الدور التأثيرى لحوكمة أمن المعلومات فى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية – دراسة ميدانية

د/ على محمود مصطفى خليل
مدرس بقسم المحاسبة
كلية التجارة – جامعة بنها

د/ منى مغربى محمد إبراهيم
مدرس بقسم المحاسبة
كلية التجارة – جامعة بنها

الدور التأثيرى لحوكمة أمن المعلومات فى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية – دراسة ميدانية

د/ على محمود مصطفى خليل
مدرس بقسم المحاسبة
كلية التجارة – جامعة بنها

د/ منى مغربى محمد إبراهيم
مدرس بقسم المحاسبة
كلية التجارة – جامعة بنها

ملخص البحث:

يتمثل الهدف الرئيسى للبحث فى دراسة الدور الذى تقوم به حوكمة أمن المعلومات فى الحد من المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية فى الشركات المصرية، وذلك فى ضوء المعايير الدولية الخاصة بمجال أمن المعلومات مثل الإصدار الخامس من معيار الـCOBIT الصادر فى عام ٢٠١٣، ومعايير الأيزو ISO/IEC 27016, 27038 الصادرة فى عام ٢٠١٤، وأثر تطبيق تلك الإصدارات الحديثة على أمن نظم المعلومات المحاسبية.

وقد قام الباحثان لتحقيق هذا الهدف بإجراء دراسة ميدانية على عينة من الشركات والبنوك العاملة فى القرية الذكية بجمهورية مصر العربية من خلال توزيع قائمة استقصاء لاختبار مجموعة من الفروض تمثلت فى: مدى اختلاف الأهمية النسبية للمخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية، والتعرف على الأسباب وراء حدوث تلك المخاطر، ومدى قيام المنظمات المصرية بتطبيق حوكمة أمن المعلومات، وأخيرًا مدى وجود تأثير جوهرى لمعايير حوكمة أمن المعلومات فى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.

وتوصلت الدراسة إلى أن هناك العديد من المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية يتمثل أهمها فى المخاطر الخارجية، كما يتمثل أهم أسباب حدوث تلك المخاطر فى عدم وجود سياسات وبرامج لأمن المعلومات داخل تلك الشركات، بالإضافة إلى عدم قيام عدد كبير من عينة الدراسة بتطبيق الأهداف والمبادئ الخاصة بحوكمة أمن المعلومات، وعدم تضمينها داخل استراتيجيتها المستقبلية، وأخيرًا توصلت الدراسة إلى وجود تأثير معنوى لتطبيق معايير حوكمة أمن المعلومات بشكل مستقل على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية، وأن أكثر تلك المعايير تأثيرًا هو معيار الـCOBIT.

وأوصى الباحثان فى نهاية الدراسة بضرورة وجود نشرات إرشادية لتوعية المنظمات المصرية عن دور وأهمية حوكمة أمن المعلومات من خلال قيام وزارة الاستثمار – مركز المديرين– بإصدار دليل لقواعد ومبادئ ومعايير حوكمة أمن المعلومات بحيث يكون من مرفقات دليل قواعد ومبادئ حوكمة الشركات، وقيام الهيئة العامة للرقابة المالية بإلزام الشركات بتطبيق ما ورد به من قواعد ومعايير.

المصطلحات الأساسية: مخاطر نظم المعلومات المحاسبية الإلكترونية – حوكمة أمن المعلومات – معايير الأيزو ISO/IEC 27K – معيار COBIT 5 – معيار ITIL.

(١) القسم الأول: الإطار العام للبحث

(١/١) مقدمة:

أدت الزيادة السريعة في استخدام التكنولوجيا والإنترنت خلال العقدين الأخيرين إلى الدخول لمجتمع المعلومات، وأصبحت المنظمات تعتمد على أنظمة المعلومات الإلكترونية فى تنفيذ المهام والوظائف المنوطة بها، ومن أهم تلك الأنظمة نظم المعلومات المحاسبية الإلكترونية والتي تُمثل نتائجها نقطة الاتصال بين المنظمة والأطراف ذات العلاقة.

وتواجه نظم المعلومات المحاسبية الإلكترونية مخاطر خطيرة يمكن أن تَستغل نقاط الضعف والثغرات – المعروفة وغير المعروفة على حدٍ سواء – فى هذه النظم. وتتمثل تلك المخاطر فى الهجمات المستهدفة، وتعطل العمل بسبب الكوارث الطبيعية والبشرية، وأخطاء النظام، والفشل الهيكلى، وتسريب البيانات السرية، و... غيرها، وتتضح خطورة هذه المخاطر فى أن قيمة أعمال الجريمة الإلكترونية أصبحت تُقدر بحوالى ١٠٥ بليون دولار سنويًا، وهذا الرقم يفوق قيمة أعمال تجارة المخدرات فى جميع أنحاء العالم (Bose & Leung, 2014).

وتؤثر مخاطر أمن المعلومات سلبيًا على المنظمات وعملياتها وأصولها والعاملين بها وقد تؤدى إلى تهديد غيرها من المنظمات، بالإضافة إلى أن حدوث تلك المخاطر يؤدى إلى انخفاض القيمة السوقية للمنظمة (Ito et al., 2010)؛ حيث إنها تهدد سرية ونزاهة ومدى توافر المعلومات المحاسبية التى يتم معالجتها وتخزينها وإرسالها أو الإفصاح عنها بواسطة نظم المعلومات المحاسبية الإلكترونية (National Institute of Standards and Technology, 2011). ولذلك لجأت العديد من المنظمات إلى تطبيق حوكمة أمن المعلومات، التى تهدف إلى حماية الأصول الإلكترونية من مختلف المخاطر المحتملة، من خلال استخدام مجموعة من المعايير الدولية والتى يتم استخدامها على نطاق واسع للتأكد من الوصول لمستوى الأمن المطلوب والكافى.

(٢/١) طبيعة المشكلة:

اصبحت تكنولوجيا المعلومات أكثر تعقيدًا من ذى قبل، وارتبط بذلك احتمالات تعرض تلك التكنولوجيا لمخاطر من شأنها أن تؤثر على كفاءة وفعالية نظم المعلومات، وبصفة خاصة نظام المعلومات المحاسبى، ومن ثم على جودة المعلومات المحاسبية؛ حيث يؤدى تعرض تلك النظم للمخاطر إلى التأثير على سرية ونزاهة وتوافر المعلومات، وعلى الرغم من ذلك فإنه فى مجال المال والأعمال لا يمكن الاستغناء عن تلك التكنولوجيا أو حتى الإقلال من الاعتماد عليها، بل على العكس يزداد اهتمام المسئولين بالمنظمات المختلفة بتطوير تكنولوجيا المعلومات وتحقيق أقصى استفادة ممكنة من الإمكانات المتاح استخدامها.

وأصبح من الضرورى على المنظمات أن تهتم بوضع نظم وإجراءات تعمل على الحد من تلك المخاطر، ووضع نظام جيد لإدارتها، ووُجِدَ أن الحلول التكنولوجية ضرورية ولكنها غير كافية فى

مواجهة تحديات ومخاطر أمن المعلومات، ومن ثم زاد الاهتمام بأمن المعلومات باعتبارها من المسئوليات التنفيذية المهتمة بالبنية التحتية التكنولوجية على مستوى المنظمة وزيادة التركيز على استراتيجيات متطلبات العمل وإشراك الأشخاص المناسبين، وتوظيف التكنولوجيا المناسبة، وحماية أصول المعلومات الهامة، الأمر الذى أدى بتلك المنظمات إلى اتباع تطبيق منهج شامل يهدف إلى حماية الأصول الأكثر أهمية بالنسبة للمنظمة وهى المعلومات ويعرف هذا المنهج "بحوكمة أمن المعلومات".

ويتزايد الاعتراف بحوكمة أمن المعلومات كقضية بالغة الأهمية للمنظمات من حيث المسئولية، والواجبات الإئتمانية، وتقديم قيمة لتلك المنظمات، وتحسين الوضع التنافسى لها. وتهتم تلك الحوكمة بتأسيس بيئة رقابية مع ضمان توفير الحماية اللازمة للأصول المعلوماتية من المخاطر المختلفة، وكذلك وضع خطة للتطوير المستمر لإدارة المخاطر (Sengupta & Mazumdar, 2011). ولتحقيق ذلك تقوم حوكمة أمن المعلومات بالعمل على تطبيق بعض المعايير الدولية والتى تتناول على وجه التحديد قضايا أمن المعلومات للمنظمة، ومن تلك المعايير: معايير الأيزو ISO، معيار COBIT، معيار ITIL.

وتهتم الجهات التى تُصدر تلك المعايير بالعمل على تطويرها وتحديثها باستمرار حتى تتمكن من مواكبة التطور المماثل الذى يحدث فى مجال تكنولوجيا المعلومات، والجرائم المرتبطة به.

وعلى الرغم من الأهمية المتزايدة لحوكمة أمن المعلومات ودورها الفعال فى إدارة المخاطر التي تتعرض لها نظم المعلومات الإلكترونية داخل المنظمة بصفة عامة، ونظم المعلومات المحاسبية الإلكترونية بصفة خاصة، إلا أنها لم تلق الاهتمام البحثى الكافى فى البيئة العربية بما يكشف عن ماهية وطبيعة حوكمة أمن المعلومات، وما هى أهدافها، ومدى تأثيرها فى الحد من المخاطر التى تتعرض لها أنظمة المعلومات المحاسبية الإلكترونية. ومن ثم تتمثل مشكلة البحث فى الإجابة عن التساؤلات التالية:

١- ما هى طبيعة المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية، وما هى أنواعها؟

٢- ما هى أسباب تَعرُض نظم المعلومات المحاسبية الإلكترونية لتلك المخاطر؟

٣- ما هى حوكمة أمن المعلومات؟ وما هو الدور الذى تلعبه فى حماية الأصول المعلوماتية للمنظمات؟

٤- ما هى المعايير الدولية التى يتم استخدامها فى إطار حوكمة أمن المعلومات؟

٥- هل تساهم معايير حوكمة أمن المعلومات فى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية؟

(٣/١) هدف البحث:

يهدف هذا البحث إلى توضيح الدور الذى تقوم به حوكمة أمن المعلومات فى الحد من المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية من خلال المعايير الدولية لحوكمة أمن المعلومات، ويتحقق هذا الهدف الرئيسى من خلال الأهداف الفرعية التالية:

١- التعرف على نوعية المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية.

٢- استكشاف أسباب تعرض نظم المعلومات المحاسبية الإلكترونية إلى المخاطر.

٣- التعرف على ماهية حوكمة أمن المعلومات، والتحقق من مدى استخدامها فى بيئة الأعمال المصرية.

٤- تحديد المعايير المستخدمة عند تطبيق حوكمة أمن المعلومات، وتحديد المعايير الأكثر تأثيرًا فى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.

(٤/١) أهمية البحث:

تنبع أهمية البحث فى هذا الموضوع من خلال الاهتمام المتزايد بالمخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية فى المنظمات المختلفة، وقيام الجهات المعنية بإصدار المعايير الدولية بمحاولة مواكبة التطورات السريعة والمتلاحقة فى هذا المجال. ويمكن إيضاح أهمية البحث من خلال ما يلى:

الأهمية العلمية: تتمثل الأهمية العلمية فى محاولة إلقاء الضوء على تنوع وتعدد المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية، وتوضيح المحاولات التى تقوم بها المنظمات للحد من تلك المخاطر، وكذلك إلقاء الضوء على منهج شامل يستخدم فى مواجهة هذه المخاطر وهو حوكمة أمن المعلومات، ومعرفة المعايير التى يتم استخدامها عند تطبيق حوكمة أمن المعلومات داخل المنظمات المختلفة.

الأهمية العملية: تتضح الأهمية العملية من خلال الحصول على دليل ميدانى من بيئة الأعمال المصرية حول المخاطر التى تتعرض لها نظم المعلومات المحاسبية، والوسائل والأساليب المستخدمة فى التعامل مع تلك المخاطر، ومدى قيام المنظمات المصرية بتطبيق معايير حوكمة أمن المعلومات للحفاظ على الأصول المعلوماتية لديها.

(٥/١) منهج البحث:

اعتمد الباحثان على المنهج العلمى بشقيه الاستنباطى والاستقرائى لتحليل وتقييم الدراسات والبحوث السابقة التى تناولت مخاطر نظم المعلومات المحاسبية الإلكترونية والوسائل والإجراءات التى تتبعها المنظمات فى الحد من تلك المخاطر، ودور حوكمة أمن المعلومات فى ذلك، كما قام الباحثان بإجراء دراسة ميدانية بهدف التعرف على نوعية المخاطر التى تتعرض لها نظم المعلومات المحاسبية

فى بيئة الأعمال المصرية، ومدى استخدام حوكمة أمن المعلومات والمعايير المتعلقة بها فى الحد من تلك المخاطر.

(٦/١) حدود البحث:

١- يقتصر البحث على المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية فقط، دون الدخول فى التفسيرات أو الدوافع من وراء تلك المخاطر.

٢- يقتصر البحث على دور حوكمة أمن المعلومات فى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية من خلال المعايير الدولية التى يتم تطبيقها فى إطار حوكمة أمن المعلومات، دون الدخول فى الوسائل والإجراءات الأخرى المتبعة من قِبَل المنظمات للحد من تلك المخاطر والتى من ضمنها إجراءات المراجعة الداخلية.

