات (التكامل الفعلي) الذي يحميها كمجموعة وليس أفراداً وتدريب العنصر البشري ، وتصنيف المعلومة بحسب السرية ، وتوعية المجتمع كل ذلك يدفع المنظمات إلى أنشاء (هيئة عليا) تنسق الجهود وتراقب المخرجات وتتدخل في أوقات الطوارئ .

وعلى هذا يمكن إيجاز مشكلة الدراسة بعدد من التساؤلات الأتية :

١- ما أبرز التحديات الأمنية التي تواجه المصارف العراقية التي تتعامل بتكنولوجيا المعلومات ؟
٢- كيف تستطيع تلك المصارف حماية أمن المعلومات وخصوصيتها من خلال أتباع سياسات أدارية وفنية تمنع تلك الاختراقات أو تحد منها ؟
٣- إلى أي مدى تستطيع تلك المصارف مواجهة المخاطر والتهديدات من خلال تطبيق سياسات مواجهة المخاطر ؟
٤- هل يتم الاعتماد على فرق متخصصة في أمن المعلومات ؟ أم أنشاء أدارة متخصصة في إدارة المخاطر الرقمية لتحقيق التكامل ؟
٥- إلى أي مدى يؤدي أنشاء إدارة متخصصة في امن المعلومات يسهم في تنسيق وتكامل المنظومة الأمنية ؟ وماهي مسؤوليتها ؟

ثانياً : أهداف الدراسة (study objective) : تهدف الدراسة إلى الاتي :

١- التعرف على السياسات المتبعة من قبل المصارف العراقية التي تتعامل مع تكنولوجيا المعلومات للحد من الاختراقات الأمنية .
٢- معرفة وفهم خطوات أنشاء أدارة متخصصة في أمن المعلومات .
٣- التعرف على المعايير الدولية (ISO) الخاصة بأمن وخصوصية المعلومات .
٤- تدريب العاملين على مختلف المجالات في المنظومة الأمنية من خلال أدارة متخصصة بأمن المعلومات ترتبط بها الجهات المسؤولة عن امن وتقنية المعلومات .

ثالثاً : أهمية الدراسة (study Importance) : تكمن أهمية الدراسة بالأتي :

١- توفر سياسات وأجراءات من قبل تلك المصارف تسهم في تقليل أو الحد من المخاطر والتهديدات التي تواجهها .

٢- العمل على مبدأ مفهوم الترابط والاعتماد المتبادل بين وحدات أو أقسام المنظومة الأمنية عند أنشاء أدارة مخاطرة رقمية ، وكذلك التنسيق مع منظمات أسناد أخرى في اطار الجهود لمواجهة تلك الأخطار .

٣- تحديد أطار عام لواجبات الموظفين والمستشارين والمعنيين بشؤون إدارة نظم امن المعلومات وتطبيقاتها مما يسهم في تحقيق التكامل بين أنظمة أمن الشبكة ، أمن النظم وأمن التطبيقات .

٤- بناء ثقافة تنظيمية لكل أقسام أو أدارات المنظمة لمواجهة الأخطار وعدم الأعتماد على الفنيين فقط .

رابعاً : فرضيات الدراسة (Hypotheses of study) : تهدف الدراسة إلى تحقيق الفروض الاتية :

لا بد من الإجابة على السؤال الرئيسي التالي ثم أختبار الفرضيات الاتية :

السؤال : ما مستوى السياسات والإجراءات المتبعة من قبل المصارف العراقية (مجتمع الدراسة) للحد من الأختراقات والتهديدات الأمنية ؟

ومن هذا السؤال تم تحديد الفرضيات للدراسة على النحو الاتي :

الفرضية الأولى : تطبق المصارف العراقية سياسات أدارية لمواجهة مخاطر أستخدام تكنولوجيا المعلومات .

الفرضية الثانية : تطبق المصارف العراقية سياسات فنية لمواجهة مخاطر أستخدام تكنولوجيا المعلومات .

الفرضية الثالثة : تطبق المصارف العراقية سياسات للحد من تكرار المخاطر والتهديدات الخاصة بأستخدام تكنولوجيا المعلومات .

خامساً : منهج الدراسة (study Method) : تم أعتماد المنهج ألاستطلاعي في عملية جمع البيانات من العينة ، علاوة عن أستخدام المنهج الوصفي في عرض بيانات الدراسة ، والمنهج التحليلي لغرض تحليل النتائج الذي لايقف عند حد جمع المعلومات لوصف الظاهرة ، انما يعمد إلى تحليلها وكشف العلاقات بين أبعادها (البياتي و القاضي ، ٢٠١٠ : ٦٠) .

سادساً: مجتمع وعينة الدراسة (society and study sampling) :

تمثل مجتمع وعينة الدراسة بمجموعة المصارف العراقية في محافظتي بابل وكربلاء التي تتعامل في معاملاتها بالتعاملات الإلكترونية و أستخدامات تقنية المعلومات (الصراف الألي ATM) البطاقات الذكية visacard ، التحويل الإلكتروني ، الدفع عن طريق نقال البيع (pos) ، الشراء والتعاقد عن طريق الأنترنيت وأختيرت عينة قصدية من مسؤولي (شبكة المعلومات ، تقنية المعلومات ، صيانة الأجهزة ، أمن المعلومات ، البنية التحتية ، مستخدمين) بلغ عددهم (٤٠) فرداً جرى مسح آرائهم من خلال أستبيان مخصص لهذا الغرض

جدول رقم (1) خصائص عينة الدراسة طبقا للبيانات الشخصية

الجهة	الجنس		السن			الشهادة					الخبرة			
	ذكر	أنثى	اقل من ٣٠	٣٠ – ٤٠	اكثر من ٤٠	إعدادية	دبلوم	بكالوريوس	ماجستير	دكتوراه	١- ٥ سنة	٦- ١٠ سنة	١٠ فمافوق	العدد
مصرف بغداد فرع بابل	7	3	3	5	2	–	–	9	1	–	3	5	2	10
مصرف أو فرع كربلاء	5	5	2	5	3	–	1	9	–	–	3	3	4	10
المصرف التجاري العراقي فرع بابل	4	6	2	4	4	–	3	7	–	–	2	5	3	10
المصرف التجاري العراقي فرع كربلاء	7	3	4	2	4	1	2	7	–	–	3	3	4	10
المجموع	40													

المصدر : الباحث بالاعتماد على الاستبانه

الجدول رقم (2) خصائص عينة الدراسة طبقاً للمركز الوظيفي

الجهة	مدير شبكة	مشرف تقنية	مسؤول صيانة	مسؤول امن المعلومات	مسؤول البنية التحتية	مستخدمي المعلومات	أخرى	العدد
مصرف بغداد فرع بابل	–	1	1	1	–	6	1	10
مصرف بغداد فرع كربلاء	1	1	1	1	1	4	1	10
المصرف التجاري العراقي فرع بابل	1	–	1	1	–	5	2	10
المصرف التجاري العراقي فرع كربلاء	1	1	1	1	–	5	1	10
المجموع	40							

المصدر : الباحث بالاعتماد على الاستبانه

سابعآ: أدوات الدراسة ومصادر جمع البيانات : study tools and sources of information gathering : واجه الباحث صعوبة لقلة المصادر والدراسات السابقة في هذا المجال : تم الحصول على البيانات والمعلومات اللازمة لاتمام هذه الدراسة بجانبها النظري والميداني بأعتماد أساليب عديدة وكما يأتي :

أولا : المراجع والكتب التي لها علاقة بالدراسة .

- النشرات والمجلات العلمية
- البحث عن طريق مواقع الأنترنيت

ثانياً : أستمارة الاستبانة : تم جمع البيانات الخاصة بهذه الدراسة بواسطة أستبانة مصممة لهذا الغرض وقد أستخدمت من قبل الدراسة الخاصة بـ (الشيتي ، ٢٠١٤) بعد تكيفة بما يتلائم بهذه الدراسة وقد تضمنة جزأين على النحو الاتي :

الجزء الأول : تمثل البيانات الشخصية لأفراد العينة وهي خمس فقرات .

الجزء الثاني : وقد تضمن ثلاثة محاور وهي على النحو الاتي :

متغيرات الدراسة	عدد الفقرات	رقم الفقرات
المحور الأول : السياسة الإدارية	24	
- السياسات الإدارية		1-10
- سياسة أدارة أصول المعلومات		11-15
- سياسة المقاييس والأدوات المستخدمة		16-24
المحور الثاني : السياسة الفنية	27	
- سياسة توفر مجموعة البرامج لحماية امن المعلومات		25-30
		31-44
- سياسة التحكم والوصول وخصوصية تشفير البيانات		45-51
	14	
- سياسة أدارة الحوادث والتعامل مع البريد الإلكتروني		52-57
		58-65
المحور الثالث : سياسة مواجهة المخاطر		
- تتكرر المخاطر نتيجة قلة الوعي والتدريب		
- تتكرر المخاطر نتيجة ضعف أو عدم توفر الأجهزة والأدوات المستخدمة		

ثامنآ: أداوات التحليل والمعالجة الأحصائية : statistical and analysis tools : لأغراض التحليل والمعالجة الأحصائية فقد أستخدم الإحصاء الوصفي البسيط المتمثل في التكرارات والنسب المئوية للأجابة على

أسئلة الدراسة وأدخلت على الحاسب لمعالجة البيانات و استخراج المتوسطات الحسابية والأنحراف المعياري ومعامل الأختلاف.

تاسعاً : حدود الدراسة (study Bounders) :

١- الحدود المكانية (place Bounders) : تم أختيار مجموعة من المصارف العراقية التي تستخدم تكنولوجيا المعلومات في تعاملاتها الإلكترونية في محافظتي بابل وكربلاء .

٢- الحدود الزمانية (Time Bounders) : أمتد الجهد الإحصائي للمدة الواقعة بين ١/٦ لغاية ٢٠١٥/٤/٣٠ . وتتضمن هذه المدة التحضير إلى الجانب النظري وجمع البيانات الاولية عن المجتمع الدراسة وتوزيع الاستبانة وأستردادها .

٣- الحدود العلمية (scientific Bonders) : أن الدراسة محددة علميا بما جاء بأهدافها

المبحث الثاني : الإطار النظري

يتضمن هذا المبحث : ثلاثة مطاليب ، أختص المطلب الأول عرضاً لبعض المفاهيم المرتبطة بأدارة المخاطرة الرقمية فيما أختص المطلب الثاني أنشاء نظام أدارة المخاطرة الرقمية وفقآ للأسس والمعايير الدولية وأهم السياسات المتبعة فيما ركز المطلب الثالث على هيكل وتنظيم أدارة المخاطرة الرقمية

المطلب الأول : المفاهيم المرتبطة بإدارة المخاطرة الرقمية

أولا- مفهوم أدارة المخاطرة Concept of risk management

تعددت المفاهيم المرتبطة بأدارة المخاطرة نظراً لأختلاف الرؤى بمختلف الأختصاصات فأن الدراسة ستركز على المفاهيم المرتبطة بأدارة المخاطرة الناشئة من أندماج تطبيقات الهندسة في برامج الحاسوب والأنترنيت وتقنيات المعلومات .

فقد عرفها (حماد ، ٢٠٠٧ : ٥٠) بأن أدارة المخاطرة عبارة عن منهج أو مدخل علمي للتعامل مع المخاطر البحتة عن طريق توقع الخسائر العارضة المحتملة وتصميم وتنفيذ إجراءات من شأنها أن تقلل أمكانية حدوث الخسارة أو الأثر المالي للخسائر التي تقع إلى حد أدنى وعرفها (collective ، **2003: p.22**) بأنها عبارة عن أجراء منتظم للتخطيط من اجل تحديد الأستجابة ومتابعة المخاطر المتعلقة بأي مشروع وتتضمن الأجراءات والأدوات والتقنيات التي ستساعد مدير المشروع على تعظيم إمكانية وأسباب تحقيق نتائج أيجابية وتخفيض أمكانية وأسباب تحقيق نتائج غير ملائمة .

وينظر (**1998** ، Hamilton) إلى أن أدارة المخاطرة على أنها نشاط يمارس بشكل يومي سواء على مستوى الأفراد أو المنظمات ، لأن أي قرار ترتبط نتائجه بالمستقبل ،وطالما أن المستقبل غير مؤكد فلابد من الأعتماد على مبادئ أدارة المخاطر.

وأوضح Hamilton أن أدارة المخاطر تتضمن الأنشطة التالية :(Hamilton ,1998:pp.70-78).

١- تجميع المعلومات عن الأصول الخطرة للمنظمة

٢- تحديد التهديدات المتوقعة Threats لكل أصل .
٣- تحديد مواطن الخلل (vuluer abilities) الموجودة بالنظام والتي تسمح للتهديدات بالتأثير في الآصل
٤- تحديد الخسائر التي يمكن ان تتعرض لها المنظمة اذا حدث التهديد المتوقع .
٥- تحديد الأساليب والأدوات البديلة التي يمكن الأعتماد عليها لتدنية أو تجنب الخسائر .
٦- تحديد الأساليب والأدوات التي قررت المنظمة الأعتماد عليها في أدارة المخاطر المحتملة .

