دراسة أثر إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية: مع دراسة ميدانية على الشركات المصرية

ا.د/ رضا ابراهيم صالح ا.د/ أحمد عبد السلام أبوموسي

أ / ندا حامد توفيق أبو سعدة

دراسة أثر إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية: مع دراسة ميدانية على الشركات المصرية

ملخص البحث

يهدف هذا البحث إلى محاولة معرفة أثر إدارة أمن المعلومات على نجاح برنامج أمن المعلومات في بيئة الأعمال المصرية، ولقد قدم البحث إطاراً نظريًا لأهم العوامل والمتغيرات التي تؤثر على فعالية إدارة أمن المعلومات وأثرها على نجاح برنامج أمن المعلومات، كما قام البحث باختبار عناصر ذلك الإطار ميدانيًا على عينة من فروع الشركة المصرية للاتصالات WE، وذلك باستخدام قائمة الاستقصاء التي تم تصميمها خصيصًا لهذا الغرض. ولقد تم تجميع البيانات اللازمه لاختبار الفروض الإحصائية باستخدام البرنامج الإحصائى SPSS، وعمل التحليل الإحصائى الوصفى وكذلك الاختبارات الإحصائية المعلمية لاختبار الفروض، وقد توصلت نتائج الدراسة إلي أن إدارة أمن المعلومات لها تأثير جوهري وإيجابي على نجاح برنامج أمن نظم المعلومات المحاسبية فى البيئة المصرية، كما أوصت بضرورة اهتمام منظمات الأعمال بإدراة أمن المعلومات باعتبارها عنصراً هاما وضرورياً لنجاح برنامج أمن المعلومات فى منظمات الأعمال المصرية.

Abstract

This research aims to try to find out the impact of information security management on the success of the information security program in the Egyptian business environment. The study introduced a proposed theoretical framework which includes the most important factors and variables that might affect the effectiveness of information security management, and achieve the success of information systems security programs. A questionnaire had been designed and distributed to collect the required data to examine the research hypotheses from a sample of branches of the Egyptian Telecommunications Company WE using SPSS. The results of the study revealed that reached Information Security Management have a significant positive impact on the success of the Accounting Information Systems Security Program in the Egyptian environment. The study recommended to pay more attention of implementing information security management and consider it a mandatory element of their agenda to achieve the success of the information security program in the Egyptian business organizations

١- الإطـــار العام للبحـــث

١/١ مقدمـــة

أدى تطور تكنولوجيا المعلومات والاتصالات إلى إحداث تطور كبير في مجال المعلومات الذي زامنه ظهور تهديدات كبيرة ومتنوعة تهدد أمن نظم المعلومات وسلامة المعلومات التي تتضمنها، ولضمان أمن المعلومات تقوم المنظمات عادة بإدخال سياسات ومبادئ توجيهية تتاح لجميع الأعضاء (Rotvold, 2008)، ومع ذلك لاتزال هناك تهديدات وحوادث أمنية ونقاط ضعف ومخاطر تعصف بالعديد من المنظمات لذلك أصبح أمن المعلومات واحداً من أهم التحديات التي تواجه المنظمات في الوقت الراهن، والتي تتطلب من إدارات المنظمات الإدارة الجيدة لأمن نظم المعلومات، والتي تعرف بأنها نهج أمني مستمر ومنظم لإدارة حماية معلومات المنظمة من التعرض للخطر من قبل الأطراف غير المسئولة ولضمان بقاء المعلومات آمنة (Zammani & Razali, 2016).

وتختلف إدارة أمن المعلومات عن حوكمة أمن المعلومات حيث تهتم حوكمة أمن المعلومات بتأسيس بيئة رقابية مع ضمان توفير الحماية اللازمة للأصول المعلوماتية من المخاطر المختلفة، وكذلك وضع خطة للتطوير المستمر لإدارة المخاطر، وعلى الرغم من هذا الاختلاف فإن كلاهما يسعى لتخفيف المخاطر التي تواجه نظم المعلومات المحاسبية الإلكترونية.

٢/١ مشكلـــة البحـــث

أصبح حماية المعلومات في عصر العولمة أمراً بالغ الأهمية من أجل ضمان استمرارية الأعمال، حيث إن التصدي للتهديدات الأمنية لنظم المعلومات أصبح تحدياً يواجه العديد من المنظمات، فأمن المعلومات لا يعني تأمين المعلومة والحفاظ على سرية ونزاهة المعلومات وتوافرها فقط ولكن أيضاً تأمين البنية التحتية التي تسهل استخدامها من أجهزة وبرمجيات وعوامل بشرية ومادية.

واعترافاً بذلك بذلت المنظمات جهوداً كبيرة في إدارة ومعالجة أمن المعلومات، وأصبح من الضروري عليها أن تهتم بوضع نظم وإجراءات تعمل على الحد من تلك المخاطر ، ووضع نظام جيد لإدارتها والعمل على نجاح برنامجها الأمني.

وبذلك يمكن صياغة مشكلة البحث في السؤال البحثي التالي:

ما مدى تأثير إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية؟

ويمكن الإجابة على السؤال البحثي الرئيسي من خلال الإجابة على الأسئلة البحثية الفرعية التالية:

1. **ما المقصود ببرنامج أمن المعلومات؟ وما الفرق بين إدارة أمن المعلومات وحوكمة أمن المعلومات؟**

٢. هل يؤثر التنفيذ المستمر للسياسات المتعلقة بأمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية؟

٣. هل يؤثر وجود إجراءات لتنفيذ عمليات وأنشطة سياسات أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية؟

٤. هل يؤثر وجود فريق متخصص في إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية؟

٥. هل يؤثر وجود فريق تنسيق لإدارة أمن المعلومات حيث التواصل بفعالية مع جميع المستويات بالمنظمة على نجاح برنامج أمن نظم المعلومات المحاسبية؟

٦. هل يؤثر وجود فريق مسئول عن ضمان ضوابط الرقابة على نجاح برنامج أمن نظم المعلومات المحاسبية؟

٧. هل يؤثر التقييم الجيد لإدارة أمن نظم المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية؟

٣/١ هدف البحـــــث

يتمثل الهدف الرئيسي للبحث في "دراسة مدى تأثير إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية في البيئة المصرية"

ويمكن تحقيق هذا الهدف من خلال تحقيق الأهداف الفرعية التالية:

١. تحديد المفاهيم الأساسية المرتبطة ببرنامج أمن المعلومات، ودراسة أوجه الاختلاف بين إدارة أمن المعلومات وحوكمة أمن المعلومات.

٢. دراسة أثر التنفيذ المستمر للسياسات المتعلقة بأمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية.

٣. دراسة أثر وجود إجراءات لتنفيذ عمليات وأنشطة سياسات أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية.

٤. دراسة أثر وجود فريق متخصص في إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية.

٥. دراسة أثر وجود فريق تنسيق لإدارة أمن المعلومات يعمل علي التواصل بفعالية مع جميع المستويات بالمنظمة على نجاح برنامج أمن نظم المعلومات المحاسبية.

٦. دراسة أثر وجود فريق مسئول عن ضمان ضوابط الرقابة على نجاح برنامج أمن نظم المعلومات المحاسبية.

٧. دراسة أثر التقييم الجيد لإدارة أمن نظم المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية.

٤/١ أهميـــة البحـــث

تتمثل أهمية البحث في الأهمية العلمية والعملية على النحو التالي:

١/٤/١ الأهمية العلمية

تتمثل في محاولة إلقاء الضوء على تنوع وتعدد المخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية، وكذلك توضيح المحاولات التي تقوم بها المنظمات للحد من تلك المخاطر عن طريق إدارة أمن المعلومات وحوكمة أمن المعلومات.

٢/٤/١ الأهمية العملية

- **قد يساعد البحث العاملين في مجال أمن نظم المعلومات المحاسبية في اتخاذ القرارات ووضع الخطط والبرامج والسياسات التي تعمل على التخفيف من حدة المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية وأمن نظم المعلومات المحاسبية .**
- **يساعد البحث على الفهم الجيد لإدارة أمن برامج نظم المعلومات وكيفية تطبيقها وتنفيذها في منظمة الأعمال.**

٥/١ فروض البحث

في ضوء مشكلة البحث والهدف منها يمكن صياغة الفرض البحثي الرئيسي التالي:

تؤثر إدارة أمن المعلومات إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية في منظمات الأعمال المصرية.

ويندرج تحت هذا الفرض الفروض الفرعية التالية:

- **الفرض الفرعي الأول:** "يؤثر التنفيذ المستمر للسياسات المتعلقة بأمن المعلومات إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية".
- **الفرض الفرعي الثاني:** "يؤثر وجود إجراءات لتنفيذ عمليات وأنشطة سياسات أمن المعلومات إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية".
- **الفرض الفرعي الثالث:** "يؤثر وجود فريق متخصص في إدارة أمن المعلومات إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية".
- **الفرض الفرعي الرابع:** "يؤثر وجود فريق تنسيق لإدارة أمن المعلومات حيث التواصل بفعالية مع جميع المستويات بالمنظمة إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية".

- **الفرض الفرعي الخامس:** " يؤثر وجود فريق مسئول عن ضمان ضوابط الرقابة إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية".
- **الفرض الفرعي السادس:** "يؤثر التقييم الجيد لإدارة أمن نظم المعلومات إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية".

٦/١ منهج البحث

اعتمد الباحثون على المنهج العلمي بشقيه الاستقرائي والاستنباطي، وذلك على النحو التالي:

١/٦/١ المنهج الاستنباطي Deductive Approach

اعتمد الباحثون على المنهج الاستنباطي Deductive Approach لدراسة والتعرف على إدارة أمن المعلومات ودورها في نجاح برنامج أمن نظم المعلومات المحاسبية في منظمات الأعمال المصرية، وفي إطار ذلك قام الباحثون بدراسة وتحليل الدراسات والمقالات والبحوث العلمية والعملية المختلفة التي لها صلة بموضوع البحث بهدف اشتقاق الفروض الإحصائية التي سيتم اختبارها في الدراسة الميدانية.

٢/٦/١ المنهج الاستقرائي Inductive Approach

اعتمد الباحثون على المنهج الاستقرائي Inductive Approach في إجراء الدراسة الميدانية للتعرف على مدى تأثير إدارة أمن المعلومات علي نجاح برنامج أمن نظم المعلومات المحاسبية، واختبار الفروق الجوهرية بين الوظائف المختلفة فيما يختص بمدى إدراكها لأهمية إدارة أمن المعلومات في بيئة الأعمال المصرية عن طريق قائمة الاستقصاء Questionnaire التي أعدت خصيصاً لتحقيق هذا الغرض، وكذلك أسلوب المقابلات الشخصية لأفراد عينة البحث الميداني ثم اختبار فروض البحث والوصول إلى نتائج وتوصيات البحث.