٣- يقتصر البحث على حوكمة أمن المعلومات، دون التطرق لكل من حوكمة الشركات وحوكمة تكنولوجيا المعلومات، إلا بالقدر الذى يخدم البحث.

٤- يقتصر البحث على إجراءات حوكمة أمن المعلومات التى تتم لحماية عمليات المعلومات الإلكترونية فقط من المخاطر التى تتعرض لها، دون التطرق لحماية عمليات المعلومات المادية.

٥- يقتصر البحث على استقصاء آراء عينة الدراسة وهم: المديرون الماليون والمحاسبون، وموظفو إدارة تكنولوجيا المعلومات، والمراجع الخارجى لشركات الاتصالات، وشركات تكنولوجيا المعلومات، والبنوك العاملة فى القرية الذكية بجمهورية مصر العربية، دون التطرق للشركات والبنوك التي يتم الاستعانة فيها بمصادر خارجية (تعهيدات) لتوفير خدمات تكنولوجيا المعلومات لديها، ودون التطرق لفئات العاملين الأخرى داخل تلك الشركات.

(٧/١) تنظيم البحث:

تحقيقًا لأهداف البحث يتم تقسيمه على النحو التالى:

القسم الأول: الإطار العام للبحث.

القسم الثانى: الدراسات السابقة.

القسم الثالث: الإطار العام لحوكمة أمن المعلومات.

القسم الرابع: الدراسة الميدانية.

القسم الخامس: النتائج والتوصيات والتوجهات البحثية المستقبلية.

(٢) القسم الثانى: الدراسات السابقة:

(١/٢) استعراض الدراسات السابقة المرتبطة بموضوع البحث:

يمكن تقسيم الدراسات السابقة حسب ارتباطها بموضوع البحث إلى نوعين هما:

(١/١/٢) دراسات سابقة مرتبطة بمخاطر نظم المعلومات المحاسبية الإلكترونية.

(٢/١/٢) دراسات سابقة مرتبطة بحوكمة أمن المعلومات.

ويمكن تناول كل منها على النحو التالى:

(١/١/٢) دراسات سابقة مرتبطة بمخاطر نظم المعلومات المحاسبية الإلكترونية:

تعددت صور وأشكال المخاطر التى تواجه نظم المعلومات المحاسبية الإلكترونية، فقد تم تصنيفها وتبويبها من وجهات نظر مختلفة، **فيمكن تبويبها من حيث مصدرها إلى:** مخاطر داخلية ومخاطر خارجية؛ حيث يمثل موظفو الشركة المصدر الرئيسى للمخاطر الداخلية، بينما يمثل قراصنة المعلومات أهم مصدر للمخاطر الخارجية. **وأيضًا يتم تبويب المخاطر على أساس العمدية إلى:** مخاطر ناتجة عن أعمال متعمدة Intentional مثل: الإدخال المتعمد لبيانات غير صحيحة، ومخاطر ناتجة عن أعمال غير متعمدة Unitentional مثل: الإدخال غير المتعمد لبيانات غير صحيحة، أو تدمير البيانات نتيجة الخطأ. **كما تُبوب المخاطر بناءً على الآثار الناتجة عنها إلى:** مخاطر ينتج عنها أضرار مادية مثل: تدمير وسائط التخزين، ومخاطر فنية تصيب البيانات الموجودة على الحاسب مثل: إدخال الفيروسات إلى البرنامج الذى يعمل على تشغيل البيانات. **وأخيرًا يمكن تبويب المخاطر على أساس علاقتها بمراحل النظام إلى:** مخاطر تصيب المدخلات، ومخاطر التشغيل، ومخاطر تتعرض لها مخرجات النظام (أبو موسى، ٢٠٠٤؛ الساكنى والعواودة، ٢٠٠٤).

وقد استهدفت دراسة (Abu-Mousa, 2006) تقييم المخاطر الأمنية التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية فى القطاع المصرفى المصرى، وتوصلت هذه الدراسة إلى أن أهم المخاطر الأمنية التى تتعرض لها تلك النظم تتمثل فى: الإدخال الخاطئ المتعمد وغير المتعمد للبيانات، والتدمير غير المقصود للبيانات من قِبَل الموظفين، ودخول فيروسات الحاسب إلى النظام، وتبادل كلمات المرور بين الموظفين، والكوارث الطبيعية، والتى من صنع الإنسان، وسوء توجيه وتوزيع المعلومات لأشخاص غير مصرح لهم. كما أشارت الدراسة إلى أن إدارة المراجعة الداخلية بالشركة هى أكثر الإدارات التى أبلغت عن حدوث تلك المخاطر بالمقارنة مع إدارة تكنولوجيا المعلومات.

وقد اتفقت مع تلك النتائج، الدراسة التى قام بها كل من (Hayale & Abu-Khadra, 2008) بالتطبيق على القطاع المصرفى فى الأردن، واعتبرت الدراسة أن كلاً من: الإدخال الخاطئ المتعمد وغير المتعمد للبيانات، والتدمير غير المقصود للبيانات من قِبَل الموظفين، وتبادل كلمات المرور بين الموظفين هى من أكثر أربعة مخاطر تواجه البنوك المحلية فى الأردن، كما أن معظم تلك المخاطر يتم إنشاؤها داخليًا وتكون غير مقصودة.

كما قامت دراسة (Zainol et al., 2012) باستكشاف المخاطر الأمنية القائمة على العاملين فى القطاع المصرفى فى ماليزيا مثل: عدم المبالاة من الأشخاص الموثوق بهم عند دخولهم على أنظمة المعلومات، والفشل فى متابعة الإجراءات التى تم وضعها، وسوء التدريب والإشراف، والسهو، وفقد البيانات أو عدم وضعها فى المكان الصحيح، والأخطاء المنطقية، و... غيرها. ومن ناحية أخرى فقد يقوم الموظفون عن عمد بالتلاعب فى أصول المعلومات نظرًا لبعض الأسباب الشخصية مثل: التخريب، والهجمات التى تتم على الشبكات، وتحميل البرامج الخبيثة، والوصول غير المصرح به للمعلومات السرية، والاختلاس.

وقامت الدراسة بالتطبيق على البنوك التجارية والبنوك الإسلامية فى ماليزيا، وتوصلت إلى أن هناك احتمال تعرض البنوك الماليزية إلى المخاطر الأمنية غير المعتمدة ولكن بنسبة ضئيلة، وترجع تلك النتائج إلى قيام تلك البنوك بتطبيق إجراءات رقابة كافية وفعالة لأمن نظم المعلومات لديها.

كما أرجعت دراسة (Hanini, 2012) وجود المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية إلى نقص خبرة الموظفين فى حفظ أمن المعلومات، والتى تتمثل فى عدم تدريب الموظفين على استخدام وسائل حماية النظم المحاسبية قبل البدء فى عملهم، وعدم وجود أنظمة التعيين المناسبة التى تقضى بأن يتم تعيين الأشخاص المناسبين فى المكان المناسب، وذلك بالتطبيق على القطاع المصرفى فى الأردن.

وقامت دراسة (Muhrtala & Ogundeji, 2013) بفحص توقعات المحاسبين ومديرى تكنولوجيا المعلومات فى الشركات النيجيرية حول المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية، وقد اتفقت آراء المستطلعين حول تعرض نظم المعلومات المحاسبية الإلكترونية إلى المخاطر الداخلية والخارجية على حد سواء. وتوصلت الدراسة إلى أن أهم المخاطر الأمنية التى تتعرض لها تلك النظم تتمثل فى: قيام الموظفين ببعض الأفعال غير المتعمدة (العرضية)، مثل: إدخال بيانات غير سليمة، وتدمير البيانات، ومشاركة كلمات السر. كما يوجد بعض المخاطر العمدية الأخرى مثل: دخول فيروسات إلى البرامج والأجهزة المستخدمة، والدخول غير المصرح إلى أنظمة المعلومات، وعرض الوثائق السرية على شاشات العرض.

وأيضًا تناولت دراسة (Tarmidi et al., 2013) المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية فى قطاع الخدمات العامة الماليزية، حيث قامت بتقسيم تلك المخاطر إلى: مخاطر متعلقة بإدخال البيانات، ومخاطر متعلقة بقواعد البيانات، ومخاطر متعلقة بعمليات التشغيل، ومخاطر متعلقة بالمخرجات. وقد توصلت الدراسة إلى أن أغلب المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية تنبع من مصادر داخلية (الموظفين)، وأرجعت الدراسة تعرض تلك الأنظمة إلى المخاطر المختلفة إلى: نقص التدريب بين الموظفين الذى يؤدى إلى سوء فهم وسوء استخدام النظام، وعدم إدراك الموظفين لخطورة هجوم الفيروسات على أنظمة المعلومات؛ حيث ينظر إليها على أنها لا تشكل أى خطر على النظام.

وقد قامت جمعية الرقابة والمراجعة على نظم المعلومات ISACA بإجراء دراسة عن المخاطر المتعلقة بتكنولوجيا المعلومات (COBIT 5 for Risk) وتم تعريف مخاطر تكنولوجيا المعلومات على أنها "مخاطر الأعمال، وتحديدًا مخاطر الأعمال المرتبطة باستخدام وملكية وتشغيل ومشاركة وتأثير وتبنى تكنولوجيا المعلومات التى يمكن أن تؤثر على الأعمال التجارية داخل الشركة". (ISACA, 2013).

ووفقًا لتلك الدراسة تم تصنيف مخاطر تكنولوجيا المعلومات إلى ثلاث مجموعات على النحو التالى:

١) **مخاطر إضافة قيمة/ فائدة لتكنولوجيا المعلومات IT Benefit/Value Enablement Risk:** وهى تلك المخاطر المتعلقة بالفرص الضائعة لاستخدام تكنولوجيا المعلومات فى تحسين كفاءة أو فعالية العمليات التجارية.

٢) **مخاطر تقديم مشروع وبرامج تكنولوجيا المعلومات IT Programme and Project Delivery Risk:** وهى تلك المخاطر المتعلقة بمساهمة تكنولوجيا المعلومات فى تقديم حلول جديدة أو تحسين حلول قائمة لمشاكل الأعمال التجارية، ويكون ذلك عادة فى شكل مشاريع أو برامج كجزء من المحافظ الاستثمارية.

٣) **مخاطر عمليات تكنولوجيا المعلومات وتقديم الخدمات IT Operations and Service Delivery Risk:** وهي تلك المخاطر المتعلقة بجميع جوانب أداء نظم وخدمات تكنولوجيا المعلومات والتى يمكن أن تؤثر سلبيًا (بالتدمير أو التخفيض) على قيمة الشركة.

(٢/١/٢) دراسات سابقة متعلقة بحوكمة أمن المعلومات:

تناولت العديد من الدراسات السابقة حوكمة أمن المعلومات كإطار عام يمكن تطبيقه فى الشركات المختلفة، مع توضيح المميزات التى يمكن أن تحققها الشركات من وراء تطبيقها، فقد استهدفت دراسة (Solms, 2005) اختبار التوافق بين الاستخدام المتكامل لكل من الـ ISO 17799, COBIT كآليات لإدارة أمن المعلومات، وتوصلت الدراسة إلى أن كلاً من الإطارين السابقين يوفر محتوى أكثر فائدة لتطبيق بيئة شاملة وموحدة لحوكمة أمن المعلومات؛ حيث يوفر الـCOBIT إرشادات جيدة لماهية حوكمة أمن المعلومات، بينما يوفر الـ ISO 17799 المزيد من التفاصيل اللازمة لكيفية تطبيق تلك الحوكمة.

كما استهدفت دراسة (Ohki et al., 2009) تقديم إطار عمل موحد لحوكمة أمن المعلومات يجمع بين العديد من برامج أمن المعلومات الموجودة بالشركات اليابانية، وتوصلت الدراسة إلى أن نموذج حوكمة أمن المعلومات يتكون من توجيه، ورصد، وتقييم، ومراقبة، والتقرير عن أنشطة أمن المعلومات، كما يجب أن يشتمل هذا النموذج على تغطية وظائف أمن المعلومات التى لا يتم تطبيقها بتلك الشركات، ويتوقف ذلك على الهيكل التنظيمى للشركات وتبادل الأدوار والمسئوليات.

أما دراسة (Abu Musa, 2010) فقد قامت باختبار وجود وتطبيق حوكمة أمن المعلومات فى المنظمات السعودية، وتقييم الوضع الحالى والملامح الرئيسية لحوكمة أمن المعلومات فى البيئة

السعودية، وتوصلت الدراسة إلى أنه على الرغم من أن غالبية المنظمات السعودية تدرك أهمية حوكمة أمن المعلومات كعامل مكمل لنجاح تكنولوجيا المعلومات وحوكمة الشركات، فإنه لم يتم التعرف بوضوح على الأدوار والمسئوليات الخاصة بأمن المعلومات، كما أن المنظمات السعودية ليس لديها استراتيجيات أو سياسات أمن معلومات واضحة ومكتوبة، وليس لديها خطط التعافى من الكوارث للتعامل مع حوادث أمن المعلومات وحالات الطوارئ، ولا يتم تنفيذ إجراءات تقييم المخاطر بشكل كافٍ وفعال.