ثانيآ : مفهوم أدارة المخاطرة الرقمية : (Concept of digital risk management)

يقول (بروكتور ، ٢٠١٤) : بأنها النهج الأفتراضي لأدارة المخاطر الرقمية ، وسيؤثر مديرو المحاطر الرقمية بشكل كبير على الحوكمة ، الرقابة ، وأتخاذ القرارات المرتبطة بالأعمال الرقمية .

وعرفها (Forouzan,2008:p.3) هي عملية التعرف على نقاط الضعف والتهديدات الموجهة إلى موارد المعلومات التي تستخدمها المنظمة أو الشبكة المعلوماتية في تحقيق الأهداف التجارية أو الأخرى ، والحد والتقليل من نقاط الضعف أن وجدت ، لتأخذ في الحد من المخاطر إلى مستوى مقبول ، على أساس قيمة موارد المعلومات في المنظمة .

ويوضح هذا التعريف الأتي :

١- عملية أدارة المخاطر هي تكرار العمليات الجارية ويجب أن تتكرر إلى ما لا نهاية لأن بيئة العمل متغيرة بأستمرار ، والتهديدات الجديدة والضعف تظهر كل يوم .
٢- أختيار التدابير المضادة (الرقابة) المستخدمة لأدارة المخاطر يجب أن توازن بين الإنتاجية و التكلفة ، وفاعلية التدابير المضادة ، وقيمة الموجودات وحماية البيانات .

و قد عرفها الباحث : هي تلك الإدارة التي ترتبط بها كل الوحدات أو الجهات المسؤولة عن (أمن المعلومات ، الشبكة و الأنترنيت ، تقنية المعلومات ، تطبيقات تقنية المعلومات ، البنى التحتية ، .....) ووضع السياسات والأجراءات لمواجهة المخاطر والأختراقات لأمن المعلومات ، وتكون مسؤولة أمام الأدارة العليا في رفع التقارير عن أمن المعلومات وتطوير أساليب العمل .

ثالثآ: الخطر (danger) :

عرفها (Emmetts vaughon , etal) : الخطر هو الأنحراف في النتائج التي يمكن أن تحدث خلال مدة محدودة في وقت معين (ابوبكر و السيفير ٢٠٠٩ :٢٦).

وعرفة willett : الخطر هو" عدم التأكد عن موضوع متعلق بتحقيق حادث غير مرغوب فيه "(أبو بكر و السيفير ، ٢٠٠٩ : ٢٧) .

الخطر (Forouzan , 2008: p.3) : هو احتمال أن شيئاً ما سيئاً سيحدث بسب الأذى لأحد الأصول المعلوماتية (أو الخسارة في الأصول) الضعف هو الضعف الذي يمكن أن يستخدم لتعريضها الخطر أو التسبب

في ضرر لأحد الأصول المعلوماتية ، التهديد أي شيء فعل (من صنع الأنسان أو فعل من أفعال الطبيعية) لدية القدرة على التسبب في ضرر.

رابعا : أمن المعلومات (Information security).

الأدوات والأساليب التي تستخدم في توفير الحماية للمعلومات من المخاطر التي تهددها أو الأعتداء عليها وذلك من خلال توفير الأدوات و الوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية ، المعايير و الأجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات و لضمان أصالة وصحة هذه الأتصالات

"http://ar.wikipedia.org/w/index.phph?title= امن – المعلومات & olded=1413377"2014

خامساً : الاختراقات (Breaches): هو اصطلاح توصف به مختلف أنماط الأعتداءات التقنية وبالتالي يكون مرادفآ أيضا للاعتداءات ، وهو مختلف الهجمات مثل هجمات البرامجيات أو هجمات انكار الخدمة (انكار التصرفات الصادرة عن الشخص)، هجمات الموظفين الحاقدة ...(المري ،٢٠١٤)

سادسا : حرب المعلومات (Informtion warfare) : وهو أصطلاح في بيئة الأنترنيت للتعبير عن أعتداءات تعطيل المواقع وأنكار الخدمة والاستيلاء على المعطيات (البيانات والمعلومات والأوامر والبرامجيات وغيرها) وكما يشير الاصطلاح فأن الهجمات والهجمات المقابلة هي التي تدل على وجود حرب حقيقية وقد تأخذ أشكال مختلفة (المري ، ٢٠١٤) .

سابعا : الجرائم الإلكترونية (cybercrime) : وهو الدال على مختلف جرائم الكمبيوتر والأنترنيت على الرغم من انه كان محصوراً بجرائم شبكة الأنترنيت (د.م:دن http://ar.wikipedia.orq/wiki/20/12/2011(

المطلب الثاني : نظام أدارة المخاطرة الرقمية .

أن أدارة المخاطرة الرقمية (Digital Risk ManageMement). تلعب دورآ مهماً في حماية أصول المنظمة وكثيراً ما تعرضت تلك المنظمات لحوادث أمنية ، مثل تشوية المواقع ، قرصنة الخادم ، وتسريب البيانات ،....) وعليها أن تدرك بانها بحاجة للمزيد من الموارد لحماية أصول المعلومات .

والمنظمات التي تسعى لتطبيق نظام لأدارة المخاطرة الرقمية لابد لها من تأسيس نظام ، تنفيذ ، أدارة ، مراقبة ، تصحيح ، صيانة وتحسين نظام موثق لأدارة المخاطرة الرقمية في سياق الأنشطة العامة للمنظمة والمخاطر التي تواجهها . لذا بدات المنظمات بالبحث عن طرائق مختلفة لحماية المعلومات منها . (الهيئة الدولية للكهروتقنية / السودان ، ٢٠١٠ : ٦)

أولاً :المعايير والمقاييس المتعلقة بأمن وخصوصية المعلومات التي منها معايير المنظمة الدولية (International organization for standardization) (ISO) الذي انشئ في عام ١٩٤٧ وهو هيئة غير حكومية تتعاون مع اللجنة الكهرو تقنية (International Electrotectnical commission) (IEC

) والاتحاد الدولي للاتصالات (International telecommunication union) (ITU) وعلى تكنولوجيا المعلومات والاتصالات (Information and communication technologies) (ICT) ومن اشهر المعايير التابعة لها : (المدرع ، ٢٠١٤ : ٤) و(www.tech.wd.ccom / wd / tag / itu)

١- ISO 27005 لعام 2011 الذي يعطي المديرين والعاملين في مراكز وأدارات تكنولوجيا المعلومات أطار عمل مفصل لتنفيذ وتطبيق مدخل متكامل لأدارة المخاطر والتهديدات التي تواجههم في أدراة نظم امن المعلومات . وتعتبر أدارة المخاطر احد العناصر الرئيسية في الحد من عمليات الأحتيال والخداع وسرقة المعلومات ، والضرر والأذى فيما يتعلق بمواقع الويب ،وفقدان البيانات الشخصية. (الهادي ، ٢٠١٣ : ١٠)

يرتبط هذا المعيار بتكنولوجيا المعلومات حيث يختص بأساليب الأمن المتعلقة بأدارة أمن المعلومات وما يرتبط بها من أفعال مما يسهم في تمكين كل المنظمات باختلاف أنواعها في ترشيد وتحسين سبل الأمن بها. كما يساند هذا المعيار المفاهيم العامة المحددة في المعايير التي أصدرتها المنظمة في السابق وهي ISO/IEC27001 لعام 2005 الذي يتعلق بتكنولوجيا المعلومات وأساليب الأمن ونظم أدارة أمن المعلومات ومتطلبات ذالك حيث أنه يعتبر معيار ضروري لمن يريد تطبيق أدارة المخاطر (الهادي ،٢٠١٣ : ١٠-١١) وعلى هذا الأساس فأن ISO/IEC27005 لعام 2011 سوف يساعد مستخدميه في تنفيذ معيار ISO / IEC27001 لعام 2005 المتعلق بنظام أدارة أمن المعلومات المبنى على مدخل أدارة المخاطر وعلى الصعيد الدولي يعتبر كل من معيار ISO/27001 ومعيار ISO/27002 لعام 2005 الخاصين بتكنولوجيا المعلومات وأساليب الأمن وأكواد المزاولة لأدارة أمن المعلومات مما يعتبر مهماً لفهم تلك المعايير الدولية بطريقة عادلة . مما تقدم فان عملية أدارة المخاطر تتضمن المهام الاتية :

- أنشاء السياق العام
- تقديم وتقييم المخاطر
- قبول المخاطر
- نقل المخاطر
- مراجعة وضبط المخاطر

وعلى ذلك ، فأن المعيار ISO/27005 لا يقدم أي منهجية معينة لأدارة مخاطر امن المعلومات ، ولكنة يمثل مدخلاً عضوياً لذلك ، فهو يعتمد على المنظمة أن تعرف مدخلها لأدارة المخاطر التي تتعلق بها .

٢- **المعيار ISO/27001** لعام 2005 : هذا المعيار يقدم نموذج دوري يعرف بـ (PDCA) وهو أختصار Plan – Do–check–Act وهو يهدف إلى تحديد الأحتياجات اللازمة لأقامة وتنفيذ وتشغيل ورصد واستعراض وصيانة وتحسين توثيق أدارة امن المعلومات داخل المنظمة ويتم على أربعة مراحل : (http://www.iso27001security.com/index.html-1)

أ- الخطة (plan) : تأسيس نظام لأدارة امن المعلومات .

ب- التنفيذ (Do) : البدء في تنفيذ الخطط وتشغيلها .

ت- التحقق (checks) : مراجعة النظام بعد تنفيذه .

ث- العمل (Act) : صيانة وتحسين النظام .

٣- **المعيار ISO 27002** لعام 2005: هذا المعيار يتضمن بعض السياسات والتوجهات منها: (http://coeia.edu.sa/index.php/ar/asu-security.html) (يوسف ، ٢٠١٣ : ١٤)

أ- السياسة الأمنية security policy

ب- تنظيم أمن المعلومات organization of information security

ت- أدارة الأصول Asset management

ث- أمن الموارد البشرية Human Resourees security

ج- الأمن البيئي والمادي physical and Enivornment securit

ح- الاتصالأت وأدارة العمليات Communications and operations management

خ- التحكم في الوصول accessc control

د- أقتناء نظم المعلومات وتطويرها Information system a cquistion development and maintance

ذ- أدارة الحوادث الأمنية للمعلومات Information security Incident management

ر- أدارة أستمراية الأعمال Business continuity management

ز- أدارة الأمتثال أو التوافق compliance management

وقد تم تحديث هذا المعيار لكي يعكس محتوى وثائق أدارة المخاطر المتمثلة في المعايير التالية :(الهادي ،٢٠١٣: ١٠-١١).

٤- **المعيار ISO31000** لعام 2005 عن مبادئ وتوجيهات أدارة المخاطر وهو توفير مبادئ ودلائل توجيهية عامة في أدارة المخاطر ، ويسعى هذا المعيار إلى تقديم نموذج لممارسات أدارة المخاطر معترف بها دولياً للعاملين في المنظمات التي تقوم باجراءات أدارة المخاطر لتحل محل عدد من المعايير ، وركز المعيار (ISO/31000) بصفة أكبر على تحقيق الانسجام بين البرامج وتشمل الاتي :

- نقل ثغرات المسؤولية إلى أدارة مخاطر المنظمة
- التوفيق بين أهداف برامج الحوكمه مع هذا المعيار
- دمج نظام أدارة أليات الإبلاغ
- خلق معايير وتقييم قياس موحد للمخاطر

ويمتد نطاق هذا النهج لأدارة المخاطر هو تمكين المهام الاستراتيجية ، الأدارية، التشغيلية، في جميع الإجراءات والمشاريع والوظائف التي تكون متماشية مع مجموعة الأهداف المشتركة لأدارة المخاطر .

وقد وضع (Barryw .Boehm) نموذجاً تم بموجبة تقسيم أدارة المخاطر إلى مجموعتين أساسيتين .

- تقيم المخاطر : تتكون من ثلاثة أقسام وهي تعريف ،تحليل ،وتحديد الأولوية بالنسبة للمخاطر التي تتعرض لها المنظمة .
- مراقبة المخاطر : تنقسم إلى ثلاثة أقسام وهي تخطيط أدارة المخاطر ، إيجاد الحلول للمخاطر ،والمتابعة .

ومعيار (ISO31000:2009) مخصص لمجموعة من أصحاب المصلحة بما في ذلك : (الهادي :٢٠١٣، ١٠-١١).

