عوامل نجاح برامج أمن نظم المعلومات المحاسبية ودورها في تفعيل حوكمة الشركات: دراسة ميدانية على الشركات السعودية

The Critical Success Factors of Accounting Information Systems' Security Programs and its Role in Activating Corporate Governance: An Empirical Study in Saudi Companies

إعــداد

دكتور / أحمد عبد السلام أبو موسى
أستاذ مساعد بقسم المحاسبة
كلية التجارة
جامعة طنطا

دكتور / محمد شحاتة خطاب
مدرس بقسم المحاسبة
كلية التجارة
جامعة طنطا

٢٠١٢

عوامل نجاح برامج أمن نظم المعلومات المحاسبية ودورها في تفعيل حوكمة الشركات: دراسة ميدانية على الشركات السعودية

مستخلص Abstract

يهدف هذا البحث إلى دراسة عوامل نجاح برامج أمن نظم المعلومات المحاسبية ودورها في تفعيل حوكمة الشركات وذلك من خلال دراسة ميدانية على عينة من الشركات السعودية. ولقد قدم البحث نموذجاً وصفياً مقترحاً لعوامل نجاح برامج أمن نظم المعلومات المحاسبية كما تناول البحث أهمية أمن المعلومات وضرورة الحفاظ عليها ضد المخاطر العديدة التي قد تتعرض لها، ودور مبادئ حوكمة الشركات كعامل أساسي من عوامل نجاح برامج أمن نظم المعلومات المحاسبية. ولقد قام البحث بوضع واختبار عدداً من الفروض البحثية المتعلقة بعوامل نجاح برامج أمن نظم المعلومات المحاسبية في بيئة الأعمال السعودية، ولقد أبرزت نتائج الدراسة الميدانية أهمية عوامل نجاح برامج أمن نظم المعلومات المحاسبية المختارة بالنسبة للشركات السعودية، وأوصت الدراسة بضرورة أخذ هذه العوامل في الحسبان وحث الإدارة العليا والمستويات الإدارية الأخرى بالمنشأة وكل العاملين بها على تبنى هذه العوامل وجعلها جزء من ثقافة العاملين بالمنشأة.

المصطلحات المستخدمة Key Words

[أمن المعلومات Information Security – إدارة أمن المعلومات Information Security Management (ISM) – عوامل النجاح الحاسمة Critical Success Factors (CSFs) – برامج أمن المعلومات Information Security Programs – تكنولوجيا المعلومات Information Technology (IT) – حوكمة الشركات Corporate Governance]

١. مقدمة

يمثل العصر الذي نعيش فيه الآن واحداً من أهم عصور المعرفة والتكنولوجيا في شتى المجالات ومنها مجال المعلومات، الذي يمثل بحق حرب مستمرة بين الشركات والكيانات الاقتصادية المتنافسة في العالم، فباستخدام المعلومات يمكن تحقيق أرباح كبيرة لشركة ما وتحقيق خسائر ضخمة لشركة أخرى منافسة، ولذلك يجب على كل شركة أو كيان اقتصادي العمل على تأمين المعلومات ضد المخاطر المحتملة التي قد تتعرض لها.

إن تهديدات ومخاطر أمن نظم المعلومات المحاسبية يمكن أن تكون في شكل تحريف المدخلات، سرقة وقت أجهزة الكمبيوتر واستخدامه في الأغراض الشخصية، سرقة البيانات / المعلومات، عدم الحفاظ على سرية البيانات، الدخول غير المصرح به للنظم والشبكات، الاستخدام غير المصرح به للبيانات، التلاعبات والاختلاسات، الغش في استخدام المعلومات، الخسائر الناتجة عن عدم تكامل المعلومات، التغيير المتعمد وغير المصرح به للبيانات، تخريب وتدمير بعض الملفات، فشل النظام وسقوط شبكة الاتصال، منع الأشخاص المخول لهم بالدخول إلى النظام من

ممارسة هذا الحق Denial of Services، الكوارث الطبيعية مثل الحرائق والفيضانات أو انقطاع مصدر الطاقة، الكوارث غير الطبيعية والتي هي من صنع الإنسان مثل الحرائق المفتعلة وغيرها، إدخال فيروس الكمبيوتر للنظام، طمس أو تدمير بنود معينة من مخرجات الحاسب، خلق مخرجات زائفة / غير صحيحة، عمل نسخ غير مصرح (مرخص) بها من مخرجات الحاسب، الإظهار غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق؛ طبع وتوزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك، توجيه المطبوعات والمعلومات خطأً إلى أشخاص غير مخول لهم / ليس لهم الحق في الإطلاع عليها أو الحصول على نسخة منها، تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية وذلك بغرض تمزيقها أو التخلص منها، وكذلك مقاطعة تحويل البيانات من أماكن بعيدة **[أحمد أبو موسى، ٢٠٠٥ ,Schweitzer 1987; OECD, 1992; Loch et al., 1992; Davis, 1996 and 1997; FFIEC, 1996; Henry, 1997; Haugen and Selin, 1999; Abu Musa, 2003]**

ويؤكد البعض على أن نظم المحاسبة الإلكترونية تتعرض لكثير من المخاطر والتهديدات ومنها التلاعب في البيانات بقصد تدميرها سواء بالحذف، أو بالدمج غير الصحيح لبعضها، أو بخلطها ببيانات أخرى غير حقيقية أو تبويبها بشكل خاطئ تفقد معه مدلولها ومعناها؛ وأن ذلك التلاعب يمكن أن يحدث في أجزاء مختلفة من نظام المعلومات المحاسبي كحسابات التكاليف، أو المخزون، أو النقدية، أو المبيعات، أو المصروفات، أو قد يكون تدمير البيانات ناتجاً عن تغيير (تعديل) في البيانات Data Change (Modification) بشكل يجعلها لا تعبر عن الحقائق التي نتجت عنها أصلاً. وتتضمن أمثلة التغيير في البيانات، التلاعب في حسابات المدينين والدائنين بقصد الغش. وقد يحدث هذا التلاعب في مراحل مختلفة من النظام مثل المدخلات أو التشغيل أو التخزين أو المخرجات. وأن تدمير البيانات قد يكون جزئياً أو كلياً وفى الحالة الأخيرة قد يصعب تصحيح البيانات أو استعادتها، مما يشكل خسارة كبيرة لنظام المعلومات وما ينتج عنه من قرارات. وكذلك قد يغير من نتائج أعمال الشركة أو مركزها المالي ويتيح تغطية سرقات أو اختلاسات في أصول الشركة. وقد يهدف التلاعب بالنظام إلى الإطلاع على بيانات سرية Disclosure of confidential Data مثل بيانات تخطيط الربحية، أو بيانات الأفراد (الرواتب والترقيات والعلاوات). ويمكن للمتلاعب في هذه الحالة ليس فقط الإطلاع على البيانات وإساءة استخدامها بل أيضاً سرقة بعضها أو كلها. ذلك كله قد ينتج عنه خسائر للمنشآت تكون كبيرة في بعض الحالات **[سمير هلال، ١٩٩٢، ص ٥٨-٥٩]**.