٧/١ حدود البحث

- **يقتصر البحث على المخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية فقط دون الدخول في التفسيرات أو الدوافع من وراء ذلك.**
- **اقتصرت الدراسة الميدانية على الشركة المصرية للاتصالات WE فقط، وذلك لعدم تجاوب كل من شركة فودافون وشركة أورانج في تقديم المساعدة والإجابة على الاستبيان.**

٢- الإطار النظري للبحـــث

١/٢ أمن نظم المعلومات والمخاطر التي تهدد المعلومات وأنظمتها

بدأ علم أمن المعلومات وتطور مع بداية تقنية المعلومات وتطورها، فعندما بدأت الحاسبات الآلية باحتواء معلومات مهمة بدأ القلق على أمن هذه المعلومات والأجهزة التي تعالجها. لذلك بدأ التفكير في تأمين المعلومات والأجهزة التي تحتويها ضد المخاطر المحتملة التي قد تتعرض لها. ومن هذا يجب توضيح الآتي:

١/١/٢ مفهوم أمن المعلومات Information Security (IS)

وضح Withman &Mattord (٢٠٠٥) أمن المعلومات كما عرفته لجنة أنظمة الأمن القومي الأمريكية Committee on National Security Systems (CNSS) بأنه "حماية المعلومات وعناصرها المهمة بما في ذلك الأنظمة والأجهزة التي تستخدم هذه المعلومات وتخزنها وترسلها".

ويرى دعدوع (٢٠١٦) أنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها سواء كانت هذه المخاطر داخلية أو خارجية وذلك من خلال توفير الأدوات والوسائل اللازمة لحمايتها والمعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين.

٢/١/٢ متطلبات أمن المعلومات

إن حماية أمن المعلومات يتطلب نشر الوعي بين العاملين في المنظمة بالأخطار التي تهدد أمن المعلومات ومن هذه المتطلبات ما يلي: (أبو موسى وخطاب، ٢٠١٢)

يرى حامد والحمود (٢٠٠٩) مخاطر أمن نظم المعلومات بأنها جميع الممارسات البشرية والأحداث السياسية والتأثيرات البيئية المقصودة وغير المقصودة سواء كانت داخل المنظمة أو خارجها وينتج عنها إتلاف أو تدمير أو سرقة أو تزوير لبعض أو كل من نظم المعلومات المحاسبية متبوعة في كثير من الأحيان بتحقيق خسائر في الوقت والجهد والأموال.

وتتعرض نظم المعلومات الإلكترونية للكثير من المخاطر والتهديدات ومنها التلاعب في البيانات بقصد تدميرهاسواء بالحذف، أو بالدمج غير الصحيح لبعضها، أو بخلطها ببيانات أخرى غير حقيقية أو تبويبها بشكل خاطئ تفقد معه مدلولها ومعناها؛ وقد يحدث التلاعب في البيانات بشكل يجعلها لا تعبر عن الحقائق التي نتجت عنها أصلاً، كما أن هذا التلاعب يحدث في مراحل مختلفة من النظام حيث المدخلات أو التشغيل أو التخزين أو المخرجات. ومن الممكن أن تكون تلك التهديدات في شكل سرقة وقت أجهزة الكمبيوتر واستخدامه في الأغراض الشخصية والدخول غير المصرح به للنظم والشبكات وتخريب وتدمير بعض الملفات، فشل النظام وسقوط شبكة الاتصال، منع الأشخاص المخول لهم بالدخول إلى النظام، الكوارث الطبيعية مثل الحرائق والفيضانات أو انقطاع مصدر الطاقة، الكوارث غير الطبيعية مثل الحرائق المفتعلة وغيرها،

إدخال فيروسات للكمبيوتر، الإظهار غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها وتوزيعها بواسطة أشخاص غير مصرح لهم بذلك، وكذلك مقاطعة تحويل البيانات من أماكن بعيدة.(أبو موسى، ٢٠٠٥ ؛ أبو موسى وخطاب، ٢٠١٢)

٢/٢ إدارة أمن المعلومات Information Security Management (ISM)

إدارة أمن المعلومات هي نهج أمني مستمر ومنظم لإدارة حماية معلومات المنظمة من التعرض للخطر من قبل الأطراف غير المسئولة ولضمان بقاء المعلومات آمنة (Zammani & Razali, 2016)، فغالباً ما يواجه أمن المعلومات بالعديد من المشاكل سواء في الأجل الطويل أو الأجل القصير، وقد تركز معظم منظمات الأعمال على منع حدوث مشاكل أمن المعلومات في الأجل القصير دون الاهتمام بمدى خطورة مشاكل الأجل الطويل. لذا يجب على الإدارة وضع خطة طويلة الأجل لمنع حدوث أي تهديد لأمن المعلومات في الأجل الطويل وتخفيض آثارها السلبية على المنظمة إلى أدني حد ممكن في حالة حدوثها، كما يجب عليها تحديد نوع القضايا الهامة التي تواجه أمن المعلومات وأن تدرسها بعناية وتتفهم طبيعة المشاكل المتعلقة بكل قضية حتى تستطيع تجنب تلك المشاكل في المستقبل وتقديم حلول مناسبة لها (أبو موسى وخطاب، ٢٠١٢).

ولإدارة أمن المعلومات مجموعة من المتغيرات الداخلية التي تعمل على نجاح برامج أمن نظم المعلومات وهذه المتغيرات هي:

١- سياسة أمن المعلومات IS Policy

سياسة أمن المعلومات هي مزيج من المبادئ والأنظمة والمنهجيات والتقنيات والأدوات التي أنشئت لحماية المنظمة من التهديدات (Tryfonas et al., 2001)، ويرى Alnatheer (٢٠١٥) أنها وثيقة استراتيجية بمعني أنها تنشأ قبل القيام بأي نشاط من أنشطة أمن المعلومات فهي تتكون من الأهداف والاتجاهات والقواعد التي يجب وضعها واتباعها من قبل الموظفين والأطراف الأخري التي تتعامل مع المنظمة، لذا يجب أن تكون هذه السياسة واضحة في تحديد الأهداف والأدوار ومسئوليات الموظفين والأطراف الأخرى ذات المصلحة، كما يجب أن تكون شاملة بمعنى أنها تغطي جميع جوانب متطلبات وضوابط أمن المعلومات وأن تكون متناسقة مع سياسة المنظمة ورؤيتها.

وتمثل سياسة أمن المعلومات حجر الزاوية في إدارة أمن المعلومات الجيدة (Fung et al., 2003)، كما أن هذه السياسة ليست ثابتة أي يجب أن يتم مراجعتها بانتظام على الأقل مرة واحدة في السنة للتأكد من أنها ذات صلة باحتياجات الوقت الحاضر ويتم إرسالها إلى كامل الموظفين والأطراف الأخرى ذات المصلحة مع مراعاة أنه عند قيام المنظمة بإحلال أساليب أمن تكنولوجية حديثة بدلاً من أساليب أمن المعلومات التقليدية يجب المفاضلة من حيث درجة الاستفادة ونجاح برامج أمن المعلومات بين البقاء على الأساليب التقليدية لأمن المعلومات مع

تكاملها مع أساليب أمن المعلومات الحديثة أم الإحلال التام أكثر إفادة؟ (أبوموسى وخطاب، ٢٠١٢).

وينبغي لسياسة أمن المعلومات على المستوى المؤسسي أن تعالج أساسيات هيكل إدارة أمن المعلومات في المنظمة، بما في ذلك: (Alnatheer, 2015)

أدوار ومسئوليات أمن المعلومات، بيان خط الأساس للضوابط الأمنية وقواعد تجاوز خط الأساس، وقواعد السلوك التي من المتوقع أن يتبعها مستخدمو المنظمة والحد الأدنى من العواقب المترتبة على عدم الامتثال.

وفيما يلي بعض المعايير التي ينبغي على المنظمة اتباعها من أجل تنفيذ سياسة أمن فعالة:

١. يجب أن تكون سياسة أمن المعلومات واضحة ومفهومة من قبل جميع الأطراف المعنية وأن يتم متابعة هذه السياسة بانتظام لمعرفة ما إذا كان يتم انتهاكها (Madigan et al., 2004)، كما يجب وجود مبادئ توجيهية إجرائية محددة بشكل جيد للتعامل مع حوادث انتهاك السياسة (Hone& Eloff, 2002).

٢. أن تكون ملائمة للثقافة التنظيمية، وملائمة للنمط الذي يتسق مع أسلوب الاتصال العام في المنظمة (Doherty& Fulford, 2005).

٣. استخدام لغة بسيطة لضمان سهولة فهمها، وتحديد الغرض من السياسة ونطاق المنظمة وشرح ماهو النشاط المقبول وما هو غير مقبول (Tryfonas et al., 2001).

٤. ينبغي وضع سياسة أمن المعلومات على أساس الاحتياجات الأمنية والأهداف التجارية للمنظمة (Mckay, 2003) .

٢- إجراءات أمن المعلومات IS Procedures

يرتبط أمن المعلومات بمجموعة من الإجراءات المصممة لحماية المعلومات (Gordon& Loeb, 2006) فالإجراءات هي المبادئ التوجيهية لتنفيذ العمليات والأنشطة القائمة على أساس الاحتياجات الموضحة في سياسة أمن المعلومات بمعني أنها إرشادات التشغيل التي تشرح كيفية تنفيذ سياسة أمن المعلومات حيث يتم اشتقاق الإجراءات من سياسة الأمن وذلك لضمان تنفيذ ISM بشكل مناسب وصحيح. كما يجب أن تكون الإجراءات واضحة ومحددة في وصف الخطوات اللازمة لإنجاز العمليات والأنشطة، وينبغي استعراضها بطريقة دورية أو عند تغيرات بيئة الأمن نتيجة التطورات التكنولوجية المستمرة لذلك فإنه من الضروري وجود إدارة مسئولة عن إدارة برنامج التغيير وقادرة على رسم إجراءات وخطوات ملائمة لإدارة ذلك التغيير حيث إنه قبل إجراء أي تغيير لابد من وضع تخطيط جيد يضمن أن اقتناء التكنولوجيا

الجديدة لن يؤثر سلبياً على سلامة أمن المعلومات ومدى الاستفادة منها (Singh & Gupta, 2014).

يتضح مما سبق أن إجراءات أمن المعلومات أقرب إلى المستخدمين والأجهزة من السياسة الأمنية حيث إنها توفر الخطوات التفصيلية للتركيب والإعداد والتهيئة، فهي تعمل على تحويل السياسات والتوجيهات إلى أرض الواقع ومن البيئة النظرية إلى بيئة تشغيلية حقيقية.

٣- فريق إدارة أمن المعلومات ISM Team

يتكون فريق إدارة أمن المعلومات من الموظفين المشاركين في معظم أنشطة أمن المعلومات، حيث يجب أن يتمتع هذا الفريق بالمعرفة والمهارات الواسعة والتعاون في تنفيذ عمليات ISM وأن يكون دائم التحديث مع القضايا الأمنية الحالية، كما ينبغي أن يمتلك المهارة التقنية التي تؤهله للقيام بالأعمال والمهام الجديدة (Maarop et al., 2015)

٤- فريق تنسيق إدارة أمن المعلومات Coordinator Team

يعمل فريق تنسيق إدارة أمن المعلومات كحلقة وصل بين كل من الإدارة العليا وفريق ISM ومراجعي أمن المعلومات والموظفين، فهو المسئول عن تنظيم التدريب والتوعية بالبرامج وإدارة الموارد المالية والبشرية وتقديم تقرير عن التقدم في ISM إلى الإدارة العليا، كما ينبغي أن يتوافر في أفراد فريق التنسيق مهارات التواصل الجيدة مع الآخرين والمعرفة الكاملة بأنشطة ISM حيث القدرة على التواصل بفعالية مع جميع المستويات في المنظمة (Zammani & Razali, 2016).