- أصحاب المصلحة على الصعيد التنفيذي
- الموظفون في مجموعة أدارة المخاطر
- المحللون والمسؤولون عن أدارة المخاطر
- المدراء التنفيذيون ومديري المشاريع
- المدققين الداخلين والخارجين
- الممارسون المستقلون

٥- معيار ISO/IEC31010 لعام 2009 لقياس أساليب تقدير وتقييم المخاطر المتعلقة بإدارة المخاطر .

٦- دليل معيار ISOGuide لعام 2009 عن المصطلحات المختلفة المتضمنة في أدارة المخاطر

ثانياً : سياسات وإجراءات أدارة المخاطرة الرقمية : Policies and Procedures digital Risk Management

عرفت .(هيئة الاتصالات السعودية ، ١٤٣٢هـ :٢١-٢٣)٠ سياسات أدارة المخاطرة الرقمية : هي قواعد عملية وفنية موثقة لحماية جهة ما من مخاطر أمن المعلومات التي تحدق بأعمالها وبنيتها التحتية التقنية ، وتقدم وثائق السياسات هذه وصفاً عاماً للضوابط المختلفة التي ستستخدمها المنظمة لأدارة مخاطر أمن المعلومات لديها ، وتعتبر وثائق سياسات أدارة المخاطر اعلاناً رسمياً عن نية الأدارة لحماية أصول المعلومات لديها من المخاطر ذات العلاقة ،وتبين هذه الأجراءات الأنشطة الرئيسية اللازمة لتطبيق تلك السياسات * [١] أدناه أهم مجالات سياسة أدارة المخاطر الرقمية كالأتي :(الشيتي ،٢٠١٤ : ١٦)

١- السياسات الإدارية : ويقصد بها قيام أدارة المخاطرة وضع سياسات وإجراءات ومواصفات قياسية لأمن المعلومات ،سياسة أدارة أصول المعلومات ، المقاييس التي تستخدم في أدارة أمن المعلومات ، أدوات أمن المعلومات المستخدمة في المنظمة ، سحب حقوق صلاحيات أستخدام الموظف لموارد وأجهزة تقنية المعلومات عند انتهاء الخدمة ، تنظيم دورات تدريبية للموظفين الجدد حول سياسات وأجراءات امن المعلومات

٢- السياسات الفنية : وهي السياسة الخاصة بتوفير برامج حماية لأمن المعلومات والشبكات ، وضع كلمات مرور ذات قوة وطول أمنة ، أستخدام برامج مكافحة الفيروسات ، توفر برامج لكشف التسلل

[١] * تم تضمين أستمارة الأستبانة بتلك السياسات مع الأخذ بنظر الاعتبار ما ورد في نموذج دون باركر الخاص بأمن المعلومات . (www.sana1111.Files.wordbrss.com/d988d8b3d8..8aa-10dos/)

والاختراق ، توفر برامج الجدران النارية ، توفر برامج استخدام الشبكة اللاسلكية ويسمح لموظفين محددين ، وضع سياسة خصوصية البيانات المتمثلة في تحديد صلاحيات الدخول للأطراف الخارجية ، الأبلاغ الفوري عن نقاط الضعف في حماية أمن المعلومات ، وكذلك وضع سياسة تشفير البيانات المتمثلة بوضع سياسة تشفير وفقآ للمعايير الدولية ISO ، تشفير نسخ الحفظ الأحتياطية ، توفير أجراءات التخلص من وسائط التخزين المختلفة المنتهية الصلاحية ، كما توفر سياسة أدارة وصول المستخدمين المتمثلة بتوفير أجراءات أنظمة بأنشاء أدارة حسابات المستخدمين وسحب حقوق الدخول ، تخصيص هوية وكلمة مرور بكل مستخدم ، التزام المستخدمين بعدم أفشاء المعلومات الخاصة بالمنظمة والتوقيع عليها ، وتضع الإدارة سياسة أدارة الحوادث الأمنية المتمثلة التزام الموظفين بأعداد تقارير بالحوادث الأمنية ، أنشاء رسائل التبنية الخاصة بكشف التسلل ، توفر أجراءات تعقب التعديلات Audit Trails ، توفر سياسات لتقيم الثغرات ونقاط الضعف ، أستخدام أدوات المسح للتعرف على نقاط ضعف الحماية ، كما توفر الأدارة سياسة التعامل مع البريد الإلكتروني S/MIME لتشفير رسائل البريد الإلكتروني ، وتشغيل برامج مضادة للفيروسات لفحص الرسائل .

٣- سياسات مواجهة المخاطر : تشمل المخاطر والتهديدات التي يتعرض لها نظام أمن المعلومات متمثلة بالعبث بالبيانات أو أتلافها من قبل المستخدمين ، سرقة بيانات الهوية ،الأدخال غير المقصود لقلة الخبرة والتدريب للمستخدمين ، الوصول غير المرخص لمعلومات الأشخاص ، دخول الفيروسات ، التلاعب والخداع من المحترفين والقراصنة ، الالتقاط السلكي وتحليل الاتصالات وسرقة المعلومات عبر الشبكة ، الاحتيال عبر البريد الإلكتروني وسرقة المعلومات ، اختراق الشبكة اللاسلكية ، الكوارث الطبيعية .

ثالثاً : مستلزمات أدارة المخاطرة الرقمية : Digital Risk Management Requirements

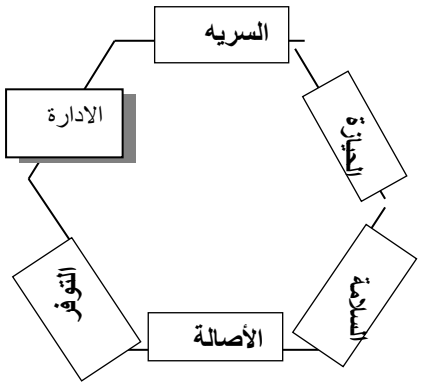
١- توفير الأمكانيات المادية والمعنوية .
٢- توفير الموارد البشرية من محللين ومصممين ومبرمجين وخبراء المعلومات والإداريين .
٣- تحديد جميع الثغرات والمخاطر (الشيتي ،٢٠١٤ :١٥).
٤- تطبيق المعايير الدولية (ISO) المناسبة لأدارة المخاطرة الرقمية .
٥- تطبيق الأجراءات على جميع أقسام أو وحدات أدارة المخاطرة الرقمية .
٦- يجب تدعيمها بالأدوات الأمنية والقوانين والمراسيم الأدارية .(الشيتي،٢٠١٤ :١٥)
٧- تحديد المسؤوليات والصلاحيات على كل مستويات الهيكل التنظيمي .
٨- ألزام الجميع بأدارة الجودة والتحسين المستمر .
٩- يجب أن تكون موثقة .

المطلب الثالث : هيكل وتنظيم إدارة المخاطرة الرقمية

اولآ – المبادئ الرئيسية لإدارة المخاطرة الرقمية : TheBasic principles For managing digital risk

حددت أهم المفاهيم في أمن المعلومات بالثالوث (CIA) وهي السرية Confidentiality والتكامل (Integrity) والتوافر (Availabitity) ، وأن العديد من المتخصصين في مجال أمن المعلومات يؤمنون أيمانا راسخا بان المساءلة ينبغي أن تضاف كمبدأ أساسي لأمن المعلومات (wiley & sons ,2006 :p.60) و (perrin ,2012) .

وفي عام ٢٠٠٢ اقترح دون باركر نموذجآ بديلا للثالوث التقليدي (CIA) يتكون نموذج باركر من ستة عناصر من امن المعلومات ، العناصر هي السرية ، الحيازة ، السلامة ، الأصالة ، التوفر والأداة ، أن سداسي باركر هو موضوع نقاش بين المتخصصين في مجال الامن (ويكيبيديا ، ٢٠١٤) والشكل (1) يمثل عناصر نموذج باركر .



الشكل (١) يوضح عناصر امن المعلومات لنموذج دون باركر

المصدر : الباحث

وعليه فان ابسط انواع الحماية هي استخدام نظام التعريف بشخص المستخدم ، وثوقية الأستخدام ، مشروعيتة هذه الوسائل تهدف إلى ضمان أستخدام النظام او الشبكة من قبل الشخص المخول بالأستخدام .ويمكن توضيح هذه الأبعاد الثلاثة بإيجاز كالاتي : (Aranson &willett, 2008:P3) .

١- السرية (confidentially) : هو المصطلح المستخدم لمنع الكشف عن معلومات لأشخاص غير مصرح لهم بالاطلاع عليها او الكشف عنها مثل بطاقة الأئتمان وذلك لتقيد الوصول إلى الأماكن التي تم تخزين الرقم و البيانات بها سوى للمصرح لهم . وقد يأخذ خرق السرية اشكالآ عديدة ،تجسس شخص ما على الحاسوب لسرقة كلمة السر ، أو رؤية بيانات سرية بدون علم مالكها وغيرها .

٢- التكامل (Integrity): تسعى أدارة المخاطرة الرقمية إلى التكامل (السلامة) للحفاظ على البيانات من التغير أو التعديل من الأشخاص غير المخولين بالوصول اليها ، بقصد أو غير قصد بحذف أو أنتهاك سلامة ملفات البيانات الهامة أو الأضرار بها ، وهو غير مخول بذلك ، يعد هذا أنتهاكا لسلامة البيانات ، أو عندما يصيب فيروس حاسوب ، أو يقوم موظف غير مخول قادر على تعديل راتبة في قاعدة البيانات ، أو عندما يقوم شخص بتخريب الموقع على الأنترنيت ، وقد تنشأ التغيرات غير مقصودة أو لا تحفظ تغيرات قد تمت فعلا (Forouzan , 2008 :p.3)

٣- توفر البيانات (Availability) : تهدف إدارة المخاطر الرقمية أن تكون المعلومات متوفرة عند الحاجة اليها ، وهذا يعني ان تعمل العناصر الأتية بشكل صحيح ومستمر(forozan,2008:p.3)

- الأنظمة الحاسوبية المستخدمة لتخزين ومعالجة المعلومة .
- الضوابط الأمنية المستخدمة لحماية النظام .
- قنوات الاتصال المستخدمة للوصول .
- نظم عالية السرية تهدف إلى استمرارية الحماية في جميع الأوقات
- منع انقطاع الخدمة بسبب انقطاع التيار الكهربائي، أو تعطل الأجهزة،.....
- ضمان منع الهجمات .

ثانياً: ستراتيجية أدارة المخاطرة الرقمية : Digital Risk Management strategy

أن استراتيجية أدارة المخاطرة الرقمية : هي مجموعة القواعد التي تطبقها المنظمة لدى التعامل مع التقنية ومع المعلومات وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها وأدارتها (المري ،٢٠١٤)

أ- **أهداف أستراتيجية أدارة المخاطرالرقمية : Strategic goals digital risk management**

لاتقل أهداف أدارة المخاطر الرقمية أهمية عن أهداف القطاعات والأقسام الأخرى في المنظمة ، حيث تعني أدارة المنظمة بأن يؤدي جميع الأفراد واجباتهم الوظيفية وتحدد لأدارة المخاطرة الرقمية الأهداف الأستراتيجية الأتية :(المري ،٢٠١٤)

- تعريف المستخدمين والأداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم الكمبيوتر والشبكات وكذلك حماية المعلومات بكافة أشكالها ، وفي مراحل أدخالها ومعالجتها ونقلها وإعادة استرجاعها.
- تحديد الأجهزة الإلكترونية التي يتم من خلالها تحقيق وتنفيذ الواجبات المحددة على كل من له علاقة بالمعلومات ونظمها وتحديد المسؤوليات عند حصول الخطر
- بيان الأجراءات المتبعة لتجاوز التهديدات والمخاطر والتعامل معها والجهات المناط بها القيام بذلك .

ب- **أعداد سترتيجية أدارة المخاطر الرقمية : Preparation of digital strategy Risk management**

لكي تكون هذه الأستراتيجية فاعلة ومنتجة وهادفة لا بد أن يساهم في أعدادها وتقبلها وتنفيذها مختلف مستويات الوظيفة في المنظمة الواحدة أضافة إلى حاجتها إلى التعاون والدعم الكامل ،من هنا فأن المعنيين بأعداد سياسة أدارة المخاطر يتوزعون إلى أفراد وجهات عديده داخل المنظمة ، لكن بوجه عام تشمل مسؤولي أمن الموقع ومديري الشبكات وموظفي وحدة الأعمال والتسويق والبحث وغيرها وتشمل أيضا فريق الأستجابة للحوادث والأعطال وممثلي مجموعات المستخدمين ومستويات الأدارة العليا إلى جانب الأدارة القانونية .(المري ، ٢٠١٤)

ت- **اليقظة الاستراتيجية لأدارة المخاطرة الرقمية : vigilance strategy to manage digital risk**

يمكن تعريف دور اليقظة الاستراتيجية (لمجد ، ٢٠٠٩ : ١٧٧) بانها مجموعة من عمليات البحث والمعالجة الخاصة بنشر المعلومات لغرض أستعمالها .