ولقد شهد الفكر المحاسبي بوجه عام ونظم المعلومات المحاسبية بوجه خاص تطوراً سريعاً وملحوظاً أظهرته العديد من الأبحاث المنشورة في هذا المجال، وبدأ يظهر ملامحها في الواقع العملي بالشركات التي تريد البقاء والاستمرار والتنافس في السوق خاصة الشركات الصناعية بدول اليابان والولايات المتحدة الأمريكية ومعظم دول أوروبا وجنوب شرق أسيا.

ومما لاشك فيه أن تكنولوجيا المعلومات قد أصبحت أساساً لإدارة العمليات والمعرفة اللازمتين لخلق والمحافظة على الأنشطة الاقتصادية والاجتماعية للشركات، حيث أصبحت قدرة الشركات على البقاء والنمو والاستمرار تعتمد بدرجة كبيرة على مدى كفاءتها في إدارة تكنولوجيا المعلومات للاستفادة من الفرص والمزايا وكذلك مدى قدرتها على مواجهة التحديات وإدارة المخاطر المتعلقة بها. إن حوكمة تكنولوجيا المعلومات يمكن أن تسهم بدور فعال في خلق مزايا تنافسية وإضافة قيمة حقيقية للشركات وذلك من خلال تحسين السمعة، تحقيق الريادة في المنتجات، زيادة النصيب السوقي، تقديم منتجات جديدة ذات جودة عالية وبتكلفة أقل، وزيادة درجة إرضاء المستهلكين والأطراف الأخرى ذات العلاقة مما يؤدى إلى زيادة قيمة المنشآت وثروة الملاك. وتعد حوكمة تكنولوجيا المعلومات أحد المحددات الإستراتيجية المهمة لنجاح أو فشل تلك الشركات نظراً لما تتطلبه من استثمارات ضخمة وما تتضمنه من درجات مخاطرة عالية **[أبو موسى، ٢٠٠٥]**. وفى ضوء ما تتعرض إليه الأسواق العالمية والاقتصاد العالمي من انكماش وتدهور وتعرض العديد من الشركات العالمية الكبرى للإفلاس، كان لزاما على الإدارة توجيه الاهتمام بعمليات جمع المعلومات وتصنيفها وتبويبها وتخزينها بطرق آمنه. ومن ثم فلقد أصبح أمن المعلومات التي تحتويها النظم الإلكترونية، وخاصة المالية والمحاسبية، موضع اهتمام وقلق لإدارات المؤسسات والمنشآت التي تستخدم هذه النظم، ولمراجعي الحسابات الذين يقومون بفحصها ومراجعة البيانات المالية المستخرجة منها لإبداء الرأي في مدى سلامتها. ويرجع هذا القلق إلى تزايد أنواع واحتمالات المخاطر المحيطة بهذه النظم والتي تهدد صحة وموثوقية وسرية وتكامل البيانات المالية والمحاسبية فيها **[أبو موسى، ٢٠٠٥]**.

٢. الإطار العام للبحث

٢-١. مشكلة البحث والباعث على الدراسة

لقد واجهت العديد من الشركات الأمريكية منافسة حادة من قبل الشركات اليابانية منذ الثمانينيات من القرن الماضي، ولقد تعرض العديد من الشركات العالمية العملاقة في الوقت الحاضر (العقد الأول من القرن الحادي والعشرون الميلادي) للإفلاس نتيجة الأزمة العالمية الحادة التي تعرض لها الاقتصاد العالمي. ولقد رأى بعض مديري تلك الشركات أن المعلومات المستمدة من النظم المحاسبية لديها سوف تساعدهم على مواجهة هذه المنافسة، ولكنهم يحتاجون إلى نظام معلومات قوى يعكس كل المعلومات الدقيقة والصحيحة عن العمليات الداخلية للشركة ومعلومات عن القوانين والسياسات المحيطة بها ومعلومات عن العاملين بها، ومعلومات عن الشركات المنافسة وغيرها من المعلومات.

وقد أصبح هناك اعتماد متزايد من قبل المنشآت على نظم المعلومات نتيجة التطور في الاتصالات والتوسع في فتح واستخدام شبكات الإنترنت تتطلب ضرورة تحقيق درجات كافية من أمن المعلومات، وبالتالي يجب على المنشآت الحديثة ضرورة توافر مجموعة من عوامل النجاح

الضرورية والمهمة لنجاح برامج أمن المعلومات. ولذلك تحتاج هذه المعلومات إلى حماية من قبل إدارة المنشأة حتى لا تتعرض للسرقة أو التدمير من قبل الشركات والكيانات الاقتصادية المنافسة، وعليه ظهرت الحاجة إلى ضرورة البحث عن مجموعة من العوامل التي تؤدى إلى نجاح برامج أمن المعلومات.

٢-٢. هدف البحث

يهدف البحث إلى وضع إطار مقترح لتحديد ودراسة عوامل نجاح برامج أمن نظم المعلومات المحاسبية، ودورها في تفعيل حوكمة الشركات واختبار هذه العوامل في بيئة الأعمال السعودية. ولتحقيق ذلك الهدف يحاول البحث الإجابة على الأسئلة الآتية:

(١) ما أهمية أمن المعلومات بالنسبة للشركات؟
(٢) ما دور مبادئ حوكمة الشركات في تعزيز أمن المعلومات؟
(٣) ما أسباب التعرف على ودراسة مجموعة العوامل التي تؤدى إلى نجاح برامج أمن المعلومات؟
(٤) ما دور عوامل نجاح برامج أمن نظم المعلومات المحاسبية في تفعيل حوكمة الشركات؟
(٥) ما أهمية الإطار المقترح لعوامل نجاح برامج أمن نظم المعلومات المحاسبية وتأثيره على بيئة الأعمال السعودية؟

٢-٣. فروض البحث

في ضوء مشكلة البحث وأهداف البحث وأسئلة البحث تم استخلاص وصياغة مجموعة فروض لاختبارها ميدانياً على عينة من الشركات السعودية:

الفرض الأول: لا توجد اختلافات جوهرية بين المنشآت السعودية في القطاعات الاقتصادية المختلفة فيما يتعلق بمدى إدراكها لعوامل النجاح الهامة لبرامج أمن نظم المعلومات المحاسبية.

الفرض الثاني: لا توجد اختلافات جوهرية بين إدراك الوظائف المختلفة داخل المنشآت السعودية فيما يتعلق بعوامل النجاح الهامة لبرامج أمن نظم المعلومات المحاسبية.

الفرض الثالث: لا توجد اختلافات جوهرية بين المنشآت السعودية التي تستخدم نظماً محاسبية مختلفة فيما يتعلق بمدى إدراكها لعوامل النجاح الهامة لبرامج أمن نظم المعلومات المحاسبية.

