

العنوان:	أثر تكامل حوكمة أمن المعلومات وخدمات تأكيد الثقة على الحد من مخاطر نظم المعلومات المحاسبية الالكترونية: دراسة ميدانية
المصدر:	مجلة الدراسات والبحوث المحاسبية
الناشر:	جامعة بنها - كلية التجارة - قسم المحاسبة
المؤلف الرئيسي:	خليل، علي محمود مصطفى
مؤلفين آخرين:	الملاح، شيرين شوقي السيد، العوامري، عبير عيسى علي عطية(م. مشارك)
المجلد/العدد:	ع1
محكمة:	نعم
التاريخ الميلادي:	2022
الشهر:	يونيو
الصفحات:	537 - 569
رقم MD:	1405355
نوع المحتوى:	بحوث ومقالات
اللغة:	Arabic
قواعد المعلومات:	EcoLink
مواضيع:	نظم المعلومات الالكترونية، المعلومات المحاسبية، حوكمة أمن المعلومات
رابط:	http://search.mandumah.com/Record/1405355

للإستشهاد بهذا البحث قم بنسخ البيانات التالية حسب إسلوب
الإستشهاد المطلوب:

إسلوب APA

خليل، علي محمود مصطفى، الملاح، شيرين شوقي السيد، و
العوامري، عيبر عيسى علي عطية. (2022). أثر تكامل حوكمة أمن
المعلومات وخدمات تأكيد الثقة على الحد من مخاطر نظم المعلومات
المحاسبية الالكترونية: دراسة ميدانية. مجلة الدراسات والبحوث
المحاسبية، ع1، 537 - 569. مسترجع من
<http://search.mandumah.com/Record/1405355>

إسلوب MLA

خليل، علي محمود مصطفى، شيرين شوقي السيد الملاح، و عيبر
عيسى علي عطية العوامري. "أثر تكامل حوكمة أمن المعلومات وخدمات
تأكيد الثقة على الحد من مخاطر نظم المعلومات المحاسبية الالكترونية:
دراسة ميدانية." مجلة الدراسات والبحوث المحاسبية ع1 (2022): 537 -
569. مسترجع من <http://search.mandumah.com/Record/1405355>

أثر تكامل حوكمة أمن المعلومات وخدمات تأكيد الثقة على الحد من مخاطر
نظم المعلومات المحاسبية الالكترونية
دراسة ميدانية

أ.د/ علي محمود مصطفى خليل أ.د/ شيرين شوقي السيد الملاح أ.د/ عيسى علي عطية العوامري
أستاذ المحاسبة المالية أستاذ المحاسبة والمراجعة المساعد معيدة بقسم المحاسبة
ووكيل الكلية السابق لشئون خدمة المجتمع كلية التجارة - جامعة بنها كلية التجارة - جامعة بنها
وتنمية البيئة كلية التجارة - جامعة بنها

أثر تكامل حوكمة أمن المعلومات وخدمات تأكيد الثقة على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية (دراسة ميدانية)

أ.د/ علي محمود مصطفى خليل أ.د/ شيرين شوقي السيد الملاح أ.د/ عيسى علي عطية العوامري
أستاذ المحاسبة المالية أستاذ المحاسبة والمراجعة المساعد معيدة بقسم المحاسبة
ووكيل الكلية السابق لشئون خدمة المجتمع كلية التجارة - جامعة بنها كلية التجارة - جامعة بنها
وتنمية البيئة كلية التجارة - جامعة بنها

ملخص

يهدف البحث إلى استكشاف أثر تكامل حوكمة أمن المعلومات وخدمات تأكيد الثقة على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية؛ وذلك بغرض زيادة الموثوقية، والمصدقية في نظم المعلومات المحاسبية الإلكترونية ومخرجاته.

وفي سبيل تحقيق هذا الهدف هناك مجموعة من الخطوات التي تمثل أهداف فرعية للهدف الرئيسي وهي: التعرف على أنواع مخاطر نظم المعلومات المحاسبية الإلكترونية، وأسبابها، والتعرف على أهمية تطبيق حوكمة أمن المعلومات، وذلك في ضوء المعايير الدولية الخاصة بمجال أمن المعلومات مثل: معايير الأيزو 27 ISO/IEC، الإصدار الخامس من معيار COBIT، معيار ITIL، ودورها في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية، وتحديد مدى أهمية خدمات تأكيد الثقة، وذلك في ضوء مبادئ الخمسة (الأمن، جاهزية النظام، نزاهة العمليات، الخصوصية، السرية)، ودورها في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية، واختبار مدى إمكانية التكامل المقترح بين حوكمة أمن المعلومات وخدمات تأكيد الثقة في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية، فقد قامت الباحثة بعمل دراسة ميدانية بهدف التوصل إلى مدى يساهم التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.

وتوصلت الدراسة إلى عدة نتائج أهمها: تتعرض نظم المعلومات المحاسبية الإلكترونية للعديد من المخاطر يتمثل أهمها في المخاطر الداخلية، كما يتمثل أهم أسباب حدوث تلك المخاطر في عدم كفاءة وفعالية الإجراءات والضوابط الرقابية لنظم المعلومات داخل تلك الشركات، بالإضافة إلى عدم تضمين عدد كبير من عينة الدراسة لأهداف ومبادئ كل من حوكمة أمن المعلومات وخدمات تأكيد الثقة داخل استراتيجيتها المستقبلية، وأخيراً توصلت الدراسة إلى وجود تأثير معنوي لتطبيق معيار COBIT5 لحوكمة أمن المعلومات والمبادئ الخمسة لخدمات تأكيد الثقة على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية. الكلمات المفتاحية: مخاطر نظم المعلومات المحاسبية، حوكمة أمن المعلومات، خدمات تأكيد الثقة.

Abstract

Purpose: This Research aims to explore The Impact of The Integration of Information Security Governance and Trust Assurance Services on Reducing the Risks of Electronic Accounting Information Systems; this is for The Purpose of increasing The Reliability, and Authenticity in Electronic Accounting Information Systems and its Outputs.

In order to achieve This Goal, There are a set of Steps that represent Sub-Goals, the Main ones: identifying the types of Risks of Electronic Accounting Information Systems and their Causes, Identifying the Importance of implementing Information Security Governance, in light of International Standards in the field of Information Security such as: ISO/IEC 27, COBIT5 Standard, ITIL Standard, and their Role in reducing The Risks of Electronic Accounting Information Systems, and determining the importance of Trust Assurance Services, in light of its five Principles(Security, System Availability, Integrity of Operation, Privacy, Confidentiality), and its Role in reducing the Risks of Accounting Information Systems, and Testing the Possibility of the Purposed Integration between Information Security Governance and Trust Assurance Services in reducing Risks of Electronic Accounting Information Systems. The Researcher conducts a Field study to determine what extent the Integration between Information Security Governance and Trust Assurance Services contribute in reducing the Risks of Electronic Accounting Information Systems.

Findings: The Study reached Several Results, the most important of which are: Electronic Accounting Information Systems are exposed to many Risks, the most important of which is Internal Risks, as well as the most important reasons for the occurrence of these risks in the inefficiency and ineffectiveness of the Control Procedures and controls for Information Systems within those Companies, in addition to this indicates that a large number of the Study sample did not include the objectives and principles of each the Information Security Governance and Trust Assurance Services within its Future Strategies, and Finally the Study found a significant effect implementation of the COBIT5 Standard for Information Security Governance and the Principles of Trust Assurance Services to reduce the Risks of Accounting Information Systems.

Keywords: Electronic Accounting Information Risks, Information Security Governance, Trust Assurance Services.

(١) الإطار العام للبحث:

(١/١) المقدمة وطبيعة المشكلة:

فى ظل ما يشهده عالم اليوم من تغيرات مستمرة وسريعة، أصبح لزاماً على الشركات أن تواكب التطور باستخدام تقنيات العصر، وعلى وجه الخصوص استخدام تكنولوجيا المعلومات، والتي تمثل عنصراً هاماً فى الشركات حيث أنها أتاحت اختراق حاجز المكان والزمان، وبالإضافة إلى السرعة الفائقة التى تنقل المعلومات فور حدوثها، وكان لنظم المعلومات المحاسبية نصيب كبير من التطور المتزايد فى تكنولوجيا المعلومات، الأمر الذى أدى إلى التحول من الاعتماد على نظم المعلومات التقليدية إلى الاعتماد على نظم المعلومات الإلكترونية وذلك لما يوفره التشغيل الإلكتروني للبيانات من مزايا خاصة بسرعة ودقة تنفيذ العمليات؛ وعلى الرغم من المزايا التى حققتها تكنولوجيا المعلومات فى بيئة الأعمال التى تعتمد على نظم المعلومات المحاسبية الإلكترونية، إلا أنه قد صاحب استخدامها ظهور مجموعة من المخاطر والتهديدات والتمثلة فى مخاطر الاختراق، مخاطر الإصابة بالفيروسات، مخاطر ناتجة عن عدم الاحتفاظ بسرية البيانات بالدخول غير المصرح للنظم والشبكات، الاستخدام الغير مصرح به للبيانات والتلاعبات والاختلاس، تخريب وتدمير بعض الملفات،..... وغيرها من المخاطر التى تعوق فرص الحصول على معلومات محاسبية موثوقة بالإضافة إلى المخاطر المتعلقة بأصول وموجودات ومعلومات الشركة، ففى ضوء تلك المخاطر تتابعت الجهود البحثية والمهنية لملى الفجوة بين النظم الإلكترونية والضوابط الرقابية (نظراً لأن التطور فى تكنولوجيا المعلومات لم يصاحبه تطوراً مماثلاً فى الممارسات والضوابط الرقابية). والعقبة الرئيسية الناتجة من انتشار مخاطر نظم المعلومات المحاسبية الإلكترونية هو انعدام الثقة لدى مستخدمى تلك النظم التى يتعاملون معها، التى عرفت بفجوة الثقة الإلكترونية (المساحة بين ما يحتاجه مستخدمو مخرجات نظم المعلومات من وراء هذه النظم وبين ما تتمتع به هذه النظم فعلاً من صفات ومقومات تحقق الأمن من جهة والمصادقية من جهة أخرى).

ومن ثم أصبحت هناك حاجة ملحة إلى وجود منهج متكامل لإدارة مخاطر نظم المعلومات المحاسبية الإلكترونية والتعامل مع عنصر التقنية على المستوى الاستراتيجي والتشغيلي على التوازي للوصول بتلك المخاطر إلى الحد المسموح به.

ونتيجة لذلك فقد ظهر منهج شامل يهدف إلى إنشاء بيئة رقابية مناسبة للحفاظ على سرية وسلامة وتوافر المعلومات ودعم العمليات والنظم الخاصة بها، وحماية المعلومات (الأصول الأكثر أهمية للشركة) من مختلف المخاطر التى قد تتعرض لها، ويعرف هذا المنهج (بحوكمة أمن المعلومات)، وتهتم تلك الحوكمة بتأسيس بيئة رقابية مع ضمان توفير الحماية اللازمة والضرورية للأصول المعلوماتية من المخاطر المختلفة، بالإضافة إلى وضع خطة للتطوير المستمر لإدارة المخاطر، ومع تزايد أهمية حوكمة أمن المعلومات فى تحقيق العديد من المنافع

للشركات التي تقوم بتطبيقها وتقديم وإضافة قيمة حقيقية للشركة وكذلك خلق مزايًا تنافسية جديدة إلا أنها لم تلق الاهتمام البحثي الكافي في بيئة الأعمال المصرية. كما أصبحت الحاجة ملحة إلى إيجاد خدمات جديدة تواجه مخاطر نظم المعلومات المحاسبية الإلكترونية وتدعم وتؤكد الثقة في النظم وترجع أهمية هذه الخدمات إلى تدعيم الثقة والمصداقية على المعلومات التي تعيد متخذى القرارات في اتخاذ قراراتهم الاقتصادية الرشيدة، وتريد من فاعلية وكفاءة نظم المعلومات المحاسبية وخاصة تلك النظم التي تعتمد على النظم الإلكترونية.