٥- فريق مراجعة أمن المعلومات IS Audit Team

فريق مراجعة أمن المعلومات هو فريق مسئول عن ضمان ضوابط الرقابة، وأنه يتم تنفيذ العمليات والإجراءات والأنشطة بشكل صحيح، فينبغي أن يتمتع هذا الفريق بمهارات الاتصال الجيدة والإلتزام بالوقت المحدد لإنهاء عملية مراجعة أمن المعلومات، ولكي يتم نجاح برامج أمن المعلومات يجب أن يكون لدى فريق مراجعة أمن المعلومات فهم جيد لعمليات ISM حيث إن نقص المعرفة قد تؤدي إلى طرح الأسئلة بطريقة خاطئة وبذلك وجود معلومات مغلوطة (ISACA, 2012)

٦- تقييم إدارة أمن نظم المعلومات

يتم تقييم إدارة أمن نظم المعلومات من خلال:

الإدارة المستمرة للأعمال (خطة استمرارية الأعمال): الشئ المهم في استمرارية الأعمال هي خطة استمرارية الأعمال، لذلك يجب على المنظمة تحديد متطلبات أمن المعلومات وجعلها جزء لا يتجزأ من خطة استمرارية الأعمال، وأن تقوم المنظمة أيضاً بتحديد خطة العمليات والإجراءات والموارد والمسئوليات للسيطرة على الحوادث والكوارث ولضمان استمرارية الأعمال أثناء الأحداث غير المقصودة وبعدها، ينبغي تطوير هذه الخطة وتوثيقها

والموافقة عليها من قبل الإدارة كما يجب اختبارها لمراقبة فعاليتها (ISO/IEC 27002:2013).

٣/٢ حوكمة أمن المعلومات Information Security governance (ISG)

الحوكمة بوجه عام هي عملية إدارة وتوجيه ومراقبة والتأثير على القرارات والإجراءات والسلوكيات التنظيمية (Greene, 2014)، والهدف الرئيسي لمنظمة أمن المعلومات ISO 27002:2013 هو "إنشاء إطار إداري لبدء ومراقبة تنفيذ وتشغيل أمن المعلومات داخل المنظمة"

١/٣/٢ مفهوم حوكمة أمن المعلومات

عرف معهد حوكمة تكنولوجيا المعلومات IT Governance Institute (٢٠٠٦) حوكمة أمن المعلومات على أنها "عنصر أساسي لحوكمة الشركات يتكون من القيادة والهياكل التنظيمية والعمليات المشاركة في حماية الأصول المعلوماتية، ومن خلالها يمكن لمنظمات الأعمال معالجة قضايا أمن المعلومات من منظور حوكمة الشركات"

ويرى Abu-Musa (٢٠١٠) أن حوكمة أمن المعلومات هي "مجموعة من المسئوليات والممارسات التي يقوم بها مجلس الإدارة والإدارة التنفيذية بهدف توفير التوجيه الاستراتيجي، وضمان تحقيق الأهداف، والتأكد من إدارة مخاطر أمن المعلومات على نحو مناسب، وكذلك التحقق من أن موارد أمن المعلومات تستخدم بشكل فعال"

٢/٣/٢ أهداف حوكمة أمن لمعلومات

- إرساء ودعم أمن تكنولوجيا المعلومات لضمان أن أهداف الأعمال ومتطلبات أصحاب المصلحة لحماية المعلومات يتم الوفاء بها باستمرار.
- إنشاء بيئة رقابية ملائمة للحفاظ على سرية وتكامل وتوافر المعلومات.
- دعم العمليات والنظم الخاصة بها، وأيضاً حماية المعلومات من مختلف المخاطر التي يمكن أن تواجهها (Abu-Musa, 2010).

وتحقق حوكمة أمن المعلومات العديد من المنافع لمنظمات الأعمال التي تقوم بتطبيقها، ومن أهم تلك المنافع مايلي: (Whitman and Mattord, 2013)

- ارتفاع قيمة أسهم منظمات الأعمال التي تطبق ممارسات الحوكمة.
- تعزيز تخصيص الموارد الأمنية المحدودة.
- إدارة المخاطر بكفاءة وفعالية، وتحسين العمليات وكذلك الاستجابة السريعة للحوادث المتعلقة بأمن المعلومات.
- وضع سياسة فعالة لأمن المعلومات، والالتزام بتلك السياسة.

- **تخفيض حالة عدم التأكد من خلال تحديد المخاطر المتعلقة بأمن المعلومات والعمل على تخفيضها إلى مستويات مقبولة.**
- **توفير مستوى من التأكيد على أن اتخاذ القرارات الحاسمة والهامة لا تستند على معلومات غير صحيحة ومضللة.**

٤/٢ الفرق بين حوكمة أمن المعلومات وإدارة أمن المعلومات

لا ينبغي الخلط بين حوكمة أمن المعلومات وإدارة أمن المعلومات فحوكمة أمن المعلومات (ISO 38500) هي النظام الذي تقوم المنظمة من خلاله بتوجيه ومراقبة أمن المعلومات.

ويصف المعهد الوطني للمعايير والتكنولوجيا National Institute of Standards and Technology (NIST) (٢٠٠٦) إدارة أمن المعلومات بأنها عملية إنشاء وصيانة إطار لتوفير ضمان أن استراتيجيات أمن المعلومات تتماشى مع أهداف الأعمال وتدعمها، وتتماشى مع القوانين واللوائح المعمول بها من خلال الالتزام بالسياسات والضوابط الداخلية، وتوفير إسناد المسئولية، كل ذلك في محاولة لإدارة المخاطر.

كما أن إدارة أمن المعلومات تهتم باتخاذ قرارات للتخفيف من المخاطر؛ أما الحوكمة فهي تحدد من هو المخول باتخاذ القرارات، وتحدد الحوكمة إطار المساءلة وتوفر الرقابة لكفالة التخفيف من حدة المخاطر على نحو كافٍ، في حين تكفل الإدارة تنفيذ الضوابط للتخفيف من حدة المخاطر، وتوصي الإدارة باستراتيجيات أمنية، أما الحوكمة تضمن مواءمة الاستراتيجيات الأمنية مع أهداف الأعمال واتساقها مع الأنظمة.

ويمكن توضيح الفرق بين حوكمة أمن المعلومات وإدارة أمن المعلومات من خلال الجدول التالي:

(جدول ١: الفرق بين حوكمة أمن المعلومات وإدارة أمن المعلومات)

حوكمة أمن المعلومات	إدارة أمن المعلومات
تعني القيام بالشئ الصحيح	القيام بالأمور بشكل صحيح
الرقابه	التنفيذ
يأذن بحقوق القرار	أذن باتخاذ القرار
سن السياسات	فرض السياسات
المساءله	المسئولية
التخطيط الاستراتيجي	تخطيط المشاريع
تخصيص الموارد	استخدام الموارد

المصدر (Allen, 2007)

يتضح مما سبق أن الغرض الرئيسي من أي حوكمة داخل المنظمة هو مساءلة الإدارة أمام أصحاب المصلحة؛ ولذلك يجب أن يكون الغرض من حوكمة أمن المعلومات هو مساءلة الإدارة عن حماية أصول المعلومات المتاحة في المنظمة والوصول بالمخاطر والانتهاكات المرتبطة بأمن المعلومات إلى أدني حد ممكن ، فالحوكمة سواء كانت مالية أو تجارية أو قانونية أو أمن المعلومات تدور حول جعل الناس يفعلون الشيء الصحيح في الوقت المناسب.

٥/٢ برامج أمن المعلومات

يرى البعض أنه لا يكفي أن يكون لدى المنظمة بعض سياسات الأمان والتركيز فقط على تأمين الشبكة الخاصة بها، حيث إنه لدمج الأمان في العمليات التجارية، تحتاج المنظمة إلى برنامج قوي لأمن المعلومات يقوم بتعيين المحركات التجارية ومتطلباتها القانونية والتنظيمية والمخاطر والتهديدات التي تتعرض لها (Vizcayno, 2012)، لذلك من الضروري معرفة ما يلي:

١/٥/٢ مفهوم ومكونات برنامج أمن المعلومات

معظم المنظمات قد لا يكون لديها فهم واضح فيما يختص ببرنامج أمن المعلومات وأهدافه وكيفية بنائه، لذلك يجب النظر إلى أفضل الممارسات في هذه الصناعة للحصول على بعض التوجيه، فالمبدأ التوجيهي الأكثر استخداماً في جميع أنحاء العالم لبناء برامج الأمن هو ISO 27001:2005، الذي تم اشتقاقه من المعيار البريطاني القياسي (BS 7799)، وهو معيار معترف به دولياً لإدارة أمن المعلومات يوفر توصيات مفاهيمية رفيعة المستوى بشأن أمن المنظمة؛ ويتألف هذا المعيار من جزأين هما:

- الجزء الأول: هو دليل تنفيذ مع مبادئ توجيهية حول كيفية بناء بنية تحتية شاملة لأمن المعلومات.
- الجزء الثاني: هو دليل لمراجعة الحسابات يستند إلى المتطلبات التي يجب تلبيتها لكي تعتبر المنظمة متوافقة مع المعيار ISO 27001:2005، ويتم تقسيم المستند إلى المكونات التالية (شكل ١) التي يجب أن يتضمنها برنامج الأمن: (Vizcayno, 2012)

١. سياسة أمن المعلومات للمنظمة Information security policy for the organization: وهي بمثابة خريطة لأهداف العمل ودعم الإدارة والأهداف والمسئوليات الأمنية.

٢. الأمن التنظيمي Organizational security: وهو إنشاء وصيانة هيكل أمني تنظيمي من خلال استخدام منتدى الأمن، وضابط الأمن، وتحديد المسئوليات الأمنية، وعملية الترخيص، والاستعانة بمصادر خارجية، والمراجعة المستقلة.

٣. تصنيف الأصول ومراقبتها **Assest classification and control**: حيث تطوير بنية تحتية أمنية لحماية الأصول التنظيمية من خلال إجراءات المساءلة والجرد والتصنيف.

٤. أمن الموارد البشرية **Human Resources security**: وهو الحد من المخاطر الكامنة في التفاعل البشري من خلال فحص الموظفين، وتحديد الأدوار والمسئوليات، وتدريب الموظفين بشكل صحيح وتوثيق تداعيات عدم تلبية التوقعات.

٥. الأمن المادي والبيئي **Physical and environmental security**: وهو حماية أصول المنظمة عن طريق اختيار موقع المنظمة بشكل صحيح، وإقامة وصيانة المحيط الأمني، وتنفيذ مراقبة الدخول وحماية المعدات.