وفحصت دراسة (Bahl & Wali, 2014) تصورات القائمين على توفير خدمات البرمجيات الهندية بشأن حوكمة أمن المعلومات، وتأثيرها على جودة خدمات أمن المعلومات المقدمة للعملاء، وتم التطبيق على موظفى شركات خدمات التعهيد Outsourced Service فى الهند، وقد توصلت الدراسة إلى أن شركات خدمات تعهيد تكنولوجيا المعلومات والتى تعمل على تقديم خدمات البرمجيات يكون لها تأثير جوهرى وهام على جودة الخدمة وأمن المعلومات – التى يمكن التنبؤ بها–، بالإضافة إلى وجود علاقة إيجابية بين عناصر حوكمة أمن المعلومات (مجتمعة) وبين جودة خدمات أمن المعلومات.

(٢/٢) تحليل وتقييم عام للدراسات السابقة:

توصلت الدراسات السابقة إلى نتائج هامة تؤكد على أهمية الاتجاه إلى حوكمة أمن المعلومات كمنهج شامل للتعامل مع المخاطر الناتجة عن استخدام تكنولوجيا المعلومات داخل الشركات المختلفة بصفة عامة، ومع مخاطر نظم المعلومات المحاسبية الإلكترونية على وجه الخصوص. ومن استعراض الدراسات السابقة يمكن للباحثين استنتاج ما يلى:

١- تتعدد صور المخاطر التى تواجه نظم المعلومات المحاسبية الإلكترونية ما بين **مخاطر داخلية** يتمثل أهمها فى: إدخال متعمد / غير متعمد للبيانات من قِبَل الموظفين، وتدمير متعمد / غير متعمد للبيانات من قِبَل الموظفين، وإدخال فيروسات لبرامج التشغيل، وتبادل كلمات السر، والدخول غير المصرح به لملفات بها معلومات سرية، وعرض البيانات السرية على شاشات العرض. **ومخاطر خارجية** يتمثل أهمها فى: الاختراقات – سرقة البيانات والمعلومات السرية واستخدامها فى الاستيلاء على الأموال–، وإدخال البرامج الخبيثة كالفيروسات وأحصنة طروادة والديدان و...غيرها من البرامج التى من شأنها تعطيل النظام، وتخريب الشبكات.

٢- تتمثل أسباب حدوث المخاطر فى: نقص تدريب الموظفين على استخدام وحماية نظم المعلومات، وسوء اختيارهم، وعدم وجود إجراءات وضوابط كافية تعمل على معالجة والوقاية من حدوث المخاطر، وعدم متابعة التطورات الحديثة فى مجال تكنولوجيا المعلومات والجرائم المرتبطة بها.

٣- أن المخاطر الداخلية تُعد من أكثر المخاطر تهديدًا لنظم المعلومات المحاسبية الإلكترونية؛ حيث إنها تُعد فى الأساس مشكلة أفراد على علم تام بالنظام ونقاط القوة والضعف به، وأن إهمال التعامل معها والعمل على الوقاية منها قد يؤدى إلى تعرض الشركات لبعض الأضرار المحتملة مثل خسائر فى الإيرادات، أو خسارة فى سمعة الشركة أو الملكية الفكرية، ومن ثم فإن الحلول والإجراءات

التكنولوجية لا تكفى وحدها لمواجهة تلك المخاطر، وبالتالى يجب على الشركات اتباعُ منهجٍ متكاملٍ لإدارة أمن المعلومات بحيث يقوم على تقييم التكنولوجيا المستخدمة داخل الشركة، وتقييم سلوكيات الأفراد، والاهتمام بالجوانب التنظيمية؛ حتى يسهل التنبؤ بالمخاطر الداخلية وإحباط أى محاولة للقيام بها. **ويرى الباحثان** أن حوكمة أمن المعلومات هى أكثر المداخل التى توفر تحقيق تلك الأهداف.

٤- تعمل حوكمة أمن المعلومات على توفير إطار للرقابة لضمان أن المخاطر التى تتعرض لها نظم المعلومات يتم الوصول بها إلى المستوى المسموح به، كما تعمل على التأكيد بأن استراتيجيات الأمن التى تتبعها الشركة تتفق مع الأهداف الاستراتيجية.

٥- يتم تطبيق حوكمة أمن المعلومات من خلال مجموعة من المعايير الدولية المقبولة قبولاً عامًا، والتى تتفق مع استراتيجيات الأعمال فى الشركات المختلفة. ويتم تحديث تلك المعايير بصفة دورية لتتوافق مع التطورات فى البيئة التكنولوجية الحديثة؛ حيث أصدرت مؤخرًا المنظمة الدولية للمعايير (ISO) مجموعة من المعايير الخاصة بأمن المعلومات تعرف بـISO 27K، كما أصدرت جمعية الرقابة والمراجعة على نظم المعلومات (ISACA) النسخة الخامسة من COBIT.

٦- هناك نقص فى الدراسات السابقة على المستوى العالمى عمومًا والعربى تحديدًا التى تناولت قياس أثر استخدام حوكمة أمن المعلومات على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية من خلال تطبيق المعايير التى صدرت حديثًا، وقد يرجع ذلك إلى حداثة تلك المعايير، بالإضافة إلى أن الدراسات التى تناولت هذا الموضوع تمت فى بيئات أجنبية.

(٣) القسم الثالث: إطار عام لحوكمة أمن المعلومات:

(١/٣) العلاقة بين حوكمة أمن المعلومات وحوكمة الشركات:

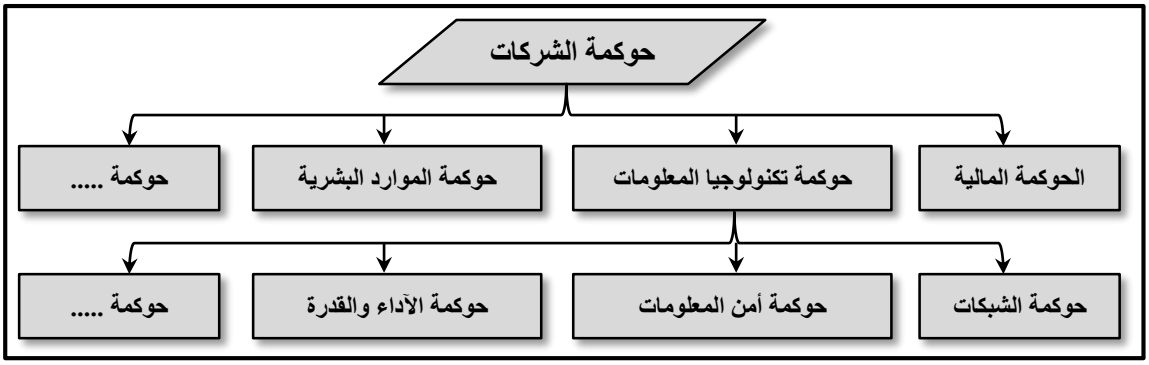
تمثل الحوكمة بشكل عام اصطلاحًا يعنى "نظام للمراقبة بصورة متكاملة وعلنية تدعيمًا للشفافية والموضوعية والمسئولية" (مزريق ومعموى، ٢٠١٢)، ومن ثم يمكن تعريف "حوكمة الشركات" بشكل مبسط على أنها "نظام يتم به إدارة ومراقبة الشركات". وقد تم تعريف حوكمة الشركات طبقًا لدليل قواعد ومعايير حوكمة الشركات بجمهورية مصر العربية فى فبراير ٢٠١١ على أنها "مجموعة القواعد والنظم والإجراءات التى تحقق أفضل حماية وتوازن بين مصالح مديرى الشركات والمساهمين فيها وأصحاب المصالح الأخرى المرتبطة بها".

ويقوم كل من مجلس الإدارة والإدارة التنفيذية للشركة بتطبيق مبادئ وآليات حوكمة الشركات للتأكد من تحقق الأهداف الاستراتيجية للشركة، وأن المخاطر يتم إدارتها، وأن موارد الشركة يتم استخدامها بشكل مسئول (Baydoun et al., 2013).

وتنقسم حوكمة الشركات عند القيام بتطبيقها إلى أنواع فرعية من الحوكمة مثل: الحوكمة المالية، وحوكمة الموارد البشرية، وحوكمة تكنولوجيا المعلومات، و... غيرها (Von Solms, 2007).

ومن ثم تعتبر حوكمة تكنولوجيا المعلومات جزءً مكملاً لحوكمة الشركات، وتهدف إلى استخدام تكنولوجيا المعلومات بشكل استراتيجى لتحقيق المهام التنظيمية وتحقيق منافسة فعالة، كما تعمل على ضمان التأكيد بأن مصادر تكنولوجيا المعلومات فى الشركة يتم إدارتها بفعالية (Romney & Steinbart, 2012). ويمكن تعريف حوكمة تكنولوجيا المعلومات (Juiz et al., 2014) على أنها "القدرة التنظيمية التى يمارسها كل من مجلس الإدارة والإدارة التنفيذية وإدارة تكنولوجيا المعلومات لإحكام الرقابة على صياغة وتنفيذ استراتيجية تكنولوجيا المعلومات، وذلك لضمان التأكد من اندماج أهداف إدارة تكنولوجيا المعلومات مع باقى الإدارات بالشركة"، وبالتالى فإن حوكمة تكنولوجيا المعلومات تعتبر عملية لاستخدام موارد تكنولوجيا المعلومات بكفاءة وفعالية وبشكل استراتيجى؛ وذلك لتحقيق المهام التنظيمية وتحقيق منافسة فعالة (Romney & Steinbart, 2012).

وتنقسم حوكمة تكنولوجيا المعلومات إلى أنواع فرعية من الحوكمة مثل: حوكمة الأداء والقدرة، وحوكمة الشبكات، وحوكمة أمن المعلومات، و...غيرها (Von Solms, 2007). ويوضح الشكل التالى العلاقة بين كل من: حوكمة أمن المعلومات، وحوكمة تكنولوجيا المعلومات، وحوكمة الشركات (Solms & Solms, 2009):



شكل رقم (١) العلاقة بين حوكمة أمن المعلومات وحوكمة الشركات

ويرى الباحثان أن حوكمة أمن المعلومات تعتبر من أهم مكونات حوكمة تكنولوجيا المعلومات، وهى أيضًا مجموعة فرعية من حوكمة الشركات. وتظهر العلاقة بين كل من حوكمة الشركات وحوكمة تكنولوجيا المعلومات وحوكمة أمن المعلومات بشكل واضح من خلال أن حوكمة الشركات تشتمل على جميع جوانب الحوكمة التى تتعامل مع كل أنواع المخاطر التى تتعرض لها الشركة، بالإضافة إلى أن المديرين التنفيذيين للشركات هم المسئولون عن تطبيق حوكمة الشركات بجميع فروعها.

(٢/٣) حوكمة أمن المعلومات – المفهوم والأهداف:

تعرف حوكمة أمن المعلومات بأنها "مجموعة من المسئوليات والممارسات التى يقوم بها مجلس الإدارة، والإدارة التنفيذية بهدف توفير اتجاه نحو استراتيجية لأمن المعلومات وضمان تحقيق أهدافها والتأكد من أن مخاطر أمن المعلومات يتم إدارتها بصورة ملائمة، وكذلك التأكد من أن موارد أمن المعلومات يتم استخدامها بشكل فعال" (Abu-Musa, 2010). كما يمكن تعريفها على أنها "عنصر أساسى لحوكمة الشركات يتكون من القيادة والهياكل التنظيمية والعمليات المشاركة فى حماية الأصول

المعلوماتية، ومن خلالها يمكن للشركات معالجة قضايا أمن المعلومات من منظور حوكمة الشركات" (IT Governance Institute, 2006).

وتهدف حوكمة أمن المعلومات إلى إنشاء وصيانة بيئة رقابية مناسبة للحفاظ على سرية وسلامة (تكامل) وتوافر المعلومات، ودعم العمليات والنظم الخاصة بها، وأيضًا حماية المعلومات من مختلف المخاطر التى يمكن أن تواجهها (Abu-Musa, 2010). ومن ثم تحقق حوكمة أمن المعلومات العديد من المنافع للشركات التى تقوم بتطبيقها، وتتمثل أهم تلك المنافع فيما يلى (Whitman & Mattord, 2013):

١- زيادة قيمة أسهم الشركات التى تطبق ممارسات الحوكمة.

٢- زيادة القدرة على التنبؤ، وتخفيض حالة عدم التأكد من خلال تحديد المخاطر المتعلقة بأمن المعلومات والعمل على تخفيضها إلى مستويات مقبولة.

٣- الحماية من إمكانية زيادة المسئولية المدنية أو القانونية؛ والناتجة عن عدم دقة المعلومات أو عدم بذل العناية الواجبة.

٤- تحسين وتعزيز تخصيص الموارد الأمنية المحدودة.

٥- ضمان وضع سياسة فعالة لأمن المعلومات، والالتزام بتلك السياسة.

٦- إدارة المخاطر بكفاءة وفعالية، وتحسين العمليات، والاستجابة السريعة للحوادث المتعلقة بأمن المعلومات.