وبذلك تتمثل مشكلة البحث في مجموعة من التساؤلات التالية:

- (١) ما هي طبيعة وأنواع ومصادر المخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية؟
- (٢) هل تطبيق آليات حوكمة أمن المعلومات يساهم في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية؟
- (٣) ما مدى تأثير مبادئ خدمات تأكيد الثقة على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية؟
- (٤) هل يساهم التكامل بين المستوى الاستراتيجي (COBIT5) والمستوى التشغيلي (مبادئ خدمات تأكيد الثقة) في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية؟

(٢/١) هدف البحث:

يتمثل الهدف الرئيسي للبحث في توضيح أثر تكامل حوكمة أمن المعلومات وخدمات تأكيد الثقة على الحد من المخاطر التي تتعرض نظم المعلومات المحاسبية الإلكترونية، ويمكن تحقيق هذا الهدف من خلال الأهداف الفرعية التالية:-

- التعرف على أنواع مخاطر نظم المعلومات المحاسبية الإلكترونية، وأسبابها.
- التعرف على أهمية تطبيق حوكمة أمن المعلومات، ودورها في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.
- تحديد مدى أهمية خدمات تأكيد الثقة، ودورها في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.
- اختبار مدى إمكانية التكامل المقترح بين حوكمة أمن المعلومات وخدمات تأكيد الثقة في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.

(٣/١) أهمية البحث:

تتبع أهمية البحث من أن نظم المعلومات المحاسبية الإلكترونية يتم الاعتماد عليها بصورة متزايدة فضلاً عن وجود العديد من المخاطر والتهديدات التي يجب الاهتمام بها ومحاولة تجنبها والتصدي لها، ومن هنا تتبّع أهمية البحث في اتجاهين:

- الأهمية العملية:

يستمد البحث أهميته العلمية من أهمية قضية تنوع وتعدد المخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية، وتوضيح آثارها على الأداء المالي للشركات التي تتعرض لها، وما يصاحبها من تدنى في جودة وموثوقية المعلومات المحاسبية، وبالتالي فإن هناك حاجة ماسة لتطوير الإجراءات والضوابط الرقابية التي تعمل على الحد من تلك المخاطر، بالإضافة إلى إلقاء الضوء على منهج شامل ومتكامل يستخدم في مواجهة هذه المخاطر وهي حوكمة أمن المعلومات، ومعرفة المعايير التي يتم استخدامها عند تطبيقها داخل شركات الأعمال المختلفة، وأيضاً عرض خدمات تناولتها أدبيات المراجعة وهي خدمات تأكيد الثقة في النظم الإلكترونية، والتي مازالت في مراحلها الأولية وتلقى اهتماماً من الهيئات التنظيمية والمهنية، إذ لا يزال موضوع دور خدمات تأكيد الثقة في مواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية من الموضوعات الحديثة نسبياً في ظل متغيرات بيئة الأعمال المعاصرة.

- الأهمية العملية:

تتبع الأهمية العملية للبحث من خلال اتجاه العديد من الشركات نحو استخدام نظم المعلومات المحاسبية الإلكترونية، ودور آليات حوكمة أمن المعلومات وخدمات تأكيد الثقة في إدارة المخاطر التي تؤثر على النظام المحاسبي الإلكتروني، وبذلك تكون هناك محاولة التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة للحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.

(٤/١) حدود ونطاق البحث:

- يقتصر البحث على دور حوكمة أمن المعلومات في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية، دون التطرق لكل من حوكمة الشركات وحوكمة تكنولوجيا المعلومات، إلا بالقدر الذي يخدم البحث.
- يقتصر البحث على إطار أهداف الرقابة على المعلومات والتكنولوجيا ذات الصلة COBIT دون التطرق لغيره من آليات تطبيق حوكمة أمن المعلومات.
- يقتصر البحث على دور خدمات تأكيد الثقة في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية من خلال مبادئها (الأمن، جاهزية النظام، تكامل العمليات، السرية والخصوصية) التي يتم تطبيقها في إطار خدمات تأكيد الثقة في النظم الإلكترونية، دون التطرق إلى أنواع خدمات التأكيد الأخرى، إلا في حدود ما يخدم البحث.
- يقتصر البحث على المخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية، دون التدخل في التفسيرات أو الدوافع من وراء تلك المخاطر.

(٥/١) منهج وأسلوب البحث:

تحقيقاً لأهداف البحث واختبار فروضه لاستكشاف مدى مساهمة التكامل المقترح بين حوكمة أمن المعلومات وخدمات تأكيد الثقة في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية يعتمد الباحث على ما يلي في إعداد البحث:

أولاً: منهج البحث: تركز الباحثة من خلال الدراسة على منهجين:

- المنهج الاستقرائي: حيث يتم استقراء الدراسات ذات الصلة بموضوع البحث.
- المنهج الاستنباطي: حيث تحاول الباحثة استنباط الأثر التكاملي بين حوكمة أمن المعلومات وخدمات تأكيد الثقة بهدف الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.

ثانياً: أسلوب البحث: سيتم الاعتماد في إعداد البحث على الأسلوبين التاليين:

- أسلوب الدراسة النظرية المكتبية: حيث يتم دراسة وتحليل المؤلفات والأبحاث والدراسات السابقة باللغة العربية والأجنبية التي تتعلق بموضوع البحث.
- الأسلوب الميداني (الاستكشافي): حيث تقوم الباحثة بعمل دراسة استكشافية من خلال اختبار الفروض التي تم صياغتها في بيئة الأعمال الحديثة.

(٦/١) خطة البحث:

تحقيقاً لأهداف البحث واختبار فروضه، فقد تم تقسيم ما تبقى من البحث كما يلي:

- ٢- الدراسات السابقة.
- ٣- الإطار الفكري لنظم المعلومات المحاسبية الإلكترونية ومخاطرها.
- ٤- الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية باستخدام التكامل المقترح بين حوكمة أمن المعلومات وخدمات تأكيد الثقة.
- ٥- الدراسة الميدانية.
- ٦- النتائج والتوصيات ومجالات البحث المستقبلية.

(٢) الدراسات السابقة:

تحاول الباحثة من خلال هذا الجزء عرض أهم الدراسات السابقة المرتبطة بموضوع البحث للوقوف على ما توصلت إليه من نتائج، والاستفادة منها في استكمال جوانب البحث في هذا الموضوع، ويمكن تقسيم الدراسات السابقة حسب ارتباطها بموضوع البحث إلى محورين هما: المحور الأول: دراسات تناولت تكامل العلاقة بين حوكمة أمن المعلومات وخدمات تأكيد الثقة، والمحور الثاني: دراسات تناولت تحليل العلاقة بين حوكمة أمن المعلومات وخدمات تأكيد الثقة على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.

المحور الأول: دراسات تناولت تكامل العلاقة بين حوكمة أمن المعلومات وخدمات تأكيد الثقة:

هدفت دراسة (Rubino, et al., 2017) إلى تحليل أثر معيار COBIT على تفعيل نظام الرقابة الداخلية، حيث يوفر هذا المعيار بعض المؤشرات للمديرين والمراجعين التي تقيم نظام الرقابة الداخلية، ويقترح الحلول والأدوات التي يمكن أن تساعد المديرين والمراجعين لمعالجة تقييم بيئة الرقابة، وتوصلت الدراسة إلى أن معيار COBIT يمكن الشركات من تطبيق نظام الرقابة الداخلية الذي يسمح بالتغلب على قيود لجنة المنظمات الراعية، ويسمح هذا الإطار أيضاً بمعالجة احتياجات الشركة ويؤثر في المقام الأول على إدارة الموارد والهيكل التنظيمي بشكل عام والفصل بين الواجبات والتركيز على التحسين المستمر والاتصال.

وهدفت دراسة (Al- Dmour, 2018) إلى التحقق من صحة أثر تنفيذ إطار عمل خدمة الثقة في النظم (مبادئ ومعايير) كوسيلة للرقابة الداخلية لضمان موثوقية نظام المعلومات المحاسبي، وقد توصلت الدراسة إلى ضرورة استغلال البنية التحتية لتكنولوجيا المعلومات لمزيد من التنبؤ والتكيف والتكامل مع التطبيقات الاستثمارية للشركات، الحاجة إلى تعميق فهم موثوقية معايير نظم المعلومات المحاسبية بين موظفي هذه الشركات من خلال إعداد وتنفيذ برامج التدريب المتخصصة.

كما هدفت دراسة (Nicho, 2018) إلى التحقق من تطبيق عملية حوكمة أمن المعلومات من خلال نموذج يعرف باسم دورة خطة تنفيذ المهام Plan-do-check-act واختصاره (PDCA)، وقد توصلت الدراسة إلى أن التركيز على تنفيذ نموذج حوكمة أمن المعلومات يعمل على تعيين NIST / ISO 27k يعمل على التحكم في عناصر تحكم تكنولوجيا المعلومات ذات الصلة المحددة من أطر عمل حوكمة أمن المعلومات، أهمية آلية التغذية العكسية باستخدام القياسات المناسبة، أهمية غرس أمن تكنولوجيا المعلومات وأيضاً ثقافة حوكمة تكنولوجيا المعلومات في أي منظمة قبل وأثناء عملية حوكمة أمن المعلومات، كما وفرت هذه الدراسة أفضل الإرشادات التي يجب مراعاتها في كل مرحلة.

بينما هدفت دراسة (Yassine & Abdelkebir, 2019) إلى استكشاف ممارسات المنظمات المشاركة في استراتيجية إدارة أمن المعلومات، وقد توصلت الدراسة إلى أن اقتراح إطار لقياس مدى نضج أمن المعلومات بهدف توفير أداة لعملية قياس وتحسين الحكم، تم تنفيذ إطار عمل في مؤسسة متوسطة لدفع وتحسين نضج حوكمة أمن المعلومات وكانت النتائج مرضية وأثبتت أن النموذج سيكون قادراً على تقديم دعم كبير للمنظمات بأحجام مختلفة ومختلف قطاعات النشاط، استخدام إجراءات وتقنيات مطورة ذات منهجية لإدارة أمن المعلومات يساعد في توفير بيئة آمنة تماماً وذلك من خلال تنفيذ المنظمات لحوكمة أمن المعلومات، أن هناك علاقة وثيقة بين إدارة المخاطر وإدارة أمن المعلومات والامتثال لها أهمية بالغة لتحقيق الأهداف.

المحور الثاني: دراسات تناولت تحليل العلاقة بين حوكمة أمن المعلومات وخدمات تأكيد الثقة على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية:

هدفت دراسة (عبد السميع، ٢٠١٦) إلى تحقيق عدة محاور أساسية متمثلة في بيان المخاطر التي تواجه نظم المعلومات المحاسبية في ظل التشغيل الإلكتروني، والتعرف على أهمية تنفيذ آليات حوكمة تكنولوجيا المعلومات لما لها من أهمية كبيرة في التعظيم من القيمة المتوقعة للاستخدام والاستثمار في تكنولوجيا المعلومات، بالإضافة إلى تقديم مقترح لتحقيق التكامل بين حوكمة تكنولوجيا المعلومات ومبادئ الثقة للوصول لنظم معلومات محاسبية أكثر فعالية وكفاءة، وقد توصلت الدراسة إلى أن بنوك القطاع العام التجارية هي الأكثر تنفيذاً لإجراءات مبادئ الثقة بينما تتساوى البنوك التجارية العامة والخاصة في تطبيقها لإجراءات توافر النظام، والبنوك التجارية الخاصة هي الأكثر تنفيذاً لإجراءات حوكمة تكنولوجيا المعلومات، وتطبيق مبادئ خدمات الثقة يؤثر بشكل إيجابي على زيادة فعالية نظم المعلومات المحاسبية، وتطبيق إجراءات مبادئ خدمات الثقة وحوكمة تكنولوجيا المعلومات مجتمعين يؤثر بشكل إيجابي على زيادة فعالية نظم المعلومات المحاسبية.