وبذلك يمكن القول بانها توفير المعلومات التي من خلالها تتمكن المنظمة من مواجهة التغيرات التي تحدث في المستقبل ، وتحدث في البيئة المحيطة لأكتشاف الفرص وتجنب التهديدات مما له الأثر على المخاطر التي تواجهها .

ويمر مسار اليقظة الستراتيجية في معالجة المخاطر بالمراحل التالية : (لمجد ،٢٠٠٩: ١٨٧)

المرحلة الأول (الشيء المستهدف) : يتمثل في تحديد المخاطر التي ترغب المنظمة بمعرفتها ، فهي تهدف إلى تحديد المواضيع التي يتم مراقبتها اضف الى ذلك مصادر المعلومات التي يمكن ان تلجا أليها .

المرحلة الثانية (الملاحظة) : فهي تتمثل في تعيين الأفراد الذين لهم قابلية جمع المعلومات حول المخاطر المتوقعة ، وتزويدهم بالطرق والوسائل المناسبة التي يتم أستعمالها لتحقيق ذلك .

المرحلة الثالثة (السير والحركة) : نقصد هنا حركة المعلومات الخاصة بالمخاطر داخل المنظمة ،وذلك من خلال نشر المعلومات التي تم جمعها ووضعها في متناول أصحاب القرار.

المرحلة الرابعة (المعالجة): تعني معالجة المعلومات الخاصة بالمخاطر المتوقعة لغرض تحويلها إلى قوة تصلح لأتخاذ القرارات وتجعل المنظمة تكسب ميزة تنافسية من خلال قدرتها للحصول على معلومات هامة عن الخطر المتوقع ، وتوظيفها توظيفاً فاعلاً في صنع القرار المستقبلي للمنظمة .

من خلال ذلك يتضح أهمية اليقظة الأستراتيجية لأدارة المخاطر الرقمية من خلال مساهمتها في تتبع المخاطر الناتجة من البيئة التي تعمل فيها المنظمة ، ومساهمتها في توقع المخاطر المحدقة وهي تبقي المنظمة دائما على استعداد لمواجهة أي خطر قادم ومنة تقليل الخسائر وتفاديها وتكامل وحدات تلك الأدارة فيما بينها .

ثالثاً – المهام والواجبات الأدارية لمدير المخاطرة الرقمية : Administration and Responbilities

أن مهام مدير المخاطرة الرقمية تبدا في الأساس من حسن اختيارالافراد المؤهلين وعمق معارفهم النظرية والعلمية ، وبهذا الصدد يقول الدكتور بروكتور نائب رئيس المحللين لدى شركة (جارتنر Gartner) ان طبيعية عمل مديري المخاطر الرقمية ستتطلب التحلي بمزيج متناغم من الفطنة والأدراك العالي ووجود معرفة فنية واسعة للتمكن من أتمام عمليات التقييم وتقديم التوصيات الصحيحة للتصدي بشكل مناسب لمخاطر الأعمال الرقمية (جريدة الرياض ، ٢٠١٤ : العدد ٢٧١٦٨٣٤).

ويقع على أدارة المخاطر الرقمية المهام الإدارية والتنظيمية التي تتكون من عناصر أوسبع مجموعات رئيسة هي: (المري ، ٢٠١٤) .

- تحليل المخاطر
- المشاركة في وضع السياسة والستراتيجية لأدارة المخاطر الرقمية
- وضع البناء التقني والأمني
- توظيف الأجهزة والمعدات والوسائل
- تنفيذ الخطط والسياسات

- بناء ثقافة الأمن لدى العاملين والتي تتوزع بين وجوب وأعادة أخلاقيات استعمال التقنية وبين الإجراءات المطلوبة من الكل لدى ملاحظة اي خلل .
- تحديد المسؤوليات للمستخدمين وما يتعين عليهم القيام به في معرض أستخدامهم للوسائل التقنية المختلفة .

رابعآ – الوظائف الأساسية لإدارة المخاطرة الرقمية : Basic function to manage digital risk

تتكون أدارة المخاطرة من مجموعة من الوظائف الأساسية و الساندة والتي تتكامل فيما بينها ، وهي تختلف من منظمة إلى أخرى حسب احتياجاتها و كما يلي : *

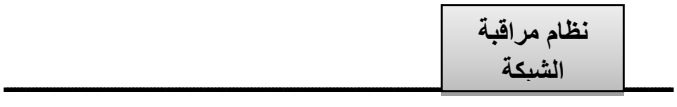
١- وظيفة تطبيقات تقنية المعلومات (function of information Technology application) وهي الوظيفة المسؤولة عن معالجة المعلومات المتعلقة بوظائف أدارة المخاطر وترتبط مباشرة بها وتتولى المهام التالية:

- يتم معالجة المعلومات بأستخدام أنواع مختلفة من تطبيقات تقنية المعلومات مثل برامج خوادم التطبيقات ، برامج خوادم الويب ، تطبيقات التعاملات الإلكترونية (التجارة الإلكترونية)..
- يتم الوصول إلى المعلومات عبر تطبيقات تقنية المعلومات من قبل المستخدمين بأستعمال تطبيقات العميل الموجودة في أجهزة الحاسوب ، الأجهزة المحمولة ، أجهزة المساعد الشخصي PDA إلخ ..
- يتم حفظ المعلومات في قاعدة البيانات ، أجهزة الحاسوب ، أليات التخزين المركزية للبيانات (النسخ المساندة) ، أجهزة التخزين المتنقلة،.....

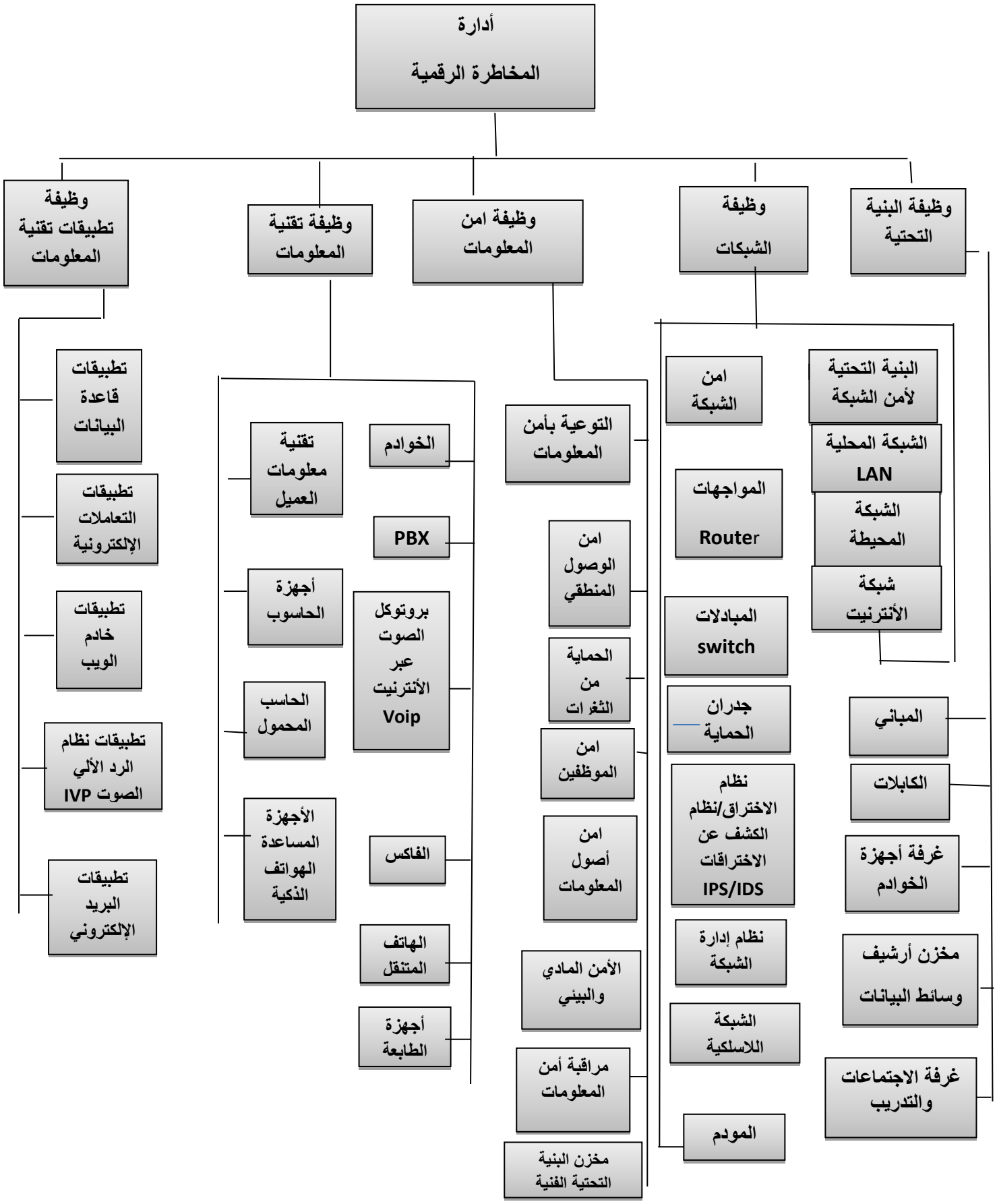
٢- وظيفة الشبكات (function network) وهي الوظيفة المسؤولة عن الشبكات المحلية (LAN) أو الواسعة (WAN) وتامين الوصول من خلالها إلى تقنية المعلومات وتتولى المهام التالية :

- تبادل المعلومات
- المشاركة في البرامج التطبيقة (Sharing software) : تحقيق أمكانية المشاركة في البرامج المتاحة في مجتمع شبكة المعلومات .
- المشاركة في موارد الشبكات (Sharing Hard ware) : استغلال خاصية موارد الشبكة مثل الطابعات ، أجهزة التصوير ، الفاكس ،...
- البريد الإلكتروني E-Mail
- إنشاء مجموعات العمل Work Groups : تتيح الشبكات فرصة تكوين مجموعات العمل وتكون بتخصيص جزء من مساحة التخزين على الشبكة لأفراد هذه المجموعة بعيدآ عن باقي أفراد الشبكة
- الإدارة المركزية central Management

والشكل (١) يوضح وظائف ادارة المخاطرة الرقمية



* **راجع الدليل الارشادي لهيئة الاتصالات وتقنية المعلومات – السعودية – ١٤٣٢ هـ – الطبعة الاولى**


أدارة
المخاطرة الرقمية
وظيفة البنية التحتية
وظيفة الشبكات
وظيفة امن المعلومات
وظيفة تقنية المعلومات
وظيفة تطبيقات تقنية المعلومات
البنية التحتية لأمن الشبكة
الشبكة المحلية LAN
الشبكة المحيطة
شبكة الأنترنيت
المباني
الكابلات
غرفة أجهزة الخوادم
مخزن أرشيف وسائط البيانات
غرفة الاجتماعات والتدريب
امن الشبكة
المواجهات Router
المبادلات switch
جدران الحماية
نظام الاختراق/نظام الكشف عن الاختراقات IPS/IDS
نظام إدارة الشبكة
الشبكة اللاسلكية
المودم
التوعية بأمن المعلومات
امن الوصول المنطقي
الحماية من الثغرات
امن الموظفين
امن أصول المعلومات
الأمن المادي والبيئي
مراقبة أمن المعلومات
مخزن البنية التحتية الفنية
الخوادم
PBX
بروتوكول الصوت عبر الأنترنيت Voip
الفاكس
الهاتف المتنقل
أجهزة الطابعة
تقنية معلومات العميل
أجهزة الحاسوب
الحاسب المحمول
الأجهزة المساعدة الهواتف الذكية
تطبيقات قاعدة البيانات
تطبيقات التعاملات الإلكترونية
تطبيقات خادم الويب
تطبيقات نظام الرد الألي الصوت IVP
تطبيقات البريد الإلكتروني

الشكل (١) يوضح وظائف أدارة المخاطرة الرقمية

المصدر : الباحث

- التأمين security التحكم في عمليات الولوج Enter والأتاحة Access
- القدرة على ربط أنظمة التشغيل المختلفة Access to other operating system
- تحسين الإنتاجية Improve producivily تعمل على تحسين التعاون بين أفراد المجتمع .

٣- وظيفة تقنية المعلومات (function of information Technology) هي الوظيفة المسؤولة عن تقنيات المعلومات ضمن أدارة المخاطرة وتتولى المهام التالية :

- توفير أجهزة الحاسوب وملحقاته وضمن مواصفات تتلائم مع أحتياجات المنظمة.
- توفير الأجهزة المساعدة الرقمية / الشخصية / الهواتف الذكية .
- توفير أجهزة الفاكس والهاتف المتنقل ، وخوادم الأنظمة ، وبرتوكل الصوت عبر الأنترنيت Voip
- صيانة الأجهزة والمعدات .