٦. التحكم في الوصول **Access control**: حيث التحكم في الوصول إلى الأصول استنادًا إلى متطلبات العمل وإدارة الهوية وأساليب المصادقة والمراقبة.

شكل رقم (١) مكونات برنامج أمن المعلومات.
(المصدر: من إعداد الباحثون)

٧. إدارة الاتصالات والعمليات **Communications and operations management**: وذلك من خلال تنفيذ أمن العمليات حيث الإجراءات التشغيلية،

ومراقبة التغيير السليم، والتعامل مع الحوادث، والفصل بين الواجبات، وتخطيط القدرات، وإدارة الشبكات، والتعامل مع وسائل الإعلام.

٨. تطويرالنظام وصيانته **System development and maintenance**: حيث تنفيذ الأمن في جميع مراحل عمر النظام من خلال التطوير والتنفيذ والصيانة والتخلص.

٩. إدارة استمرارية الأعمال **Business continuity management**: مكافحة تعطيل العمليات العادية باستخدام تخطيط الاستمرارية والاختبار.

١٠. الامتثال **Compliance**: الامتثال للمتطلبات التنظيمية والتعاقدية والقانونية باستخدام الضوابط التقنية، ومراجعة حسابات النظام والوعي القانوني.

٢/٥/٢ أهداف برامج أمن المعلومات

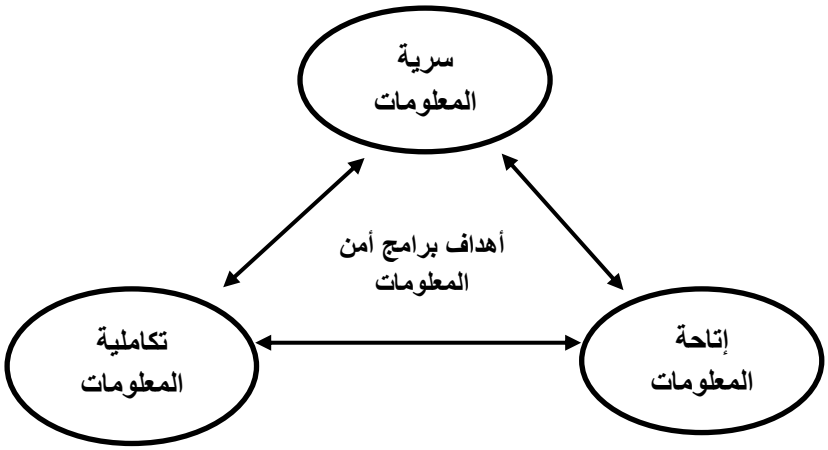
توجد عدة أهداف رئيسية وفرعية لبرامج أمن المعلومات، ولكن تتمثل الأهداف الرئيسية في جميع برامج الأمن (شكل ٢) في:

- سرية المعلومات (خصوصية المعلومات) **Confidentially**

سرية المعلومات هي إخفاء المعلومات أو الموارد بمعنى حماية المعلومات من عدم اطلاع أي شخص غير مخول له بالاطلاع عليها (White, 2011).

- تكاملية المعلومات (سلامة المحتوى) **Integrity of Information**

تكاملية المعلومات تعني ضمان سلامة محتوى المعلومات وضمان عدم تغييرها أو تدميرها من قبل جهات غير مخولة.



شكل رقم (٢) أهداف برامج أمن المعلومات
المصدر: (من إعداد الباحثون)

- **إتاحة المعلومات (القدرة على الوصول) Availability of Information**

إتاحة المعلومات تعني التأكد من استمرار عمل نظام المعلومات، واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمستخدم المعلومات وتوافرها عند الحاجة إليها، والتأكد من أن مستخدمي تلك المعلومات لن يتعرضوا إلى منع استخدامهم لها بطريقة غير مشروعة.

٣- الدراسات السابقة

١/٣ استقراء الدراسات السابقة

١. دراسة Solms (2005)

قامت هذه الدراسة باختبار التوافق بين الاستخدام المتكامل لكل من ال COBIT, ISO 17799 كآليات لإدارة أمن المعلومات.

ومن أهم النتائج التي توصلت إليها هذه الدراسة ما يلي:

١. أن كلاً من COBIT, ISO 17799 يوفر محتوى أكثر فائدة لتطبيق بيئة شاملة وموحـــدة لحوكمة أمن المعلومات.

٢. يوفر COBIT إرشادات جيدة لماهية حوكمة أمن المعلومات.

٣. يوفر ISO 17799 المزيد من التفاصيل اللازمة لكيفية تطبيق حوكمة أمن المعلومات.

٢. دراسة ISACA (2008)

قامت جمعية ضبط وتدقيق المعلومات Information Systems Audit and Control Association (ISACA) بوضع نموذج كمنهج رئيسى لإدارة أمن المعلومات وأظهر النموذج عد مجالات رئيسية إذا اتبعتها المنظمة سوف تصل إلى عدة عوامل تؤدي إلى نجاح برامج أمن المعلومات وهذه المجالات تتمثل في:

- حوكمة برامج المعلومات.
- إدارة خطر المعلومات.
- تطوير برامج أمن المعلومات.
- إدارة والاستجابة لحوادث أمن المعلومات.

ومن أهم النتائج التي توصلت إليها هذه الدراسة ضرورة قيام منظمات الأعمال بتطبيق تلك المجالات حتى تصل إلى عدة عوامل تساعد في تفعيل ونجاح برامج أمن المعلومات.

٣. دراسة حامد والحمود (٢٠٠٩)

تناولت هذه الدراسة أشكال نظم المعلومات المحاسبية المستخدمة في القطاع الصناعي الأردني ودرجة حوسبتها، كما تناولت أهم المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في شركات القطاع الصناعي الأردني؛ وأثر العلاقة بين العوامل الديموغرافية للقائمين على نظم المعلومات المحاسبية الإلكترونية ودرجة إدراكهم لأهمية مخاطر أمن نظم المعلومات المحاسبية الإلكترونية، وقامت هذه الدراسة أيضاً بدراسة العلاقة بين الأنشطة التي تزاولها منظمات الأعمال الصناعية الأردنية والمخاطر التي تهدد أمن نظم المعلومات المحاسبية وأيضاً أثر العلاقة بين العوامل الديموغرافية للقائمين على نظم المعلومات المحاسبية الإلكترونية ودرجة إدراكهم لعدد مرات تكرار مخاطر أمن نظم المعلومات المحاسبية الإلكترونية.

ومن أهم النتائج التي توصلت إليها هذه الدراسة ما يلي:

١. أظهرت النتائج درجة مقبولة من الوعي والإدراك لأهمية المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية من قبل القائمين عليها في محمل المتغيرات الديموغرافية.

٢. كان ترتيب المخاطر الهامة الخمسة الأولي من حيث معدل تكرار التهديد لأمن نظم المعلومات المحاسبية الإلكترونية المستخدمة من قبل منظمات الأعمال الصناعية الأردنية كما يلي:

أ- إهدار وسرقة وقت الحاسب الآلي من قبل الموظفين.

ب- تعرض أجهزة الحاسب الآلي للإصابة بالفيروسات والبرامج الخبيثة.

ج- الإدخال الخاطئ غير المتعمد من قبل الموظفين.

د- اشتراك الموظفين بكلمة مرور واحدة.

هـ- التأخير غير المتعمد لإدخال بعض البيانات والمستندات.

٣. أظهرت عملية التحليل وجود اختلافات جوهرية في إدراك القائمين على نظم المعلومات الإلكترونية في منظمات الأعمال الصناعية وذلك عند قياس معدل تكرار ودرجة أهمية المخاطر التي تهدد أمن النظم والنشاط الذي تزاوله هذه المنظمات وأيضاً عند قياس أهمية المخاطر التي تهدد النظم التي يشرفون عليها مع العوامل الديموغرافية للمشاركين في هذه الدراسة، بينما عدم وجود اختلافات جوهرية عند قياس معدل معدل تكرار المخاطر التي تهدد أمن النظم التي يشرفون عليها مع العوامل الديموغرافية للمستجيبين على تساؤلات هذه الدراسة.

٤. دراسة Abu-Musa (2010)

هدفت هذه الدراسة إلى البحث في خصائص وأهمية تطبيق حوكمة أمن نظم المعلومات، وأيضاً تقييم الوضع الحالي والملامح الرئيسية لحوكمة أمن نظم المعلومات في منظمات الأعمال السعودية.

ومن أهم النتائج التي توصلت إليها هذه الدراسة ما يلي:

١. معظم منظمات الأعمال السعودية تدرك أهمية حوكمة أمن المعلومات لنجاح إدارة المنشأة إلا أن معظمها ليس له سياسة أو استراتيجيات أمن واضحة ومحددة.

٢. معظم منظمات الأعمال السعودية تعاني من حوادث أمن المعلومات والتي يصعب قياسها وتحديدها.

٣. عدم امتلاك منظمات الأعمال السعودية خطط التعافي من الكوارث للتعامل مع حوادث أمن المعلومات وحالات الطوارئ، ولا يتم تنفيذ إجراءات تقييم المخاطر بشكل كافٍ وفعال.

وأوصت الدراسة مجالس الإدارة في منظمات الأعمال السعودية بضرورة الاهتمام بحوكمة أمن نظم المعلومات واعتبارها عنصراً إلزامياً في أجندتها.

٥. دراسة Muhrtala and Ogundeji (2013)

تناولت الدراسة معرفة التهديدات المحتملة لنظم المعلومات المحاسبية الإلكترونية والمستخدمة في مجال الأعمال التجارية وأيضاً كيفية التغلب على هذه التحديات في اقتصاديات الدول النامية.

ومن أهم النتائج التي توصلت إليها هذه الدراسة ما يلي:

١. أن الموظفين تشكل التهديدات الرئيسية لأصول المعلومات المستخدمة في المحاسبة الإلكترونية عندما لا يتم التحكم فيها على نحو فعال، وهذا يشير إلى أن الإدارة ينبغي أن تضع في إجراءات الترخيص على أساس الحاجة إلى معرفة فقط.

٢. يجب أن يكون هناك تسجيل منتظم ورصد الوصول المنطقي إلى الأنظمة والبيانات والسياسات والإجراءات مع الفصل بين الواجبات وحقوق الوصول للسجلات والمعاملات.

٣. يجب على المستخدمين المصرح لهم الوصول إلى التطبيقات والبيانات المطلوبة فقط لأداء مهام محددة فقط.

٦. دراسة خليل وإبراهيم (٢٠١٦)

تهدف هذه الدراسة إلى توضيح الدور الذي تقوم به حوكمة أمن المعلومات في الحد من المخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية من خلال المعايير الدولية لحوكمة أمن المعلومات حيث التعرف على نوعية المخاطر التي تتعرض لها هذه النظم، وأسباب تعرضها للمخاطر، وأيضاً التعرف على ماهية حوكمة أمن المعلومات والتحقق من مدى استخدامها في بيئة الأعمال المصرية، وتحديد المعايير المستخدمة عند تطبيق حوكمة أمن المعلومات.