٧- توفير مستوى من التأكيد على أن اتخاذ القرارات الحاسمة والهامة لا يستند على معلومات غير صحيحة ومضللة.

وبالإضافة إلى ما سبق فإن حوكمة أمن المعلومات تؤدى إلى إضافة قيمة للشركة (ITGI, 2006) من خلال: تحسين الثقة فى العلاقات مع العملاء، وحماية سمعة الشركة، وتقليل احتمالات انتهاك الخصوصية، وتوفير قدر أكبر من الثقة عند التعامل مع الأطراف الخارجية، وإيجاد وتوفير طرق جديدة وأفضل لمعالجة المعاملات الإلكترونية، وتقليل التكاليف التشغيلية عن طريق توفير نتائج يمكن التنبؤ بها، والتقليل من عوامل الخطر التى قد تؤدى إلى إيقاف العمليات.

ومما سبق يرى الباحثان أن حوكمة أمن المعلومات الجيدة تحقق العديد من الفوائد للشركات التى تقوم بتطبيقها، وأن تلك الفوائد ليست مجرد تخفيض المخاطر أو الحد من تأثير إجراءات خاطئة، ولكن حوكمة أمن المعلومات يمكن أن تؤدى إلى تحسين الثقة داخل وخارج الشركة، وتحسين سمعة الشركة، وكذلك تحسين الكفاءة فى أداء المهام المختلفة من خلال تجنب إهدار الوقت والجهد اللازمين لخروج الشركة من أى حادث أمنى.

وتتبع أهمية حوكمة أمن المعلومات من قيام أمن المعلومات بتغطية جميع عمليات المعلومات المادية والإلكترونية؛ حيث تقوم بحماية المعلومات وسرية وتوافر (الإتاحة) ونزاهة المعلومات فى جميع مراحل دورة حياة المعلومات واستخدامها داخل الشركة. ويتطلب ذلك استراتيجية أمنية شاملة مرتبطة

بشكل مباشر وصريح بعمليات الأعمال واستراتيجية الشركة، وبحيث تحتوى على عناصر وبنود شاملة لكل العمليات والسياسات المتعلقة بالنواحى التكنولوجية والمادية داخل الشركة (ITGI, 2006).

(٣/٣) معايير حوكمة أمن المعلومات:

تم وضع العديد من المعايير الأمنية لتوفير التوجيه اللازم وضمان وجود مستوى معين من الحماية للمعلومات، بالإضافة إلى التأكد من أن كافة العناصر ذات الصلة بالأمن تتم معالجتها فى استراتيجية الأمن داخل الشركة؛ والتأكد من أن الموارد الإلكترونية للشركة يتم استخدامها بشكل مسئول. ومن المعايير الدولية الأكثر استخدامًا فى مجال أمن المعلومات ما يلى:

(١/٣/٣) معايير الأيزو ISO/IEC 27K:

هى سلسلة من المعايير التى أصدرتها المنظمة الدولية للمعايير (ISO) وتم تطويرها بالتعاون مع اللجنة الكهروتقنية الدولية (IEC)، وهى معايير متعلقة بأمن المعلومات وتعمل على تقديم الإرشادات المقبولة عامة بشأن الممارسات الجيدة لأنظمة إدارة أمن المعلومات المصممة لحماية سرية وسلامة وتوافر محتوى المعلومات ونظم المعلومات (حب الله، ٢٠٠٩). ومن أهم تلك المعايير والتى صدرت حديثًا (ISS, 2014):

أ) **معيار (ISO/IEC 27001:2013):** تم تعديل هذا المعيار وأُصدِرَ فى سبتمبر ٢٠١٣، وهو يحدد بشكل رسمى المتطلبات الإلزامية لنظام إدارة أمن المعلومات، كما يوفر هذا المعيار إطارًا للإدارة الشاملة الذى تقوم الشركة من خلاله بتحديد ومعالجة المخاطر الأمنية للمعلومات، ويضمن أن الترتيبات الأمنية تم ضبطها بدقة لمواكبة التغييرات الأمنية التى تحدث واكتشاف نقاط الضعف.

ب) **معيار (ISO/IEC 27002:2013):** يُعَرف هذا المعيار فى السابق بـISO 17799، وتم تعديله فى عام ٢٠٠٥ ثم فى عام ٢٠١٣ ليظهر بهذه الصورة، وهو معيار يوضح الممارسات الجيدة لأمن المعلومات، ويعمل على تقديم إرشادات توجيهية مفصلة حول كيفية تنفيذ إطار إدارة الأمن، وكيفية الالتزام بالقوانين واللوائح والمعايير. ويتعلق هذا المعيار بأمن جميع أشكال المعلومات مثل بيانات الكمبيوتر والوثائق والمعرفة والملكية الفكرية، وليس فقط أمن تكنولوجيا المعلومات (Nemati, 2013).

ج) **معيار (ISO/IEC 27016:2014):** أُصدِرَ هذا المعيار فى ٢٠١٤، ويهدف إلى تقديم المبادئ التوجيهية القائمة على الممارسات الجيدة المقبولة عمومًا، والتى يمكن استخدامها وفهمها من قِبَل أصحاب الخبرة فى مجال أمن المعلومات والمديرين، وذلك لمناقشة الخطوات الإجرائية والبدائل المتاحة لبرنامج أمن المعلومات من حيث النتائج المالية المتوقعة. وبمعنى آخر فإن هذا المعيار يهدف إلى تقديم مبادئ توجيهية حول كيفية قيام الشركات باتخاذ قرارات لحماية أمن المعلومات وفهم النتائج الاقتصادية لهذه القرارات فى إطار متطلبات التنافس على الموارد.

د) **معيار (ISO/IEC 27038:2014):** أُصدِرَ هذا المعيار فى مارس ٢٠١٤، ويسمى أيضًا بمعيار التنقيح "Redaction" ويعنى إبعاد المعلومات الحساسة – مثل أسماء ومواقع يجب أن تظل مجهولة، ومختلف المعلومات الشخصية أو الملكية الأخرى التى يجب أن تبقى سرية للغاية – من

داخل الملفات الأصلية حتى لا يتم نشرها لأطراف ثالثة أو لعامة الناس. ويهدف هذا المعيار إلى تحديد الخصائص التكنولوجية للقيام بعملية التنقيح الرقمى على الوثائق الرقمية، كما يحدد متطلبات أدوات برامج التنقيح، وطرق الفحص والاختبار التى تمت على عمليات التنقيح الرقمى التى تم الانتهاء منها بشكل آمن.

(٢/٣/٣) معيار COBIT 5:

يعتبر COBIT (أهداف الرقابة على المعلومات والتكنولوجيا ذات الصلة) مجموعة من أفضل الممارسات لإدارة تكنولوجيا المعلومات والتى تم إنشاؤها بواسطة معهد حوكمة تكنولوجيا المعلومات (ITGI) وتطويرها بالتعاون مع جمعية الرقابة والمراجعة على أنظمة المعلومات ISACA، ويهدف COBIT إلى دعم مجموعة من الأدوات تتيح للمديرين سد الفجوة بين متطلبات الرقابة والقضايا التكنولوجية ومخاطر الأعمال، كما يتيح تطوير سياسة واضحة وممارسات جيدة للرقابة على تكنولوجيا المعلومات، ويؤكد على الالتزام بالقوانين التنظيمية ويساعد الشركات على زيادة القيمة التي تحصل عليها من استخدام تكنولوجيا المعلومات، وأخيرًا يعمل على المواءمة وتبسيط تنفيذ تكنولوجيا المعلومات وإطار الرقابة عليها (ISACA).

وبعد إصدار النسخة الخامسة من COBIT من قِبَل ISACA فى عام ٢٠١٣، والتى تعتبر أداة فعالة لإدارة المقاييس الأمنية والعمليات والمراقبة الأمنية والمؤشرات اللازمة لدعم برامج الحماية، وتشتمل النسخة الخامسة COBIT 5 على مجموعة من الإصدارات لتوفير توجيهات وإرشادات إضافية حول العوامل المساعدة ضمن إطار الـCOBIT، وكيفية قيام المتخصصين باستخدام الـCOBIT فى توصيل خدمات تكنولوجيا المعلومات (Stroud, 2012)، وتنقسم تلك الإصدارات إلى مجموعتين هما:

- COBIT 5 دليل المساعدة: وتحتوى هذه المجموعة على COBIT 5 لتمكين العمليات، COBIT 5 لتمكين المعلومات.
- COBIT 5 دليل المتخصصين: وتحتوى هذه المجموعة على:

COBIT 5 للتطبيق، COBIT 5 لأمن المعلومات، COBIT 5 للتأكيد، COBIT 5 للمخاطر، COBIT 5 لتقييم البرنامج.

ويقدم معيار COBIT 5 لأمن المعلومات إطارًا يحتوى على جميع جوانب التأكد من معقولية ومناسبة موارد أمن المعلومات التى يتم إنشاؤها على مجموعة من المبادئ التى يجب أن تقوم الشركة بوضعها، واختبار سياسات الأمن والمعايير والإرشادات والعمليات والرقابة عليها، كما يوفر إطارًا شاملاً لإجراء تكامل بين الأمن والعمليات التجارية بالشركة (الأمن المادى)، ويقدم مجموعة من العوامل التى تساعد على التأكد من رضا أصحاب المصالح، وعلى تشغيل الأعمال بكفاءة داخل الشركة (Olzak, 2013).

(٣/٣/٣) معيار Information Technology Infrastructure Library (ITIL):

يعتبر معيار ITIL (مكتبة البنية التحتية لتكنولوجيا المعلومات) من أكثر المناهج قبولاً فى العالم لإدارة خدمات تكنولوجيا المعلومات، تم وضعه من قِبَل مكتب التجارة الحكومى فى المملكة

المتحدة، وهو عبارة عن مجموعة من الإرشادات لأفضل الممارسات فى مجال إدارة خدمات تكنولوجيا المعلومات؛ فهو يصف العمليات والوظائف والهياكل التى تعمل على تدعيم خدمات تكنولوجيا المعلومات من وجهة نظر مقدمى الخدمة. ويعتبر أمن المعلومات واحدًا من العديد من العمليات التى يصفها معيار ITIL (Clinch, 2009).

ويتكون معيار ITIL من ثمانية جوانب رئيسية هى: دعم الخدمة، وتوصيل الخدمة، وإدارة البنية التحتية لتكنولوجيا المعلومات والاتصالات، وإدارة الأمن، وإدارة التطبيقات، وإدارة الأصول (البرمجيات)، والتخطيط لتنفيذ إدارة الخدمات، والتنفيذ على نطاق صغير (Susanto et al., 2011).

ومما سبق يرى الباحثان أن قيام الشركات بتطبيق معايير حوكمة أمن المعلومات متمثلة فى معايير الأيزو (ISO/IEC 27K)، ومعيار COBIT 5، ومعيار ITIL كإطار عمل متكامل لحوكمة أمن المعلومات – حيث لا يمكن لأحد تلك المعايير منفردًا أن يفى باحتياجات ومتطلبات الشركة فى تحقيق أهدافها – سوف يحقق لها العديد من الفوائد والمميزات وتحقيق للأهداف الاستراتيجية المرجوة من تطبيق حوكمة أمن المعلومات وهى الحد من المخاطر التى تتعرض لها أنظمة المعلومات الإلكترونية بصفة عامة وأنظمة المعلومات المحاسبية الإلكترونية على وجه التحديد، وتحقيق رؤية وأهداف الشركة الاستراتيجية.

وبناءًا على ما سبق يقوم الباحثان بإجراء دراسة ميدانية على البيئة المصرية لاستطلاع الآراء حول مدى إمكانية تأثير معايير حوكمة أمن المعلومات فى الحد من المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية.

(٤) القسم الرابع: الدراسة الميدانية:

تتمثل مقومات الدراسة الميدانية فيما يلى:

(١/٤) هدف الدراسة:

يتمثل الهدف الرئيسى من هذه الدراسة فى تحليل أثر استخدام المعايير المختلفة لحوكمة أمن المعلومات على الحد من المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية، ويتطلب تحقيق هذا الهدف التوجه نحو الكشف عما يلى:

١- الأهمية النسبية للمخاطر المختلفة التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى المنظمات المصرية.
٢- أسباب حدوث المخاطر المختلفة التى تهدد أمن المعلومات المحاسبية الإلكترونية.
٣- مدى استخدام المنظمات المصرية لحوكمة أمن المعلومات فى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.
٤- التعرف على أكثر معايير حوكمة أمن المعلومات تأثيرًا على الحد من المخاطر.

(٢/٤) فروض الدراسة:

لتحقيق أهداف الدراسة يتم اختبار الفروض التالية:

١- تختلف الأهمية النسبية للمخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية.

٢- يؤدى عدم وجود سياسات وبرامج محددة لأمن المعلومات إلى زيادة المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية.

٣- تعمل المنظمات المصرية على تطبيق حوكمة أمن المعلومات فى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.

٤- يوجد اختلاف معنوى فى تأثير معايير حوكمة أمن المعلومات بشكل مستقل على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.