٤- وظيفة البنية التحتية : (function infrastructure) :هي الوظيفة المسؤولة عن تسهيل عملية التفاعل والتعامل بين الأطراف المختلفة ذات العلاقة مثل العملاء ، الموردين ، الشركاء ، المقاولين ، الجهات الحكومية ، ويكون لها مستويات وصول مختلفة إلى المعلومات بناء على دورها الذي يتم تحديده ، ومن أهم المهام التي تقوم بها

- تهيئة المباني .
- توفير الكابلات.
- توفير أجهزة الخوادم.
- تهيئة وسائط خزن البيانات .
- تهيئة مخزن للمعدات ومستلزمات البنية التحتية .
- تهيئة قاعة للأجتماعات والتدريب ووسائل الإيضاح .

٥- وظيفة أمن المعلومات : (Function information security) وهي الوظيفة المسؤولة عن الجوانب الأمنية المتعلقة ببيئة أدارة المخاطرة ومختلف وظائفها ومن أهم المهام التي تقوم بها .

- التوعية بأمن المعلومات
- أدارة الوصول المنطقي
- الحماية من الشفرات الخبيثة
- أدارة حوادث أمن المعلومات
- أمن الموظفين
- أدارة امن وأصول المعلومات
- الأمن المادي والبيئي
- مراقبة أمن المعلومات
-

خامسا – مكونات نظام أدارة المخاطرة الرقمية : Components of digital risk management system

تنفيذ وتشغيل نظام أدارة المخاطرة الرقمية يتكون من الآتي : (الهادي ، 2006)

١- العمليات (prosses): تعتبر العمليات لا غنى عنها لأي نظام أدارة ، فهي ذات طبيعة مستمرة ، والأخذ بالمعايير التي تم التطرق اليها في الدراسة لتشغيل نظام أدارة المخاطرة ISO/27005,ISO 27001 ,ISO 27002 وكذلك ISO/31000، ISO/3010 الذي أقرتها المنظمة الدولية للتوحيد القياسي والتي تعتبر مدخل لإدارة المخاطرة وتطبيق العمليات بطريقة منظمة كما تراجع بأستمرار في اطار الخبرة المتراكمة بغية استبعاد الأخطاء والمخاطر .

٢- البشر (people) : الذين يمثلون العاملين ، المستشارين ، المتعاقدين ، والفنين والذين ينجزون كل العمليات والخدمات ، ويحتاج إلى تواجدهم بأعداد وتخصصات ملائمة وبمهارات وخبرات تتلائم ووظائف أدارة المخاطرة الرقمية .

٣- التكنولوجيا (Technology) : تعتبر متوافره وجاهزة ، ولمنتجاتها دورات حياة قصير نسبيآ ، وتعتبر سوق تكنولوجيا المعلومات ذات طبيعة تنافسية ، يتوافر لها عدد كبير من المنتجين والموردين والبائعين والموزعين الذين يأتون ويذهبون ، لذلك من الصعب تقيم التكنولوجيا عما كانت علية في الماضي.

٤- الثقافة (culture) : ترتبط بتغير بيئة الأعمال وتتعلق بأخلاقيات المنظمة ، حيث يكون لإدارة المخاطرة دورا رئيسيا تؤديه في حفظ ثقافة المنظمة ومن الثقافات التي تؤديها أدارة المخاطرة الرقمية .

أ- الأستخبارات ، الأمن والدفاع المعلوماتي .

ب- الصرافة ، التبادل الخارجي والتأمين للتعاملات الإلكترونية .

المبحث الثالث : اختبار وتحليل فرضيات الدراسة :

يتناول هذا المبحث نتائج التحليل الإحصائي للدراسة الميدانية والتي تم الحصول عليها عبر تحليل البيانات التي شملها الاستبيان للمصارف العراقية (مجتمع الدراسة) التي تتعامل الكترونيا . تتمثل عينة الدراسة من الموظفين العاملين في تقنية المعلومات ومستخدمي تقنية المعلومات والبالغ عددهم (40) فردا :

- تم أستخدام مقياس لكيرت الخماسي في توزيع الدرجات وكما يأتي :

التصنيف	موافق بشدة	موافق	أتفق إلى حد ما	غير موافق	غير موافق بشدة
الدرجة	5	4	3	2	1

كلما أقتربت النتيجة من الدرجة (5) أزدادت شدة الموافقة على العبارة في حين تزداد شدة المعارضة كلما أقتربت النتيجة من الدرجة (1) وستخدم هذا المقياس في المحور الأول والثاني من أستمارة الأستبيان ، أما المحور الثالث فقد كان المقياس المستخدم هو :

التصنيف	مرة على الأقل يوميا	مرة على الأقل أسبوعيا	مرة على الأقل شهريا	مرة على الأقل سنويا	لا تحدث مخاطرة ابداً
الدرجة	1	2	3	4	5

كلما اقتربت الإجابة من الدرجة (5) فان مرات حدوث المخاطرة ينخفض إلى درجة انعدام المخاطرة ، ويزداد عدد مرات حدوث المخاطرة كلما كانت الإجابة (1) ، أما اذا كانت الإجابة (3) فان ذلك يعني أن عدد مرات حدوث المخاطر متوسط نسبيا .

اولاً : الأجابات على أسئلة مدى توافر سياسات الحماية الأدارية في المصارف العراقية .

١- يوضح الجدول (1) نتائج التحليل الإحصائي لمتغيرات الدراسة والتي تشمل المتوسطات الحسابية والانحراف المعياري ومعامل الأختلاف ودرجة الموافقة للأجابات الخاصة بتوافر السياسات الإدارية في نظام أمن المعلومات في المصارف العراقية .

الجدول رقم (1) نتائج التحليل الإحصائي لسياسات الأدارية في المصارف العراقية

ت	الفقرات	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %	درجة الموافقة
١	**توجد إدارة خاصة بأدارة المخاطرة الرقمية**	**1.65**	**0.695**	**42.1**	**2**
٢	**توفر موظفون متخصصون بأمن المعلومات وحمايتها**	**4.18**	**0.873**	**20.9**	**4**
٣	**توفر سياسات وأجراءات ومواصفات قياسية لأمن المعلومات**	**3.93**	**1.07**	**27.2**	**4**
٤	**أهتمام الإدارة العليا بأمن المعلومات عالية جدا**	**3.88**	**1.68**	**43.3**	**4**
٥	**توقيع الموظفين على الألتزام بكافة السياسات والأجراءات والمعايير والأرشادات الخاصة بأمن المعلومات**	**4.23**	**0.768**	**18.2**	**4**
٦	**الموظفين يمارسون بصورة دائمة تحديث العمليات**	**4.00**	**1.07**	**29.0**	**4**
٧	**تنظيم دورات تدريبية للموظفين الجدد حول سياسات وأجراءات أمن المعلومات**	**4.33**	**0.859**	**19.8**	**4**
٨	**سحب حقوق صلاحيات أستخدام الموظف لموارد وأجهزة تقنية المعلومات عند انتهاء خدمته**	**4.15**	**0.949**	**22.9**	**4**
٩	**المنظمة تتعامل بيقظة مع المخاطر المحدقة بها**	**3.73**	**0.877**	**23.5**	**4**
١٠	**تخطط المنظمة أنشاء أدارة متخصصة بالمخاطر الرقمية يتكامل عملها من خلال الوحدات التي ترتبط بها**	**4.03**	**0.660**	**13.4**	**4**

المصدر : الباحث بالأعتماد على الحاسوب

يتضح من الجدول السابق ما يلي :

- أتفقت عينة الدراسة على عدم توافر أدارة خاصة بأدارة المخاطرة الرقمية وقد بلغ المتوسط الحسابي للإجابات (1.65) وهذا مؤشر على عدم وجود إدارة خاصة بإدارة المخاطر الرقمية .
- أتفقت عينة الدراسة على توفر موظفون متخصصون في امن المعلومات وحمايتها وتوفر مواصفات قياسية لأمن المعلومات ، كذلك اهتمام الإدارة العليا بأمن المعلومات وتوقيع الموظفين على الألتزام بكافة السياسات والأجراءات والمعايير الخاصة بأمن المعلومات ، الموظفين يمارسون بصورة دائمة تحديث العمليات ، تنظيم دورات للموظفين الجدد ، سحب حقوق وصلاحيات استخدام الموارد وأجهزة التقنية عند انتهاء خدمته ، كذلك المنظمة تتعامل بيقظة مع المخاطر المحدقة بها ، وانها تخطط لأنشاء إدارة متخصصة ، حيث بلغ أجمالي متوسط الحسابي للفقرات أعلاه على التوالي , 4.03) 4.18 , 3.93 , 3.88 , 4.23 , 4.00 , 4.33 , 4.15 , 3.73).

٢- الجدول رقم (2) يوضح المتوسطات الحسابية والانحراف المعياري ومعامل الاختلاف للأجابات الخاصة بتوافر سياسة لإدارة أصول المعلومات في نظام أمن المعلومات في المصارف العراقية.

الجدول رقم (2) نتائج التحليل الإحصائي لتوافر سياسة لإدارة أصول المعلومات

ت	الفقرات	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف%	درجة الموافقة
١١	**تولي جهة مسؤولة عن كل أصل من أصول المعلومات يكون له الحق في أصدار ترخيص الأستخدام**	**3.93**	**1.070**	**27.2**	**4**
١٢	**تصنف المعلومات على أساس الحساسية ، الأهمية ، الخصوصية ، المعلومات العامة**	**4.00**	**0.816**	**20.4**	**4**
١٣	**مراجعة أصول المعلومات بصورة دورية للتأكد من تصنيفها بشكل سليم**	**4.10**	**0.841**	**20.5**	**4**
١٤	**يتم أجراء تداول وتخزين ونقل أتلاف أصول المعلومات وفقا للقواعد المحددة في نظام أمن المعلومات**	**3.68**	**1.140**	**31.0**	**4**
١٥	**تحديد الأفراد والمجموعات المخولة من قبل مالك المعلومات بالوصول إلى المعلومات الحساسة**	**4.28**	**1.11**	**27.8**	**4**

المصدر : الباحث بالأعتماد على الحاسوب .

يتضح من الجدول السابق ما يلي :

- أتفقت غالبية عينة الدراسة على توافر سياسات لأدارة أصول المعلومات في المصارف العراقية للفقرات (11 , 12 , 13 , 14 , 15) وبلغ المتوسط الحسابي لها , 4.00 , , 4.10 , 3.68 , 4.28) 3.93) على التوالي ، وهذا يعكس اهتمام الإدارة بأصول معلوماتها .

٣- الجدول رقم (3) يوضح المتوسطات الحسابية والانحراف المعياري ومعامل الأختلاف للأجابات الخاصة بسياسة استخدام مجموعة من المقاييس والأدوات الخاصة بأمن المعلومات .

الجدول (3) نتائج التحليل الإحصائي الخاصة باستخدام مجموعة من المقاييس والأدوات الخاصة بأمن المعلومات

ت	الفقرات	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %	درجة الموافقة
16	توفر نمط شبكة العين	3.30	1.40	42.4	3
17	توفر بصمة الأصبع	3.45	1.36	39.4	3
18	توفر نمط الصوت	2.25	1.47	65.3	2
19	توفر نمط الضغط على لوحة المفاتيح	4.00	1.11	27.3	4

المصدر : الباحث بالأعتماد على الحاسوب

يتضح من الجدول السابق الاتي :

أتفقت عينة الدراسة على توافر سياسة أدارية بأستخدام المقاييس والأدوات في المصارف متوسطة للفقرات (16 , 17) وبلغ المتوسط الحسابي (3.30 , 3.45) في حين كانت درجة الموافقة على استخدام نمط الصوت في التعاملات الإلكترونية منخفضة الفقرة (18) وبلغ المتوسط الحسابي (2.25) ، بينما كانت تستخدم إدارة نمط الضغط على لوحة المفاتيح بدرجة موافقة عالية الفقرة (19) حيث بلغ المتوسط الحسابي (4.00) .

٤ – الجدول رقم (4) يوضح المتوسطات الحسابية والانحراف المعياري ومعامل الاختلاف للأجابات الخاصة بتوافر سياسة باستخدام أدوات تكنولوجيا نظام أمن المعلومات في المصارف العراقية .