كما هدفت دراسة (Hossin & Ayedh, 2016) إلى التعرف على طبيعة المخاطر التي تهدد سرية نظم المعلومات ومعدلات تكرارها، تحديد أسباب المخاطر المختلفة التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في البنوك، تحديد الأساليب الوقائية التي تعتمد عليها البنوك للحد من هذه المخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية، وتوصلت الدراسة إلى أن المخاطر التي تحدث في البنوك الإلكترونية تحدث بسبب قلة خبرة ووعي موظفي البنك، عدم توافر تدابير وإجراءات وأساليب حماية كافية لمواجهة المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية في البنوك.

ولقد هدفت دراسة (Al- Sharairi, et al., 2018) إلى تحديد أثر مخاطر مدخلات نظم المعلومات المحاسبية على الرقابة المحاسبية، والرقابة الإدارية، والرقابة الداخلية في البنوك التجارية في الأردن، وقد توصلت الدراسة إلى النتائج الآتية: تأثير مخاطر نظم المعلومات المحاسبية الإلكترونية على الرقابة الإدارية والمتمثلة في: الإزديولوجية في إدخال البيانات المحاسبية تؤثر على القرارات الإدارية، التلاعب في مدخلات النظام المحاسبي يؤثر على توثيق العمليات المنفذة من قبل البنك للملاء وبالتالي قد تؤدي إلى فقدان حقوقهم، الاستخدام غير المصرح به للنظام المحاسبي يؤثر على وسائل تحقيق السيطرة الفعالة على أصول البنك.

كما هدفت دراسة (Al-Fatlawi, et., 2021) إلى استكشاف دور تطبيق حوكمة تكنولوجيا المعلومات باستخدام إطار عمل COBIT5 في تحسين أمن أنظمة المعلومات المحاسبية، بالإضافة إلى تقييم مستوى حوكمة تكنولوجيا المعلومات في مصرف التجارة العراقي TBI من خلال عمليات COBIT5 بما في ذلك أربعة أبعاد (التخطيط والتنظيم، والاستخاوذ والتنفيذ، الدعم والتسليم، المراقبة) من خلال دراسة حالة أجريت

في مصرف التجارة العراقي، وقد توصلت الدراسة إلى أن تطبيق آليات حوكمة تكنولوجيا المعلومات COBIT5 يقلل من مخاطر معالجة البيانات ويحسن أمن أنظمة المعلومات المحاسبية الآلية، كما توصلت الدراسة إلى أن بنك التجارة العراقي يمكنه تنفيذ إطار عمل COBIT5، بالإضافة إلى أن النظام المحاسبي المستخدم في البنك يحتوي على جميع ميزات حوكمة تكنولوجيا المعلومات التي تضمن من ناحية سرية معلومات العملاء، ومن ناحية أخرى تمنع النظام من الاختراق.

تقييم عام للدراسات السابقة:

في ضوء التحليل السابق للدراسات السابقة اتضح للباحثة ما يلي:

- ١- ركزت الدراسات على بيان أهمية تطبيق حوكمة أمن المعلومات ومدى تأثيرها على كفاءة وفعالية استراتيجية أمن المعلومات وسياسات الأمن.
- ٢- معظم الدراسات وإن لم يكن جميعها ركزت على مدى الحاجة الماسة إلى وجود خدمات جديدة تساهم في تقييم الضوابط ذات الصلة بالأمن، والتوافر، وتكامل، وسلامة التشغيل، وسرية وخصوصية المعلومات التي تتم معالجتها من قبل النظام المحاسبي الإلكتروني، وتعرف بإسم خدمات تأكيد الثقة في النظم الإلكترونية.
- ٣- هناك ندرة في الدراسات التي تناولت COBIT5 ودوره في دعم الرقابة على تكنولوجيا المعلومات وإدارة المخاطر الناتجة عن نظم المعلومات المحاسبية الإلكترونية- في حدود علم الباحثة- ولذا فهذا البحث يتناول معيار COBIT5 كإطار للحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.
- ٤- قلة الدراسات التي تناولت تكامل العلاقة بين حوكمة أمن المعلومات وخدمات تأكيد الثقة.
- ٥- اتفقت الدراسات على أهمية نظم المعلومات المحاسبية الإلكترونية ومدى الحاجة إليها، إلا أنها لم تلتق الاهتمام الكافي حتى الآن، وخاصة ما يتعلق بحاجة إلى منهج متكامل لإدارة أمن المعلومات من خلال تقييم التكنولوجيا المستخدمة، وتقييم سلوكيات الأفراد، والاهتمام بالجوانب التنظيمية، وهو ما يمثل أحد أهم أبعاد المشكلة.
- ٦- ظهرت الحاجة الماسة إلى وجود إطار تكاملي مقترح بين حوكمة أمن المعلومات وخدمات تأكيد الثقة كمنطلق للحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.

(٣) الإطار الفكري لنظم المعلومات المحاسبية الإلكترونية ومخاطرها:

(١/٣) نظم المعلومات المحاسبية الإلكترونية (نظرة عامة):

لقد تعددت التعريفات الخاصة بنظم المعلومات المحاسبية الإلكترونية. وقد عرفها (Kaluvarachchi, 2015) على أنها "أداة تجمع بين أنظمة المعلومات والتكنولوجيا وقد تم تصميمه لمساعدة الإدارة في السيطرة على المجال الاقتصادي والمالي للمنشأة". وأيضاً عرفتها دراسة (الزغبى، ٢٠١٢) بأنها "مجموعة من الأجزاء المتكاملة والمتربطية التي صممت ونظمت لمعالجة البيانات المحاسبية إلكترونياً من خلال قبول وتخزين بيانات المدخلات، ثم تشغيلها وإنتاج نتائج المخرجات وفقاً لتوجيهات برنامج يشتمل على تعليمات تفصيلية خطوة بخطوة لما يجب عمله لتحقيق الهدف من التشغيل".

- كما يتمتع نظام المعلومات المحاسبي الإلكتروني بعدة مواصفات أهمها ما يلي (أبو مهادي، ٢٠١٧):
- إنتاج معلومات موجهة نحو إجراءات محددة ومعلومات متعلقة بالمستقبل وليس الماضي فقط، بالإضافة إلى المعلومات التقليدية.
 - تسجيل الأحداث الاقتصادية فور حدوثها وإنتاج معلومات محاسبية حديثة تعكس الواقع الاقتصادي في لحظة إصدارها، كما يقوم بإنتاج المعلومات الدورية.
 - قدرته على القيام بالدمج (Integration) بين نظام المعلومات المحاسبية وبقية أجزاء نظام المعلومات الإداري لأن اتخاذ القرارات لا تتم بالاعتماد على نظام المعلومات المحاسبي وحده، كما أن قسماً كبيراً من البيانات المحاسبية ينتج ضمن بقية أنظمة المعلومات الموجودة في إطار الشركة.
 - البرامج المستخدمة سهلة لذلك يمكن استخدامها من قبل أقسام الحسابات والأقسام المالية والمراجعين وبقية الإدارات ولا تقتصر على المبرمجين والمختصين بعلم الحاسوب.
 - يضمن الحاسوب تخزين صحيح للبيانات المحاسبية وتسجيلها بما يتناسب مع المبادئ والقواعد المحاسبية ويمنع إلى حد ما حالات الغش والتلاعب والخطأ المقصود وغير المقصود.
 - يوجد العديد من البرامج مما يتيح فرصة الاختيار والمفاضلة بينها حسب الحاجة.
- (٢/٣) المخاطر والتحديات التي تواجه نظم المعلومات المحاسبية الإلكترونية:

تتمثل أهم المخاطر والتحديات التي يتعرض لها نظم المعلومات المحاسبية الإلكترونية فيما يلي:
فقد عرض أحد الكتاب (Romney & Steinbart, 2015) مجموعة من المخاطر التي تهدد نظم المعلومات:

- ١- الكوارث الطبيعية والسياسية.
 - ٢- تصرفات بشرية مقصودة.
 - ٣- تصرفات بشرية غير مقصودة.
 - ٤- أخطاء في البرامج والأجهزة.
- كما أوضحت دراسة قام بها المجتمع الأمريكي للمراجعين الداخليين مع المجتمع الأيرلندي لتكنولوجيا المعلومات مجموعة من المخاطر التي تواجه نظم المعلومات المحاسبية الإلكترونية والمرتبطة بتكنولوجيا المعلومات كما يلي (Pickett, K.H. Spencer, 2010):
- ١- مخاطر تلف وتدمير الأجهزة.
 - ٢- مخاطر تدمير الوسائط المخزنة.
 - ٣- مخاطر تلف أو فقد البرامج.
 - ٤- مخاطر اختراق النظام.
 - ٥- مخاطر الإصابة بفيروسات.
 - ٦- مخاطر السهو والخطأ.
 - ٧- مخاطر أخطاء المستخدمين.

- في حين أن التطورات المتلاحقة في تكنولوجيا المعلومات أثرت على جودة نظم المعلومات المحاسبية الإلكترونية، كما أدت إلى زيادة فرص ارتكاب الجرائم المرتبطة بالحاسب وصعوبة تتبعها واكتشافها وذلك نتيجة ما يلي:
- ١- عدم وجود ضوابط وإجراءات حماية كافية في الشركات التي تقوم بالاتصال بالشبكة العالمية وأيضاً عدم تطبيق معايير ومبادئ حوكمة أمن المعلومات وخدمات تأكيد الثقة في النظم الإلكترونية يضمن تخفيض المخاطر أو الحد منها.
 - ٢- عدم اتباع منهج متكامل لإدارة أمن نظم المعلومات يقوم على تقييم التكنولوجيا المستخدمة لتحقيق الموازنة بين المخاطر والعائد من استخدام تكنولوجيا المعلومات.
 - ٣- عدم وجود تشريعات قانونية تلزم الشركات بتطبيق الأهداف والمبادئ الخاصة بحوكمة أمن المعلومات وتضمينها داخل استراتيجيتها المستقبلية.
- ومن التحديات المتعلقة بنظم المعلومات المحاسبية الإلكترونية والتي تتمثل في الآتي
(عبد السميع، ٢٠١٦):

حيث أشارت الدراسة التي أعدت من قبل لجنة تكنولوجيا المعلومات التابعة لـ IFAC في ٢٠٠٢ وكانت بعنوان E-Business and The accountant إلى أن مخاطر بيئة تكنولوجيا المعلومات تشمل:

(أ) مخاطر البنية التحتية المتعلقة بتكنولوجيا المعلومات وتتمثل في الآتي:

- ١- عدم كفاية التشفير للبيانات والمعلومات Inadequate encryption.
- ٢- عدم ملاءمة إجراءات منع السرقة والوصول غير المشروع للمعلومات.
- ٣- غياب أو عدم سلامة إجراءات الدعم والمساندة.
- ٤- مواجهة المخاطر المادية كالحرائق.
- ٥- غياب إجراءات النسخ الاحتياطي Backups.

(ب) مخاطر متعلقة بتطبيقات تكنولوجيا المعلومات وتشمل:

- ١- عدم كفاية إجراءات تأمين البرمجيات المتصلة بأمن البنية التحتية لتكنولوجيا المعلومات.
- ٢- عدم كفاية ضوابط الإدخال واستخراج البيانات.
- ٣- الخلل أو الأخطاء في تطبيقات تكنولوجيا المعلومات.
- ٤- التغيرات الغير مصرح بها في البرامج المستخدمة.

(ج) مخاطر تتعلق بالتجارة الإلكترونية:

أدى التطور الهائل والسريع في نظم الاتصالات وتكنولوجيا المعلومات إلى ارتباط التجارة الإلكترونية باستخدام وسائل دفع إلكترونية مما أدى إلى الحاجة لوجود نظام معلومات محاسبي آمن، ومتاح، ومرن لكافة أطراف التعامل التجاري.