ومن أهم النتائج التي توصلت إليها هذه الدراسة ما يلي:

١. يوجد العديد من المخاطر التي تتعرض لها نظم االمعلومات المحاسبية الإلكترونية يتمثل أهمها في المخاطر الخارجية.

٢. من أهم أسباب حدوث تلك المخاطر هي عدم وجود سياسات وبرامج لأمن المعلومات داخل منظمات الأعمال، وأيضاً عدم تطبيق الأهداف والمبادئ الخاصة بحوكمة أمن المعلومات وعدم تضمينها داخل استراتيجيتها المستقبلية.

وأوصت هذه الدراسة بضرورة وجود نشرات إرشادية لتوعية منظمات الأعمال المصرية عن دور وأهمية حوكمة أمن المعلومات من خلال قيام وزارة الاستثمار بإصدار دليل لقواعد ومبادئ ومعايير حوكمة أمن المعلومات بحيث يكون من مرفقات دليل قواعد ومبادئ حوكمة الشركات، وقيام الهيئة العامة للرقابة المالية بإلزام منظمات الأعمال بتطبيق ما ورد به من قواعد ومعايير.

٧. دراسة Zammani and Razali (2016)

تهدف هذه الدراسة إلى تخفيف التهديدات الأمنية ونقاط الضعف التي تعصف بالعديد من المنظمات من خلال وضع مجموعة من العوامل الرئيسية لإدارة أمن المعلومات من المؤلفات الموجودة أولاً ومن ثم تأكيد العوامل واكتشاف عوامل أخرى ذات صلة من منظور الممارسين والمختصين، ومن هذه العوامل: (الموظفين، الأطراف الخارجية ذات المصلحة، تخطيط الموارد، السياسات والإجراءات، فريق تنسيق ومراجعة أمن المعلومات، إدارة المخاطر، تطوير الكفاءات والتوعية)

ومن أهم النتائج التي توصلت إليها هذه الدراسة ما يلي:

أثبت الدراسة صحة العديد من العوامل التي تعمل على نجاح إدارة أمن المعلومات، وأوضحت أيضاً وجود فهم عالٍ لدى الممارسين لهذه العوامل. وأوصت الممارسين بتنفيذ هذه العوامل في إدارة أمن المعلومات من خلال التركيز على العمليات التي تحتاج إلى تنفيذ والوثائق الاستراتيجية والتقنية للمنظمة.

٢/٣ تحليل الدراسات السابقة

تطبق حوكمة أمن المعلومات من خلال معايير دولية مقبولة قبولاً عاماً، ويتم تحديث تلك المعايير بصفة دورية للتوافق مع التطورات البيئية التكنولوجية الحديثة.

ضرورة قيام منظمات الأعمال بتطبيق مجالات حوكمة أمن المعلومات وإدارة أمن المعلومات بالإضافة إلي تطوير برامج الأمن حتى تصل المنظمة إلى عدة عوامل تساعد في تفعيل ونجاح برامج أمن المعلومات.

٣/٣ أوجه الاختلاف بين الدراسات السابقة والدراسة الحالية

- **على الرغم من الأهمية المتزايدة لإدارة أمن المعلومات ودورها في نجاح برنامج أمن نظم المعلومات المحاسبية، إلا أنها لم تلق الاهتمام البحثي الكافي في البيئة العربية وهذا ما دعا الباحثون إلى تناوله بالبحث والدراسة.**
- **الدراسات السابقة تم إجراؤها في عدد من الدول العربية والأجنبية، ولا شك أن بيئة الأعمال المصرية تختلف عن غيرها من الدول العربية والأجنبية.**

٤- الدراسة الميدانية

استكمالاً لما تناوله البحث من التأصيل النظري قامت أيضاً بقياس مدى تأثير إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية, وذلك من خلال تحليل واستقراء آراء المختصين بهذا المجال وذلك كما يلي:

١/٤ هدف الدراسة الميدانية

يتمثل الهدف الرئيسي من الدراسة الميدانية في اختبار فروض الدراسة وذلك من خلال التعرف على آراء فئات عينة الدراسة حول تأثير إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية.

٢/٤ فروض الدراسة الميدانية

في ضوء طبيعة مشكلة الدراسة وتحقيقاً للهدف منها يمكن صياغة فرض البحث في صورة الفرض البديل وذلك كما يلي:

يتمثل الفرض الرئيسي للبحث في:

"تؤثر إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية في منظمات الأعمال المصرية"

ويندرج تحت هذا الفرض الفروض الفرعية التالية:

- **الفرض الفرعي الأول: "يؤثر التنفيذ المستمر للسياسات المتعلقة بأمن المعلومات إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية".**

- **الفرض الفرعي الثاني: "يؤثر وجود إجراءات لتنفيذ عمليات وأنشطة سياسات أمن المعلومات إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية".**
- **الفرض الفرعي الثالث: "يؤثر وجود فريق متخصص في إدارة أمن المعلومات إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية".**
- **الفرض الفرعي الرابع: "يؤثر وجود فريق تنسيق لإدارة أمن المعلومات حيث التواصل بفعالية مع جميع المستويات بالمنظمة إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية".**
- **الفرض الفرعي الخامس: " يؤثر وجود فريق مسئول عن ضمان ضوابط الرقابة إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية".**
- **الفرض الفرعي السادس: "يؤثر التقييم الجيد لإدارة أمن نظم المعلومات إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية".**

٣/٤ أداة البحث

اعتمد الباحثون على استمارة الاستقصاء (ملحق ١) والتي تم تصميمها خصيصاً لتجميع البيانات اللازمة لاختبار فروض البحث.

٤/٤ وسيلة البحث

اعتمد الباحثون على الاختبارات الإحصائية للتحقق من معنوية فروض البحث وهي:

- **النسب المئوية لتكرار إجابات الأطراف الرئيسية للاستقصاء حول أسئلة الاستقصاء، وذلك من خلال إجراء التحليلات الوصفية Descriptive Analysis للبيانات التي تم تجميعها للتعرف على الخصائص الأساسية لعينة البحث ومتغيراته.**
- **إجراء بعض الاختبارات المعلمية مثل: مثل اختبار T لعينة واحدة، اختبار تحليل التباين ANOVA، وختبار Chi-Square، وذلك لاختبار فروض البحث والتعرف على الفروق الجوهرية بين الوظائف المختلفة فيما يتعلق بإدراكها لتأثير إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية.**

٥/٤ مجتمع وعينة الدراسة الميدانية

تناول البحث تأثير إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية في بيئة الأعمال المصرية فقط، ولقد تم اختيار عينة البحث من شركات الاتصالات المصرية فقط دون التطرق إلي أي شركات أخرى أو قطاعات أخرى من الشركات، حيث تم اختبار عينة البحث على الشركة المصرية للاتصالات WE فقط فروع (القرية الذكية، رمسيس، الأسكندرية، كفر الشيخ، دسوق) نظرا لعدم تجاوب كل من شركة فودافون وشركة أورانج في تقديم المساعدة والإجابة على الاستبيان، كما تم تجميع بيانات الدراسة الميدانية في عام ٢٠٢٠.

في سبيل تحقيق الهدف من البحث تم الاعتماد على أسلوب العينة العشوائية الطبقية في اختيار عينة الدراسة والمكونة من (١٢٠) فرد، وقام الباحثون بتوزيع عدد من قوائم الاستقصاء على مفردات العينة والتي شملت خمس فروع من شركة WE والمتمثلة في (فرع WE القرية الذكية, فرع رمسيس, فرع كفر الشيخ, فرع دسوق, فرع اسكندرية)، والجدول التالي يوضح عدد استمارات الاستقصاء المرسلة والمستلمة والخاضعة للتحليل الإحصائي.

(جدول ٢: فئات عينة الدراسة وحجم استمارات الاستقصاء المرسلة والمستلمة والخاضعة للتحليل الإحصائي)

بنود العينة	الاستمارات المرسلة	الاستمارات المستلمة	نسبة الاستمارات المستلمة إلي المرسلة	الاستمارات المستبعدة	الاستمارات الصحيحة	الاستمارات الخاضعة للتحليل الإحصائي	
						العدد	النسبة
فرع WE القرية الذكية	٣٦	٣٣	%٩١,٧	٣	٣٠	٣٠	%٢٥
فرع رمسيس	١٦	١٤	%٨٧,٥	٢	١٢	١٢	%١٠
فرع كفر الشيخ	٣٨	٣٦	%٩٤,٧	٢	٣٤	٣٤	%٢٨,٣
فرع دسوق	٢٢	١٩	%٨٦,٤	١	١٨	١٨	%١٥
فرع اسكندرية	٢٩	٢٨	%٩٦,٦	٢	٢٦	٢٦	%٢١,٧
الاجمالي	١٤١	١٣٠	٩٢,٢	١٠	١٢٠	١٢٠	%١٠٠

المصدر: نتائج التحليل الإحصائي

٥/٤ خصائص عينة الدراسة

بالنسبة للخصائص الديموغرافية لعينة الدراسة فقد تم استخراج التكرارات والنسب المئوية وذلك بهدف التعرف على خصائص أفراد عينة الدراسة وذلك كالآتي:

أولاً: بالنسبة للمسمى الوظيفي

تم استخراج التكرارات والنسب المئوية لتوزيع أفراد عينة الدراسة وفقاً للمسمى الوظيفي وذلك كما هو موضح بجدول (٣):

جدول (٣)
التكرارات والنسب المئوية لوصف خصائص عينة الدراسة حسب متغير المسمى الوظيفية

الفئات	محاسب مالي		مراجع داخلي		محاسب تكاليف		مراقب عام		مراجع لنظم المعلومات الالكترونية		رئيس قسم		مدير عام		إجمالي	
	تكرار	نسبة %	تكرار	نسبة %	تكرار	نسبة %	تكرار	نسبة %	تكرار	نسبة %	تكرار	نسبة %	تكرار	نسبة %	تكرار	نسبة %
إجمالي	٣٣	٢٧,٥	١٢	١٠	٥	٤,٢	٩	٧,٥	١٢	١٠	٤٥	٣٧,٥	٤	٣,٣	١٢٠	١٠٠

المصدر: نتائج التحليل الإحصائي

من الجدول السابق والذى يمثل التكرارات والنسب المئوية لوصف خصائص أفراد عينة الدراسة وفقا للمسمى الوظيفي فنجد أن ٣٣ مفردة بنسبة ٢٧,٥% من حجم عينة الدراسة يعملون محاسبون ماليون, في حين نجد أن ١٢ مفردة بنسبة ١٠% من حجم عينة الدراسة يعملون كمراجع داخلي, كما نجد أن ٥ مفردات بنسبة ٤,٢% من حجم عينة الدراسة يعملون محاسبين تكاليف, وأيضا نجد أن ٩مفردات بنسبة ٧,٥% من حجم عينة الدراسة يعملون مراقب عام, في حين نجد أن ١٢ مفردة بنسبة ١٠% من حجم عينة الدراسة يعملون في وظيفة مراجع لنظم المعلومات الإلكترونية , كما نجد أن ٤٥ مفردة بنسبة ٣٧,٥% من حجم عينة الدراسة يعملون كرؤساء أقسام, وأخيراً نجد أن ٤ مفردات بنسبة ٣,٣% من حجم عينة الدراسة يعملون كمدير عام, وهذا يدل على أن عينة الدراسة لديها الإلمام الكافي بموضوع الدراسة.