(٣/٤) تصميم الدراسة:

تقوم الدراسة على استخدام ثلاثة متغيرات مستقلة يتوقع أن يكون لها تأثير على مخاطر أمن نظم المعلومات المحاسبية الإلكترونية، تتمثل فى معايير حوكمة أمن المعلومات وهى: معايير الأيزو، ومعيار COBIT، ومعيار ITIL، بينما تتمثل المتغيرات التابعة فى المخاطر المختلفة لأمن نظم المعلومات المحاسبية الإلكترونية، **ويحاول الباحثان** دراسة تأثير كل متغير مستقل (معايير حوكمة أمن المعلومات) على المتغيرات التابعة (المخاطر المختلفة لنظم المعلومات المحاسبية الإلكترونية).

وقد قام الباحثان باستخدام قائمة استقصاء كأداة لجمع البيانات اللازمة لاختبارات الفروض احصائيًا، وذلك من خلال المقابلات الشخصية لمفردات العينة، كما تم شرح طبيعة مشكلة الدراسة والهدف منها فى بعض الحالات التى استلزمت ذلك، وقد راعى الباحثان عند تصميم القائمة تنوع الأسئلة؛ فبعض الأسئلة يتم الإجابة عليها بـ(نعم) أو (لا)، والبعض الأخر يتم الإجابة عنها باستخدام مقياس ليكرت الخامسى، كما اشتملت القائمة على بعض الأسئلة المفتوحة لمعرفة المزيد من آراء المستقصى منهم والتوجهات الاستراتيجية للشركات التى يعملون بها.

(٤/٤) مجتمع وعينة الدراسة:

يتكون مجتمع الدراسة من شركات الاتصالات، وشركات تكنولوجيا المعلومات، والبنوك العاملة فى القرية الذكية بجمهورية مصر العربية. وقد تم اختيار عينة عشوائية ممثلة لمجتمع الدراسة من تلك الشركات والبنوك بلغ عددها خمس شركات لتكنولوجيا المعلومات بواقع ٨٠ استمارة، وسبع شركات اتصالات بواقع ١٠٠ استمارة، وأربعة بنوك بواقع ١٢٠ استمارة، وقد تم توزيع استمارات الاستقصاء داخل تلك الشركات والبنوك على الفئات الآتية:

١- المديرين الماليين والمحاسبين بإعتبارهم القائمين على التعامل مع نظم المعلومات المحاسبية الإلكترونية.

٢- الموظفين فى إدارة تكنولوجيا المعلومات من متخصصين، ومراجعى نظم معلومات إلكترونية، ومديرى إدارات.

٣- المراجعين الخارجيين الذين يقومون بمراجعة أنظمة تلك الشركات والبنوك.

ويمكن توضيح التوزيع النسبى لمفردات العينة من خلال الجدول التالى:

جدول رقم (١) التوزيع النسبى لاستمارات الاستقصاء على مفردات العينة

مفردات العينة	العدد	النسبة
شركات تكنولوجيا المعلومات	٨٠	%٢٧
شركات الاتصالات	١٠٠	%٣٣
البنوك	١٢٠	%٤٠
الإجمالى	**٣٠٠**	**%١٠٠**

(٥/٤) إدخال ومعالجة البيانات:

قام الباحثان بمراجعة استمارات الاستقصاء للتأكد من اكتمالها وصلاحيتها لإدخال البيانات والتحليل الإحصائى، وتم استبعاد الاستمارات التى لا تتوافر فيها الشروط اللازمة. ويوضح الجدول التالى عينة الدراسة ومعدلات الإجابة الصحيحة القابلة للتحليل من بين مفردات العينة.

جدول رقم (٢) عدد الاستمارات المرسلة، والواردة والمستبعدة والصحيحة

مفردات العينة	المرسل	الوارد		المستبعد		الصحيح	
		العدد	النسبة	العدد	النسبة	العدد	النسبة
شركات تكنولوجيا المعلومات	٨٠	٦٧	%٨٤	١٧	%٢١	٥٠	%٦٣
شركات الاتصالات	١٠٠	٧٨	%٧٨	٢٠	%٢٠	٥٨	%٥٨
البنوك	١٢٠	٩٨	%٨٢	٩	%٧،٥	٨٩	%٧٤
الإجمالى	**٣٠٠**	**٢٤٣**	**%٨١**	**٤٦**	**%١٥**	**١٩٧**	**%٦٦**

(٦/٤) أساليب التحليل الإحصائى للبيانات:

قام الباحثان بتفريغ الإجابات على الأسئلة بجداول البيانات، وتم تحليلها بهدف تحديد مدى تحقق فروض الدراسة واستخلاص النتائج من خلال تطبيق بعض الأساليب الإحصائية الواردة بمجموعة البرامج الإحصائية للعلوم الاجتماعية (SPSS) وتحديدًا تم الاستعانة بالأساليب التالية:

- **أساليب الإحصاء الوصفى:**
  - ١- الوسط الحسابى Mean
  - ٢- الانحراف المعيارى Standard Deviation
  - ٣- التكرار والنسبة Frequency & Percent
- **أساليب الإحصاء الاستدلالى:**
  - ١- اختبار المصداقية والاعتمادية Reliability Analysis
  - ٢- اختبار "ت" T. Test
  - ٣- اختبار فريدمان Friedman Test
  - ٤- اختبار كروسكال والاس Kruskal-Wallis Test
  - ٥- اختبار "كا^{٢}" Chi Square

(٧/٤) نتائج الاختبارات الإحصائية لفروض الدراسة:

(١/٧/٤) اختبار الثبات والصدق:

ويطلق عليه معامل ثبات (ألفا) Cronbatch Alpha، وهو مقياس يوضح مدى الاعتماد على نتائج قائمة الاستقصاء، ومدى إمكانية تعميم النتائج على مجتمع الدراسة، وكذلك يوضح ثبات المحتوى لمتغيرات الدراسة.

وقد بلغت قيمة معامل الثبات للاستمارة ككل ٠،٩٨٥، ومعامل الصدق – وهو الجذر التربيعى لمعامل الثبات – ٠،٩٩١، مما يدل على ثبات أداة البحث ووجود درجة كبيرة من الاتساق الداخلى بين عبارات قائمة الاستقصاء ككل.

(٢/٧/٤) نتائج اختبار الفرض الأول:

ينص الفرض الأول على:

"تختلف الأهمية النسبية للمخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية"

أولاً: التحليل الوصفى:

تم استخدام تحليل التباين لتوصيف آراء العينة حول المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية من خلال المقاييس الإحصائية (الوسط الحسابى، واختبار "ت"، الانحراف المعيارى)، وذلك كما يوضحه الجدول رقم (٣) فيما يلى:

جدول رقم (٣) توصيف الآراء من خلال المقاييس الإحصائية حول المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية

السـؤال	العدد	الوسط الحسابى	الانحراف المعيارى	T.Test
١- إدخال غير متعمد لبيانات غير سليمة بواسطة الموظفين.	١٩٧	٤،٢٩	١،٠٩	٠،٠٠**
٢- إدخال متعمد لبيانات غير سليمة بواسطة الموظفين.	١٩٧	٢،٨٨	٠،٩٣	٠،٠٠**
٣- تدمير غير متعمد للبيانات بواسطة الموظفين.	١٩٧	٤،٢١	١،١٦	٠،٠٠**
٤- تدمير متعمد للبيانات بواسطة الموظفين.	١٩٧	٢،٩٤	٠،٩٨	٠،٠٠**
٥- دخول غير المصرح به للبيانات بواسطة الموظفين.	١٦٩	٤،٢٠	١،١٦	٠،٠٠**
٦- تبادل الموظفين لكلمات المرور.	١٩٧	٤،٠٨	١،٢٢	٠،٠٠**
٧- إدخال فيروسات الحاسب إلى النظام المحاسبى.	١٩٧	٤،٢١	١،٢٤	٠،٠٠**
٨- تدمير أو سرقة بعض المعلومات (مخرجات النظام).	١٩٧	٤،٠٨	١،٢٤	٠،٠٠**
٩- عمل نسخ غير مصرح بها من مخرجات النظام.	١٩٧	٤،٢٨	١،١٦	٠،٠٠**
١٠- عرض بيانات سرية على شاشات العرض.	١٩٧	٤،١٦	١،١٠	٠،٠٠**
١١- كوارث طبيعية مثل الحرائق أو انقطاع الطاقة.	١٩٧	٤،١٦	١،١٩	٠،٠٠**
١٢- مخاطر خارجية متمثلة فى البرامج الخبيثة والاختراقات و... غيرها.	١٩٧	٤،٤٠	١،٠٤	٠،٠٠**
الإجمالى	**١٩٧**	**٤**	**١،١٣**	

** دال إحصائيًا عند مستوى معنوية ٠،٠٥

ويتضح من الجدول السابق أن الوسط الحسابى العام يميل إلى الموافقة على أن العناصر التى تم ذكرها تمثل المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية، وذلك بوسط حسابى عام قيمته (٤)، وانحراف معيارى عام (١،١٣).

ومن ثم يشير الانحراف المعيارى إلى انخفاض التشتت أى يوجد تجانس فى الآراء حول تلك المخاطر، كما يشير اختبار "ت" إلى أن النتائج أقل من مستوى معنوية (٠،٠٥) بمعنى أن الفروق معنوية وجميع العناصر – بصفة عامة – تعتبر من المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية.

ثانياً: اختبار فريدمان:

يوضح هذا الاختبار الأهمية النسبية للعبارات أى معرفة العنصر الأكثر أهمية من وجهة نظر مفردات العينة بشأن المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية، وذلك من خلال متوسط الرتب حيث يأخذ العنصر الأكثر أهمية من وجهة نظر مفردات العينة أعلى متوسط للرتب ويتضح ذلك من خلال الجدول التالى:

جدول رقم (٤) ترتيب الأهمية النسبية للمخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية

البيـــان	متوسط الرتب	مستوى المعنوية
١- مخاطر خارجية متمثلة فى البرامج الخبيثة والاختراقات و...غيرها.	٨،٢٥	٠،٠٠**
٢- إدخال غير متعمد لبيانات غير سليمة بواسطة الموظفين.	٧،٧٤	
٣- عمل نسخ غير مصرح بها من مخرجات النظام.	٧،٥٧	
٤- إدخال فيروسات الحاسب إلى النظام المحاسبى.	٧،٤٠	
٥- تدمير غير متعمد للبيانات بواسطة الموظفين.	٧،٣٩	
٦- دخول غير مصرح به للبيانات بواسطة الموظفين.	٧،٢٨	
٧- كوارث طبيعية مثل الحرائق أو انقطاع الطاقة.	٧،١٠	
٨- عرض بيانات سرية على شاشات العرض.	٧،٠٢	
٩- تدمير أو سرقة بعض المعلومات (مخرجات النظام).	٦،٦٩	
١٠- تبادل الموظفين لكلمات المرور.	٦،٦٧	
١١- تدمير متعمد للبيانات بواسطة الموظفين.	٢،٥٢	
١٢- إدخال متعمد لبيانات غير سليمة بواسطة الموظفين.	٢،٣٥	

** دال إحصائيًا عند مستوى معنوية ٠،٠٥

ويتضح من الجدول السابق ما يلى:

١- أن مستوى المعنوية أقل من (٠،٠٥)، مما يدل على وجود اختلاف معنوى فى الأهمية النسبية من وجهة نظر مفردات العينة حول مخاطر نظم المعلومات المحاسبية الإلكترونية.

٢- أن أعلى متوسط للرتب يتمثل فى أن المخاطر الخارجية المتمثلة فى البرامج الخبيثة والاختراقات و.... غيرها تعد من أهم المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية، بينما يتمثل كل من التدمير المتعمد للبيانات، والإدخال المتعمد لبيانات غير سليمة من أقل المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية حيث إنها تأخذ أقل مستوى للرتب.

ثالثًا: اختبار كروسكال والاس:

ويتم إجراء هذا الاختبار لقياس التباين – الاتفاق والاختلاف – فى آراء مفردات العينة حول المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية، ويتضح ذلك من خلال الجدول التالى:

جدول رقم (٥) قياس التباين فى آراء مفردات العينة حول مخاطر نظم المعلومات المحاسبية الإلكترونية

البيـــان	مفردات العينة	العدد	متوسط الرتب	مستوى المعنوية
مخاطر أمن نظم المعلومات المحاسبية الإلكترونية	شركات تكنولوجيا المعلومات	٥٠	٩٨،٠١	٠،٤٩١
	شركات الاتصالات	٥٨	٩١،٨٦	
	البنوك	٨٩	١٠٣،١٠	

ويتضح من الجدول السابق أن مستوى المعنوية للعناصر الممثلة لمخاطر نظم المعلومات المحاسبية الإلكترونية مجتمعة أكبر من (٠،٠٥)، مما يعنى وجود اتفاق فى آراء مفردات العينة حول اختلاف الأهمية النسبية للمخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية.

وبناءً على نتائج التحليل السابق فقد ثبت صحة الفرض الأول للدراسة والذى ينص على: "**تختلف الأهمية النسبية للمخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية**".

(٣/٧/٤) نتائج اختبار الفرض الثانى:

ينص الفرض الثانى للدراسة على: "**يؤدى عدم وجود سياسات وبرامج محددة لأمن المعلومات إلى زيادة المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية**".