٢-٤. منهج البحث

لقد تم تطبيق المنهج الإستقرائى Inductive Approach لدراسة والتعرف على عوامل نجاح برامج أمن نظم المعلومات المحاسبية ودورها في الحفاظ على وحماية أمن المعلومات وتفعيل حوكمة الشركات. ولقد قام الباحثان بإجراء دراسة ميدانية للتعرف على أهم عوامل نجاح برامج أمن نظم المعلومات المحاسبية؛ واختبار الفروق الجوهرية بين المنشآت المختلفة فيما يختص بمدى

إدراكها لأهمية تلك العوامل في بيئة الأعمال بالمملكة العربية السعودية؛ مستخدماً في ذلك استمارة استقصاء (ملحق ١) أعدت خصيصاً لتحقيق هذا الغرض. ولقد قام الباحثان بإجراء التحليلات الوصفية Descriptive Analysis (مثل معدل التكرارات والنسب) للبيانات التي تم تجميعها للتعرف على الخصائص الأساسية لعينة البحث ومتغيرات الدراسة. كما تم إجراء بعض الاختبارات اللامعلمية Non-Parametric Tests (مثل اختبار كارسوكال – ولاس Krsukal-Wallis واختبار تحليل التباين ANOVA) لاختبار فروض البحث والتعرف على الفروق الجوهرية بين المنشآت المختلفة وكذلك الوظائف المختلفة فيما يتعلق بإدراكها لعوامل نجاح برامج أمن نظم المعلومات المحاسبية في المنشآت السعودية.

٢-٥. خطة البحث

في إطار محاولة الإجابة على مجموعة الأسئلة البحثية، ولتحقيق هدف البحث، تم وضع خطة البحث على النحو الآتي:

- تحليل الدراسات السابقة المتعلقة بعوامل نجاح برامج أمن نظم المعلومات المحاسبية.
- أهمية أمن المعلومات وضرورة الحفاظ عليها.
- التعرف على دور أمن المعلومات في تفعيل حوكمة الشركات وتعزيزها.
- عوامل نجاح برامج أمن نظم المعلومات المحاسبية ودورها في تفعيل حوكمة الشركات.
- الإطار المقترح لعوامل نجاح برامج أمن نظم المعلومات المحاسبية.
- دراسة ميدانية لاختبار مدى أهمية عوامل نجاح برامج أمن نظم المعلومات المحاسبية في منشآت الأعمال السعودية وتطبيقها.
- خلاصة البحث.

٣. الدراسات السابقة

تناولت العديد من الدراسات السابقة موضوع أمن المعلومات وأهمية الحفاظ عليها ضد المخاطر المحتملة التي تتعرض لها، إلا أن الدراسات السابقة لم تتناول موضوع عوامل نجاح برامج أمن نظم المعلومات المحاسبية بالقدر الكافي، ومن الدراسات التي تمت في هذا المجال:

(١) دراسة ISACA 2005

جمعية مراجعة ومراقبة نظم المعلومات Information Systems Audit and Control Association (ISACA) ، هي جمعية مهنية رائدة ومتخصصة في مراجعة نظم المعلومات، وقامت بالعديد من الدراسات في مجالات متنوعة منها حوكمة تكنولوجيا المعلومات IT Governance ورقابة وأمن وتأمين المعلومات، كما تناولت الدراسة عوامل نجاح برامج أمن نظم المعلومات المحاسبية في المنشآت المختلفة.

وقد قدمت هذه الجمعية اقتراحات من خلال مسح شامل قامت به وأصدرت تقريراً تضمن مجموعة من العوامل التي تؤثر في نجاح برامج أمن المعلومات. وقد كان ١٠٪ من المشاركين في الدراسة متخصصين في إدارة أمن المعلومات ويعملون في منشآت تجارية وحكومية واستشارية من ثمانية دول منها كندا وفرنسا وألمانيا وإيطاليا واليابان والولايات المتحدة، إلا أن هذا التمثيل لا يشمل كل أعضاء الجمعية، وضمت مجموعة الاستجابات في المسح الشامل ١٥٧ ممثل من عدة منشآت مثل منشآت الخدمات المالية وخدمات النقل وتجارة الجملة وتجارة التجزئة والمنشآت الحكومية والصناعية والصحية والاستشارية. وقد أضافت الدراسة مجموعة من العوامل الهامة التي تؤثر في نجاح برامج أمن المعلومات منها: فهم الإدارة لإصدارات أمن المعلومات والتخطيط المسبق لبرامج أمن المعلومات وغيرها من العوامل.

(٢) دراسة ISACA 2008

تناولت هذه الدراسة وضع نموذج كمنهج رئيسي لإدارة أمن المعلومات وأظهر النموذج عدة مجالات رئيسية إذا اتبعتها المنشأة سوف تصل إلى عدة عوامل تؤدى إلى نجاح برامج أمن المعلومات وهذه المجالات تتمثل في:

- حوكمة برامج أمن المعلومات Information Security Governance
- إدارة خطر المعلومات Information Risk Management
- تطوير برامج أمن المعلومات Information Security Program Development
- إدارة برامج أمن المعلومات Information Security Program Management
- إدارة والاستجابة لحوادث أمن المعلومات Incident Management and Response

وقد جاءت نتائج الدراسة تؤكد على ضرورة قيام المنشآت بتطبيق تلك المجالات حتى تصل إلى عدة عوامل تساعد في تفعيل ونجاح برامج أمن المعلومات.

(٣) دراسة Jenster, 1987

قامت هذه الدراسة بمسح لاستطلاع الرأي للتعرف على درجة العلاقة بين عوامل النجاح الهامة Critical Success Factors (CSFs) وأداء المنشآت، وكان الهدف من الدراسة البحث حول إمكانية التوصل إلى كيفية تحديد أثر استراتيجيات الأعمال المتولدة بالمنشأة على اختيار عوامل النجاح وعلى العلاقة بين عوامل النجاح وأداء المنشأة، وكانت نتيجة الدراسة أن هناك علاقة جوهرية بين عوامل النجاح الهامة وأداء المنشأة.

(٤) دراسة Kokolakis, et al. 2000

قامت هذه الدراسة بفحص أساليب نماذج تشغيل الأعمال كمساهمة لتحديد متطلبات مفاهيمية ومنهجية للمساعدة في تحسين برامج أمن المعلومات، وقد اكتشفت الدراسة أساليب عديدة نتيجة الفحص الذي قامت به، وقد ركزت تلك الدراسة على تحليل مخاطر أمن المعلومات وتوصلت

إلى اقتراح إطار يمكن للشركات تطبيقه والاعتماد عليه لتحسين والحفاظ على أمن المعلومات، وهذا الإطار يضم مجموعة من العوامل منها : تحليل عمليات وأنظمة المنشأة وتحديد النظم الملائمة لها، وتحليل أمن النظم المتوافرة للمنشأة، وتحليل المخاطر التي تتعرض لها أنظمة المنشأة، وتصميم أمن نظم المعلومات لدى المنشأة، ووضع وسائل لإرشاد وإدارة أمن المعلومات.