فيذكر معهد المحاسبين القانونيين الأمريكي على موقعه عبر الإنترنت، أن بعض الدراسات بينت أن الخسائر التي تكبدها المؤسسة الأمريكية في عام ١٩٩٩ من اختراقات لبطاقات الائتمان فقد بلغت أربعمائة مليون دولار ويتوقع أن ترتفع سنوياً إلى مبلغ ستين بليون دولار بحلول عام ٢٠٠٥، ومن هذه الحقيقة يشير المعهد إلى مدى الحاجة لإنشاء آلية حماية على الشبكة، فترجع مخاطر التجارة الإلكترونية إلى الأسباب الآتية (Hussain, 2013), (Al-Refaee, 2012):

- ١- الهجمات المتعمدة **Intentional Attacks**: وتحدث بواسطة قرصنة الإنترنت أو منافسي الشركة بهدف الوصول إلى المعلومات السرية للشركة، كأرقام بطاقات اعتماد العملاء مثلاً، والمعلومات السرية المتعلقة بالعملاء، وحجم المبيعات، وأمور كثيرة قد يصعب حصرها.
- ٢- خصوصية التعامل **The Privacy Debate**: تعد التعاملات الإلكترونية التي تتم بين الأفراد والشركة ذات طابع معلوماتي مهم جداً، وذلك لأنها تحفظ على ذاكرة النظام الرقمية، وهي معلومات قيمة جداً، فإن تمكن أحد من معرفتها أو حتى تتبعها: مثل تتبع رقم بطاقة اعتماد العميل. ومن هنا يستشعر العميل بأن خصوصيته قد تم اختراقها وبالتالي سيفقد الثقة بالشركة التي تعامل معها من منطلق أنها لم تتمكن من حماية خصوصيته.
- ٣- فقدان الثقة **Loss of Trust** (عبد الكريم، ٢٠١٠)، يقصد بها فقدان ثقة الشركة بمعلومات عميلها، فمن المتعارف عليه أن العميل يستخدم ما يسمى التوقيع الرقمي **Digital Signature** الخاص به لدخول نظام الشركة وذلك لإتمام عملياته المرغوب فيها، فكيف إذا تمكن الشخص غير الصحيح بالدخول مستخدماً توقيع العميل.
- ٤- فشل عملية التحويل **Transmission Failure**، على الرغم أن عملية الشراء الإلكترونية تتم بسرعة كبيرة جداً، إلا أنها عرضة لخطر فشل عملية التحويل، فمن المتعارف عليه أن عملية الشراء عبر التجارة الإلكترونية تتم من خلال عدة خطوات، فيبدأ المستهلك بملء النموذج الابتدائي وخطوات أخرى قد تكون ضرورية وفقاً لسياسات الشركة، ففي كل مرحلة تفتح صفحة جديدة عبر موقع الشركة ولأسباب تقنية أو أخرى، قد تقبل إحدى الخطوات، وهنا ستظهر مشكلة جديدة وهي عدم التأكد من إتمام العملية.
- ٥- غياب التوثيق **Lack of Authentication**، يتم في التجارة التقليدية عادة توثيق الصفقة بأوراق ثبوتية مرسومة بشعار الشركة وموقعة من قبل الشخص المناسب، وبواسطة اتصال شخصي ومباشر بين البائع والمشتري، ولكن تعد جميع تلك الأمور في التجارة الإلكترونية شبه مفقودة بالكامل، وهذه الحقيقة تزيد من احتمالية التعامل مع الشخص غير الصحيح.
- ٦- سرقة الهوية **Theft of Identity**، مع غياب التوثيق المناسب كما في التجارة التقليدية أصبح من السهل على المجرمين انتحال شخصية الغير والقيام بالعمليات دون علمه.

٧- تروير الحقائق Window Dressing، سوف تكون خدمات بعض مسوقي ومزودي خدمات الحماية، خدمات تجميلية فقط في غياب آلية معينة تؤكد مصداقيتهم وفاعلية خدماتهم.

٨- آثار ضغوط الاقتصاد Effects of Economic Pressures، أدى النمو المتسارع للتجارة الإلكترونية، إلى أن أصبح سوقها سوقاً تنافسياً، كما أصبحت قوة المتنافس الحقيقية تكمن في نجاح آليات الأمان والتوكيدية والموثوقية المتعلقة بنظامه المحاسبي، فكل من يستطيع توفير هذه الآليات يكون نصيبه أكبر في هذا السوق التكنولوجي العالمي.

فالخطر من العناصر الملازمة لكافة أنشطة الشركة فمن الممكن للأفراد أن يرتكبوا الأخطاء، بينما الآلات يمكن أن تتعرض للعديد من أشكال القصور والأعطال والأفراد المتلاعبون يمكن أن يستغلوا الثغرات الأمنية للقيام بأعمال غير نظامية مقصودة (الساكني، ٢٠١٢).

وتعرف الثغرات الأمنية Vulnerability بأنها نقاط الضعف في النظام كعدم وجود برنامج مضاد للفيروسات أو عدم وجود إجراءات لإنهاء خدمات موظف. (Mukhanova, 2014)

د) مخاطر متعلقة بالإختراقات التي تتم عبر شبكة الإنترنت:

- وترجع أسباب صعوبة تعقب الاختراقات التي تتم عبر شبكة الإنترنت والتي تتمثل في النقاط الآتية:
- ١- سرعة العملية، قد لا يحتاج الدخيل (المخترق) إلى أكثر من بعض دقائق لاخترق موقع معين والتلاعب به ومغادرة الموقع قبل أن يتم تعقبه.
 - ٢- عدم وجود هوية محددة، لا يمكن معرفة ماهية المخترق، ولا بأي شكل من الأشكال.
 - ٣- تباعد المسافات، قد يكون المخترق لموقع ما يبعد آلاف الكيلومترات وفي بلد آخر، فشبكة الإنترنت صممت بشكل عالمي.
 - ٤- إمكانية الدخول من عدة أماكن، فالمعامل عبر الإنترنت لا يحتاج إلى مكان محدد لدخول الشبكة، فأى شخص يمكنه الدخول إلى الشبكة من أي مكان يوجد فيه جهاز كمبيوتر وخط اتصال، مثل مقاهي الإنترنت ومختبرات الجامعات والمدارس.
 - ٥- عدم وجود قوانين دولية، فشبكة الإنترنت شبكة عالمية ذات معايير موحدة للاستخدام فقط ولو أننا افترضنا اكتشاف أحد المخترقين بدولة مغايرة لدولة الشركة التي تم اختراقها، فإنه ليس من الضرورة وجود قوانين موحدة للتعامل مع المخترق.
 - ٦- إمكانية إتلاف بيانات جهاز الكمبيوتر في حالة شعور أي مخترق بإمكانية تعقبه تستطيع إتلاف جهازه بضغطة زر بسيطة، مما يجعل عملية تعقبه عديمة الجدوى والفائدة.

ما سبق يمكن للباحثة استنتاج ما يلي:

١- جاءت التحديات والمشاكل الخاصة بالنظم الإلكترونية نتيجة الممارسات المتبعة في نظم المعلومات المحاسبية الإلكترونية، والتي اختلفت نتيجة غياب الإرشادات والضوابط الرقابية والمعايير التي تعمل على التنظيم والتحكم في تلك الممارسات.

٢- ترجع هذه التحديات والمشاكل إلى طبيعة الخصائص التكنولوجية التي تتميز بها شبكة الإنترنت فهي شبكة عالمية والتي يمكن التغلب عليها من خلال استخدام الوسائل التكنولوجية الرقابية المناسبة.

٣- تؤثر هذه التحديات والمشاكل في مدى الثقة في هذه النظم بالإضافة إلى المصدقية في مخرجات تلك النظم.

(٣/٣) مدى حاجة بيئة الأعمال الحديثة لإجراءات وقائية لنظم المعلومات المحاسبية الإلكترونية:

مع ظهور البيئة المستخدمة للحسابات الإلكترونية يواجه مراجع الحسابات الداخلي مشاكل عديدة تتطلب منه ضرورة التغلب عليها حتى يتمكن من إنجاز متطلباته المهنية، فمن أمثلة هذه المشاكل عدم وجود مستندات المدخلات، عدم وجود مسار مرئي للمعاملات التجارية، عدم وجود مخرجات مرئية وواضحة. فبمرور الوقت تصبح الشركات مهتمة بكفاءتها التشغيلية سواء في الإنتاج أو في الإدارة، ومن أجل زيادة الكفاءة في كثير من أوجه النشاط، تحتاج الشركات إلى إدخال تقنية حديثة أو تطوير التقنية المستخدمة (الدهراوي، ٢٠١٠). فإن عدم وجود ضوابط وإجراءات ملائمة تتيح فرص التلاعب والتخريب في نظم المعلومات المحاسبية الإلكترونية بواسطة أشخاص غير مسئولين من داخل أو خارج الشركة.

فقد تناولت عدة دراسات مجال إدارة المخاطر وقدمت مفاهيم عديدة لها وتعريفات تتمحور حول كونها مجموعة من الإجراءات والعمليات التي تقوم بها الشركة من خلال مجلس الإدارة ولجنة المراجعة والعاملين بالشركة ولتحديد ودراسة الأهداف، ومن ثم دراسة وتقييم الأحداث التي تؤثر على تلك الأهداف، ومعرفة ما إذا كانت تمثل تهديداً للشركة أو فرصة أي أن الحدث إيجابي أم سلبي، ومن ثم تقييم هذه المخاطر وتصميم وتنفيذ الأنشطة الرقابية المناسبة لمواجهةها بل قد تصل عملية إدارة المخاطر إلى المواجهة الرقابية للمخاطر وإلى مراقبة وتقييم الأنشطة الرقابية والتقرير عن فاعليتها كتغذية عكسية للقائمين والعاملين على تنفيذ إدارة المخاطر وهذا لضمان تحقيق أهداف الشركة في ظل أدنى تهديد ممكن للمخاطر (عقل، ٢٠١٥).

(٤) الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية باستخدام التكامل المقترح

بين حوكمة أمن المعلومات وخدمات تأكيد الثقة:

(١/٤) ماهية حوكمة أمن المعلومات:

تعرف حوكمة أمن المعلومات بأنها "عملية إنشاء والفاظ على إطار ودعم هيكل الإدارة لتحقيق أهدافها، وضمان توافق استراتيجيات أمن المعلومات مع أهداف العمل ودعمها، بما يتماشى مع القوانين واللوائح من خلال الالتزام بالسياسات والضوابط الداخلية، وتوفير إنشاء المسؤولية للإدارة، وكل هذا لمحاولة إدارة المخاطر (Bedeau et al., 2010).

كما تعرف على أنها " تعمل على إنشاء وصيانة بيئة التحكم لإدارة المخاطر المتعلقة بسرية المعلومات وتكاملها وتوافرها، كما أنها تدعم العملية والأنظمة التي لا تشكل جزءاً من المراجعة والتدقيق (ضمان أن عملية الحوكمة قد تم تأسيسها بشكل صحيح وتعمل) والتشغيل الآمن وتطوير الأمن (هندسة تكنولوجيا المعلومات أو سير العملية لتحقيق الأهداف الأمنية)". (Fazlida& Said, 2015)

فقد أشارت إحدى الدراسات (Abu-Musa, 2010) أن حوكمة أمن المعلومات تهدف إلى إنشاء وصيانة بيئة رقابية مناسبة وملاءمة للحفاظ على سرية وسلامة ونزاهة وتوافر المعلومات، ودعم العمليات والنظم الخاصة بها، وأيضاً حماية المعلومات من مختلف المخاطر التي يمكن أن تتعرض لها، وعلاوة على ما سبق فإن حوكمة أمن المعلومات تؤدي إلى إضافة قيمة للشركة عن طريق:

- ١- تحسين الثقة في التعاملات مع العملاء،
- ٢- حماية سمعة الشركة،
- ٣- تقليل احتمال انتهاكات الخصوصية
- ٤- توفير قدر كبير من الثقة عند التعامل مع الأطراف الخارجية،
- ٥- إيجاد وتوفير طرق جديدة وأفضل لمعالجة المعاملات الإلكترونية،
- ٦- تقليل التكاليف التشغيلية من خلال توفير نتائج يمكن التنبؤ بها،
- ٧- التقليل من عوامل الخطر التي قد تؤدي إلى إيقاف العمليات. (ITGI, 2006)

(٢/٤) مدخل مفاهيمي لخدمات تأكيد الثقة

تعد خدمات التأكيد من المفاهيم الحديثة نسبياً، فقد بدأ مفهومها في الظهور مع بداية ثمانينات القرن الماضي، ولكن الاهتمام المتزايد به لم يبدأ إلا مع بداية القرن الحالي، وفيما يلي عرض لبعض التعاريف الخاصة بخدمات التأكيد وذلك لبيان المقصود منها وما اشتملت عليه لتحديد طبيعة خدمات التأكيد. فقد عرفها (Arens, et al., 2012) على أنها "خدمات مهنية مستقلة تعمل على تحسين جودة المعلومات لمتخذي القرارات، حيث تعتبر تلك الخدمات ذات قيمة حيث أنها مستقلة وتعبّر عن رأي في غير متحيز للقائمين بالخدمة، نظراً لاعتماد متخذي القرارات عليها للحصول على المعلومات الكافية والملاءمة لاتخاذ قراراتهم" (Arnes& Elderand, 2012).