أولاً: التحليل الوصفى:

يوضح الجدول التالى توصيف آراء العينة بشأن أسباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية من خلال المقاييس الإحصائية الوسط الحسابى والانحراف المعيارى واختبار "ت":

جدول رقم (٦) توصيف الآراء حول أسباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية

البيـــان	العدد	الوسط الحسابى	الانحراف المعيارى	T.Test
١- عدم توافر الخبرة اللازمة والتدريب الكافى للموظفين.	١٩٧	٤،٢٢	١،٢٢	٠،٠٠**
٢- عدم توافر الحماية الكافية ضد مخاطر الفيروسات.	١٩٧	٤،٠٥	١،٢٢	٠،٠٠**
٣- عدم تحديد المسئوليات والصلاحيات لكل فرد داخل الهيكل التنظيمى.	١٩٧	٤،٢٠	١،١٥	٠،٠٠**
٤- عدم وجود سياسات وبرامج محددة لأمن نظم المعلومات.	١٩٧	٤،٢٨	١،١٤	٠،٠٠**
٥- عدم تطبيق مبادئ ومعايير حوكمة أمن المعلومات.	١٩٧	٤،٢٠	١،١٥	٠،٠٠**
الوسط الإجمالى	**١٩٧**	**٤،١٩**	**١،١٩**	

** دال إحصائيًا عند مستوى معنوية ٠،٠٥

ويلاحظ من الجدول السابق أن الوسط الحسابى العام يميل إلى الموافقة حول أسباب المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية، وذلك بوسط حسابى عام (٤،١٩)، وانحراف معيارى (١،١٩)، مما يشير إلى انخفاض التشتت أى يوجد تجانس فى الأراء بشأن تلك الأسباب، كما يشير اختبار "ت" إلى أن النتائج أقل من مستوى معنوية (٠،٠٥)، بمعنى أن الفروق معنوية وجميع العناصر تعتبر من ضمن الأسباب التى تؤدى إلى زيادة فى مخاطر نظم المعلومات المحاسبية الإلكترونية.

ثانياً: اختبار فريدمان:

يوضح الجدول التالى قياس وترتيب الأهمية النسبية لأسباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية:

جدول رقم (٧) ترتيب الأهمية النسبية حول أسباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية

البيـــان	متوسط الرتب	مستوى المعنوية
١- عدم وجود سياسات وبرامج محددة لأمن نظم المعلومات.	٣،٢٠	٠،٠٠**
٢- عدم توافر الخبرة اللازمة والتدريب الكافى للموظفين.	٣،٠٤	
٣- عدم تحديد المسئوليات والصلاحيات لكل فرد داخل الهيكل التنظيمى.	٣،٠١	
٤- عدم تطبيق مبادئ ومعايير حوكمة أمن المعلومات.	٢،٩٨	
٥- عدم توافر الحماية الكافية ضد مخاطر الفيروسات.	٢،٧٧	

** دال إحصائيًا عند مستوى معنوية ٠،٠٥

ويتضح من الجدول السابق ما يلى:

١- أن مستوى المعنوية أقل من (٠،٠٥)، مما يدل على وجود اختلاف معنوى فى الأهمية النسبية من وجهة نظر مفردات العينة بشأن أسباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية.

٢- أن أعلى متوسط للرتب يتمثل فى أن عدم وجود سياسات وبرامج محددة لأمن نظم المعلومات يُعد من أهم أسباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية، بينما يتمثل أقل متوسط للرتب فى عدم توافر الحماية الكافية ضد مخاطر الفيروسات.

ثالثًا: اختبار كروسكال والاس:

ويوضح الجدول التالى قياس التباين فى آراء مفردات العينة حول أسباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية:

جدول رقم (٨) قياس التباين فى آراء مفردات العينة حول أسباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية

البيـــان	مفردات العينة	العدد	متوسط الرتب	مستوى المعنوية
أسباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية	شركات تكنولوجيا المعلومات	٥٠	١٠٨،١٦	٠،٣٢٢
	شركات الاتصالات	٥٨	٩٨،٩٤	
	البنوك	٨٩	٩٣،٨٩	

ويتضح من الجدول السابق أن مستوى المعنوية لأسباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية أكبر من (٠،٠٥)، مما يعنى وجود اتفاق فى آراء مفردات العينة حول أسباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية.

وبناءً على نتائج التحليل السابق يتضح ثبوت صحة الفرض الثانى للدراسة والذى ينص على: "**يؤدى عدم وجود سياسات وبرامج محددة لأمن المعلومات إلى زيادة المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية**".

(٤/٧/٤) نتائج اختبار الفرض الثالث:

ينص الفرض الثالث للدراسة على: "**تعمل المنظمات المصرية على تطبيق حوكمة أمن المعلومات فى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية**".

<u>الأساليب الإحصائية المستخدمة:</u>

١- يتم استخدام اختبار "التكرار والنسبة"، حيث يوضح عدد آراء مفردات العينة حول الأسئلة محل الاستقصاء، ونسبة هذا العدد – وذلك كأحد أساليب الإحصاء الوصفى-.

٢- استخدام اختبار "كا^{٢}" لمعرفة الدلالة المعنوية لفروق التكرار – وذلك كأحد أساليب الإحصاء الاستدلالى-.

٣- استخدام اختبار "كروسكال والاس" لقياس التباين فى آراء مفردات العينة بشأن الإجابة عن الأسئلة محل الاختبار – وذلك كأحد أساليب الإحصاء الاستدلالى-.

يوضح الجدول التالى التوزيع التكرارى والنسبى، واختبار "كا^{٢}"، واختبار "كروسكال والاس" بشأن مدى قيام عينة الدراسة بتطبيق حوكمة أمن المعلومات:

جدول رقم (٩) التوزيع التكرارى والنسبى، واختبار "كا^{٢}"، واختبار "كروسكال والاس" حول مدى قيام العينة بتطبيق حوكمة أمن المعلومات

البيان	التكرار	النسبة	اختبار "كا^{٢}"		اختبار "كروسكال والاس"		
			مستوى المعنوية	الدلالة الإحصائية	مفردات العينة	متوسط الرتب	مستوى المعنوية
لا	١٤٣	٧٢،٦	٠،٠٠**	معنوى	شركات تكنولوجيا المعلومات	١٠١،٦٩	٠،٤٦**
نعم	٥٤	٢٧،٤			شركات الاتصالات	٩٩،٢٥	
الإجمالى	**١٩٧**	**١٠٠**			البنوك	٩٥،٤٤	

** دال إحصائيًا عند مستوى معنوية ٠،٠٥

ويتضح من الجدول السابق أن أكثر مفردات العينة لا تقوم بتطبيق حوكمة أمن المعلومات ضمن استراتيجيتها للحد من مخاطر نظم المعلومات المحاسبية الإلكترونية وذلك بنسبة ٧٢،٦% من إجمالى حجم العينة، عند مستوى معنوية أقل من (٠،٠٥)، مما يدل على وجود فروق ذات دلالة إحصائية فى آراء مفردات العينة، كما تبين من اختبار "كروسكال والاس" أن مستوى المعنوية أكبر من

(٠،٠٥) الأمر الذى يدل على وجود اتفاق بين آراء مفردات العينة بشأن عدم تطبيق الجهات التى يعملون بها لحوكمة أمن المعلومات.

والجدول التالى يوضح التوزيع التكرارى والنسبى، واختبار "كا٢"، واختبار "كروسكال والاس" بشأن قيام عينة الدراسة بتطبيق معايير دولية خاصة بأمن المعلومات.

جدول رقم (١٠) التوزيع التكرارى والنسبى، واختبار "كا٢"، واختبار "كروسكال والاس" حول مدى قيام العينة بتطبيق معايير دولية لأمن المعلومات

البيان	التكرار	النسبة	اختبار "كا٢"		اختبار "كروسكال والاس"		
			مستوى المعنوية	الدلالة الإحصائية	مفردات العينة	متوسط الرتب	مستوى المعنوية
لا	٩٤	٤٧،٧	٠،٠٠٠**	معنوى	شركات تكنولوجيا المعلومات	٩٦،٧٥	٠،٩٣
نعم	١٠٣	٥٢،٣			شركات الاتصالات	١٠٠،١٥	
الإجمالى	**١٩٧**	**١٠٠**			البنوك	٩٩،٥٢	

ويتضح من الجدول السابق أن نسبة ٥٢،٣% من إجمالى حجم العينة تقوم بتطبيق معايير دولية خاصة بأمن المعلومات، وذلك عند مستوى معنوية أقل من (٠،٠٥)، مما يدل على وجود فروق ذات دلالة إحصائية فى آراء مفردات العينة، كما يتضح من نتائج اختبار "كروسكال والاس" أن مستوى المعنوية أكبر من (٠،٠٥)، مما يدل على وجود اتفاق فى أراء مفردات العينة بشأن قيام العينة بتطبيق معايير دولية لأمن المعلومات.

والجدول التالى يوضح التوزيع التكرارى والنسبى، واختبار "كا٢" بشأن مدى تحقيق حوكمة أمن المعلومات للأهداف الاستراتيجية للشركة:

جدول رقم (١١) التوزيع التكرارى والنسبى حول تحقيق حوكمة أمن المعلومات للأهداف الاستراتيجية للشركة

البيـــان	التكرار	النسبة	اختبار "كا٢"
غير موافق	٤	٢	٠،٠٠٠**
محايد	٧	٣،٢	
موافق	١١	٥،٦	
موافق تمامًا	١٧٥	٨٨،٢	
الإجمـــالى	**١٩٧**	**١٠٠**	

** دال إحصائيًا عند مستوى معنوية ٠،٠٥

ويتضح من الجدول السابق أن إجابات مفردات العينة بشأن أهمية حوكمة أمن المعلومات ومدى تحقيقها للأهداف الاستراتيجية للشركة تميل إلى الموافقة بشكل كبير (موافق، وموافق تمامًا) وذلك بنسبة ٩٣،٨%، ومحايد بنسبة ٣،٢%، وغير موافق (غير موافق، وغير موافق على الإطلاق) بنسبة ٢%، وذلك عند مستوى معنوية أقل من (٠،٠٥)، مما يدل على أن هناك فروق ذات دلالة إحصائية فى آراء مفردات العينة.

ومن نتائج تحليل الاختبارات الإحصائية فى الجداول (٩، ١٠، ١١) **يتضح للباحثين** أن مفردات العينة مُدركة للأهمية التى تتحقق من تطبيق حوكمة أمن المعلومات وإدراجها ضمن الأجندة الاستراتيجية للشركة، ومع ذلك فإن نسبة كبيرة من العينة لا تقوم بتطبيق المبادئ والمعايير الخاصة بحوكمة أمن المعلومات، على الرغم من قيام بعض الشركات بتطبيق المعايير الدولية المتعلقة بأمن المعلومات، الأمر الذى يؤكد قيام المنظمات المصرية بوضع برامج وسياسات محددة لأمن نظم المعلومات.

ومن ثم يتضح للباحثين ثبوت خطأ الفرض الثالث للدراسة والذى ينص على "**تعمل المنظمات المصرية على تطبيق حوكمة أمن المعلومات فى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية**".

(٥/٧/٤) نتائج اختبار الفرض الرابع:

ينص الفرض الرابع للدراسة على "**يوجد اختلاف معنوى فى تأثير معايير حوكمة أمن المعلومات بشكل مستقل على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية**".

ولاختبار هذا الفرض يتم تطبيق اختبار التكرار والنسبة، واختبار "كا^{٢}"، وكذلك اختبار "كروسكال والاس". ويوضح الجدول التالى نتائج اختبار التكرار والنسبة وكذلك اختبار "كا^{٢}" واختبار "كروسكال والاس" بشأن قيام عينة الدراسة بتطبيق المعايير الخاصة بحوكمة أمن المعلومات – ITIL, COBIT, ISO – وحصولها على شهادات دولية فى مجال أمن المعلومات:

جدول رقم (١٢) التوزيع التكرارى والنسبى، واختبار "كا^{٢}"، واختبار "كروسكال والاس" حول قيام مفردات العينة بتطبيق كل من ITIL, COBIT, ISO

البيان	الاختيار	التكرار	النسبة	مستوى المعنوية "كا^{٢}"	اختبار "كروسكال والاس"		
					مفردات العينة	متوسط الرتب	مستوى المعنوية
تطبيق معايير الأيزو ISO	نعم	١٠١	٥١،٣	٠،٠٠**	شركات تكنولوجيا المعلومات	٩٥،٦٧	٠،٦٩
	لا	٩٦	٤٨،٧				
تطبيق معيار COBIT	نعم	١١٥	٥٨،٤				
	لا	٨٢	٤١،٦				
تطبيق معيار ITIL	نعم	٣٤	١٧،٣		شركات الاتصالات	٩٨،٥	
	لا	١٦٣	٨٢،٧				
حصول الشركة على شهادات دولية فى مجال أمن المعلومات	نعم	٥٠	٢٥،٤		البنوك	١٠١،٢	
	لا	١٤٧	٧٤،٦				

** دال إحصائيًا عند مستوى معنوية ٠،٠٥

ويتضح من الجدول السابق أن هناك تطبيقًا للمعايير الدولية الخاصة بحوكمة أمن المعلومات من قِبَل مفردات العينة، وأن أكثر المعايير تطبيقًا هو معيار الـCOBIT بنسبة ٥٨،٤%، يليه معايير

الأيزو ISO بنسبة ٥١،٣%، أما أقل المعايير تطبيقًا فهو معيار ITIL وذلك بنسبة ١٧،٣%، وكذلك فإن عدد قليل من مفردات العينة التى أقرت بأن الشركات التى تعمل بها قد حصلت على شهادات دولية فى مجال أمن المعلومات، وذلك من خلال تطبيقها لأحد تلك المعايير. كما تشير نتائج اختبار "كا^{٢}" أن هذه النتائج معنوية وذات دلالة إحصائية حيث مستوى المعنوية أقل من (٠،٠٥).