(٥) دراسة Chang & Ho 2006

تناولت هذه الدراسة فحص تأثير العوامل التنظيمية على فعالية إدارة أمن المعلومات لتحقيق المعيار البريطاني BS 7799 الخاص بتقييم إدارة أمن المعلومات (ISM) كأحد مقاييس رقابة أمن المعلومات، وقد توصلت الدراسة إلى وضع نموذج مقترح لدراسة أثر العوامل التنظيمية على إدارة أمن المعلومات بعد قيامها بمسح لكل الأبحاث المرتبطة بهذا الموضوع، وجاءت نتائج الدراسة لهذا النموذج المقترح تشير إلى استجابة مديري الشركات ومتخذي القرارات لتلك العوامل التي سوف تحقق أهداف أمن المعلومات ومن ثم نجاح برامج أمن المعلومات.

(٦) دراسة McFadzean, et al. 2007

أوضحت الدراسة أن أمن المعلومات أصبح له أهمية كبيرة ومتزايدة لمنشآت الأعمال التي تتعرض للخطر نتيجة التهديدات Threats والمخاطر المتنوعة سواء كانت من البيئة الداخلية Internal Environment أو البيئة الخارجية External Environment، وأكدت على أن سياسات أمن المعلومات يجب أن تتبع من قبل الإدارة العليا على أساس أن السلطة التنفيذية بالمنشأة هي القادرة على وضع المداخل والسياسات اللازمة لحماية المعلومات، بالإضافة إلى قدرتها على اقتناء وتطبيق إجراءات النظم الحديثة. ونتيجة لاستمرار عدم فهم أهمية الإستراتيجية اللازمة لإدارة أمن المعلومات، بالإضافة إلى وجود فجوة في العلاقة بين إدراك وفهم الإدارة وإستراتيجية أمن المعلومات، قامت الدراسة بمحاولة تقليل تلك الفجوة بين إدراك وفهم الإدارة لأمن معلومات منشآتهم والعوامل التي تؤثر في قراراتهم لتطوير وإنجاز إستراتيجية أمن المعلومات والتي تكون بمثابة عوامل لإنجاح برامج أمن المعلومات.

وقد خلصت الدراسة إلى أن قدرة وإدراك العاملين بأهمية أمن المعلومات يبدأ من تطوير إستراتيجية لأمن المعلومات، وتشجيع المديرين للتركيز على كل من المخاطر الداخلية والخارجية التي تواجه الشركة، وتشجيع الإدارة العليا للتفكير في وضع أهداف واضحة لشركاتهم وضرورة استجابة إستراتيجية أمن المعلومات لتحقيق تلك الأهداف. كما أن إدراك العاملين بأهمية أمن المعلومات يعتبر أداة مفيدة لتشجيع المديرين للتركيز على مخاطر أمن المعلومات التي تحدث فعلا والمتوقع حدوثها في المستقبل، وتشجيع المديرين أيضا على كشف العوامل التي تؤثر في وضع برامج أساسية لأمن المعلومات، ومساعدة الإدارة العليا على فحص تلك البرامج والاستراتيجيات التي تؤثر في نجاح برامج أمن المعلومات.

(٧) دراسة Chang & Lin 2007

تناولت هذه الدراسة تأثير الثقافة التنظيمية على فعالية إدارة أمن المعلومات، وقد أخذت الدراسة عينة من العوامل التنظيمية وطبقت على شركات تايوانية وأوصت بتطبيقها في دول أخرى، ومن العوامل المختارة في الدراسة :

- ضرورة تحقيق درجة من التعاون بين جميع المستويات التنظيمية Cooperativeness على أساس أن هذا العامل سيؤدى إلى حماية والحفاظ على المعلومات مما يساعد كعامل من عوامل نجاح برامج أمن نظم المعلومات المحاسبية.
- ضرورة تحقيق درجة من الابتكار والإبداع Innovativeness للوصول إلى أفكار وطرق وأساليب للحفاظ على وحماية المعلومات.
- تحقيق درجة كبيرة من الاتساق والتناغم Consistency بين أهداف المنشأة وهدف أمن المعلومات، ولمنع تضارب الأهداف بين العاملين مما يساعد على حماية المعلومات.
- تحقيق درجة من الفعالية Effectiveness .

وقد جاءت نتائج الدراسة الميدانية على عينة الشركات المختارة تؤكد أن لتلك العوامل الخاصة بالثقافة التنظيمية تأثير كبير في زيادة فعالية إدارة أمن المعلومات.

(٨) دراسة أبوموسي ٢٠٠٥

لقد قام أبوموسى (٢٠٠٥) بدراسة نظرية للتعرف على بعض عوامل نجاح أسلوب حوكمة تكنولوجيا المعلومات ودوره في تفعيل حوكمة الشركات. حيث تناول الباحث بالدراسة والتحليل الإطار الفكري الذي يمكن من خلاله فهم مكونات وأبعاد حوكمة تكنولوجيا المعلومات، ومدى إمكانية تفعيل دور المحاسب الإداري من خلال تطوير وتطبيق نموذج "المقياس المتوازن للأداء" كنموذج مقترح لقياس وتقويم الأداء الإستراتيجي لحوكمة تكنولوجيا المعلومات، وذلك لربط الأهداف الإستراتيجية لتكنولوجيا المعلومات بالأهداف والإستراتيجية العامة لمنظمات الأعمال من أجل تفعيل دور حوكمة الشركات وتعزيز القدرة التنافسية لمنظمات الأعمال من خلال آليات أسلوب حوكمة تكنولوجيا المعلومات.

(٩) دراسة Shah, et al. 2007

تناولت هذه الدراسة فحص عوامل النجاح التنظيمية الهامة التي تساعد في نجاح البنك الإلكتروني الذي يعتمد بصورة كبيرة على تنقل المعلومات عبر الانترنت مما يعرضها إلى عدم الأمان، وبالتالي تحتاج إلى عوامل لإنجاح برامج أمن المعلومات. وقد توصلت الدراسة إلى مجموعة متنوعة من العوامل الضرورية لإنجاح تأمين معلومات البنك الالكتروني، ونتيجة لقلة الأبحاث في هذا المجال فقد قامت الدراسة باختيار مجموعة من العوامل مع ترتيبها حسب أهميتها الأكبر تتمثل في:

- عوامل إستراتيجية Strategic Factors

- عوامل تشغيلية Operational Factors
- عوامل تكنيكية (فنية) Technical Factors

وقد جاءت نتائج الدراسة تؤكد على تحقيق عدة منافع هامة منها: سرعة الاستجابة لخدمة العميل ومن ثم سرعة تسليم الخدمة له، ترويج وتوسيع عمليات التجارة الإلكترونية وحث العاملين بالمنشأة على أهمية التحول إلى التجارة الإلكترونية في العصر الحالي، وتحقيق فعالية وتحسين أفضل في أمن المعلومات.