ثانياً: بالنسبة لسنوات الخبرة

تم استخراج التكرارات والنسب المئوية لتوزيع أفراد عينة الدراسة وفقاً لسنوات الخبرة وذلك كما هو موضح بجدول (٤):

جدول(٤)

التكرارات والنسب المئوية لوصف خصائص عينة الدراسة حسب سنوات الخبرة

أقل من سنة		من سنة إلي أقل من ٥سنوات		من ٥ سنوات إلي أقل من ١٠سنوات		من ١٠سنوات إلي أقل من ١٥سنة		من ١٥ سنة إلي أقل من ٢٠سنة		من ٢٠سنة فاكثر		إجمالي	
العدد	% النسبة	العدد	% النسبة	العدد	% النسبة	العدد	% النسبة	العدد	% النسبة	العدد	% النسبة	العدد	% النسبة
٢	٧,١	١٣	٨,١٠	١٦	٣,١٣	٣٢	٧,٢٦	٣٦	٣٠	٢١	٥,١٧	١٢٠	١٠٠

المصدر: نتائج التحليل الإحصائي

من الجدول السابق والذى يمثل التكرارات والنسب المئوية لوصف خصائص أفراد عينة الدراسة وفقاً لسنوات الخبرة فنجد أن ٢ مفردة بنسبة ١,٧% من حجم عينة الدراسة لديهم خبرة أقل من سنة, في حين نجد أن ١٣ مفردة بنسبة ١٠,٨% من حجم عينة الدراسة لديهم خبرة من سنة إلى أقل من ٥ سنوات, كما نجد أن ١٦ مفردة بنسبة ١٣,٣% من حجم عينة الدراسة لديهم خبرة من ٥ سنوات إلى أقل من ١٠ سنوات, وأيضا نجد أن ٣٢ مفردة بنسبة ٢٦,٧% من حجم عينة الدراسة لديهم خبرة من ١٠ سنوات إلى أقل من ١٥ سنة, بينما نجد أن ٣٦ مفردة بنسبة ٣٠% من حجم عينة الدراسة لديهم خبرة من ١٥سنة إلى أقل من ٢٠ سنة, أخيراً نجد أن ٢١ مفردة بنسبة ١٧,٥% من حجم عينة الدراسة لديهم خبرة من ٢٠ سنة فأكثر, وهذا ينعكس بدوره على قدره أفراد العينة على فهم أسئلة الاستقصاء والإجابة عليها بدقة.

ثالثاً: بالنسبة للنظام المحاسبي في المنظمة

تم استخراج التكرارات والنسب المئوية لتوزيع أفراد عينة الدراسة وفقا للنظام المحاسبي للمنظمة, وذلك كما هو موضح بجدول (٥):

جدول (٥)
التكرارات والنسب المئوية لوصف خصائص عينة الدراسة حسب النظام المحاسبي للمنظمة

يدوي لا يستخدم الحاسبات الآلية		خليط من العمل اليدوي والتشغيل الالكتروني بالكمبيوتر		يعتمد بدرجة كبيرة علي الكمبيوتر		إجمالي	
العدد	النسبة %	العدد	النسبة %	العدد	النسبة %	العدد	النسبة %
١	٠,٨	٤٣	٣٥,٨	٧٦	٦٣,٣	١٢٠	١٠٠

المصدر: نتائج التحليل الإحصائي

من الجدول السابق والذى يمثل التكرارات والنسب المئوية لوصف خصائص أفراد عينة الدراسة وفقاً للنظام المحاسبي للمؤسسة, فنجد أن مفردة واحدة بنسبة ٠,٨% من حجم عينة الدراسة يعملون بشكل يدوي لا يستخدم الحاسبات الآلية, في حين نجد أن ٤٣ مفردة بنسبة ٣٥,٨% من حجم عينة الدراسة عملهم كخليط من العمل اليدوي والتشغيل الإلكتروني بالكمبيوتر, كما نجد أن ٧٦ مفردات بنسبة ٦٣,٣% من حجم عينة الدراسة يعتمد عملهم بدرجة كبيرة على الكمبيوتر, وهذا يدل أيضاً على أن العينة التي تم إجراء الدراسة عليها يتوقع أن يكون لديها المعرفة المطلوبة عن موضوع الدراسة.

تم الاعتماد في تصميم قائمة الاستقصاء على مقياس ليكرت الخماسي وذلك لقياس إجابات أفراد العينة وذلك كما هو موضح في جدول (٦):

جدول (٦)
التصنيف وفقا لمقياس ليكرت

التصنيف	موافق تماما	موافق	محايد	غير موافق	غير موافق تماما
الدرجة	٥	٤	٣	٢	١

٦/٤ اختبار ثبات وصدق المقاييس المستخدمة في الدراسة

يمكن اختبار ثبات وصدق المقاييس المستخدمة في الدراسة وذلك كما يلي:

١/٦/٤ التحقق من مستوى الثبات في المقاييس

تم استخدام معامل "ألفا كرونباخ" " Cronbach's Alpha" لقياس مدى الثبات في المقياس وذلك كما يلي:

جدول(٧) : تقييم ثبات المقياس الخاص بتحديد تأثير إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية

عدد المقاييس	Correlated item_ total correlation	معامل الفا كرونباخ (مقياس الثبات)	عدد العبارات المحذوفة	معامل الفا كرونباخ بعد الحذف
$X1_1$	٠,٤٥٣	٠,٧٨٦	—	٠,٧٨٦
$X1_2$	٠,٥٧٤			
$X1_3$	٠,٥٠٦			
$X1_4$	٠,٦١٧			
$X1_5$	٠,٦١٥			
$X1_6$	٠,٤٦٣			

المصدر: نتائج التحليل الإحصائي

من الجدول السابق نجد أن جميع عبارات هذا المقياس ذات معامل إرتباط إجمالي أعلى من ٣٠% بالإضافة إلى أن معامل الفا لهذا المقياس يبلغ (٠,٧٨٦) وهو معامل ثبات مرتفع وبالتالي نجد هذا المقياس يتمتع بدرجة عالية من الثبات.

٢/٦/٤ التحقق من مستوى الصدق في استمارة الاستقصاء

ويمكن قياس الصدق في المقياس بعدة أنواع, هي صدق المحتوي, والصدق الذاتي, وصدق الاتساق الداخلي, وذلك كما هو موضح في الآتي:

أولاً : صدق المحتوى

تم عرض الأداة على الخبراء في مجال التخصص, ويطلب منهم الحكم علي مدى صلاحية فقراته في قياس الشيء المراد قياسه.

ثانيا: الصدق الذاتي

تم حساب الصدق الذاتي للأبعاد وذلك عن طريق إيجاد الجذر التربيعي لمعامل الثبات كما يلي:

جدول (٨)
نتائج الصدق الذاتي لمقاييس الدراسة

البعد	معامل الفا كرونباخ (مقياس الثبات)	الصدق الذاتي
أثر إداره أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية	٠,٧٨٦	٠,٨٨٧

المصدر : نتائج التحليل الإحصائي

من جدول (٨) السابق نجد أن جميع البعد تتمتع بدرجة صدق مرتفعة وهذا يؤكد على أن الاستقصاء تتمتع بدرجة عالية من الصدق.

ثالثاً: صدق الاتساق الداخلي

يمكن قياس صدق الأداة المستخدمة وذلك بقياس قوة الارتباط بين درجة المجال المستخدم ودرجات أسئلة المقياس الكلية وذلك كما هو موضح في الجدول (٩):

جدول (٩)

نتائج معامل الارتباط بين درجة المجال والدرجة الكلية للاستقصاء

البعد	المتوسط العام للاستقصاء
تأثير إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية.	,١٥٧**

المصدر: نتائج التحليل الإحصائي

من الجدول السابق نجد أن معامل الارتباط السابق مقبول ودال إحصائياً وبذلك يكون الباحثون قد تأكدوا من ثبات وصدق استمارة الاستقصاء وبذلك أصبح الاستقصاء صالح للتطبيق على عينة الدراسة.

٧/٤ الأساليب الإحصائية المستخدمة في الدراسة

اعتمد الباحثون على اختبار كولمجروف سمرنوف لمعرفة مدى تبعية بيانات الدراسة للتوزيع الطبيعي وذلك كما هو موضح بالجدول (١٠):

جدول (١٠)
نتائج اختبار(K-S) لاختبار طبيعية توزيع البيانات

أبعاد الدراسة	احصاء الاختبار Kolmogorov_ Smirnov	مستوى الدلالة الإحصائي Asymp Sig	القرار
تأثير إداره أمن المعلومات علي نجاح برامج أمن نظم المعلومات المحاسبية	١,٢٤٢	٠,٠٩١	طبيعي

المصدر: نتائج التحليل الإحصائي

من الجدول السابق نجد أن مستوى الدلالة الإحصائية (Sig) لهذا البعد أكبر من مستوى المعنوية (α=0.05) وبالتالي تم قبول الفرض العدمي بأن البيانات الخاصة له مسحوبة من مجتمع يتبع التوزيع الطبيعي وبالتالي تم الاعتماد على الأساليب الإحصائية الخاصة بالاختبارات المعلمية وهي:

أولاً: عمل تحليل وصفى لكل فقرة من فقرات الاستقصاء

ثانياً: اختبار T لعينة واحدة

ثالثاً: أسلوب تحليل التباين أحادي الاتجاه One – Way ANOVA

٨/٤ اختبار فروض الدراسة ونتائج التحليل الإحصائي

١/٨/٤ نتائج اختبارات التحليل الإحصائي

ينص الفرض الرئيسي للدراسة على أنه: "تؤثر إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية في بيئة الأعمال المصرية".