وتشير نتائج اختبار "كروسكال والاس" إلى أن مستوى المعنوية أكبر من (٠،٠٥)، مما يعنى أن هناك اتفاق فى آراء مقررات العينة حول النتائج التى تم التوصل إليها.

ويوضح الجدول التالى التوزيع التكرارى والنسبى واختبار "كا^{٢}" حول مدى قيام المعايير المختلفة لحوكمة أمن المعلومات فى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية:

جدول رقم (١٣) التوزيع التكرارى والنسبى واختبار "كا^{٢}" حول استخدام معايير حوكمة أمن المعلومات فى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية

البيـــان	التكرار والنسبة	درجات الموافقة					"كا^{٢}" مستوى المعنوية
		غير موافق على الإطلاق	غير موافق	محايد	موافق	موافق تمامًا	
استخدام معايير الأيزو ISO فى الحد من المخاطر	التكرار	٢	٦	١٢	٢٠	١٥٣	٠،٠٠٠**
	النسبة	١	٣	٦،١	١٠،٢	٧٧،٧	
استخدام معيار COBIT فى الحد من المخاطر	التكرار	١	١٠	١٢	١٦	١٦٠	
	النسبة	٠،٥	٥،١	٦،١	٨،٦	٨١،٢	
استخدام معيار ITIL فى الحد من المخاطر	التكرار	٨	١٨	٢٩	٣٨	١٠٤	
	النسبة	٤،١	٩،١	١٤،٧	١٩،٣	٥٢،٨	

** دال إحصائيًا عند مستوى معنوية ٠،٠٥

ويتضح من الجدول السابق أن هناك اتفاقًا فى آراء مفردات العينة بمستوى معنوية أقل من (٠،٠٥)، مما يدل على أن هناك فروقًا ذات دلالة إحصائية فى آراء مفردات العينة، كما تبين أن هناك اتفاقًا بين مفردات العينة على تأثير معايير حوكمة أمن المعلومات فى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية، وأن أكثر تلك المعايير تأثيرًا هو معيار COBIT بنسبة موافقة ٨٩،٨%، يليها فى ذلك معايير الأيزو ISO بنسبة موافقة ٨٧،٩%، ثم معيار الـITIL بنسبة موافقة ٧٢،١%.

ومما سبق يمكن للباحثين استنتاج صحة الفرض الرابع للدراسة والذى ينص على "**يوجد اختلاف معنوى فى تأثير معايير حوكمة أمن المعلومات بشكل مستقل على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية**".

وبعد اختبار فروض الدراسة، يقوم الباحثان فى القسم التالى (الخامس) بعرض النتائج التى تم التوصل إليها، بالإضافة إلى التوصيات والتوجهات البحثية المستقبلية.

(٥) القسم الخامس: النتائج والتوصيات والتوجهات البحثية المستقبلية:

(١/٥) النتائج:

فى إطار هدف ومنهج البحث توصل الباحثان إلى مجموعة من النتائج تتمثل فى:

(١/١/٥) نتائج الدراسة النظرية:

١- تتعدد صور المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية ما بين مخاطر داخلية، ومخاطر خارجية، وتعتبر المخاطر الداخلية من أكثر المخاطر تهديدًا لنظم المعلومات المحاسبية؛ لأنها تُعد فى الأساس مشكلة أفراد على علم تام بالنظام ونقاط القوة والضعف به. وأن إهمال التعامل معها والعمل على الوقاية منها قد يؤدى إلى تعرض الشركات لبعض الأضرار المحتملة مثل: خسائر فى الإيرادات، أو خسارة سمعة الشركة أو حقوق الملكية الفكرية.

٢- تتمثل أسباب حدوث تلك المخاطر فى: نقص تدريب الموظفين على استخدام وحماية نظم المعلومات، وسوء اختيارهم، وعدم وجود ضوابط وإجراءات كافية تعمل على معالجة والوقاية من حدوث هذه المخاطر، وعدم متابعة التطورات الحديثة فى مجال تكنولوجيا المعلومات والجرائم المرتبطة بها.

٣- لا تكفى الحلول التكنولوجية بمفردها فى مواجهة المخاطر المختلفة التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية، ومن ثم يجب على الشركات اتباع منهجٍ متكاملٍ لإدارة أمن المعلومات بحيث يقوم على تقييم التكنولوجيا المستخدمة، وتقييم سلوكيات الأفراد، والاهتمام بالجوانب التنظيمية حتى يسهل التنبؤ بالمخاطر وإحباط أى محاولة للقيام بها. وتعتبر حوكمة أمن المعلومات من أكثر المداخل التى تعمل على تحقيق تلك الأهداف.

٤- تعمل حوكمة أمن المعلومات على توفير إطار للرقابة لضمان أن المخاطر التى تتعرض لها الشركات يتم الوصول بها إلى المستوى المسموح به، كما تعمل على التأكيد بأن استراتيجيات الأمن التى تتبعها الشركة تتفق مع الأهداف الاستراتيجية لها.

٥- يحقق التطبيق الجيد لحوكمة أمن المعلومات العديد من الفوائد، وتلك الفوائد لا تتمثل فقط فى تخفيض المخاطر أو الحد من تأثير إجراءات خاطئة، ولكنها يمكن أن تعمل على تحسين الثقة داخل وخارج الشركة، مما يؤدى إلى تحسين سمعة الشركة، وكذلك تحسين الكفاءة فى أداء المهام المختلفة من خلال تجنب إهدار الوقت والجهد اللازمين لخروج الشركة من أى حادث أمنى.

٦- تتمثل المعايير المستخدمة عند تطبيق حوكمة أمن المعلومات فى: معايير الأيزو (ISO/IEC 27K)، ومعيار COBIT 5، ومعيار ITIL، ويؤدى تطبيق تلك المعايير – فى صورة إطار عمل متكامل – إلى تحقيق الأهداف المرجوة من تطبيق حوكمة أمن المعلومات داخل الشركة.

(٢/١/٥) نتائج الدراسة الميدانية:

فى ضوء استخدام الأساليب الإحصائية (الوصفية والاستدلالية) تم التوصل إلى النتائج التالية:

١- يوجد اتفاق معنوى وتجانس فى الآراء بين مفردات عينة الدراسة بشأن تعدد المخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية، وتُعد المخاطر الخارجية متمثلة فى البرامج الخبيثة والاختراقات و... غيرها من أكثر المخاطر أهمية (أكثرها تكرارًا)، بينما يُعد التدمير المتعمد للبيانات والإدخال المتعمد لبيانات غير صحيحة من أقل المخاطر أهمية (أقلها تكرارًا).

٢- يود اتفاق فى آراء مفردات العينة بشأن اختلاف الأهمية النسبة للمخاطر التى تتعرض لها نظم المعلومات المحاسبية الإلكترونية.

٣- يوجد اتفاق فى آراء مفردات العينة حول تعدد أسباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية، ويُعد عدم وجود سياسات وبرامج محددة لأمن المعلومات من أهم تلك الأسباب.

٤- يقوم عدد كبير من مفردات العينة بتطبيق المعايير الدولية لحوكمة أمن المعلومات بصورة منفردة، إلا أنها لا تعمل على تطبيق حوكمة أمن المعلومات – ضمن استراتيجية الشركة – للحد من مخاطر نظم المعلومات المحاسبية الإلكترونية، على الرغم من إدراك مفردات العينة لأهمية تطبيق حوكمة أمن المعلومات والفوائد المتحققة منها.

٥- هناك اتفاق بين آراء مفردات العينة على تأثير المعايير الدولية لحوكمة أمن المعلومات والمتمثلة فى: معايير الأيزو، ومعيار COBIT، ومعيار ITIL فى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية، كما يوجد اتفاق على أن أكثر هذه المعايير تأثيرًا هو معيار الـCOBIT، بينما أقلها تأثيرًا هو معيار ITIL.

(٢/٥) التوصيات:

فى إطار ما جاء بالجزء النظرى، وما أكدته الدراسة الميدانية فيمكن للباحثين تقديم التوصيات التالية:

١- زيادة الاهتمام بتوعية المنظمات المصرية بأهمية استخدام مبادئ ومعايير حوكمة أمن المعلومات حتى يتسنى لها مواجهة التحديات والمخاطر التى تواجه بيئة تكنولوجيا المعلومات.

٢- الاهتمام بإعداد دورات تدريبية خاصة بتكنولوجيا المعلومات للإلمام بالتطورات الحديثة فى هذا المجال، والتعرف على الجرائم المحتملة المرتبطة بها وكيفية مواجهتها ولمتابعة التطورات المتلاحقة فى مجال المعايير الدولية لأمن المعلومات.

٣- قيام الهيئة العامة للرقابة المالية بإلزام الشركات بتطبيق المعايير الدولية الخاصة بحوكمة أمن المعلومات داخل الشركات حتى تزيد درجة الثقة والمصداقية فى المعلومات والبيانات التى تقوم تلك الشركات بالإفصاح عنها عبر الموقع الإلكترونى لها.

٤- قيام وزارة الاستثمار – مركز المديرين – بإعداد "دليل قواعد ومعايير حوكمة أمن المعلومات" كمرفقات "لدليل قواعد ومعايير حوكمة الشركات" حتى يتسنى للشركات المصرية معرفة أهمية حوكمة أمن المعلومات وخطورة عدم تنفيذها.

(٣/٥) التوجهات البحثية المستقبلية:

فى ضوء النتائج التى تم التوصل إليها، يرى الباحثان أن هناك مجالات عديدة تعتبر أساسًا لأبحاث مستقبلية تتمثل فيما يلى:

١- أثر الإفصاح عن حوكمة أمن المعلومات على زيادة القدرة التنافسية للشركات.

٢- قياس أثر التكامل بين حوكمة أمن المعلومات والمراجعة الداخلية على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية.

٣- دراسة تحليلية لأثر حوكمة أمن المعلومات على زيادة الثقة والمصداقية فى المعلومات المالية المنشورة عبر الإنترنت.

٤- إطار مقترح لتطبيق حوكمة أمن المعلومات عند الإستعانة بمصادر خارجية لتكنولوجيا المعلومات.

المراجع

أولاً: المراجع باللغة العربية:

- د. أحمد عبد السلام أبو موسى، (٢٠٠٤)، "مخاطر أمن نظم المعلومات المحاسبية الإلكترونية – دراسة ميدانية على المنشآت السعودية–"، **الإدارة العامة**، معهد الإدارة العامة، الرياض، المجلد (٤٤)، العدد الثالث، سبتمبر، ص ص٥٠٨–٥١٦.
- دليل قواعد ومعايير حوكمة الشركات، جمهورية مصر العربية، (٢٠١١)، **مركز المديرين**، وزارة الاستثمار، فبراير، ص ص١–٢٥.
- د. سعيد عبد الكريم الساكنى، أ. حنان على العواودة، (٢٠١١)، "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**، جمعية المكتبات والمعلومات السعودية، العدد الحادى عشر، مايو، ص ص٢١٩–٢٦١.
- عاشور مزريق، صورية معمورى، (٢٠١٢)، "حوكمة الشركات بين فلسفة المفهوم الإدارى وإمكانية التجسيد الفعلى"، ملتقى وطنى حول – حوكمة الشركات كآلية للحد من الفساد المالى والإدارى – مخبر مالية وبنوك وإدارة الأعمال، **كلية العلوم الاقتصادية والتجارية وعلوم التسيير**، جامعة محمد خيضر – بسكرة، الجزائر، ٦، ٧ مايو، ص ص١–١٧.
- د. عماد يوسف حب الله، (٢٠٠٩)، "حماية القضاء السيبرانى الأمور التنظيمية لأمن المعلومات والإفصاح، **ورشة عمل – بناء القدرات فى مجال الحماية القانونية على الإنترنت**–، الهيئة المنظمة للاتصالات، الجمهورية اللبنانية، ص ص١–٣٢.

ثانيًا: المراجع باللغة الإنجليزية:

- A. Sengupta & C. Mazumdar, (2011), "A Mark-up Language for the Sepcification of Information Security Governence Requirements", **International Journal of Information Security and Privacy**, Vol. 5, Issue 2, April, pp. 33-53.
- A.A. Abu-Musa, (2010), "Information Security Governance in Saudi Organization: an Empirical Study", **Information Management & Computer Security**, Vol. 18, No. 4, pp. 226-276.
- Ahmed A. Abu-Musa, (2006), "Perceived Security Threats of Computerized Accoutning Information Systems in the Egyptian Banking Industry", **Journal of Information Systems**, Spring, Vol. 20, No. 1, pp. 187-203.
- B.V. Solms, (2005), "Information Security Governance: COBIT or ISO 17799 or both?", **Computer & Security**, Vol. 24, pp. 99-104.
- C. Juiz, C. Guerrero & I. Lera, (2014), "Implementing Good Governance Principles for the Public Sector in Information Technology Governance Frameworks", **Open Journal of Accounting**, Vol. 3, No. 1, pp. 9-27.
- E. Ohki et al., (2009), "Information Security Governance Framework", Proceeding of the First ACM Workshop on Information Security Governance,

16th ACM Conference on Computer and Communications Security, New York, NY, USA, 13 November, pp. 1-5, Available at: **dl.acm.org**, Accessed: 11 June, 2014.