(١٠) دراسة Abu-Musa, 2007

لقد قام Abu-Musa (2007) بعمل دراسة ميدانية لاستكشاف وتقييم أداء حوكمة تكنولوجيا المعلومات في المنشآت السعودية باستخدام نموذج بطاقة الأداء المتوازن. ولقد خلصت نتائج الدراسة الميدانية إلى أن معظم المشاركين في الاستقصاء قد أشاروا إلى أهمية المقاييس الواردة بنموذج بطاقة الأداء المتوازن، إلا أن نسبة ضئيلة من هؤلاء المشاركين في الاستقصاء قد أشاروا إلى أن منشآتهم تقوم بقياس أداء تلك المتغيرات واستخدامها في تقييم أداء حوكمة تكنولوجيا المعلومات. ولقد اقترحت الدراسة ضرورة الاهتمام بقياس أداء حوكمة تكنولوجيا المعلومات بالمنشآت السعودية، وتفعيل وتحسين ذلك الأداء من خلال تحقيق التناسق والتناغم بين إستراتيجية تكنولوجيا المعلومات والإستراتيجية العامة للشركة، وكذلك تحقيق التكامل بين حوكمة تكنولوجيا المعلومات وحوكة الشركات، كما اقترحت الدراسة إدارة موارد تكنولوجيا المعلومات بطريقة أكثر كفاءة وكذلك إدارة المخاطر المتعلقة بتكنولوجيا المعلومات بصورة أكثر فعالية.

(١١) دراسة Rotvold, 2008

تناولت هذه الدراسة كيفية خلق ثقافة أمن المعلومات لدى جميع العاملين بالمنشأة على أساس أن أمن المعلومات يجب أن يكون جزء من ثقافة كل فرد في المنشأة وأنه سيكون أحد عوامل نجاح برامج أمن نظم المعلومات المحاسبية، وقد استهدفت الدراسة الإجابة على السؤال التالي : كيف يمكن للمنشآت انجاز برامج الوعي والإدراك بأمن المعلومات وتدريب العاملين بالمنشأة على كيفية انجاز هذه البرامج؟. وجاءت نتيجة الدراسة تؤكد على أهمية وضع برامج لتنمية إدراك ووعى العاملين بأمن المعلومات من خلال إجراء دورات تدريبية مستمرة للعاملين في المنشأة.

(١٢) دراسة Abu-Musa, 2009

لقد قام Abu-Musa عام ٢٠٠٩ بعمل دراستين ميدانيتين، **الأولى:** لدراسة أهمية وتطبيق أهداف الرقابة على المعلومات والعمليات المتعلقة بتكنولوجيا المعلومات "الكوبت" (COBIT) في المنشآت السعودية. ولقد خلصت نتائج الدراسة أن غالبية المنشآت السعودية ترى أهمية تطبيق هدف الرقابة على المعلومات والتكنولوجيا المتعلقة بها. ولقد أظهرت البنوك والمنشآت المالية اهتماماً بذات الموضوع مقارنة بالمنشآت الأخرى. كما أن المتخصصون في تكنولوجيا المعلومات

وكذلك المراجعون الداخليون والمديرين العموميين قد أظهروا اهتماماً أكبر من غيرهم بأهمية تطبيق مبادئ الكوبت في المنشآت التي يعملون بها. وفى الدراسة **الثانية:** تم اختبار مدى تطبيق مبادئ الكوبت في المنشآت السعودية وما إذا كانت تتم مراجعة ذلك للتطبيق بطرق رسمية أو غير رسمية وكذلك تحديد المسئول عن التنفيذ ومدى مساءلته في المنشآت السعودية. وتشير نتائج الدراسة إلى أن نسبة قليلة من المنشآت السعودية تقوم بتطبيق مبادئ الكوبت وأن ذلك يعد مسئولية أقسام تكنولوجيا المعلومات بالمنشآت السعودية، غير أن معظم المشاركين في الاستقصاء قد أشاروا أن التطبيق لا يتم بصورة رسمية وأنه لا يتم مراجعة الأداء في المنشآت السعودية.

وتجدر الإشارة إلى أن كل دراسة من الدراسات السابقة قد تناولت عاملاً واحداً أو عدداً محدوداً من عوامل نجاح برامج أمن نظم المعلومات المحاسبية، بينما تناولت بعض الدراسات الأخرى عوامل نجاح برامج أمن نظم المعلومات المحاسبية بصورة غير مباشرة من خلال البحث حول أهمية وضرورة الحفاظ على أمن المعلومات. ومن ثم تأتى أهمية وضرورة البحث عن مجموعة متكاملة من العوامل التي يمكن أن تؤدى إلى نجاح برامج أمن المعلومات واختبارها ميدانياً. وذلك من خلال تجميع ودراسة مجموعة العوامل التي يتوقع أن تؤدى إلى نجاح برامج أمن المعلومات ووضعها في إطار مقترح واختبارها ميدانياً على مجموعة من شركات الأعمال السعودية.

٤. أهمية أمن المعلومات وضرورة الحفاظ عليها

٤-١. طبيعة أمن المعلومات

أصبحت المعلومات في العصر الحالي من أهم الأصول التي لها قيمة كبيرة جدا للشركة إذا تم إعدادها وتكوينها وصياغتها بطريقة صحيحة وحمايتها من السرقة والتخريب والاستغلال ضد الشركة، خاصة في ظل عصر الانفتاح والانترنت. وتكتسب المعلومات أهميتها من واقع الدور الذي تمثله من خلال تزويد الأطراف ذات العلاقة بالمنشأة (إدارة – عاملين – مساهمين – مستثمرين – دائنين – عملاء) والمجتمع المحيط بها بما يحتاجون إليه من معلومات، كما تزايدت أهمية المعلومات نتيجة ما تحدثه من آثار في توسيع معرفة الأطراف المهتمة بالمنشأة سواء داخل المنشأة أو خارجها، وتنمية الوعي لدى الأفراد وإدراكهم بالظواهر والمتغيرات التي تحيط بهم.

ولقد أدى تطور تكنولوجيا الاتصالات وتكنولوجيا المعلومات إلى إحداث تطور كبير في مجال المعلومات وضرورة أمنها وسلامتها والحفاظ عليها، وبالتالي أصبحت صناعة المعلومات والتكنولوجيا المرتبطة بها وأمنها والحفاظ عليها وضرورة العمل على نجاح برامج وخطط أمن المعلومات من الموضوعات الهامة والصناعات الرائدة في العصر الحالي.