كما أن هناك عدة عوامل من الممكن أن تعكس مدى أهمية خدمات التأكيد، وهي على النحو التالي (حسين، ٢٠١٣):

- ١- تساعد خدمات التأكيد متخذي القرار في الحد من حالات عدم التأكيد المرتبطة باتخاذ القرارات المختلفة.
- ٢- تقدم معلومات كافية وشاملة، بصورة تحد من مخاطر القرار الخاطئ.
- ٣- تؤدي إلى الحد من فجوة التوقع في التدقيق.

- ٤- تتيح للشركة فرص للحصول على رأس مال بتكلفة أقل نتيجة للحد من حالات عدم التأكد المتعلقة بجوانب الأداء.
- ٥- تساعد الشركة في تطوير طرق استخدام نظم المعلومات الإلكترونية، وتحقيق رقابة أفضل على تلك النظم.
- ٦- تحد من الخصائص السلبية للمعلومات كالتحيز، وتعارض المصالح، وعدم تماثل المعلومات بين المستخدمين.
- ٧- تساهم في التغلب على المشاكل التي تتعرض لها خدمات التدقيق التقليدي.

وقد أسس معهد المحاسبين القانونيين الأمريكي (AICPA) (حسن، ٢٠١٠)، وبالتعاون مع معهد المحاسبين القانونيين الكندي (CICA) مشروعاً مشتركاً في مطلع عام ١٩٩٧م فقد قام المعهدان بتشكيل فريق عمل حددت مهامه الأولية باستقصاء حاجة السوق لخدمات التأكد، وبناءً على نتائج اللجنة قام المعهدان ومن خلال المشروع المشترك بينهما باستحداث خدمتين تأكيد مهيتين جديدتين تتعلقان بعمليات التجارة الإلكترونية وهما كالتالي:

أ) خدمة الثقة في النظام System Trust:

خدمة التأكد على الثقة في النظم خدمة مهنية تصديقية تقدم تأكيد إيجابي بشأن اختبار مدى صدق النظام وأمنه لخدمة المسؤولين عن النظم ومستخدمي مخرجاتها (عبد اللطيف، ٢٠٠٨)، فهي خدمة يقدمها مدقق الحسابات لتوفير مستوى معقول من التأكيد بأن الإدارة اتخذت خطوات لمعالجة موثوقية النظام، وتنفيذ مجموعة متوازنة من الضوابط (نبيل، ٢٠١٢)، ولتأكيد إمكانية الاعتماد على النظام يجب توفير خمسة مبادئ كما حددها المعهد الأمريكي للمحاسبين القانونيين (AICPA) وهي: الحماية، وجاهزية النظام، وتكامل المعالجة، والسرية، والخصوصية على الشبكة (AICPA, 2015).

ب) خدمة الثقة في مواقع الويب Web Trust:

وهي عملية منظمة لتجميع وتقييم الأدلة الخاصة بمزاعم الإدارة بشأن موقع الشركة على الإنترنت، لاختيار مدى ملاءمة هذه المزاعم مع معايير الثقة في الموقع، وتوصيل النتائج إلى أصحاب المصلحة في الموقع، وبصفة خاصة الإدارة وزائري الموقع نفسه (مدني، ٢٠١٥).

٣/٤) التكامل المقترح بين حوكمة أمن المعلومات وخدمات تأكيد الثقة للحد من

مخاطر نظم المعلومات المحاسبية الإلكترونية:

في ظل عصر تكنولوجيا المعلومات تعاضد دور المعلومات المالية والمحاسبية، حيث أصبحت من المدخلات الإستراتيجية للشركة والتي على أساسها تتخذ العديد من القرارات الإستراتيجية للشركة، ولذا يجب أن تكون المعلومات اقتصادية وذات جودة عالية لكي تؤدي هذه المعلومات الدور الاقتصادي المنوط بها، وهذا لن يحدث إلا بتوفر نظام معلومات محاسبي فعال ومتطور يخلو من أية مخاطر.

ولذلك تسعى الشركات إلى استحداث وتطوير معايير وأطر ومبادئ للرفع من كفاءة وجودة نظم المعلومات المحاسبية الإلكترونية ومواجهة المخاطر والتهديدات التي تتعرض لها تلك النظم، بالإضافة إلى محاولة مواكبة التغيرات والتطورات التكنولوجية المتجددة وتحديثات أمن المعلومات فقد عدلت American Institution of Certified Public Accountants (AICPA) على مبادئ خدمات الثقة (TSP Section 100) وهي مبادئ تهدف إلى زيادة فعالية وموثوقية نظم المعلومات من خلال تطبيق مجموعة من المعايير تجعل نظام المعلومات يتمتع بالأمن Security، السرية confidentiality، جاهزية النظام Availability، تكامل المعالجة Processing Integrity والخصوصية من خلال مبادئها المقبولة قبولاً عاماً (GAPP) Generally Accepted كما يسعى معيار حوكمة أمن المعلومات Cobit5 إلى تحقيق مجموعة من الأهداف لتحقيق جودة المعلومات وهي (الأهداف الجوهرية Intrinsic، وأهداف الجودة السياقية Contextual بالإضافة إلى أهداف أمن المعلومات (Information Security)).

ولقد تبين للباحثة من خلال ما سبق أن حوكمة أمن المعلومات تشكل الجانب الاستراتيجي أي الجانب الشامل لكيفية التعامل مع التقنية بالشركة بدءاً من تحديد الاحتياجات، التخطيط وتخصيص الموارد مروراً بالتطبيق والحيازة حتى الرقابة والصيانة وضمن الاستمرارية. بينما خدمات تأكيد الثقة ومبادئها فهي تمثل الشق التشغيلي أي الجانب التطبيقي لنظام المعلومات وكيفية تأمينه والحصول على قدر عال من الكفاءة والفعالية من أداءه وبالتالي القدرة على مواجهة المخاطر والتحديات التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية.

وانطلاقاً من النتائج التي تم التوصل إليها في الدراسات السابقة، تقوم الباحثة في هذه الدراسة باختبار مدى إمكانية التكامل المقترح بين حوكمة أمن المعلومات وخدمات تأكيد الثقة في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية، ولتحقيق ذلك تقوم الباحثة باختبار الفروض التالية:

- الفرض الأول: يؤدي عدم وجود إجراءات حماية كافية إلى زيادة المخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية.
- الفرض الثاني: يؤدي تطبيق معايير حوكمة أمن المعلومات إلى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.
- الفرض الثالث: يؤدي تطبيق المبادئ الخمسة لخدمات تأكيد الثقة إلى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.
- الفرض الرابع: يساهم التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.

(٥) الدراسة الميدانية:

تتمثل مقومات الدراسة الميدانية لاختبار فروض البحث فيما يلي:

(١/٥) هدف الدراسة:

- يتمثل الهدف العام للدراسة الميدانية في التعرف على آراء ومدى قبول عينة الدراسة لفكرة أثر تكامل حوكمة أمن المعلومات وخدمات تأكيد الثقة على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية، ويشق من هذا الهدف مجموعة من الأهداف الفرعية تتمثل فيما يلي:
- ١- التعرف على أنواع مخاطر نظم المعلومات المحاسبية الإلكترونية وأسبابها.
 - ٢- التعرف على أهمية حوكمة أمن المعلومات ودورها في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.
 - ٣- تحديد مدى أهمية خدمات تأكيد الثقة ودورها في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.
 - ٤- اختبار مدى إمكانية التكامل المقترح بين حوكمة أمن المعلومات وخدمات تأكيد الثقة في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.

(٢/٥) مجتمع وعينة الدراسة:

يتمثل مجتمع الدراسة في (أعضاء هيئة التدريس في أقسام المحاسبة بكليات التجارة بالجامعات المصرية، شركات المساهمة المسجلة في البورصة المصرية، المحاسبون والمراجعون ومسؤولي وحدات تكنولوجيا المعلومات بالبنوك المسجلة في البورصة المصرية)، وقامت الباحثة باختيار عينة مبنية قوامها ٥٢ مفردة من أعضاء هيئة التدريس تخصص المحاسبة والمراجعة ببعض كليات التجارة بالجامعات المصرية ما بين أستاذ وأستاذ مساعد ومدرس ومدرس مساعد ومعيد، ويوضح الجدول التالي بيان بكليات التجارة التي شملتها العينة.

جدول رقم (١) قوائم الاستقصاء المرسل والمسترده من أعضاء هيئة التدريس

قوائم الاستقصاء المستردة		قوائم الاستقصاء المرسل		الكلية / الجامعة
النسبة	العدد	النسبة	العدد	
١٨%	٨	١٩%	١٠	١- كلية التجارة - جامعة القاهرة
١٤%	٦	١٧%	٩	٢- كلية التجارة - جامعة عين شمس
٣٠%	١٣	٢٩%	١٥	٣- كلية التجارة - جامعة بنها
٢٠%	٩	١٩%	١٠	٤- كلية التجارة - جامعة طنطا
١٨%	٨	١٥%	٨	٥- كلية التجارة - جامعة الزقازيق
١٠٠%	٤٤	١٠٠%	٥٢	الإجمالي

وقامت الباحثة باختيار عينة مبدئية قوامها ٤٠ مفردة من المحاسبين والمراجعين ومسؤولي وحدات تكنولوجيا المعلومات في هذه الشركات، ويوضح الجدول التالي بيان بشركات المساهمة التي شملتها العينة.

جدول رقم (٢) قوائم الاستقصاء المرسة والمستردة من بعض شركات المساهمة المصرية

قوائم الاستقصاء الممتدة		قوائم الاستقصاء المرسة		اسم الشركة
النسبة	العدد	النسبة	العدد	
%٢٥.٧١	٩	%٢٥	١٠	١- مجموعة طلعت مصطفى القابضة (TMGH)
%٢٢.٨٦	٨	%٢٥	١٠	٢- النجاجون الشريقيون للسجاد (ORWE)
%٢٥.٧١	٩	%٢٥	١٠	٣- الشركة المصرية للاتصالات (WE)
%٢٥.٧١	٩	%٢٥	١٠	٤- فودافون مصر للاتصالات (VODE)
%١٠٠	٣٥	%١٠٠	٤٠	الإجمالي

وقامت الباحثة باختيار عينة مبدئية قوامها ٤٠ مفردة من المحاسبين والمراجعين ومسؤولي وحدات تكنولوجيا المعلومات في هذه البنوك، ويوضح الجدول التالي بيان بالبنوك التي شملتها العينة.