الجدول رقم (4) نتائج التحليل الإحصائي الخاصة بتوافر سياسة استخدام أدوات تكنولوجيا امن المعلومات

ت	الفقرات	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %	درجة الموافقة
20	أستخدام البطاقة الذكية	4.28	0.816	19.1	4
21	أستخدام كامرات مراقبة	4.43	0.747	16.9	4
22	أستخدام انظمة انذار	4.18	1.030	24.6	4
23	أستخدام زجاج غير شفاف لغرف الحاسبات	4.38	0.667	15.2	4
24	أخرى	3.48	0.994	27.5	3

المصدر : الباحث بالأعتماد على الحاسوب

يتضح من الجدول السابق الاتي :

أتفقت عينة الدراسة على توافر سياسة أدارية خاصة باستخدام أدوات تكنولوجيا أمن المعلومات للفقرات (20 , 21 , 22 , 23 , 24) حيث بلغ المتوسط الحسابي (4.28 , 4.43 , 4.18 , 4.38 , 3.48) على التوالي وهذا يؤشر أن المصارف العراقية تستخدم أدوات تكنولوجيا امن المعلومات بالإضافة إلى استخدامها تركيب أنظمة كشف الدخان ووضع مطافأ الحريق بالقرب من غرف العمل ....).

ثانياً : الإجابات على أسئلة مدى توافر سياسات فنية متبعة من قبل المصارف العراقية .

١- الجدول رقم (5) يوضح المتوسطات الحسابية والانحراف المعياري ومعامل الاختلاف للأجابات الخاصة بتوافر سياسة برامج لأمن المعلومات والشبكات في نظام أمن المعلومات .

الجدول رقم (5) نتائج التحليل الإحصائي الخاصة بتوافر سياسة برامج الحماية لأمن المعلومات والشبكات .

ت	الفقرات	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %	درجة الموافقة
25	وضع كلمة مرور تشمل حروف وارقام ذات قوة وطول امنة	4.20	1.11	26.4	4
26	تغير الإدارة كلمات المرور باستمرار	4.15	1.00	24.1	4
27	تستخدم برامج مكافحة الفيروسات اصلية ومرخصة ومجدية بصورة مستمرة	4.30	0.911	21.2	4
28	تستخدم المنظمة برامج لكشف التسلل والاختراق	4.03	1.16	28.8	4
29	توفر برامج الجدارات النارية لحماية وتامين شبكة المعلومات ومنع الوصول غير المسموح به	4.15	0.921	22.2	4
30	توفر برامج تقيد استخدام الشبكة اللاسلكية ويسمح لموظفين محددين	3.93	0.944	24.0	4

المصدر : الباحث بالأعتماد على الحاسوب

يتضح من الجدول السابق الاتي :

كانت درجة الموافقة عالية على توافر سياسة فنية خاصة باستخدام برامج الحماية لأمن المعلومات والشبكات للفقرات (25 , 26 , 27 , 28 , 29 , 30) حيث بلغ المتوسط الحسابي , 4.30 , 4.03 , 4.15) (3.93 , 4.20 , 4.15على التوالي وهذا يعكس أهتمام أدارات تقنية المعلومات بتوافر سياسات الحماية لأمن المعلومات والشبكات .

٢ – الجدول رقم (6) يوضح المتوسطات الحسابية والانحراف المعياري ومعامل الاختلاف للأجابات الخاصة بتوافر سياسة للتحكم والوصول للمعلومات في نظام أمن المعلومات

الجدول (6) نتائج التحليل الإحصائي الخاصة بتوافر سياسة للتحكم والوصول للمعلومات

ت	الفقرات	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %	درجة الموافقة
31	تحديد صلاحيات المستخدمين المصرح لهم بالدخول لنظام معلومات المنظمة	4.28	0.599	14.0	4
32	توفر سياسات تقيد الوصول وتصفح مواقع انترنيت محددة	3.925	1.12	28.5	4
33	ضبط الدخول إلى قواعد البيانات ، نظام التشغيل وبرامج التطبيقات	4.025	1.03	25.6	4
34	تخزن كافة الوسائط في بيئة امنة ومحصنة	4.25	1.01	23.8	4

يتضح من الجدول السابق الاتي :

كانت درجة الموافقة عالية على توافر سياسة فنية للتحكم والوصول للمعلومات للفقرات (31 , 32 , 33 , 34) حيث بلغ المتوسط الحسابي (4.28 , 3.925 , 4.025 , 4.25) على التوالي وتشير هذه النتائج إلى ان إدارة تقنية المعلومات بالمصارف العراقية تطبق كم كبير من سياسات الحماية الفنية لتأمين وحماية نظام المعلومات بها .

٣ – الجدول رقم (7) يوضح المتوسطات الحسابي والانحراف المعياري ومعامل الاختلاف للأجابات الخاصة بتوافر سياسة خصوصية أستخدام البيانات المتاحة في نظام أمن المعلومات .

الجدول (7) نتائج التحليل الإحصائي الخاص بتوافر سياسة حماية خصوصية البيانات .

ت	الفقرات	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %	درجة الموافقة
35	اتاحة المعلومات للموظفين طبقا لحاجة العمل	4.15	0.921	22.2	4
36	تحديد صلاحيات الدخول للاطراف الخارجية بنظام امن معلومات المنظمة	3.925	1.16	29.6	4
37	الابلاغ الفوري عن نقاط الضعف في حماية المعلومات	4.25	0.870	20.5	4

المصدر: الباحث بالأعتماد على الحاسوب

يتضح من الجدول السابق الاتي :

كانت درجة الموافقة عالية على توافر سياسة فنية لحماية خصوصية البيانات للفقرات (35 , 36 , 37) حيث بلغ المتوسط الحسابي (4.15 , 3.925 , 4.25) مما يدل على أن المصارف العراقية تطبق المزيد من السياسات الفنية لحماية امن معلوماتها .

٤ – الجدول رقم (8) يوضح المتوسطات الحسابية والانحراف المعياري ومعامل الاختلاف للأجابات الخاصة بتوافر سياسات حماية خاصة بتشفير البيانات في نظام أمن المعلومات .

الجدول (8) نتائج التحليل الإحصائي الخاص بتوافر سياسات حماية خاصة بتشفير البيانات

ت	الفقرات	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %	درجة الموافقة
38	تستخدم المنظمة سياسة التشفير وفقا للمعايير الدولية ISO لتشفير الرسائل والبيانات	4.125	0.822	19.9	4
39	تشفير نسخ الحفظ الاحتياطية	4.125	0.853	20.7	4
40	توفر اجراءات التخلص من وسائط التخزين المختلفة المنتهية الصلاحية	3.975	0.947	23.8	4

المصدر : الباحث بالأعتماد على الحاسوب

يتضح من الجدول السابق الاتي :

كانت درجة الموافقة عالية على توافر سياسات حماية فنية خاصة بتشفير البيانات في المصارف العراقية للفقرات (38 , 39 ,40) حيث بلغ المتوسط الحسابي (4.125, 4.125, 3.975) مما يشير إلى أن نظام أمن المعلومات يأخذ كافة الاحتياطات الكافية لمنع حدوث اختراقات أمنية .

٥ – الجدول رقم (9) يوضح المتوسطات الحسابية والانحراف المعياري ومعامل الأختلاف للأجابات الخاصة بتوافر سياسة فنية لحماية وصول المستخدمين للمعلومات في نظام أمن المعلومات .

الجدول (9) نتائج التحليل الإحصائي الخاصة بتوافر السياسات الفنية لحماية وصول المستخدمين للمعلومات في المصارف العراقية

ت	الفقرات	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %	درجة الموافقة

41	توفر أجراءات وأنظمة بأنشاء وأدارة حسابات المستخدمين وسحب حقوق الدخول	4.00	0.785	19.6	4
42	تخصص لكل مستخدم من مستخدمي نظام المعلومات هوية وكلمة مرور	4.35	1.00	23.0	4
43	تحديد مسؤوليات المستخدمين طبقا لطبيعة عمل كل منهم	4.30	0.912	21.2	4
44	ألزام كافة المستخدمين بقراءة اتفاقية عدم الإفشاء بالمعلومات الخاصة بالمنظمة والتوقيع عليها	4.225	0.698	16.5	4

المصدر : الباحث بالأعتماد على الحاسوب

يتضح من الجدول السابق الاتي :

كانت درجة الموافقة عالية على توافر سياسة فنية خاصة لحماية وصول المستخدمين للمعلومات في نظام معلومات المصارف العراقية للفقرات (41 , 42 , 43 , 44) حيث بلغ المتوسط الحسابي , 4.30 , 4.225) (4.00 , 4.35 على التوالي وهذا يشير إلى أن المصارف تطبق سياسات حماية فنية لتعريف الموظفين بأستخدام المعلومات وكيفية الوصول أليها بطرق سليمة .

٦ – الجدول (10) يوضح المتوسطات الحسابية والأنحراف المعياري ومعامل الأختلاف للأجابات الخاصة بتوافر سياسات فنية لإدارة الحوادث الأمنية في نظام أمن المعلومات .

الجدول (10) نتائج التحليل الإحصائي لسياسة إدارة الحوادث الفنية

ت	الفقرات	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %	درجة الموافقة
45	الزام الموظفين بأعداد تقرير بالحوادث الأمنية للمعلومات بصفة إدارية	4.075	0.615	15.1	4
46	أنشاء أحدث رسائل التنبية الخاصة بكشف التسلل بحيث تقوم بالاستجابة دون تأخير	4.225	0.891	21.1	4
47	توفر أجراءات تعقب التعديلات Audit trails بحيث تكشف هوية وأنشطة المستخدمين المربوطة بالشبكة	4.075	0.730	17.9	4
48	استخدام أدوات المسح للتعرف على نقاط ضعف الحماية التي يمكن استغلالها من قبل أشخاص خارجين	4.025	1.074	26.7	4
49	توفر سياسات واضحة وفاعلة لتقيم الثغرات ونقاط الضعف في نظام امن المعلومات	4.175	0.903	21.2	4

المصدر: الباحث بالأعتماد على الحاسوب

يتضح من الجدول السابق الاتي :

كانت درجة الموافقة عالية الخاصة بتوافر سياسات فنية لإدارة الحوادث الأمنية في المصارف العراقية للفقرات (45 , 46 , 47 , 48 , 49) حيث بلغ المتوسط الحسابي , 4.225 , 4.075 , 4.025 , 4.175) 4.075 وهذا يشير إلى أن إدارة تقنية المعلومات تطبق كم هائل من المحددات التي تمنع الاختراق .

٧ – الجدول (11) يوضح المتوسطات الحسابية والانحراف المعياري ومعامل الاختلاف للأجابات الخاصة بتوافر سياسة فنية للتعامل مع البريد الإلكتروني المستخدم في نظام أمن المعلومات .

الجدول (11) نتائج التحليل الأحصائي لتوافر سياسة التعامل مع البريد الإلكتروني

ت	الفقرات	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف	درجة الموافقة
50	استخدام بروتكول البريد الإلكتروني S/ MIME لتشفير رسائل البريد الإلكتروني	4.025	0.891	22.1	4
51	التأكد من تشغيل برامج مضادة للفيروسات لفحص رسائل البريد الإلكتروني	4.175	0.903	21.6	4

يتضح من الجدول السابق الاتي :

كانت درجة الموافقة عالية على توافر سياسة فنية خاصة للتعامل مع البريد الإلكتروني للفقرات (50 , 51) حيث بلغ المتوسط الحسابي (4.025 , 4.175) وهذا يؤشر ان المصارف العراقية تطبق بروتكول التعامل مع البريد الإلكتروني S/MIME لتشفير الرسائل وتشغيل برامج مضادة للفيروسات لفحص رسائل البريد الإلكتروني .

ثالثاً : الإجابات على أسئلة مدى توافر سياسات مواجهة حدوث المخاطر في نظام امن المعلومات

١ – يوضح الجدول (12) نتائج التحليل الإحصائي لمتغيرات الدراسة والتي تشمل المتوسطات الحسابية والانحراف المعياري للمخاطر والتهديدات التي يتعرض لها نظام امن المعلومات نتيجة قلة الوعي والتدريب لمستخدمي المنظمة .