ومن ثم فلقد صدرت عدة معايير لأمن المعلومات منها الأيزو ١٧٧٩٩ (ISO 17799) والمعيار البريطاني ٧٧٩٩ (BS 7799) وهى مقاييس تقدم مجموعة شاملة من وسائل التحصين والحماية التي تحقق أساليب أفضل في أمن المعلومات، على أساس أن الأيزو ١٧٧٩٩ (ISO 17799) هو مقياس ورمز دولي لخبرة عريقة تقدم إرشادات وتوجيهات لإدارة أمن المعلومات

بالمنشآت المختلفة. أما المعيار البريطاني (BS 7799) وهو مقياس بريطاني يستخدم كمنهج رسمي لمنح شهادة بمطابقة المقياس والذي يقسم إلى عدة أقسام تشتمل على العديد من المصطلحات في مجال أمن المعلومات والتي تتمثل في: تحديد المجال Scope ، المصطلحات والتعريفات المرتبطة بأمن المعلومات Terms and Definitions، تحديد سياسة الأمن Security Policy ، تحديد الأمن التنظيمي Organizational Security ، تصنيف الأصول المستخدمة في حماية أمن المعلومات ورقابتها Assets Classification and Control ، تحديد الأمن الشخصي Personal Security ، تحديد الأمن المادي والبيئي Physical and Environment Security، إدارة الاتصالات والعمليات Communications and Operations Management، الرقابة على الوصول والدخول إلى النظام Access Control، تطوير النظم المرتبطة بأمن المعلومات وصيانتها System Development and Maintenance، إدارة استمرارية العمليات بين جميع الإدارات والأفراد داخل المنشأة وخارجها Business Continuity Management، تحديد إجراءات التنفيذ المرتبطة بجودة المطابقة Compliance والمتعلقة بأمن المعلومات **[Tang, 2008, P. 54]** . وتجدر الإشارة إلى أن تحديد هذه المصطلحات بوضوح في منشأة ما سوف يساعد في زيادة فاعلية أمن المعلومات.

إن أمن المعلومات قد أصبح واحداً من أهم التحديات التي تواجه منشآت الأعمال في الوقت الراهن، حيث مع اتساع استخدام التكنولوجيا ووسائل الاتصالات على المستوى العالمي أصبح أمام المنشآت تهديدات كبيرة ومتنوعة تتطلب من إدارات المنشآت ضرورة البحث عن وسائل وبرامج لحماية أمن المعلومات وتحديد مجموعة من العوامل التي ستساعد في نجاح تلك البرامج، وإجراءات الرقابة الفنية لأمن المعلومات سوف تساعد في الحماية ضد التهديدات التي تواجه أمن المعلومات المرتبطة بالمنشأة، إلا أن هذه الإجراءات الرقابية وحدها قد لا تساعد في الوصول لحل شامل ونهائي لجميع مشاكل حماية أمن المعلومات على أساس أن أمن المعلومات ليس مسئولية المهتمين بأمن وتكنولوجيا المعلومات فقط، بل أصبحت مسئولية كل فرد داخل المنشأة، لذلك يجب على كل مستخدمي المعلومات أن يدركوا ليس فقط دورهم ومسئولياتهم فيما يتعلق بحماية مصادر المعلومات ولكن يجب أن يدركوا أيضا ضرورة التدريب المستمر والواعي على كيفية حماية المعلومات وعلى سرعة استجابتهم نحو أي تهديد محتمل لأمن المعلومات **[Rotvold, 2008, P. 32]**.

٤-٢. متطلبات أمن المعلومات

يتطلب الأمر لحماية أمن المعلومات الإشارة إلى أهمية نشر الوعي بين العاملين في المنشأة بالأخطار التي تهدد أمن المعلومات، ومن متطلبات أمن المعلومات:

(١) وضع سياسة محددة لأمن المعلومات.

(٢) دعم الإدارة العليا لسياسات وخطط وبرامج أمن المعلومات.

(٣) تحديد أشخاص محددين كمسئولين عن أمن المعلومات.

(٤) تحديد طرق الحماية اللازم توافرها في أنظمة تشغيل المعلومات.
(٥) تحديد آليات المراقبة والتفتيش على نظم المعلومات.
(٦) حفظ وسائط التخزين.
(٧) تحديد وسائل وطرق لتشفير المعلومات.
(٨) تأمين استمرارية عمل نظم المعلومات وإتاحتها.

ويري Tondel et al. (2008) أنه على الرغم من أن الاعتماد على نموذج التهديدات والأخطار لمواجهة أمن المعلومات، إلا أن هناك بعض الخطوات التي يجب أن تؤخذ في الاعتبار كمتطلبات أساسية لأمن المعلومات تتمثل في : **[Tondel et al, 2008, P. 23]**

(١) تحديد السيناريوهات المستخدمة للحفاظ على أمن المعلومات.
(٢) تحديد الممتلكات المستخدمة للحفاظ على أمن المعلومات.
(٣) تحديد التهديدات التي تواجه أمن المعلومات.
(٤) تحديد درجة الاعتماد على نظم المعلومات.

ومن ثم فإن الحفاظ على أمن وحماية المعلومات يتطلب من المنشأة أن تراعى المحافظة على سرية وتكامل وإتاحة المعلومات (CIA) لمستخدميها، ويمكن إظهار تلك المتطلبات التي يجب توافرها للحفاظ على أمن المعلومات في الشكل رقم (١).

أولا: سرية المعلومات Confidentially

سرية المعلومات تعنى التأكد من أن المعلومات لا تكشف ولا يطلع عليها إلا الأشخاص المخول لهم بذلك، حيث يجب أن يكون هناك أشخاص بالشركة مسئولين مسؤولية كاملة عن حفظ المعلومات السرية والمهمة والحفاظ عليها للمنشأة، وعدم إطلاع أي شخص على هذه المعلومات إلا عند انجاز مهام محددة لصالح المنشأة.