جدول رقم (٣) قوائم الاستقصاء المرسة والمستردة من بعض البنوك المصرية

قوائم الاستقصاء الممتدة		قوائم الاستقصاء المرسة		اسم البنك
النسبة	العدد	النسبة	العدد	
%٢٩.٠٣	٩	%٢٥	١٠	١- بنك فيصل الاسلامي المصري (FIBE)
%٢٥.٨١	٨	%٢٥	١٠	٢- بنك قطر الوطني (QNB)
%٢٢.٥٨	٧	%٢٥	١٠	٣- البنك الأهلي المصري
%٢٥.٨١	٨	%٢٥	١٠	٤- البنك التجاري الدولي (CIB)
%١٠٠	٣١	%١٠٠	٤٠	الإجمالي

(٣/٥) الأساليب الإحصائية المستخدمة في تحليل البيانات:

قامت الباحثة بتفريغ بيانات قوائم الاستقصاء الصالحة للتحليل وتحليلها واستخلاص النتائج من خلال تطبيق بعض الأساليب الإحصائية الواردة بمجموعة البرامج الإحصائية للعلوم الاجتماعية [Statistical Package for Social Science (SPSS)]^(*)، وقد تطلبت طبيعة البيانات تحديد الأساليب

الإحصائية اللازمة والملاءمة، والتي تتمثل فيما يلي:

▪ أساليب الإحصاء الوصفي:

- ١- الوسط الحسابي.
 - ٢- الانحراف المعياري.
- Mean
Standard Deviation

(*) استخدمت الباحثة برنامج SPSS الإحصائي الإصدار (٢٨) في تحليل البيانات إحصائياً.

▪ أساليب الإحصاء الاستدلالي:

Test of Normality	٣- اختبار الطبيعية
Correlation Coefficient	٤- معامل الارتباط.
Alpha Cronbach's	٥- اختبار الصلاحية والاعتمادية
R Square	٦- معامل التحديد.
Simple Regression Model	٧- نموذج الانحدار البسيط.
T Test	٨- اختبار "ت".
(Kruskal -Wallis Test)	٩- اختبار كروسكال ويلز

(٤/٥) اختبار فروض الدراسة:

ويتم اختبار فروض الدراسة من خلال اختبار الارتباط والانحدار وذلك ما يلي:

أولاً: مصفوفة الارتباط:

قامت الباحثة بإعداد مصفوفة الارتباط بين المتغير التابع (الحد من مخاطر نظم المعلومات الحاسوبية الإلكترونية) والمتغيرات المستقلة (إجراءات الحماية الكافية لنظم المعلومات الحاسوبية الإلكترونية، تطبيق معايير حوكمة أمن المعلومات، المبادئ الخمسة لخدمات تأكيد الثقة، التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة) وذلك كما يلي:

جدول (٤) مصفوفة الارتباط بين متغيرات الدراسة

المتغير التابع	المتغيرات المستقلة	وجود إجراءات حماية كافية	تطبيق معايير حوكمة أمن المعلومات	تطبيق المبادئ الخمسة لخدمات تأكيد الثقة	التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة	الحد من مخاطر نظم المعلومات الحاسوبية الإلكترونية
وجود إجراءات حماية كافية	Spearman's Correlation	١				
	Sig.	٠.٠٠٠				
تطبيق معايير حوكمة أمن المعلومات	Spearman's Correlation	٠.٦٠٣**	١			
	Sig.	٠.٠٠٠	٠.٠٠٠			
تطبيق المبادئ الخمسة لخدمات تأكيد الثقة	Spearman's Correlation	٠.٦٠١**	٠.٨٩٩**	١		
	Sig.	٠.٠٠٠	٠.٠٠٠	٠.٠٠٠		
التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة	Spearman's Correlation	٠.٥٦٣**	٠.٦٩٥**	٠.٧٦١**	١	
	Sig.	٠.٠٠٠	٠.٠٠٠	٠.٠٠٠	٠.٠٠٠	
الحد من مخاطر نظم المعلومات الحاسوبية الإلكترونية	Spearman's Correlation	٠.٦٥٥**	٠.٦٠٤**	٠.٦٠٦**	٠.٥١٨**	١
	Sig.	٠.٠٠٠	٠.٠٠٠	٠.٠٠٠	٠.٠٠٠	٠.٠٠٠

**تشير إلى معنوية معامل الارتباط عند مستوى معنوية ٠.٠١

وحيث أن إشارة معامل الارتباط (الموجبة) تشير إلى وجود علاقة ارتباط طردية (إيجابية)، وتشير قيمة معامل الارتباط إلى قوة علاقة الارتباط، يتضح للباحثة النتائج الآتية:

▪ تشير إشارة وقيمة معامل الارتباط (الموجبة) إلى وجود علاقة طردية (إيجابية) متوسطة بين كل من (إجراءات الحماية الكافية لنظم المعلومات المحاسبية الإلكترونية، تطبيق معايير حوكمة أمن المعلومات، المبادئ الخمسة لخدمات تأكيد الثقة، التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة) وبين الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية (كمتغير تابع)، وهذا يعنى أنه كلما زادت إجراءات الحماية الكافية لنظم المعلومات المحاسبية الإلكترونية وكلما تم تطبيق معايير حوكمة أمن المعلومات، المبادئ الخمسة لخدمات تأكيد الثقة كلما أدى ذلك إلى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.

▪ تؤكد دلالة معامل الارتباط (٠.٠٠٠) والتي نقل عن مستوى المعنوية (٠.٠٠١) على قبول فرض وجود علاقة ارتباط ذات دلالة إحصائية بين الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية وبين كل من:

✓ وجود إجراءات حماية كافية

✓ تطبيق معايير حوكمة أمن المعلومات

✓ تطبيق المبادئ الخمسة لخدمات تأكيد الثقة فى نظم المعلومات المحاسبية الإلكترونية

✓ التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة فى نظم المعلومات المحاسبية الإلكترونية.

وتلخص الباحثة من نتائج تحليل الارتباط لمتغيرات الدراسة إلى النتائج التالية:

▪ يؤدي عدم وجود إجراءات حماية كافية إلى زيادة المخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية، وهو ما يدعم صحة الفرض الأول للدراسة.

▪ يؤدي تطبيق معايير حوكمة أمن المعلومات إلى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية وهو ما يدعم صحة الفرض الثانى للدراسة.

▪ يؤدي تطبيق المبادئ الخمسة لخدمات تأكيد الثقة إلى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية وهو ما يدعم صحة الفرض الثالث للدراسة.

▪ يساهم التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة فى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية وهو ما يدعم صحة الفرض الرابع للدراسة.

ثانياً: تحليل الانحدار:

يوضح الجدول التالي نتائج تحليل الانحدار البسيط لمتغيرات الدراسة وذلك للوصول لنموذج كمى يحكم علاقة تأثير كل من (إجراءات الحماية الكافية لنظم المعلومات المحاسبية الإلكترونية، تطبيق معايير حوكمة أمن المعلومات، المبادئ الخمسة لخدمات تأكيد الثقة، التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة) على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية (كمتغير تابع)، وذلك كما يلي:

١- تحليل الانحدار لمتغيرات الفرض الأول:

يوضح الجدول التالي نتائج تحليل الانحدار لإجراءات الحماية الكافية لنظم المعلومات المحاسبية

الإلكترونية، على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية (كمتغير تابع)

جدول (٥) نتائج تحليل الانحدار لمتغيرات الفرض الأول

بيــــــــــــــــان	معامل الانحدار (B)	قيم اختبار (ت)	مستوى المعنوية	الدلالة الإحصائية
المقدار الثابت (B ₀)	١.٨٥٧	٥.٥٨٧	٠.٠٠٠	دال إحصائياً
(X) إجراءات الحماية الكافية لنظم المعلومات المحاسبية الإلكترونية	٠.٥٥٨	٧.٣٣٨	٠.٠٠٠	دال إحصائياً
القيمة التفسيرية للنموذج : معامل التحديد $R^2 = ٠.٣٨٢$				
المعنوية الكلية للنموذج: مستوى المعنوية لتحليل ANOVA = ٠.٠٠٠				
قيمة اختبار (Durbin-Watson) = ٢.٢٥٢				

ويتضح من الجدول السابق النتائج التالية:

- تشير إشارة معامل الانحدار (الموجبة) للمتغير المستقل إلى وجود علاقة تأثير طردية لإجراءات الحماية الكافية لنظم المعلومات المحاسبية الإلكترونية، على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية (كمتغير تابع).
- تشير قيمة معامل الانحدار للمتغير المستقل إلى أنه كلما زاد المتغير المستقل (إجراءات الحماية الكافية لنظم المعلومات المحاسبية الإلكترونية) بمقدار وحدة واحدة كلما أدى ذلك إلى زيادة في المتغير التابع (الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية) بمقدار ٠.٥٥٨ وحدة.
- تؤكد دلالة اختبار (ت) للمتغير المستقل (٠.٠٠٠) والتي تقل عن مستوى المعنوية (٠.٠٥) على قبول فرض وجود علاقة تأثير معنوية ذات دلالة إحصائية لإجراءات الحماية الكافية لنظم المعلومات المحاسبية الإلكترونية، على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية (كمتغير تابع).
- أن قيمة (D-W) المحسوبة للنموذج بلغت (٢.٢٥٢)، وهي بذلك تقع ضمن المدى المثالي وهو الذي يقترب من (١.٥ - ٢.٥) مما يدل على عدم وجود مشكلة للارتباط الذاتي بين العناصر المكونة للمتغير المستقل تؤثر على صحة النتائج.
- يمكن صياغة نموذج كمي للانحدار البسيط بين متغيرات الفرض الأول كما يلي:

$$Y = B_0 + B X$$

الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية = ١.٨٥٧ + ٠.٥٥٨ إجراءات الحماية الكافية لنظم المعلومات المحاسبية الإلكترونية

وتلخص الباحثة من نتائج تحليل الانحدار للفرض الأول إلى أنه يؤدي عدم وجود إجراءات حماية كافية إلى زيادة المخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية، وهو ما يدعم صحة الفرض الأول للدراسة، والذي يتفق مع الدراسات السابقة الآتية: (Muhrtala&Ogundeji,2013)، (زهيري، ٢٠١٥)، (Hossin&Ayedh,2016).

٢- تحليل الانحدار لمتغيرات الفرض الثاني:

يوضح الجدول التالي نتائج تحليل الانحدار لتطبيق معايير حوكمة أمن المعلومات، على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية (كمتغير تابع)

جدول (٦) نتائج تحليل الانحدار لمتغيرات الفرض الثاني

بيــــــــــــــــان	معامل الانحدار (B)	قيم اختبار (ت)	مستوى المعنوية	الدلالة الإحصائية
المقدار الثابت (B_0)	٢.٦٣٧	٧.٨٧٩	٠.٠٠٠	دال إحصائياً
(X) تطبيق معايير حوكمة أمن المعلومات	٠.٣٨٠	٤.٩٥١	٠.٠٠٠	دال إحصائياً
القيمة التفسيرية للنموذج : معامل التحديد $R^2 = ٠.٢٢٠$				
المعنوية الكلية للنموذج: مستوى المعنوية لتحليل ANOVA = ٠.٠٠٠				
قيمة اختبار (Durbin-Watson) = ١.٩٩٦				

ويتضح من الجدول السابق النتائج التالية:

- تشير إشارة معامل الانحدار (الموجبة) للمتغير المستقل إلى وجود علاقة تأثير طردية لتطبيق معايير حوكمة أمن المعلومات، على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية (كمتغير تابع).
- تشير قيمة معامل الانحدار للمتغير المستقل إلى أنه كلما زاد المتغير المستقل (تطبيق معايير حوكمة أمن المعلومات) بمقدار وحدة واحدة كلما أدى ذلك إلى زيادة في المتغير التابع (الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية) بمقدار ٠.٣٨٠ وحدة.
- تؤكد دلالة اختبار (ت) للمتغير المستقل (٠.٠٠٠) والتي تقل عن مستوى المعنوية (٠.٠٥) على قبول فرض وجود علاقة تأثير معنوية ذات دلالة إحصائية لتطبيق معايير حوكمة أمن المعلومات، على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية (كمتغير تابع).
- أن قيمة (D-W) المحسوبة للنموذج بلغت (١.٩٩٦)، وهي بذلك تقع ضمن المدى المثالي وهو الذي يقترب من ٢، مما يدل على عدم وجود مشكلة للارتباط الذاتي بين العناصر المكونة للمتغير المستقل تؤثر على صحة النتائج.
- يمكن صياغة نموذج كمي للانحدار البسيط بين متغيرات الفرض الثاني كما يلي:

$$Y = B_0 + B X$$

الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية = ٢.٦٣٧ + ٠.٣٨٠ تطبيق معايير حوكمة أمن المعلومات

وتخلص الباحثة من نتائج تحليل الانحدار للفرض الثاني إلى أنه "يؤدي تطبيق معايير حوكمة أمن المعلومات إلى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية" وهو ما يدعم صحة الفرض الثاني للدراسة، والذي يتفق مع الدراسات السابقة الآتية: (خليل، وإبراهيم، ٢٠١٣)، (Al-Fatlawi, et., 2021).