ويندرج تحت هذا الفرض الفروض الفرعية التالية:

- **الفرض الفرعي الأول: "يؤثر التنفيذ المستمر للسياسات المتعلقة بأمن المعلومات إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية".**
- **الفرض الفرعي الثاني: "يؤثر وجود إجراءات لتنفيذ عمليات وأنشطة سياسات أمن المعلومات إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية".**
- **الفرض الفرعي الثالث: "يؤثر وجود فريق متخصص في إدارة أمن المعلومات إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية" .**
- **الفرض الفرعي الرابع: "يؤثر وجود فريق تنسيق لإدارة أمن المعلومات حيث التواصل بفعالية مع جميع المستويات بالمنظمة إيجاباً علي نجاح برنامج أمن نظم المعلومات المحاسبية".**
- **الفرض الفرعي الخامس: "يؤثر وجود فريق مسئول عن ضمان ضوابط الرقابة إيجاباً علي نجاح برنامج أمن نظم المعلومات المحاسبية".**
- **الفرض الفرعي السادس: "يؤثر التقييم الجيد لإدارة أمن نظم المعلومات إيجاباً علي نجاح برنامج أمن نظم المعلومات المحاسبية".**

يتم اختبار ذلك الفرض بفروضه الفرعية من خلال قياس استجابات عينة الدراسة على الأسئلة الخاصة بهذا الجزء في استمارة الاستقصاء وذلك من خلال عمل دراسة استكشافية للبيانات بالإضافة الى الاختبارات الخاصة بالفروض وذلك على النحو التالي:

أولاً: نتائج التكرارات والنسب المئوية والوسط الحسابي والإنحراف المعياري المتعلقة بمدى تأثير إدارة أمن المعلومات على نجاح برامج أمن نظم المعلومات المحاسبية . ويتم عمل دراسة استكشافية لهذا البعد من خلال الجدول التالي:

جدول (١١)
التكرارات والنسب المئوية والوسط الحسابي والإنحراف المعياري للعبارات الخاصة باختبار الفرض السادس

العبارة	موافق تماما	موافق	محايد	غير موافق	غير موافق تماما	الوسط الحسابي	الإنحراف المعياري	الإتجاه العام
$X1_1$	٤٥	٥٨	١٦	١	-	٤,٢٢٥٠	٠,٧٠٣٦٨	موافق
	%٣٧,٥	%٤٨,٣	%١٣,٣	٠,٨%	-			
$X1_2$	٣٩	٦٧	١٤	-	-	٤,٢٠٨٣	٠,٦٣٣٧٣	موافق
	%٣٢,٥	%٥٥,٨	%١١,٧	-	-			
$X1_3$	٥٨	٥٣	٨	١	-	٤,٤٠٠٠	٠,٦٥٣٣٧	موافق تماما
	%٤٨,٣	%٤٤,٢	٦,٧%	٠,٨%	-			
$X1_4$	٤٣	٥٦	٢١	-	-	٤,١٨٣٣	٠,٧٠٩٨٧	موافق
	%٣٥,٨	%٤٦,٧	%١٧,٥	-	-			
$X1_5$	٤٨	٥٢	٢٠	-	-	٤,٢٣٣٣	٠,٧١٨٧٠	موافق
	%٤٠	%٤٣,٣	%١٦,٧	-	-			
$X1_6$	٦٠	٤٢	١٨	-	-	٤,٣٥٠٠	٠,٧٢٩٣٤	موافق تماما
	%٥٠	%٣٥	%١٥	-	-			
الإجمالي	٢٩٣	٣٢٨	٩٧	٢	-	٤,٢٦٦٧	٠,٦٩١٤٥	موافق
	%٤٠,٧	%٤٥,٥	%١٣,٥	%٠,٣	-			

المصدر: نتائج التحليل الإحصائي

من جدول (١١) السابق نجد أن التحليل المبدئي للمتوسطات يشير إلى أن هناك اتجاه عام من أفراد عينة الدراسة على الموافقة على العبارات التي تختبر الفرض السادس والمتعلقة بمدى تأثير إدارة أمن المعلومات على نجاح برامج أمن نظم المعلومات المحاسبية, حيث نجد أن المتوسط العام للعبارات بلغ (٤,٢٦) وهو متوسط مرتفع إذا ما قورن بالمتوسط المرجح الخاص بمقياس ليكرت وهو مؤشر يوضح بشكل مبدئي أن إدارة أمن المعلومات تؤثر بشكل إيجابي على نجاح برامج أمن نظم المعلومات المحاسبية, مما يوضح بدوره أن التنفيذ المستمر للسياسات المتعلقة بأمن المعلومات ووجود إجراءات لتنفيذ عمليات وأنشطة سياسات أمن المعلومات والتقييم الجيد لإدارة أمن نظم المعلومات هي عوامل هامة تؤثر إيجاباً على نجاح برامج أمن نظم المعلومات المحاسبية.

ثانياً: اختبار T للفرض

ذكرنا سلفاً أن البيانات التي تختبر هذا الفرض تتبع التوزيع الطبيعي وبالتالي يتم إجراء الاختبارات المعلمية عليها، ويمثل أحد هذه الاختبارات اختبار T وذلك لقياس تأثير إدارة أمن المعلومات على نجاح برامج أمن نظم المعلومات المحاسبية.

جدول (١٢)
نتائج اختبار T

البعد	قيمة Tالمحسوبة	درجات الحرية df	مستوي الدلالة الإحصائية Sig	متوسط الفروق	فترة الثقة للفرق	
					الحد الأدنى	الحد الأعلى
تأثير إدارة أمن المعلومات على نجاح برامج أمن نظم المعلومات المحاسبية.	١٩,٧٢١	١١٩	,٠٠٠	٨٦٦٦٧ ,	,٧٧٩٦	,٩٥٣٧

المصدر: نتائج التحليل الإحصائي

من الجدول السابق نجد أن مستوى الدلالة الإحصائية (Sig=0.00) وهي أقل من مستوى المعنوية (α=0.05) وهذا يعني قبول الفرض البديل القائل بأن إدارة أمن المعلومات تؤثر إيجاباً علي نجاح برامج أمن نظم المعلومات المحاسبية, وذلك بدرجة ثقة ٩٥%.

ثالثاً: نتائج اختبار Chi-Square للفروض الفرعية

يتم استخدام اختبار Chi-Square لاختبار الفروض الفرعية وذلك كما هو موضح في الجدول(١٣):

جدول (١٣)
نتائج اختبارChi-Square للفروض الفرعية

العبارة	قيمة Chi-Square المحسوبة	مستوي الدلالة الإحصائية sig
• التنفيذ المستمر للسياسات المتعلقة بأمن المعلومات.	٦٨,٢٠٠	٠,٠٠٠
• وجود إجراءات لتنفيذ عمليات وأنشطة سياسات أمن المعلومات.	٣٥,١٥٠	٠,٠٠٠
• جود فريق متخصص في إدارة أمن المعلومات.	٨٧,٩٣٣	٠,٠٠٠
• وجودفريق تنسيق لإدارة أمن المعلومات حيث التواصل بفعالية مع جميع المستويات بالمنظمة	١٥,٦٥٠	٠,٠٠٠
• وجود فريق مسئول عن ضمان ضوابط الرقابة.	١٥,٢٠٠	٠,٠٠٠
• التقييم الجيد لإدارة أمن نظم المعلومات.	٢٢,٢٠٠	٠,٠٠٠

المصدر: نتائج التحليل الإحصائي

من الجدول السابق نجد أن: مستوى الدلالة الإحصائية لجميع الفروض الفرعية (sig = 0.000) وهي أقل من مستوى المعنوية (α=0.05) وهذا يعني قبول الفرض البديل القائل بأن:

١. التنفيذ المستمر للسياسات المتعلقة بأمن المعلومات يؤثر إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية.

٢. وجود إجراءات لتنفيذ عمليات وأنشطة سياسات أمن المعلومات تؤثر إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية.

٣. وجود فريق متخصص في إدارة أمن المعلومات يؤثر إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية.

٤. وجود فريق تنسيق لإدارة أمن المعلومات حيث التواصل بفعالية مع جميع المستويات بالمنظمة يؤثر إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية.

٥. وجود فريق مسئول عن ضمان ضوابط الرقابة يؤثر إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية.

٦. التقييم الجيد لإدارة أمن نظم المعلومات يؤثر إيجاباً على نجاح برنامج أمن نظم المعلومات المحاسبية.

رابعاً: اختبار تحليل التباين أحادي الاتجاه (ANOVA Test)

يتم استخدام أسلوب تحليل التباين وذلك لقياس معنوية الفرق بين آراء عينة الدراسة من جانب عدد المحاسبين في المنظمة, وعدد المتخصصين في نظم المعلومات, والمسمى الوظيفي, وعدد سنوات الخبرة, والنظام المحاسبي في المنظمة حول تأثير إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية وذلك كالآتي:

١- اختبار معنوية الفرق بين آراء عينة الدراسة وفقا لعدد المحاسبين في المنظمة

يتم قياس معنوية الفرق في آراء عينة الدراسة من جانب عدد المحاسبين, وذلك كما هو موضح من الجدول التالي:

جدول (١٤)

نتائج تحليل التباين للفرض السادس وفقاً لعدد المحاسبين في المنظمة

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	ف المحسوبة	مستوي الدلالة الإحصائية (Sig)	القرار
بين المجموعات	٢٩٩ ,٠	٣	٠,١٠٠	٠,٤٢٤	٠,٧٣٦	غير معنوي
داخل المجموعات	٢٧,٢٧٨	١١٦	,٢٣٥ ٠			
الكلي	٢٧,٥٧٨	١١٩				

المصدر: نتائج التحليل الإحصائي

من الجدول السابق نجد أن مستوى الدلالة الإحصائية (Sig= 0.736) وهي أكبر من مستوى المعنوية (α=0.05) وهذا يدل على عدم وجود فروق ذات دلالة إحصائية بين آراء عينة الدراسة وفقا لعدد المحاسبين في المنظمة حول تأثير إدارة أمن المعلومات على نجاح برامج أمن نظم المعلومات المحاسبية.

٢- اختبار معنوية الفرق بين آراء عينة الدراسة وفقا لعدد المتخصصين في نظم المعلومات

يتم قياس معنوية الفرق في آراء عينة الدراسة من جانب عدد المتخصصين في نظم المعلومات وذلك كما هو موضح من الجدول (١٥):

جدول (١٥)

نتائج تحليل التباين للفرض السادس وفقاً لعدد المتخصصين في نظم المعلومات

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	ف المحسوبة	مستوي الدلالة الإحصائية (Sig)	القرار
بين المجموعات	٠,٠٢٥ ١	٤	٠,٢٥٦	١,١١٠	٠,٣٥٥	غير معنوي
داخل المجموعات	٢٦,٥٥٣	١١٥	٠,٢٣١			
الكلي	٢٧,٥٧٨	١١٩				

المصدر: نتائج التحليل الإحصائي

من الجدول السابق نجد أن مستوى الدلالة الإحصائية (Sig= 0.355) وهي أكبر من مستوى المعنوية (α=0.05) وهذا يدل على عدم وجود فروق ذات دلالة إحصائية بين آراء عينة الدراسة من جانب عدد المتخصصين في نظم المعلومات حول تأثير إدارة أمن المعلومات على نجاح برامج أمن نظم المعلومات المحاسبية.

٣- اختبار معنوية الفرق بين اراء عينة الدراسة وفقا للمسمى الوظيفي

يتم قياس معنوية الفرق في آراء عينة الدراسة من جانب المسمى الوظيفي وذلك كما هو موضح من الجدول التالي:

جدول (١٦)

نتائج تحليل التباين للفرض السادس وفقاً للمسمى الوظيفي

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	ف المحسوبة	مستوي الدلالة الإحصائية (Sig)	القرار
بين المجموعات	٠,٩٤٤	٦	,١٥٧ ٠	,٦٦٧ ٠	٠,٦٧٦	غير معنوي
داخل المجموعات	٢٦,٦٣٤	١١٣	,٢٣٦ ٠			
الكلي	٢٧,٥٧٨	١١٩				

المصدر: نتائج التحليل الإحصائي

من الجدول السابق نجد أن مستوى الدلالة الإحصائية (Sig= 0.676) وهي أكبر من مستوى المعنوية (α =0.05) وهذا يدل على عدم وجود فروق ذات دلالة إحصائية بين آراء عينة الدراسة من جانب المسمى الوظيفي حول تأثير إدارة أمن المعلومات على نجاح برامج أمن نظم المعلومات المحاسبية.