ثانيا: تكاملية المعلومات Integrity of Information

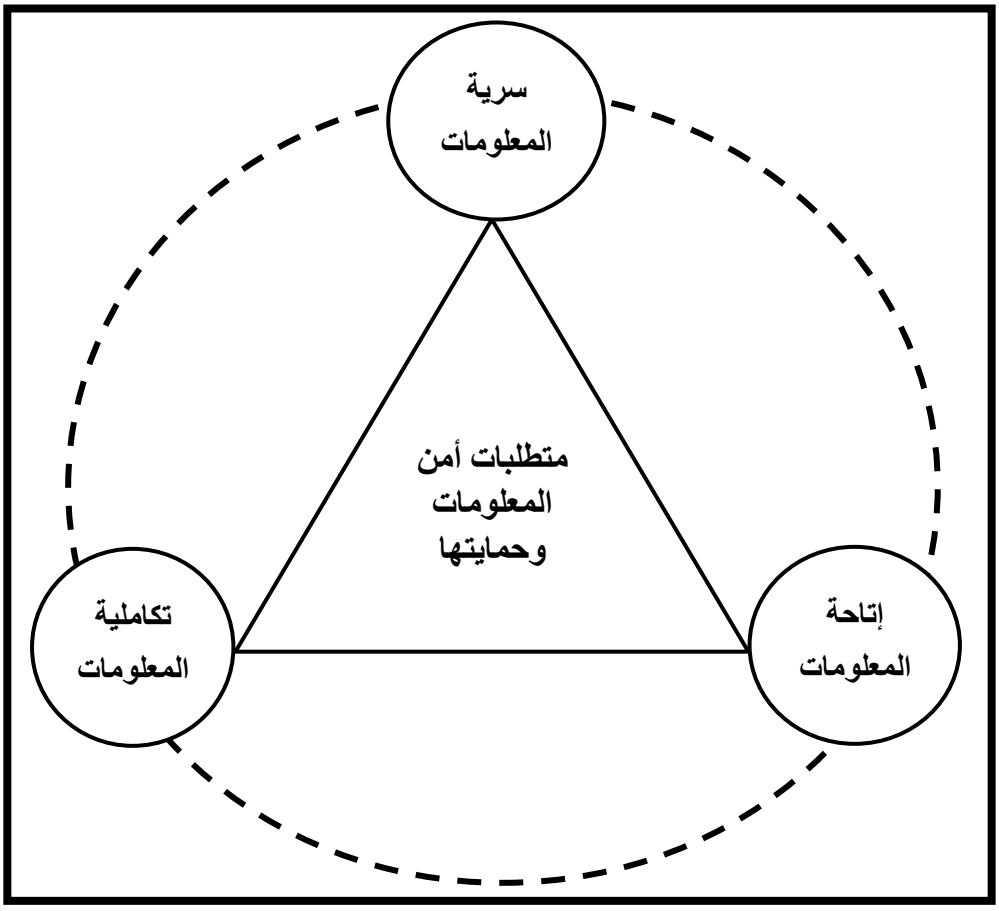
تكاملية المعلومات تعنى التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله بطريقة غير مشروعة أو العبث به أو تدميره أو تدخل غير مشروع، ويتم ذلك من خلال تدقيق المعلومات المجمعة عن أنشطة الشركة وأي معلومات أخرى من خارج الشركة تتعلق بها، مع منع أي عبث يحدث على المعلومات ويغير محتواها المطلوب.

ثالثا: إتاحة المعلومات Availability of Information

إتاحة المعلومات تعنى 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.

من الشكل رقم (١) نجد أن متطلبات حماية وأمن المعلومات يمكن تمثيلها بمثلث له ثلاث رؤوس **أولها** سرية المعلومات من خلال عدم إطلاع أي شخص غير مسئول عن المعلومات،

ثانيها تكاملية المعلومات من خلال الحرص على دقة وسلامة المعلومات، **ثالثها** إتاحة المعلومات من خلال مدى توافر المعلومات للشخص الذي سيستخدمها لمصلحة الشركة.



شكل رقم (١) العلاقة بين سرية وتكاملية وإتاحة المعلومات ومتطلبات أمن وحماية المعلومات

ولقد استخدم Tang (2008) **نموذج خطط – افعل – افحص – تصرف** – Plan – Do – Check – Action (PDCA) كما اقترحه ديمنج Deming للتطبيق على نظم إدارة أمن المعلومات Information Security Management Systems (ISMS) كما يظهر في الشكل رقم (٢) **.[Tang, 2008, P. 57]**

ومن الشكل رقم (٢) نجد أن أمن نظم المعلومات المحاسبية يتطلب:

أولا: تحديد المتطلبات والآثار المتوقعة لأمن المعلومات من داخل المنشأة.

ثانيا: تحديد الأحداث التاريخية لأمن المعلومات من خارج المنشأة.

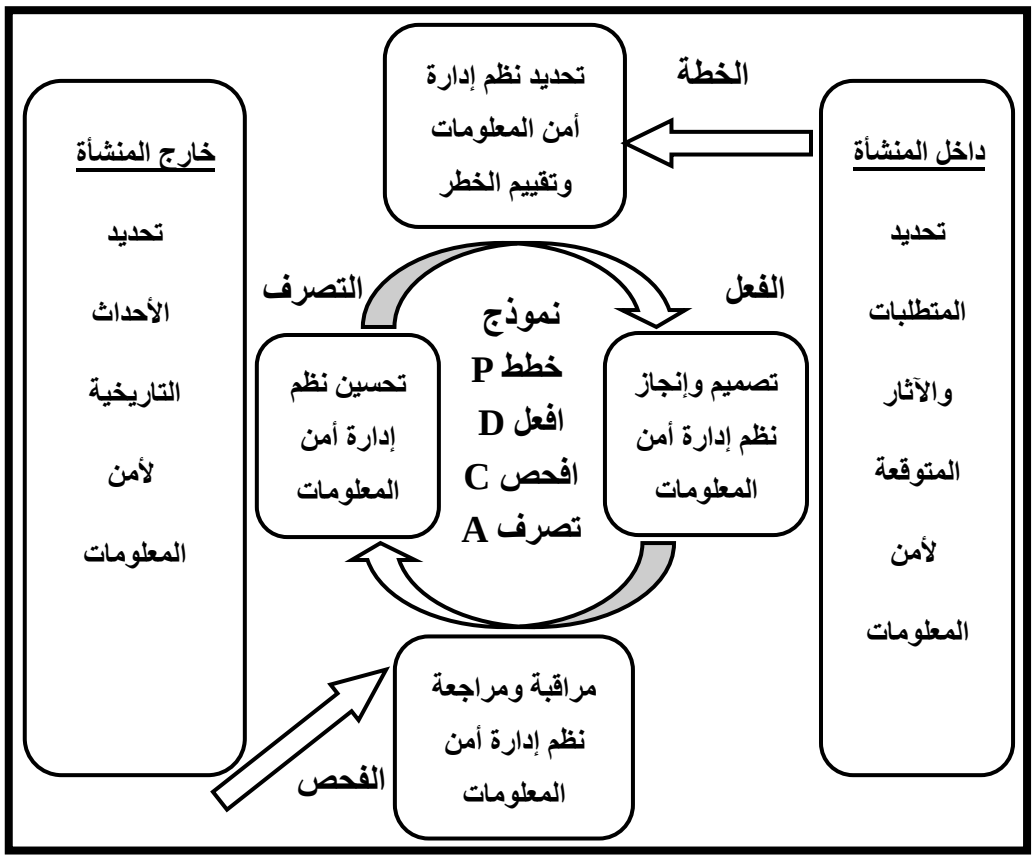
ثالثا: تطبيق نموذج خطط – افعل – افحص – تصرف (PDCA) من خلال تحديد:

(١) خطط Plan: وذلك بتحديد نظم إدارة أمن المعلومات وتقييم درجات الخطر التي تهدد أمن المعلومات بالمنشأة.