٣- تحليل الانحدار لمتغيرات الفرض الثالث:

يوضح الجدول التالي نتائج تحليل الانحدار لأثر المبادئ الخمسة لخدمات تأكيد الثقة في نظم المعلومات المحاسبية الإلكترونية، على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية (كمتغير تابع).

جدول (٧) نتائج تحليل الانحدار لمتغيرات الفرض الثالث

بيان	معامل الانحدار (B)	قيم اختبار (ت)	مستوى المعنوية الإحصائية	الدلالة
المقدار الثابت (B ₀)	٢.٤٤٦	٧.٢٦٤	٠.٠٠٠٠	دال إحصائياً
(X) المبادئ الخمسة لخدمات تأكيد الثقة في نظم المعلومات المحاسبية الإلكترونية	٠.٤٢٤	٥.٤٨٨	٠.٠٠٠٠	دال إحصائياً
القيمة التفسيرية للنموذج : معامل التحديد $R^2 = ٠.٢٥٧$				
المعنوية الكلية للنموذج: مستوى المعنوية لتحليل ANOVA = ٠.٠٠٠٠				
قيمة اختبار (Durbin-Watson) = ١.٩١٦				

ويتضح من الجدول السابق النتائج التالية:

- تشير إشارة معامل الانحدار (الموجبة) للمتغير المستقل إلى وجود علاقة تأثير طردية للمبادئ الخمسة لخدمات تأكيد الثقة في نظم المعلومات المحاسبية الإلكترونية، على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية (كمتغير تابع).
- تشير قيمة معامل الانحدار للمتغير المستقل إلى أنه كلما زاد المتغير المستقل (المبادئ الخمسة لخدمات تأكيد الثقة) بمقدار وحدة واحدة كلما أدى ذلك إلى زيادة في المتغير التابع (الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية) بمقدار ٠.٤٢٤ وحدة.
- تؤكد دلالة اختبار (ت) للمتغير المستقل (٠.٠٠٠) والتي تقل عن مستوى المعنوية (٠.٠٥) على قبول فرض وجود علاقة تأثير معنوية ذات دلالة إحصائية لتطبيق المبادئ الخمسة لخدمات تأكيد الثقة في

نظم المعلومات المحاسبية الإلكترونية، على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية (كمتغير تابع).

▪ أن قيمة (D-W) المحسوبة للنموذج بلغت (1.916)، وهي بذلك تقع ضمن المدى المثالي وهو الذي يقترب من 2، مما يدل على عدم وجود مشكلة للارتباط الذاتي بين العناصر المكونة للمتغير المستقل تؤثر على صحة النتائج.

▪ يمكن صياغة نموذج كمي للانحدار البسيط بين متغيرات الفرض الثالث كما يلي:

$$Y = B_0 + B X$$

الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية = 2.446 + 0.424 * تطبيق المبادئ الخمسة لخدمات تأكيد الثقة في نظم المعلومات المحاسبية الإلكترونية

وتخلص الباحثة من نتائج تحليل الانحدار للفرض الثالث إلى أنه " يؤدي تطبيق المبادئ الخمسة لخدمات تأكيد الثقة إلى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية "، وهو ما يدعم صحة الفرض الثالث للدراسة، والذي يتفق مع الدراسات السابقة الآتية: (مشتهى وآخرون، 2011)، (Al-Dmour, 2018).
 4- تحليل الانحدار لمتغيرات الفرض الرابع:

يوضح الجدول التالي نتائج تحليل الانحدار لأثر التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة، على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية (كمتغير تابع)

جدول (8) نتائج تحليل الانحدار لمتغيرات الفرض الرابع

بيان	معامل الانحدار (B)	قيم اختبار (ت)	مستوى المعنوية	الدالة الإحصائية
المقدار الثابت (B0)	2.067	5.760	0.000	دال إحصائياً
(X) التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة	0.509	6.208	0.000	دال إحصائياً
القيمة التفسيرية للنموذج : معامل التحديد $R^2 = 0.307$				
المعنوية الكلية للنموذج : مستوى المعنوية لتحليل ANOVA = 0.000				
قيمة اختبار (Durbin-Watson) = 1.782				

ويتضح من الجدول السابق النتائج التالية:

▪ تشير إشارة معامل الانحدار (الموجبة) للمتغير المستقل إلى وجود علاقة تأثير طردية للتكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة، على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية (كمتغير تابع).

- تشير قيمة معامل الانحدار للمتغير المستقل إلى أنه كلما زاد المتغير المستقل (التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة) بمقدار وحدة واحدة كلما أدى ذلك إلى زيادة في المتغير التابع (الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية) بمقدار ٠.٥٠٩ وحدة.
- تؤكد دلالة اختبار (t) للمتغير المستقل (٠.٠٠٠) والتي تقل عن مستوى المعنوية (٠.٠٥) على قبول فرض وجود علاقة تأثير معنوية ذات دلالة إحصائية للتكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة، على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية (كمتغير تابع).
- أن قيمة (D-W) المحسوبة للنموذج بلغت (١.٧٨٢)، وهى بذلك تقع ضمن المدى المثالي وهو الذى يقترب من ٢، مما يدل على عدم وجود مشكلة للارتباط الذاتي بين العناصر المكونة للمتغير المستقل تؤثر على صحة النتائج.
- يمكن صياغة نموذج كمي للانحدار البسيط بين متغيرات الفرض الرابع كما يلي:

$$Y = B_0 + B X$$

الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية = ٢.٠٦٧ + ٠.٥٠٩ التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة

وتلخص الباحثة من نتائج تحليل الانحدار للفرض الرابع إلى أنه "يساهم التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة فى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية" وهو ما يدعم صحة الفرض الرابع للدراسة.

ومن واقع نتائج التحليل الإحصائي للبيانات المرتبطة بفروض الدراسة وبعد اختبار هذا الفرض يمكن للباحثة تلخيص النتائج التالية:

جدول (٩) النتائج العامة للتحليل الإحصائي

نتائج التحليل الإحصائي	الاختبار / التحليل
١- جميع العناصر المستخدمة في تحليل وقياس نتائج فروض الدراسة صالحة ويمكن الاعتماد عليها فى عملية القياس؛ حيث أن معامل ألفا كرونباخ عالية جدا مما يشير إلى وجود درجة عالية من الاعتمادية والتجانس والتناسق الداخلى بين البيانات.	اختبار الصلاحية والاعتمادية (معامل ومعامل ألفا كرونباخ)
٢- تشير قيم الوسط الحسابى لجميع ردود المستقصى منهم حول جميع عناصر فروض الدراسة (أكبر من ٣) إلى أن الآراء تميل لصالح الموافقة؛ وهو ما تدل عليه نسب الوزن النسبى لجميع العناصر والتي تزيد عن ٦٠% الممثلة لاختيار "محايد".	التحليل الوصفى للبيانات من خلال بعض المقاييس الإحصائية (الوسط - الانحراف المعياري - الوزن النسبى)

الاختبار / التحليل	نتائج التحليل الإحصائي
اختبار (ت)	٣- تشير معنوية اختبار (t) وهي (٠.٠٠) لجميع العناصر والتي تقل عن (٠.٠٥) إلى أن جميع الأوساط الحسابية دالة إحصائياً وأنه يوجد اختلافات (فروق معنوية) في آراء المستقصى منهم حول جميع عناصر فروض الدراسة.
تحليل مصفوفة الارتباط	٤- تشير نتائج تحليل الارتباط لفروض الدراسة إلى وجود علاقة ارتباط طردية متوسطة ذات دلالة معنوية بين كل من (إجراءات الحماية الكافية لتنظيم المعلومات المحاسبية الإلكترونية، تطبيق معايير حوكمة أمن المعلومات، المبادئ الخمسة لخدمات تأكيد الثقة، التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة) والحد من مخاطر نظم المعلومات المحاسبية الإلكترونية).
تحليل الانحدار	٥- تشير نتائج تحليل الانحدار لفروض الدراسة إلى وجود علاقة تأثير ذات دلالة إحصائية لكل من (إجراءات الحماية الكافية لتنظيم المعلومات المحاسبية الإلكترونية، تطبيق معايير حوكمة أمن المعلومات، المبادئ الخمسة لخدمات تأكيد الثقة، التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة) على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية (كمتغير تابع)

ومن نتائج الجدول السابق ترى الباحثة ثبوت صحة فروض الدراسة، والتي تنص على:

- يؤدي عدم وجود إجراءات حماية كافية إلى زيادة المخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية.
- يؤدي تطبيق معايير حوكمة أمن المعلومات إلى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.
- يؤدي تطبيق المبادئ الخمسة لخدمات تأكيد الثقة إلى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.
- يساهم التكامل بين حوكمة أمن المعلومات وخدمات تأكيد الثقة في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.

(٦) نتائج وتوصيات و مجالات البحث المستقبلية:

(١/٦) نتائج البحث:

توصلت الباحثة من خلال الدراسة النظرية والميدانية إلى عدداً من النتائج أهمها ما يلي:
لقد أظهر الجانب النظري والميداني من البحث عدداً من النتائج ، ويمكن توضيح وتلخيص أهم تلك النتائج كما يلي:-

١- أبرزت الدراسة مدى أهمية قضية تنوع وتعدد المخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية والتي تتباين تصنيفها (ما بين ناظر داخلية، ومخاطر خارجية)، ومصادرها (ما بين عدم وجود ضوابط وإجراءات حماية كافية تضمن سلامة وأمن نظم المعلومات المحاسبية الإلكترونية، نقص الخبرة اللازمة والتدريب الكافي من قبل الموظفين)، بالإضافة إلى التأثير السلبي لتلك المخاطر على أعمال الشركة وعلى تحقيق أهدافها الإستراتيجية.

٢- تطبيق حوكمة أمن المعلومات على نحو فعال بضمن الاستثمار الجيد لنظم وتكنولوجيا المعلومات مما يؤدي إلى إضافة قيمة حقيقية للشركة، وذلك لتحقيق الأهداف الإستراتيجية للشركة، بالإضافة إلى أن حوكمة أمن المعلومات مسؤولة كلاً من مجلس الإدارة والإدارة التنفيذية فهي تتكون من مجموعة من القيادة والهياكل التنظيمية والعمليات المشاركة في حماية الأصول المعلوماتية.

٣- يساعد COBIT5 في التخطيط الجيد لإدارة المخاطر وتحليلها وتقييمها من خلال تقديم إرشادات وتوجيهات للقائمين على العمل والمتخصصين لمعالجة القضايا والمخاطر المتعلقة بنظم وتكنولوجيا المعلومات، حيث يوفر معيار COBIT5 الضوابط والإجراءات والتدابير الأمنية التي تضمن سلامة وأمن نظم المعلومات المحاسبية الإلكترونية.