الجدول (12) نتائج التحليل الإحصائي لتكرار حدوث المخاطر نتيجة قلة الوعي والتدريب في المصارف العراقية

ت	الفقرات	مرة على الأقل يوميا	مرة على الأقل أسبوعيا	مرة على الأقل شهريا	مرة على الأقل سنويا	لا تحدث مخاطرة ابدا	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة
52	العبث بالبيانات أو اتلافها من قبل المستخدمين لنظام امن المعلومات	5	10	9	1	15	3.28	1.502	متوسطة
53	سرقة بيانات الهوية من نظام امن المعلومات	2	10	5	3	15	3.10	1.795	متوسطة
54	سوء استغلال الصلاحيات الممنوحة لمستخدمي نظام امن المعلومات	2	12	6	7	13	3.425	1.02	متوسطة
55	الإدخال غير المقصود للبيانات الخاطئة من قبل المستخدمين	3	12	10	12	3	3.00	1.11	متوسطة
56	عمل نسخ غير مصرح بها من البيانات الهامة	1	10	6	8	15	3.65	1.29	عالية
57	الوصول غير المرخص به لنظام معلومات الأشخاص من خارج المنظمة	5	11	6	3	15	3.30	1.52	متوسطة

المصدر : الباحث بالأعتماد على الحاسوب

يتضح من الجدول السابق الاتي :

- يلاحظ من الجدول السابق أن درجة تكرار العبث بالبيانات أو أتلافها من قبل المستخدمين في المصارف متوسطة ، حيث تتركز اغلب التكرارات ما بين مرة على الأقل أسبوعيا أو شهريا ، وان نسبة (37.5%) أفادت ان العبث بالبيانات لا تحدث ابدا وقد حصلت الفقرة (52) على درجة أهمية بلغت في المتوسط (3.28) وبانحراف معياري (1.502) وهذا يدل على أن هناك شريحة من المستخدمين تقوم بإتلاف البيانات أو فقدانها بدون قصد ، لذلك على إدارة تقنية المعلومات تدريب وتوعية العاملين بالأضرار التي تصيب نظام أمن المعلومات من جراء ذلك .
- درجة تكرار خطر سرقة بيانات الهوية متوسطة ، حيث تتركز اغلب التكرارات مرة على الأقل أسبوعيا ، وان نسبة (37.5%) أفادت أن سرقة البيانات لا تحدث ابدا وقد حصلت الفقرة (53) على متوسط حسابي (3.10) وبانحراف معياري قدره (1.795) وهذا يدلل أن هناك تسريب لبيانات الهوية الشخصية للدخول إلى النظام .
- يتضح من الجدول السابق ان خطر سوء استغلال الصلاحيات الممنوحة هي الأخرى متوسطة ، حيث تتركز اغلب التكرارات مرة على الأقل أسبوعيا ، وان نسبة (32.5%) أفادت لا تحدث ابدا ، وقد حصلت الفقرة (54) على متوسط حسابي (3.42) وبانحراف معياري (1.02) وهذا يشير أن المصارف العراقية بحاجة إلى زيادة الوعي بأهمية الحفاظ على امن سرية المعلومات المخزنة .
- أفادت نسبة كبيرة من عينة الدراسة توجد مخاطر كثيرة تحدث بشكل متكرر مرة على الأقل أسبوعيا ، شهريا وسنويا ، وان نسبة (7.5) أفادت بان الوصول غير المرخص لا تحدث وهي نسبة قليلة ، وقد حصلت الفقرة (55) على متوسط حسابي (3.00) وبانحراف معياري (1.11) وان نسبة (92.5%) يحدث إدخال غير مقصود للمستخدمين .
- أفادت أن خطر الوصول غير المرخص به متوسطة ، حيث تتركز اغلب التكرارات مرة على الأقل أسبوعيا ، وان نسبة (37.5%) أفادت لا تحدث أبدا ، وقد حصلت الفقرة (56) على متوسط حسابي (3.65) وبانحراف معياري (1.29) وهذا يشير إلى ان المصارف العراقية معرضة للوصول غير المصرح به للبيانات الهامة .
- درجة تكرار خطر الوصول غير المرخص به متوسطاً ، حيث تتركز اغلب التكرارات مرة على الأقل أسبوعيا ، وان نسبة (37.5%) أفادت ان الوصول غير المرخص به لا تحدث أبدا ، وقد حصلت الفقرة (57) على متوسط حسابي (3.30) وبانحراف معياري (1.52) وهذا يدل على قدرة الأشخاص من خارج المصارف الوصول إلى النظام .

٢ – يوضح الجدول (13) نتائج التحليل الإحصائي لمتغيرات الدراسة والتي تشمل المتوسطات الحسابية والانحراف المعياري للمخاطر والتهديدات التي يتعرض لها نظام امن المعلومات نتيجة توافر أو ضعف الأدوات والأجهزة والبرامج الرقابية المستخدمة .

الجدول (13) نتائج التحليل الإحصائي لتكرار حدوث المخاطر نتيجة عدم توافر أو ضعف الأدوات والأجهزة والبرامج الرقابية في المصارف العراقية .

ت	الفقرات	مرة على الأقل يوميا	مرة على الأقل أسبوعيا	مرة على الأقل شهريا	مرة على الأقل سنويا	لا تحدث مخاطرة أبدا	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة
58	دخول الفيروسات في نظام امن المعلومات للمنظمة	11	6	6	9	8	2.925	1.53	منخفضة
59	التلاعب والخداع من المحترفين والقرصنة لمواقع المنظمة على شبكة الأنترنيت	7	7	5	9	12	3.30	1.51	متوسطة
60	الالتقاط السلكي وتحليل الاتصالات وسرقة المعلومات المتبادلة عبر الشبكة	4	8	5	6	17	3.60	1.46	متوسطة
61	إغراق النظام يجعل شبكة المعلومات أو النظام مشغول بصورة دائمة وذلك بأرسال الرسائل البريدية الإلكترونية دفعة واحدة	3	10	6	14	7	3.30	1.36	متوسطة
62	الاحتيال عبر البريد الإلكتروني وسرقة المعلومات الخاصة بالمستخدمين	9	13	6	7	5	2.65	1.35	منخفضة
63	تكرار حدوث عدم توفر الشبكة	5	7	9	9	10	3.30	1.36	متوسطة

64	اختراق الشبكة اللاسلكية	5	10	4	5	16	3.425	1.53	متوسطة
65	الكوارث الطبيعية مثل الحرائق والأبخرة والغازات	2	8	4	6	21	3.90	1.37	عالية

المصدر : الباحث بالأعتماد على الحاسوب

يتضح من الجدول السابق الاتي :

- أفادت نسبة كبيرة من عينة الدراسة وبدرجة مرتفعة بمتوسط حسابي (2.925) دخول الفيروسات في نظام أمن معلومات المصارف العراقية بنسبة (80%) ، حيث كانت اكبر التكرارات مرة على الأقل يوميا .
- اتضح من الجدول السابق أن درجة خطر التلاعب والخداع من المحترفين لموقع المصارف على شبكة الأنترنيت متوسطة ، حيث كانت اكبر التكرارات هي مرة على الأقل سنويا ، وتراوحت باقي التكرارات مرة على الأقل يوميا أو شهريا وقد حصلت الفقرة (59) على متوسط حسابي (3.30) وبانحراف معياري (1.51) .
- أفادت عينة الدراسة أن خطر الألتقاط السلكي وتحليل الأتصالات متوسطة ، حيث تركزت اغلب التكرارات مرة على الأقل أسبوعيا ، وأفادت نسبة (42.5) لا تحدث مخاطرة أبدا في نظام المعلومات المصارف ، وقد حصلت الفقرة (60) متوسط حسابي (3.60) وبانحراف معياري (1.46) .
- يتضح من الجدول السابق أن أغراق النظام يجعل شبكة المعلومات أو النظام مشغول بدرجة مخاطرة متوسطة ، حيث تركزت اغلب التكرارات مرة على الأقل أسبوعيا وسنويا ، وقد حصلت الفقرة (61) متوسط حسابي (3.30) وبانحراف معياري (1.36) وهذا يدل إلى ضعف أو عدم توفر سياسات لتنظيم وتأمين وصول المستخدمين .
- يتضح من الجدول أن نسبة (62.5%) من عينة الدراسة أجابة بأن خطر الاحتيال عبر البريد الإلكتروني يتكرر حدوثه مرة على الأقل يوميا ، أسبوعيا ، شهريا ، سنويا وكانت درجة الأهمية بمتوسط حسابي (2.65) وبانحراف معياري (1.35) كما ورد في الفقرة (62) وهذا يدل على عدم وجود برامج حماية كافية مثل برامج الجدران النارية في نظام معلومات المصارف العراقية .
- أفادت عينة الدراسة أن خطر تكرار حدوث عدم توفر الخدمة متوسطة ، حيث تركزت اغلب التكرارات مرة على الأقل شهريا أو سنويا وقد أحتلت الفقرة (63) بمتوسط حسابي (3.30) وبانحراف معياري (1.36) .
- يعتبر خطر اختراق الشبكة اللاسلكية بدرجة مخاطرة متوسطة ، حيث تركزت اغلب التكرارات مرة على الأقل أسبوعيا ، وأفادت نسبة (40%) لا تحدث مخاطرة أبدا في نظام معلومات المصارف ، وقد حصلت الفقرة (64) على أهمية بمتوسط حسابي (3.42) وبانحراف معياري (1.53) . وهذا يدل على سهولة التقاط كلمات المرور للشبكات اللاسلكية الموصلة وضعف إجراءات الأمن المطبقة لحماية هذه الشبكات .

- تعتبر أخطار الكوارث الطبيعية ، مثل الحرائق ، الأبخرة والغازات تحدث بدرجة قليلة في نظام معلومات المصارف ، حيث أن هذا الخطر يتكرر على الأقل أسبوعيا ، وأفادت نسبة (52.5) لا تحدث مخاطرة أبدا وهي نسبة عالية ، وقد حصلت الفقرة (65) على أهمية بمتوسط حسابي (3.90) وبانحراف معياري (1.37) وهذا يدل على وجود سياسات وإجراءات أمنية قوية لمواجهة الأخطار والكوارث الطبيعية .

رابعاً : الجدول (14) يوضح المتوسطات الحسابية والانحراف المعياري لا جمالي فقرات (المحاور الثلاثة) السياسات الإدارية ، الفنية وسياسة مواجهة المخاطر والتهديدات في نظام امن المعلومات في المصارف العراقية .

الجدول (14) نتائج التحليل الإحصائي لا جمالي السياسات (للمحاور الثلاثة) الإدارية ، الفنية وسياسة مواجهة المخاطر والتهديدات في نظام امن معلومات المصارف العراقية .

ت	الفقرات	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة
1	**المحور الأول أجمالي السياسات الإدارية (أصول المعلومات ، المقاييس المستخدمة ، أدوات تكنولوجيا المعلومات)**	**3.831**	**0.653**	**4**
2	**المحور الثاني أجمالي السياسات الفنية (برامج الحماية ، التحكم والوصول ، خصوصية البيانات ، تشفير البيانات ، وصول المستخدمين ، إدارة الحوادث الأمنية ، التعامل مع البريد الإلكتروني)**	**4.127**	**0.123**	**4**
3	**المحور الثالث أجمالي سياسات مواجهة المخاطر والتهديدات (المخاطر والتهديدات نتيجة قلة الوعي والتدريب ، نتيجة عدم توافر أو ضعف الأدوات والأجهزة والبرامج الرقابية)**	**3.296**	**0.315**	**4**
أجمالي السياسات الثلاثة		**3.751**	**0.363**	

المصدر : الباحث بالأعتماد على الحاسوب

يتضح من الجدول السابق الاتي :

أن المصارف العراقية عينة الدراسة تتبع سياسات أدارية ، فنية ، وسياسة مواجهة المخاطر والتهديدات حيث بلغ المتوسط الحسابي (3.751) وهي اعلى من مستوى المتوسط وبانحراف معياري (0.363) وقد حقق المحور الثاني السياسات الفنية اعلى متوسط حسابي (4.127) في حين حقق المحور الثالث سياسة مواجهة المخاطر والتهديدات ادنى متوسط حسابي (3.296) وهذا يدل على أن السياسات الفنية المتبعة من قبل المصارف العراقية عالية من خلال استخدام حزمة من برامج الحماية ، ووضع أنظمة تأمين التحكم والوصول للمعلومات ،

وسرية وقوة كلمات المرور ، حماية خصوصية البيانات للمستخدمين واستخدام برامج مضادة للفيروسات ومراقبة صلاحيات دخول المستخدمين .

وعلى المصارف العراقية عينة الدراسة أن تتبع سياسة اكثر قوة في مواجهة المخاطر والتهديدات من خلال زج العاملين في برامج وتدريب وأستخدام الأدوات والأجهزة والبرامج التي تحد من تلك المخاطر والتهديدات .

اختبار الفرضيات :

الفرضية الأولى : تطبق المصارف العراقية سياسات إدارية لمواجهة مخاطر أستخدام تكنولوجيا المعلومات .

الجدول (15) يبين إجابة عينة الدراسة البالغة (40) فرد على العبارات المكونة للمحور الأول (السياسات الإدارية)

one – sample statistics

	N	Mean	Std-Deviation	Std. Error Mean
AXE_1	24	3.8313	0.65329	0.13335

one – sample Test

	t	dF	Sig.(2-tailed)	Mean Difference	%95 confidence interval of the difference	
					Lower	upper
AXE_1	28.730	23	0.000	3.83123	3.5554	4.1071

تبين المخرجات أعلاه أجابات العبارات المكونة للسياسات الإدارية التي تطبقها المصارف العراقية بلغ المتوسط الحسابي (3.8313) وبانحراف معياري قدره (0.653) وبلغت قيمة (T) المحسوبة (28.73) وهي اكبر من قيمتها الجدولية البالغة (2.807) وبالتالي يمكن قبول الفرضية .

الفرضية الثانية : تطبق المصارف العراقية سياسات فنية لمواجهة مخاطر أستخدام تكنولوجيا المعلومات .