- Eman Al Hanini, (2012), "The Risks of Using Computerized Accounting Information Systems in the Jordanian Banks: Their Reasons and Ways of Prevention", **European Journal of Business and Management**, Vol. 4, No. 20, pp.53-63.
- H. Nemati, (2013), "**Privacy Solutions and Security Frameworks in Information Protection**", Chapter 7, The University of North Carolina, Greensboro, pp. 103-123.
- H. Susanto et al., (2011), "Information Security Management System Standards: A Comparative Study of the Big Five", **International Journal of Electrical & Computer Sciences IJECS-IJENS**, Vol. 11, No. 05, pp. 23-29.
- I. Bose & A.C. Leung, (2014), "Do Phishing Alerts Impact Global Corporations? A Firm Value Analysis", Decision Support Systems, Available at: **http://dx.doi-org/10.1016/j.dss.2014.04.006**, Accessed: 2 June, 2014.
- Information Security Standard (ISS), (2014), "ISO/IEC 27001: 2013 Information Technology-Security Techniques-Information Security Management Systems-Requirements", Available at: **www.iso27001security.com**, Accessed: 20 May, 2014.
- Information Systems Audit and Control Association (ISACA), "COBIT 4.1 Framework for IT Governance and Control", Available at: **www.isaca.org**, Accessed: 25 May, 2014.
- Information Systems Audit and control Association (ISACA), (2013), "**COBIT 5 for Risk**", ISACA, Rolling Meadows, USA, pp. 1-102.
- Information Technology Governance Institute (ITGI), (2006), "**Information Security Governance: Guidance for Boards of Directors and Executive Management**", 2nd Edition, ITGI, U.S.A., pp. 1-52.
- Jim Clinch, (2009), **"ITIL V3 and Information Security"**, Best Management Practice: for Portfolio, Programme, Project, Risk and Service Management, White Paper, May, pp. 1-40.
- K. Ito, T. Kagaya and H. Kim, (2010), "Information Security Governance to Enhance Corporate Value", **SANS Institute**, pp. 1-76.
- M.B. Romney & P.J. Steinbart, (2012), **"Accounting Information Systems"**, 12th Edition, New Jersy, Pearson Printic Hall, pp. 1-720.
- M.B. Tarmidi, A.A. Rashid, M.S. Bin Deris & R.A. Roni, (2013), "Computerized Accounting System Threats in Malaysian Public Services, **International Journal of Finance and Accounting**, Vol. 2, No. 2, pp. 109-113.

- M.E. Whitman & H.J. Mattord, (2013), "**Management of Information Security**", 4th Edition, Cengage Learning, pp. 1-576.
- Nabil Baydoun, William Maguire, Neal Ryan & Roger Willett, (2013), "Corporate Governance in Five Arabian Gulf Countries". **Managerial Auditing Journal**, Vol. 28, No. 1, pp. 7-22.
- **National Institute of Standard and Technology (NIST),** (2011), "Information Security", Special Pulication 800-39, March, pp. 1-48.
- Robert E. Stroud, (2012), **"COBIT 5: Simplify Complex Standards"**, ISACA, pp. 1-48.
- S. Bahl & O.P. Wali, (2014), "Perceived Significance of Information Security Governance to Predict the Information Security Service Quality in Software Service Industry: An Empirical Analysis", **Information Management & Computer Security**, Vol. 22, Iss. 1, pp. 2-23.
- S.H. Von Solms & R. Von Solms, (2009), "**Information Security Governance**", Chapter 2-3, Springer, New York, U.S.A., pp. 1-130.
- S.H. Von Solms, (2007), "The Relationship Between Corporate Governance, Information Technology (IT) Governance and Information Security Governance and, An ICT Risk Management System to Support Information Security Governance", University of Johannesburg, Johannesburg, South Africa, pp. 1-65, Avilable at: **www.ise.ac.uk**, Accessed 5 April, 2014.
- T. Olzak, (2013), "COBIT 5 for Information Security: The Underlying Principles", pp. 1-19, Available at: **www.techrepublic.com/blog/ itsecurity/....**, Accssed: 22 May, 2014.
- T.O. Muhrtala & M. Ogundeji, (2013), "Computerized Accounting Information Systems and Perceived Security Threats in Developing Economies: The Nigerian Case", **Universal Journal of Accounting and Finance**, Vol. 1, No. 1, pp. 9-18.
- Talal H. Hayale & Husam A. Abu Khadra, (2008), "Investigating Perceived Security Threats of Cpmputerized Accounting Information Systems – An Empirical Research Applied on Jordanian Banking Sector", **Journal of Economic & Administrative Sciences**, Vol. 24, No. 1, June, pp. 41-67.
- Technical Report, ISO/IEC TR 27016, (2014), "**Information Technology-Security Techniques-Information Security Management-Organizational Economics**", First Edition, Switzerland, pp. 1-15.
- Z. Zainol, S.P. Nelson & A. Malami, (2012), "Internal Human Based Threats and Security Controls in Computerized Banking Systems: Evidence from Malaysia", **Procedia-Social and Behavioral Sciences**, Vol. 65, pp. 199-204.

قائمة إستقصاء

الأستاذ الفاضل/ الأستاذة الفاضلة/ .....

السلام عليكم ورحمة الله وبركاته

يقوم الباحثان بإعداد بحث بعنوان "**الدور التأثيرى لحوكمة أمن المعلومات فى الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية – دراسة ميدانية**".

ونرجو من سيادتكم التكرم بملىء بيانات هذا الاستقصاء، ونود أن نؤكد لسيادتكم أن البيانات التى سيتم جمعها فى هذا الاستقصاء سوف تكون سرية ولن تستخدم إلا فى أغراض البحث العلمى، ونظرًا لأن إجابة سيادتكم سوف تكون على قدرٍ عالٍ من الأهمية لذلك نرجو التكرم بمراعاة الدقة فى استيفاء البيانات.

ويشكر الباحثان لكم مشاركتكم وتعاونكم الصادق

وتفضلوا بقبول فائق الإحترام والتقدير

د/ على محمود مصطفى خليل
مدرس بقسم المحاسبة
كلية التجارة – جامعة بنها
ali.khalil@fcom.bu.edu.eg

د/ منى مغربى محمد إبراهيم
مدرس بقسم المحاسبة
كلية التجارة – جامعة بنها
mona.ibrahim@fcom.bu.edu.eg

أولاً: بيانات عامة: الرجاء وضع علامة (√) أما الاختيار المناسب:

١- المؤهل العلمى:

☐ بكالوريوس ☐ دبلوم دراسات عليا ☐ ماجستير ☐ دكتوراه

٢- جهة العمل .....

٣- المسمى الوظيفى:

☐ محاسب ☐ رئيس قسم ☐ مراجع نظم معلومات إلكترونية

☐ مراجع داخلى ☐ مراقب حسابات ☐ متخصص IT

٤- عدد سنوات الخبرة:

☐ أقل من ٥ سنوات ☐ من ٥ إلى ١٠ سنوات

☐ من ١٠ إلى ١٥ سنة ☐ أكثر من ١٥ سنة

٥- النظام المحاسبى فى المكان الذى تعمل فيه:

☐ يدوى ☐ يعتمد بدرجة كبيرةعلى الكمبيوتر ☐ مختلط

٦- هل تواجه جهة عملك مخاطر أمن معلومات؟

☐ نعم ☐ لا

٧- إذا كانت الإجابة (بنعم) على السؤال السابق فهل أدت تلك المخاطر إلي وجود خسائر مالية؟ أو هل أثرت تلك المخاطر على أداء الشركة؟

☐ نعم ☐ لا

٨- هل أدت تلك المخاطر إلى التأثير السلبى على الموقف التنافسى للشركة؟

☐ نعم ☐ لا

ثانياً: أسئلة الإستقصاء:

١- يرجى اختيار الإجابة الصحيحة لتوضيح رأى سيادتكم حول أهمية (مدى تكرار) مخاطر أمن نظم المعلومات المحاسبية الإلكترونية:

البيـــــــان	هام جداً	هام	متوسط الأهمية	غير هام	عديم الأهمية
١/١ إدخال غير متعمد لبيانات غير سليمة بواسطة الموظفين.					
٢/١ إدخال متعمد لبيانات غير سليمة بواسطة الموظفين.					
٣/١ تدمير غير متعمد للبيانات بواسطة الموظفين.					
٤/١ تدمير متعمد للبيانات بواسطة الموظفين.					
٥/١ دخول غير المصرح به للبيانات بواسطة الموظفين.					
٦/١ تبادل الموظفين لكلمات المرور.					

البيـــــــان	هام جداً	هام	متوسط الأهمية	غير هام	عديم الأهمية
٧/١ إدخال فيروسات الحاسب إلى النظام المحاسبى.					
٨/١ تدمير أو سرقة بعض المعلومات (مخرجات النظام).					
٩/١ عمل نسخ غير مصرح بها من مخرجات النظام.					
١٠/١ عرض بيانات سرية على شاشات العرض.					
١١/١ كوارث طبيعية مثل الحرائق أو إنقطاع الطاقة.					
١٢/١ مخاطر خارجية متمثلة فى البرامج الخبيثة والاختراقات و... غيرها.					

٢- يرجى اختيار الإجابة الصحيحة لتوضيح رأى سيادتكم حول أسباب حدوث مخاطر أمن نظم المعلومات المحاسبية الإلكترونية:

البيـــــــان	موافق تماماً	موافق	محايد	غير موافق	غير موافق على الإطلاق
١/٢ عدم توافر الخبرة اللازمة والتدريب الكافى للموظفين.					
٢/٢ عدم توافر الحماية الكافية ضد مخاطر الفيروسات.					
٣/٢ عدم تحديد المسئوليات والصلاحيات لكل فرد داخل الهيكل التنظيمي.					
٤/٢ عدم وجود سياسات وبرامج محددة لأمن نظم المعلومات.					
٥/٢ عدم تطبيق مبادئ ومعايير حوكمة أمن المعلومات.					

٣- يرجى اختيار الإجابة الصحيحة لتوضيح رأى سيادتكم بشأن مدى تطبيق حوكمة أمن المعلومات داخل الشركة للحد من مخاطر أمن المعلومات المحاسبية الإلكترونية:

١/٣ هل تقوم الشركة بتطبيق حوكمة أمن المعلومات ضمن إستراتيجيتها للحد من مخاطر أمن نظم المعلومات المحاسبية الإلكترونية؟

☐ نعم ☐ لا

إذا كانت الإجابة (بنعم) الرجاء متابعة الأسئلة، أما إذا كانت الإجابة بـ (لا) فالرجاء ذكر الإجراءات التى تقوم الشركة بإتباعها للحماية ضد مخاطر أمن نظم المعلومات المحاسبية

.....

.....

٢/٣ هل تقوم الشركة بتطبيق معايير دولية خاصة بأمن المعلومات؟

☐ نعم ☐ لا

٣/٣ هل تعمل حوكمة أمن المعلومات على تحقيق الأهداف الإستراتيجية للشركة؟

☐ **موافق بشدة** ☐ **موافق** ☐ **محايد** ☐ **غير موافق** ☐ **غير موافق على الإطلاق**

٤/٣ هل تقوم الشركة بتطبيق معايير الأيزو ISO فى مجال أمن المعلومات؟

☐ نعم ☐ لا

إذا كانت الإجابة (بنعم) نرجو من سيادتكم ذكر هذه المعايير .....

.....

٥/٣ هل تقوم الشركة بتطبيق معيار COBIT الخاص بأمن المعلومات؟

☐ نعم ☐ لا

إذا كانت الإجابة (بنعم) نرجو من سيادتكم توضيح الإصدار الذى يتم استخدامه

.....

٦/٣ هل تقوم الشركة بتطبيق معيار ITIL فى مجال إدارة خدمات تكنولوجيا المعلومات؟

☐ نعم ☐ لا

٧/٣ هل حصلت الشركة على شهادات دولية فى مجال أمن المعلومات؟

☐ نعم ☐ لا

٨/٣ هل يؤدى استخدام أحد هذه المعايير الآتية فى التخفيف من مخاطر نظم المعلومات المحاسبية الإلكترونية؟

- معايير الأيزو:

☐ **موافق بشدة** ☐ **موافق** ☐ **محايد** ☐ **غير موافق** ☐ **غير موافق على الإطلاق**

- معيار COBIT:

☐ **موافق بشدة** ☐ **موافق** ☐ **محايد** ☐ **غير موافق** ☐ **غير موافق على الإطلاق**

- معيار ITIL:

☐ **موافق بشدة** ☐ **موافق** ☐ **محايد** ☐ **غير موافق** ☐ **غير موافق على الإطلاق**