٤- خدمات تأكيد الثقة في النظام تستخدم من أجل إضفاء الثقة لكل من الإدارة، العملاء الموردين، الملاك، الهيئات الحكومية والجهات الأخرى في نظام المعلومات المحاسبي الإلكتروني.

٥- تبين من الجانب النظري للدراسة أن كلاً من معيار حوكمة أمن المعلومات COBIT5 ومبادئ خدمات تأكيد الثقة يسعى إلى تحقيق الأمن والموثوقية في نظام المعلومات المحاسبي الإلكتروني من خلال الحد من المخاطر العديدة التي تواجه نظم المعلومات المحاسبية الإلكترونية.

(٢/٦) توصيات البحث:

بناءً على ما جاء في التأسيس النظري والميداني توصي الباحثة بما يلي:-

- ١- ضرورة اهتمام المنظمات والهيئات المهنية المعينة بالمواكبة مع التطور التكنولوجي بعقد الدورات التدريبية لرفع ثقافة إدارة المخاطر، والتدريب على أحدث الممارسات العلمية والعملية المطبقة في هذا المجال. ضرورة اهتمام الجهات الرقابية بتطبيق الإجراءات والقواعد والمبادئ الواردة في معيار COBIT لإدارة المخاطر وحماية نظم المعلومات المحاسبية الإلكترونية على نحو فعال.
- ٢- زيادة الاهتمام بتطبيق معايير حوكمة أمن المعلومات وتوعية المنظمات والجهات المهنية بمدى دورها وأهميتها في الحد من المخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية.

- ٣- قيام المنظمات والجهات المهنية بالتوسع في مجال البحث العلمي فيما يخص ممارسات إدارة المخاطر وحوكمة أمن المعلومات وخدمات تأكيد الثقة في نظم المعلومات المحاسبية الإلكترونية.
- ٤- قيام الهيئة العامة للرقابة المالية بإلزام الشركات بتطبيق معيار حوكمة أمن المعلومات COBIT5 ومبادئ خدمات تأكيد الثقة داخل الشركات لتزيد من درجة الثقة والمصداقية في نظم المعلومات المحاسبية الإلكترونية ومخرجاته التي تقوم تلك الشركات بالإفصاح عنها عبر الموقع الإلكتروني الخاص بها.
- ٥- توصي الباحثة بالاستفادة من التكامل المقترح بين حوكمة أمن المعلومات وخدمات تأكيد الثقة للحد من مخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية والذي يعتمد على المحاور التالية: تفعيل إدارة المخاطر وأمن نظم المعلومات المحاسبية الإلكترونية، وتدعيم الضوابط والإجراءات لتفعيل نظم الرقابة الداخلية، وتطوير الأنظمة المحاسبية الإلكترونية وفقاً للتطور المستمر لتكنولوجيا المعلومات، وتفعيل آليات حوكمة الشركات وحوكمة تكنولوجيا المعلومات لتدعيم حوكمة أمن المعلومات، وضع خارطة عمل ملائمة لتطبيق حوكمة أمن المعلومات وخدمات تأكيد الثقة في النظم المحاسبية الإلكترونية.

(٣/٦) مجالات البحث المستقبلية:

- في ضوء النتائج والتوصيات التي توصل إليها البحث ترى الباحثة أن هناك مجالات بحثية عديدة تمثل أساساً لأبحاث مقترحة ومنها على سبيل المثال:
- تفعيل أثر تطبيق حوكمة أمن المعلومات على نظام الرقابة الداخلية لنظم المعلومات المحاسبية الإلكترونية.
 - دور معايير حوكمة أمن المعلومات في الحد من التلاعب المالي الإلكتروني.
 - إطار مقترح بين حوكمة أمن المعلومات وخدمات تأكيد الثقة لزيادة الثقة في المعلومات المالية المنشورة عبر الإنترنت.
 - دراسة دور خدمات تأكيد الثقة في تفعيل جودة التقارير المالية الإلكترونية في ضوء حوكمة أمن المعلومات.

المراجع

أولاً: مراجع البحث باللغة العربية:

- ١) الزغبي، وليد خلف الزغبي، والنجداوي، أكرم يوسف، (٢٠١٢)، "أثر استخدام نظم المعلومات المحاسبية المحوسبة في رفع كفاءة الإدارة، المجلة العلمية للاقتصاد والتجارة، كلية التجارة، جامعة عين شمس، المجلد ٣، العدد ٢.
- ٢) الساكني، سعيد عبد الكريم، والعاودي، حنان علي، (٢٠١٢)، "مخاطر استخدام تكنولوجيا المعلومات وأثرها على أداء نظم المعلومات المحاسبية- دراسة تطبيقية على عينة من الشركات المساهمة المدرجة في بورصة عمان للأوراق المالية"، مجلة دراسات المعلومات، جامعة الإسرء، العدد ١١.
- ٣) أبو مهادي، سناء طالب عبد الكريم، (٢٠١٧)، "أثر موثوقية نظم المعلومات المحاسبية الإلكترونية على مؤشرات الأداء المصرفي- دراسة تطبيقية على المصارف المحلية العاملة في فلسطين"، رسالة ماجستير غير منشورة، كلية التجارة، الجامعة الإسلامية- غزة.
- ٤) حسن، محمد عبد الحافظ عبد العال، (٢٠١٠)، "المراجعة وتحديات الأزمة المالية العالمية"، بدون ناشر.
- ٥) حسين، علي كاظم، (٢٠١٣)، "دور معايير التدقيق الدولية في تعزيز خدمات التأكيد- بحث تطبيقي على عينة مراقبي الحسابات"، مجلة دراسات محاسبية ومالية، المجلد ٨، العدد ٢٣.
- ٦) عبد السميع، ياسمين جاد الرب، (٢٠١٦)، "إطار مقترح للتكامل بين حوكمة تكنولوجيا المعلومات ومبادئ خدمات الثقة كمنطلق لزيادة فعالية نظم المعلومات المحاسبية- دراسة تطبيقية على البنوك في جمهورية مصر العربية"، رسالة ماجستير غير منشورة، كلية التجارة، جامعة المنصورة.
- ٧) عبد اللطيف، ناصر نور الدين، (٢٠٠٨)، "إطار مقترح لخدمة التأكيد على الثقة في النظم الإلكترونية- دراسة تطبيقية"، مجلة الدراسات المالية والتجارية، جامعة بني سويف، العدد ٢.
- ٨) عقل، سلام أبو الفتوح حسن، (٢٠١٥)، "إدارة مخاطر نظم المعلومات المحاسبية الإلكترونية بفرض دعم التقرير المالي: دراسة تطبيقية"، رسالة ماجستير غير منشورة، جامعة المنصورة.
- ٩) عيسى، سمير كامل محمد، (٢٠٠٦)، "دور المراجع الخارجي في تنمية فجوة الثقة في بيئة التجارة الإلكترونية، المجلة العلمية للتجارة والتمويل، كلية التجارة، جامعة طنطا، المجلد الأول، العدد ١.
- ١٠) مهندي، محمد صبح أنيس، (٢٠١٥)، "مسئولية المحاسب القانوني عن خدمات التأكيد ودورها في ممارسات إدارة الأرباح في ضوء معايير المراجعة المصرية- دراسة ميدانية"، رسالة ماجستير غير منشورة، كلية التجارة، جامعة بنها.
- ١١) نبيل، غادة أحمد، (٢٠١٢)، "تحسين فعالية المراجعة المستمرة باستخدام خدمات الثقة"، المجلة العلمية للبحوث والدراسات التجارية- مصر، كلية الإدارة والاقتصاد، جامعة مصر للعلوم والتكنولوجيا، العدد ٤.

- 1- AICPA.(2015), "Exposure Draft, Proposed Revision of Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy", New York.
- 2- Al-Fatlawi Q.Ali, Salman, Dawood, Almagtome, Akeel ,(2021)," Accounting Information Security and IT Governance Under COBIT5 Framework: A Case Study", Faculty of Administration and Economics, University of Kufa, Najaf, Iraq, Vol.18, pp.294:310, Available at: <https://www.researchgate.net>, Retrieved at: 30-7-2021.
- 3- Al-Dmour, Ahmed H., (2018)," The Impact of the SysTrusts Framework as an Internal Control of AIS Process upon Business Performance via Mediating Role of Financial Quality Reporting: An Integrated Model", Thesis of Ph.D, Brunel University London.
- 4- Al-Fatlawi Q.Ali, Ali, Salman, Dawood & Almagtome, Akeel, (2021), "Accounting Information Security and IT Governance Under COBIT5 Framework: A Case Study", Faculty of Administration and Economics, University of Kufa, Najaf, Iraq, Vol.18, PP.294:310, Available at: <https://www.researchgate.net>, Retrieved at: 30-7-2021.
- 5- Al-Refae, Khalil M., (2012)," The Effect of E-Commerce on the Development of Accounting Information System in the Islamic Banks", American Journal of Applied University, Vol.1, No.9.
- 6- Al-Sharairi, Mohammed, Al-Hosban, Atallah & Thnaibat, Hussam, (2018)," The Impact of the Risks of the Input of Accounting Information System on Managerial Control, Accounting Control, and Internal Control in Commercial Banks in Jordan", International Journal of Business and Management, Vol.13, No.2.
- 7- Arens, Alvin A. & Elderand, Randal J., (2012), "Auditing and Assurance Service: An Integrated Approach", 14th Edition, Prentice Hall, New Jersey.
- 8- Bodeau, Deb, Boyle, Steve & Fabius- Greene, Jenn, (2010), "A Component of Mitre's Cyber Prep Methodology", Available at: <http://www.mitro.org>., Accessed:8-9-2019.
- 9- Information Technology Governance Institute (ITGI), (2006)," Information Security Governance: Guidance for Boards of Directors and Executive Management", 2th Edition, ITGI, U.S.A.
- 10- Kaluarachchi, Dana, (2015), "Impact of Computerized Accounting Information Systems Effectiveness in Increasing the efficiency of human capital", 4th Annual International Research Conference.

- 11- Mansour, Ebrahim, Al Salamat, Wasfi, Masadeh, Walid, (2017), " The Impact of Reliability Elements on Performance Indicators of Jordanian Commercial Banks", **The International Journal of Business and Finance Research**, Hashemite University, Vol.1, No.1.
- 12- Mukhanova, A.A, Fedotov, A.M, (2014), " **Vulnerability Classification of Information Security in Corporate Systems**", L.N. Gumilyov Evrasian, University, Institute of Computation Technologies SBRAS, Noro Sibirsk, Russian Fedration.
- 13- Nicho, Mathew, (2018), " A Process Model for Implementing Information Systems Security Governance", **Information & Computer Security**, Vol.26, No.1.
- 14- Yassine, Maleh & Abdelkebir, Sahid, (2019), " **Information Security Governance Practices and Commitment in Organizations**", IGI Global, Research Gate.
- 15- Hossin, Adel M.& Ayedh, Abdellah M., (2016), " The Risks of Electronic Accounting Information System in the Central Bank of Libya, **South East Asia Journal of Contemporary Business, Economic & Law**, Vol.1, No.1.
- 16- Hussain, M.Ali, (2013), " A Study of Information Security in E-Commerce Application", **International Journal of Computer Engineering Science (IJCES)**, Vol.3, Issue3.
- 17- Pickett, K.H. Spencer, (2010), "**The International Auditing Handbook**", 3rd, Wiley.
- 18- Romney, Marshall B., Steinbart, Paul John, (2015), "**Accounting Information Systems**", 13th, Prentice Hall.
- 19- Razali, M. Fazlida M.R, J. Said, (2015), "Information Security, Risk Governance and Implementation Setback", **7th International Conference on Financial Criminology**, Wadham, College, Oxford, United Kingdom.
- 20- Rubino, Michele, Vitolla, Filippo, Garzoni, Antonello, (2017), " The Impact of an IT Governance Framework on the Internal Control Environment", **Records Management Journal**, Vol.27, No.1.
- 21- Yassine, Maleh & Abdelkebir, Sahid, (2019), " **Information Security Governance Practices and Commitment in Organizations**", IGI Global, Research Gate.