الجدول (16) يبين إجابات عينة الدراسة على العبارات المكونة للمحور الثاني السياسات الفنية .

جدول (16) one – sample statistics

	N	Mean	Std. Deviation	Std-Error Mean
AXE_2	27	4.127	0.123	0.0238

one – sample Test

	T	dF	Sig.(2-tailed)	Mean Difference	%95 confidence interval of the difference Lower	upper
AXE_2	172.980	26	0.000	4.127	4.0784	4.106

تبين المخرجات أعلاه إجابات العبارات المكونة للسياسات الفنية التي تطبقها المصارف العراقية حيث بلغ المتوسط الحسابي (4.127) وبانحراف معياري قدره (0.123) وبلغت قيمة (T) المحسوبة (172.980) وهي اكبر من قيمتها الجدولية (2.779) وبالتالي يمكن قبول الفرضية .

الفرضية الثالثة : تطبق المصارف العراقية سياسات للحد من تكرار المخاطر والتهديدات لمواجهة تعقيدات تكنولوجيا المعلومات . الجدول (17) يبين اجابات عينة الدراسة على العبارات المكونة للمحور الثالث سياسات مواجهة المخاطر والتهديدات .

جدول (17) one – sample statistics

	N	Mean	Std.Deviation	Std-Error Mean
AXE_3	14	3.296	0.135	0.084

one – sample Test

	T	df	Sig.(2-tailed)	Mean difference	%95 confidence interval of the difference Lower	upper
AXE_3	39.051	13	0.000	3.296	3.114	3.479

المصدر : الباحث بالأعتماد على الحاسوب

تبين المخرجات أعلاه أجابات العبارات المكونة لسياسات مواجهة حدوث المخاطر والتهديدات التي تطبقها المصارف العراقية حيث بلغ المتوسط الحسابي (3.296) وبانحراف معياري (0.315) و بلغت قيمة (t) المحسوبة (39.051) وهي اكبر من قيمتها الجدولية (3.012) وبالتالي يمكن قبول الفرضية وهذا يشير إلى وجود مخاطر وتهديدات في نظام أمن المعلومات .

المبحث الرابع : الاستنتاجات والتوصيات

المطلب الأول : الأستنتاجات

توصلت الدراسة إلى الاستنتاجات الأتية :

١- أتفقت عينة الدراسة إلى أن المصارف العراقية تطبق سياسات حماية إدارية اعلى من المتوسط حيث بلغ المتوسط الحسابي (3.831) لأ جمالي الفقرات وقد حققت الفقرة (7) تنظيم دورات تدريبية للموظفين الجدد أعلى مستوى في حين حققت الفقرة (1) (توجد أدارة خاصة بإدارة المخاطر الرقمية) ادنى مستوى وهذا يعني عدم وجود أدارة متخصصة بأمن وأدارة المخاطر في المصارف العراقية .

٢- أتفقت عينة الدراسة على أتباع أجراءات وسياسات أدارية لأصول المعلومات بمستوى عالي حيث حققت الفقرة (15) (تحديد الأفراد والمجموعات المخولة بالوصول إلى المعلومات أعلى مستوى في حين حققت الفقرة (14) (يتم أجراء تداول ، تخزين ونقل وأتلاف أصول المعلومات وفقا للقواعد المحددة) أدنى مستوى وهذا يعني أن المصارف عينة الدراسة تتبع سياسات حماية لأدارة أصولها وفقا للمعايير والضوابط المحددة .

٣- أهتمام أدارات تقنية المعلومات باتباع العديد من الأجراءات والسياسات الأدارية باستخدام المقاييس وأدوات تكنولوجيا المعلومات بمستوى متوسط وقد حققت الفقرة (20) (استخدام البطاقة الذكية) أعلى مستوى وهذا يدلل إلى أن المصارف تخطط للتوسع بهذه الخدمة للمواطنين .

٤- أتفقت عينة الدراسة بأتباع العديد من سياسات وأجراءات الحماية الفنية لتأمين وحماية خصوصية البيانات للمستخدمين مثل وضع كلمات المرور القوية لحماية حسابات المستخدمين ، أستخدام برامج مضادة للفيروسات قوية ومحدثة بصفة مستمرة ، أدارة ومراقبة صلاحيات دخول المستخدمين لنظام المعلومات ، أنشاء رسائل التنبيه الخاصة بكشف التسلل ، الأحتفاظ بنسخ للسجلات وكافة المعلومات المهمة داخل غرف الحاسبات .

٥- أتفقت عينة الدراسة الجدول (١٢) إلى حدوث مخاطر في نظام أمن المعلومات بشكل متكرر ترجع إلى أسباب تتعلق بموظفي تقنية المعلومات نتيجة قلة الخبرة والوعي والتدريب حيث يعتبر الأدخال غير المقصود للبيانات الخاطئة ، سوء استغلال الصلاحيات الممنوحة للمستخدمين ، العبث بالبيانات أو أتلافها من قبل المستخدمين ، عمل نسخ غير مصرح بها ، الوصول غير المصرح به لنظام معلومات الأشخاص من خارج المنظمة أكثر المخاطر التي قد تحدث اكثر من مرة أسبوعيا إلى مرة شهريا .

٦- أتفقت عينة الدراسة الجدول (١٣)على وجود بعض المخاطر ألتي قد تحدث مرة على الأقل يوميا مثل العبث بالبيانات أو أتلافها من قبل المستخدمين لنظام أمن المعلومات ، الوصول غير المرخص به لنظام معلومات الأشخاص من خارج المنظمة ، الإدخال غير المقصود للبيانات الخاطئة من قبل المستخدمين ، دخول الفيروسات في نظام أمن المعلومات ، الاحتيال عبر البريد الألكتروني وسرعة المعلومات ، التلاعب والخداع من المحترفين والقرصنة لموقع المصارف على شبكة الأنترنيت .

٧- موافقة غالبية عينة الدراسة على قلة حدوث مخاطر تتعلق بالألتقاط السلكي وتحليل الأتصالات وسرقة المعلومات ، أختراق الشبكة اللاسلكية وحدوث كوارث طبيعية مثل الحرائق والأبخرة والغازات وبنسب متفاوتة .

التوصيات : توصي الدراسة بالأتي :

١- أستحداث أدارة مخاطرة رقمية في المصارف العراقية التي تتعامل ألكترونيا عبر شبكة الأنترنيت لتحقيق التكامل والدعم المتبادل بين جميع الوحدات المرتبطة بتلك الأدارة . على الرغم من أنها حققت نجاحات في مجالات سياساتها (الأدارية والفنية) الا أنها تواجه مخاطر وتهديدات في نظام أمن معلوماتها .
٢- أهمية تطوير سياسات أمن نظم المعلومات وحمايتها والعمل بالمعايير والمواصفات القياسية لأستخدامات نظم المعلومات وتطبيقها بصورة فاعلة .
٣- تطوير البرامج والأساليب لأستخدامات تداول ، تخزين وأتلاف أصول المعلومات ، تفادي سرقة الهوية وكلمات المرور ، ومنع التسلل والأختراق للشبكات اللاسلكية المتصلة بنظام المعلومات .
٤- وضع برنامج لنشر الوعي الأمني لجميع العاملين في المصارف بشتى مستوياتهم .
٥- أجراء عمليات تدقيق دوري لتقييم السياسات والإجراءات الأمنية المطبقة وتحديد نقاط الضعف والثغرات الأمنية فور حدوثها ، ثم معالجة أثارها عند حدوثها .
٦- تشجيع البحوث في مجال امن وإدارة المخاطرة الرقمية والانطلاق إلى مجالات أخرى وأفكار أخرى .
٧- العمل على أن تكون أنشطة أدارة المخاطرة الرقمية مستمرة ودائمة التطور وترتبط باستراتيجية المنظمة وجعل تلك المنظمة على استعداد دائم لكل الاحتمالات والمواقف .

المراجع :

١- أبو بكر ، عيد أحمد والسيفو ، وليد إسماعيل ، ٢٠٠٩ ، أدارة الخطر والتأمين ، دار البازوري العلمية للنشر والتوزيع ، عمان ، الأردن .
٢- الشيتي ، أيناس محمد أبراهيم ، ٢٠١٤ ، تقييم سياسات أمن وخصوصية المعلومات في المؤسسات العلمية في المملكة العربية السعودية ، المجلة المصرية للمعلومات (كمبيونت) العدد ١٤ .
٣- المري ، عايض ، ٢٠١٤ ، امن المعلومات ماهيتها وعناصرها واستراتيجيتها ، للدراسات والاستشارات القانونية .htt://www.dralMari.com/show.asp?field=res_a&id=205
٤- الهادي ، محمد محمد ، ٢٠١٣ ، المعايير الدولية الحديثة المتعلقة بأمن وخصوصية المعلومات ، المجلة المصرية للمعلومات ، ((كمبيونت)) العدد ١٣ .
٥- جريدة الرياض ، أدارة المخاطر الرقمية التحول القادم في عالم التقنية ، الأحد ٢٧ يوليو ٢٠١٤ ، العدد 16834 ، مؤسسة اليمامة الصحية .
٦- حماد ، طارق عبد العال ، ٢٠٠٧ ، إدارة المخاطر (أفراد ، أدارات ، شركات ، بنوك) كلية التجارة عين الشمس ، الدار الجامعية ، الإسكندرية .
٧- رضوان ، سمير عبد الحميد ، ٢٠٠٥ ، المشتقات المالية ودورها في أدارة المخاطر ودور الهندسة المالية في صناعة أدواتها ، الطبعة الأولى ، دار النشر للجامعات ، مصر .
٨- لمجد ، بوزيدي ، ٢٠٠٩ ، إدارة المخاطر في المؤسسات الصغيرة والمتوسطة ، رسالة ماجستير غير منشورة ، جامعة احمد بوقرة ، بومرداس ، الجزائر .
٩- هيئة الاتصالات وتقنية المعلومات السعودية ،١٤٣٢هـ ، الدليل الإرشادي لسياسات وإجراءات امن المعلومات للجهات الحكومية ، الطبعة الأولى .

١٠- ويبيكيديا ، الموسوعة الحرة ، أكتوبر ، ٢٠١٤ .
١١- يوسف ، صوار ،٢٠٠٩ ، محاولة تقدير خطر عدم تسديد القرض التنقيطي والتقنية العصبية الاصطناعية بالبنوك الجزائرية ، أطروحة دكتوراه غير منشورة ، جامعة أبو بكر بلقايد ، كمسان ، الجزائر .
١٢- المنظمة الدولية للقياس والهيئة الدولية للكهروتقنية / السودان – المركز القومي للمعلومات، ٢٠١٠، الجودة وتطوير المعايير – الطبعة الثانية .
١٣- البياتي ، محمود والقاضي ، دلال ، ٢٠١٠ ، البحث العلمي وأساليبه بأستخدام spss ، الطبعة الثانية
١٤- بروكتور ، بول ، ٢٠١٤ ، ادارة المخاطرة الرقمية التحول القادم في عالم التقنية ، الرياض الأقتصادي ، العدد ١٦٨٣٤–٢٧ يوليو
١٥- المدرع ، محمد فايز ، ٢٠١٤ ، المعايير العالمية لأمن المعلومات ، ورقة عمل ، مركز التميز لأمن المعلومات .
١٦- يوسف ، نسرين محمد فتحي ، ٢٠١٣ ، الأفصاح عن حوكمة التكنولوجية المعلومات ودورة في زيادة القدرة التنافسية – ورقة عمل مقدمة إلى المؤتمر الثالث للعلوم المالية والمصرفية – جامعة اليرموك – الأردن – للفترة من ١٧ – ١٨ أبريل

المراجع الأجنبية :

1 – Arnason , sigurjon Thro and willet , Keith D.,2008,How to Achieve 27001 certifiation An Example of Applied compliance Management , Toylor and Francis Group LLc. New York , USA.

2- Brabton J. and gold J." ,2003 , Human Resource Management : Theory and practice "3ed Great Britan , bath press .

3 – Collective project , 2003 , risk management hand book , office of project management process improvement , first edition , June .

4 – Forouzan , Behrouz A., 2008 , Introduction to cryptography and network security .

5 – Hamiloton , C.R.,1998 , new trends in risk management " information systems security " , Vol,7, No1 .

6 – John wiley and sons , Inc (2006) ." Hand book of information security ",Volume ,2, p.60.

7 – Perrin , chad ,2012, " The CIA Traid ", may , 31 .

الأنترنيت

1 – http://coeia.edu.sa/index.php/ar/asn..._security.html

2 – http://www.iso27001security.com/index.html-1.

3 – http://ar.wikipedia.org/wiki/20/12/2011.

4 – http://ar.wikipedia.org/w/index.php?title = معلومات _ امن &oldid=1413377"2014 .

5- Ait news.com/2014/07/21 البوابة العربية لأخبار التقنية