٤- اختبار معنوية الفرق بين اراء عينة الدراسة وفقا لسنوات الخبرة

يتم قياس معنوية الفرق في آراء عينة الدراسة من جانب سنوات الخبرة وذلك كما هو موضح من الجدول (١٧)

جدول (١٧)
نتائج تحليل التباين للفرض السادس وفقاً لسنوات الخبرة

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	ف المحسوبة	مستوي الدلالة الإحصائية (Sig)	القرار
بين المجموعات	١,١٠٤	٥	,٢٢١	,٩٥١	٠,٤٥١	غير معنوي
داخل المجموعات	٢٦,٤٧٤	١١٤	,٢٣٢			
الكلي	٢٧,٥٧٨	١١٩				

المصدر: نتائج التحليل الإحصائي

من الجدول السابق نجد أن مستوى الدلالة الإحصائية (Sig= 0.451) وهي أكبر من مستوى المعنوية (α =0.05) وهذا يدل على عدم وجود فروق ذات دلالة إحصائية بين آراء عينة الدراسة من جانب سنوات الخبرة حول تأثير إدارة أمن المعلومات على نجاح برامج أمن نظم المعلومات المحاسبية.

٥- اختبار معنوية الفرق بين آراء عينة الدراسة وفقا للنظام المحاسبي في المنظمة

يتم قياس معنوية الفرق في آراء عينة الدراسة من جانب النظام المحاسبي في المنشأة وذلك كما هو موضح من الجدول (١٨)

جدول (١٨)
نتائج تحليل التباين للفرض السادس وفقاً للنظام المحاسبي في المنشأة

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	ف المحسوبة	مستوي الدلالة الإحصائية (Sig)	القرار
بين المجموعات	٠,٤٠١	٢	,٢٠٠	٠,٨٦٢	٠,٤٢٥	غير معنوي
داخل المجموعات	٢٧,١٧٧	١١٧	,٢٣٢			
الكلي	٢٧,٥٧٨	١١٩				

المصدر: نتائج التحليل الإحصائي

من الجدول السابق نجد أن مستوى الدلالة الإحصائية (Sig= 0.425) وهي أكبر من مستوى المعنوية (α =0.05) وهذا يدل على عدم وجود فروق ذات دلالة إحصائية بين آراء عينة الدراسة من جانب النظام المحاسبي في المنظمة حول تأثير إدارة أمن المعلومات على نجاح برامج أمن نظم المعلومات المحاسبية.

مما سبق نستنتج أنه تم قبول الفرض البديل القائل بأن إدارة أمن المعلومات تؤثر إيجاباً وجوهرياً على نجاح برامج أمن نظم المعلومات المحاسبية, وذلك بدرجة ثقة ٩٥%.

٥- خلاصة ونتائج وتوصيات البحث والبحوث المستقبلية

١/٥ خلاصة ونتائج البحث

استهدف البحث التعرف على تأثير إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية من خلال بعض المقاييس التي تؤثر على فعالية إدارة أمن المعلومات، ويمكن تلخيص أهم نتائج البحث النظرية والميدانية على النحو التالي:

١. تعرض نظم المعلومات المحاسبية الإلكترونية للعديد من المخاطر يتمثل أهمها في العنصر البشري، لذلك يجب تدريبهم باستمرار على مواجهة المخاطر والتعامل معها.
٢. إجراءات أمن المعلومات أقرب إلى المستخدمين والأجهزة من السياسة الأمنية حيث توفير الخطوات التفصيلية لتركيب وتهيئة البرامج.
٣. وجود فروق جوهرية بين إدارة أمن المعلومات وحوكمة أمن نظم المعلومات.
٤. إدارة أمن المعلومات تؤثر إيجابياً وجوهرياً على نجاح برنامج أمن نظم المعلومات المحاسبية، وذلك بدرجة ثقة ٩٥%.

٢/٥ توصيات البحث

استناداً إلى ما تم التوصل إليه أن توصي الدراسة بما يلي:

١. اتباع نهج فعال في حماية البيانات والمعلومات يضع أمام قراصنة المعلومات تحديات صعبة تعيقهم من الوصول إلى المعلومات.
٢. ضرورة اهتمام منظمات الأعمال بإدارة أمن المعلومات واعتبارها عنصراً إلزامياً على قائمة أعمالها.
٣. ضرورة توفير برامج تدريبية متخصصة بأمن نظم المعلومات للأفراد الذين يرتبط عملهم المباشر بأمن نظم المعلومات.

٣/٥ توصيات البحوث المستقبلية

في ضوء ما توصل إليه البحث من نتائج وتوصيات، فقد ظهرت بعض المجالات البحثية المرتبطة بموضوع البحث والتي يمكن تناولها في البحوث المستقبلية ومنها:

١. **عوامل النجاح الحاسمة والهامة التي تؤثر على إدارة أمن المعلومات: دراسة ميدانية على الشركات المصرية.**
٢. **إطار مقترح لحوكمة أمن المعلومات مع دراسة تطبيقية في البيئة المصرية.**
٣. **دراسة أثر انتشار فيروس كورونا المستجد (كوفيد ١٩) على فعالية النظام المحاسبي الإلكتروني.**

٦- مراجع البحث

أولاً: المراجع العربية

- أبو موسي، أحمد عبد السلام وخطاب، محمد شحاته، (٢٠١٢)، "عوامل نجاح برامج أمن نظم المعلومات المحاسبية ودورها في تفعيل حوكمة الشركات: دراسة ميدانية علي الشركات السعودية"، ***مجلة كلية تجارة للبحوث العلمية***- كلية التجارة – جامعة الاسكندرية, ص ص ١- ٥١.
- أبو موسي، أحمد عبد السلام، (٢٠٠٥)، "الربط بين حوكمة تكنولوجيا المعلومات وتفعيل حوكمة الشركات: نموذج مقترح من سياق المحاسبة الإدارية"، ***مجلة التجارة والتمويل***، كلية التجارة- جامعة طنطا- مصر، العدد الثاني، ص ص ٥٣-١١٨.
- حامد، عاصم نائل رشيد والحمود، تركي راجي موسي، (٢٠٠٩)، "مخاطر أمن نظم المعلومات المحاسبية المحوسبة: دراسة ميدانية علي القطاع الصناعي الأردني"، ***رسالة ماجستير***، كلية الاقتصاد والعلوم الإدارية- جامعة اليرموك- الأردن، ص ص ١-٢١١.
- خليل، علي محمود مصطفي وإبراهيم، مني مغربي محمد، (٢٠١٦)، "الدور التأثيري لحوكمة أمن المعلومات في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة ميدانية"، كلية التجارة- جامعة بنها، ص ص ١- ٢٧.
- دعدوع، شهيرة، (٢٠١٦)، "مفهوم أمن المعلومات"، متاح علي الموقع التالي: https://mawdoo3.com. (٢٠١٩/٥/١٤)

ثانياً: المراجع الأجنبية

- Abu-Musa, Ahmed A, (2010), "Information Security Governance in Saudi Organizations: An Empirical Study", ***Information Management and Computer Security***, Vol. 18, No. 4, pp. 20-276.
- Allen, Julia, (2007), "Characteristics of Effective Security Governance".
- Alnatheer, M, (2015), "Information Security Culture Critical Success Factors", ***International Conference on Information Technology- New Generation***.

- Doherty, N.F &Fulford, H., (2005), "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis", ***Information Resources Management Journal***, Vol. 18, No. 2.
- Fung, P., Kwok, L. &Longley, D., (2003), "Electronic Information Security Documentation", Australian Computer Society, Vol. 21.
- Gordon, L.A &Loep, M.P, (2006), "Budgeting Process for Information Security Expenditures", Communications of the ACM, Vol. 49, No.1.
- Greene, Sari, (2014), "Security Program and Policies: Governance and Risk Management", ***Pearson IT Certification***, Available at: http://www.pearsonitcertification.com/articles/article.aspx?p=2192704 (23/11/2019).
- Hone, K &Eloff, J.H.P., (2002), "What makes an Effective Information Security Policy", Network Security, Vol. 20, No. 6.
- ISACA (2008), "Model Curriculum for Information Security Management", ***Information Systems Audit and Control Association***.
- ISACA, (2012), "COBIT 5 for Information Security".
- ISO/IEC 27002:2013, "Information Technology_ Security Techniques_ Code of Practice for Information Security Management", Geneva: ISO, 2013.
- Maarop, N; Mustapha, N; Yusoff, R; Ibrahim, R and Zainuddin, N, (2015), "Understanding Success Factors of an Information Security Management System Plan Phase Self-Implementation", ***International Journal of Computer and Information Engineering***, Vol. 9, No. 3.

- Madigan, E.M., Petrulich, C. and Motuk, K., (2004), "The Cost of Non-Compliance When Policies Fail", Proceeding of the 32nd annual ACMSIGUCCS Conference on User services, USA.
- Muhrtala, T. and Ogundeji, M., (2013), "Computerized Accounting Information Systems and Perceived Security Threats in Developing Economies: The Nigerian Case"**,** ***Universal Journal of Accounting and Finance***, Vol. 1, issue. 1, pp. 9-18.
- NIST Special Publication 800-100, (2006), "Information Security Handbook: A Guide for Managers".
- Rotvold, Glenda, (2008), "How to Create a Security Culture in Organization", ***Information Management Journal***, pp. 32-38.
- Singh, A and Gupta, M, (2014), "Identifying Factors of organizational information security management", ***Journal of Enterprise Information Management***, Vol. 27, No. 5.
- Solms, B.V., (2005), "Information Security Governance: COBIT or ISO 17799 or both?" ***Computer& Security***, Vol.24, pp. 99-104.
- Tryfonas, T., Kiountouzis, E. & Poulymenakou, A., (2001), "Embedding Security Practices in Contemporary Information Systems Development Approaches", Information Management& Computer Security, Vol. 9, No. 4.
- Vizcayno, Danieliyo, (2012), "What is Information Security Governance?", Available a White, R, (2011), "Computers at Risk: Safe Computing in the information Age", Available at: http://www.books.google.co.zw/books?isbn=0309043883 . (20/11/2019)
- White, R, (2011), "Computers at Risk: Safe Computing in the information Age", Available at: http://www.books.google.co.zw/books?isbn=0309043883 . (20/11/2019)

- Whitman, M.E &Mattord, H.J; (2005), "Principles of Information Security"
- Zammani, M and Razali, R, (2016), "An Empirical Study of Information Security Management Success Factors", ***International Journal on Advanced Science Engineering information Technology***, Vol. 6, No. 6.