(٢) افعل Do: وذلك بوضع تصميمات ووسائل انجاز لنظم إدارة أمن المعلومات بالمنشأة.

(٣) افحص Check: وذلك من خلال قيام المسئولين بمراقبة ومراجعة نظم إدارة أمن المعلومات.

(٤) تصرف Action: وذلك بالقيام بإجراء التحسينات الواجبة والتطويرات المطلوبة على نظم إدارة أمن المعلومات.



شكل رقم (٢) نموذج خطط- افعل- افحص- تصرف (PDCA) وأمن المعلومات

وتجدر الإشارة إلى أن هذه المتطلبات ما هي إلا مجموعة من العوامل التي تؤدى إلى نجاح برامج أمن المعلومات، ومن ثم فإن تجميع تلك العوامل وغيرها من العوامل في نموذج متكامل لعوامل نجاح برامج أمن نظم المعلومات المحاسبية واختبارها ميدانيا على منشآت الأعمال السعودية يمكن أن يمثل مساهمة علمية ويحقق نتائج إيجابية في تحسين برامج أمن المعلومات وتطويرها في المنشآت السعودية.

٥. دور أمن المعلومات في زيادة تفعيل حوكمة الشركات.

إن النقطة المحورية Focal Point لمنشآت الأعمال في الأوساط الإعلامية والمنظمات التشريعية على المستوى العالمي تتمثل في أمن المعلومات Information Security، حيث أن تلك المنشآت في الوقت الحاضر تواجه بمتطلبات أكثر تعقيدا تفرض عليها ضرورة مراعاة معايير الأمن

والسرية للمعلومات، ومن المعايير العالمية التي تفرضها المنظمات الدولية ISO1799 وغيرها... ، ومما يزيد ويعظم من حدة ذلك ظهور مجموعة من القوانين والتشريعات المحلية والعالمية التي تتطلب ضرورة تطبيق الحوكمة في كل المجالات ومنها :(SOX) Sarbanes – Oxley ، Gramm – Leach – Bliley، Basell II والتي تجعل المنشآت أكثر وعياً وإدراكاً بأهمية الالتزام بالقوانين والتشريعات التي تصدر وتساعدها في تحقيق تلك المتطلبات وتساعد في نموها والانتقال بها عبر حدود الدولة **[Gerber and Solms, 2008, P. 124]**.

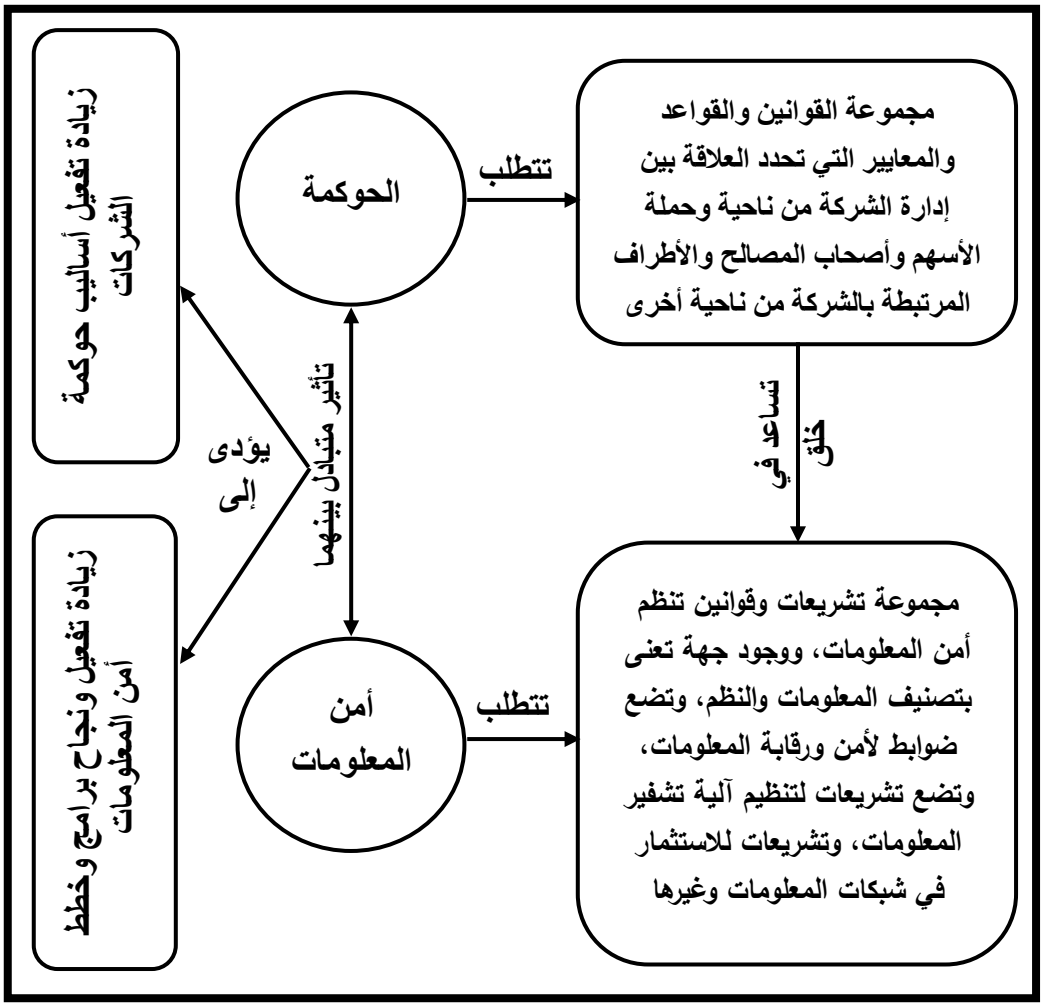
ولقد أشار إسمث **[Smith, 2009]** إلى أن العديد من الكتب والمقالات المنشورة في المجلات والدوريات العلمية التي تناولت موضوعات أمن المعلومات قد عجزت عن تناول عوامل نجاح برامج أمن نظم المعلومات المحاسبية المهمة التي ستؤدى إلى البقاء والاستمرار في هذا المجال، وأنه قد أمكن التوصل إلى كيفية حماية أمن المعلومات من خلال تبنى مفهوم حوكمة الأمن Security Governance.

فالحوكمة Governance هي مجموعة القوانين والقواعد والمعايير التي تحدد العلاقة بين إدارة الشركة من ناحية وحملة الأسهم وأصحاب المصالح والأطراف المرتبطة بالشركة من ناحية أخرى. وأمن المعلومات Security Information يتطلب ضرورة وجود تشريعات وقوانين ولوائح تنظم أمن المعلومات، ووجود جهة تعنى بتصنيف المعلومات والنظم، وتضع ضوابط لأمن ورقابة المعلومات، وتضع تشريعات لتنظيم آلية تشفير المعلومات، وتشريعات للاستثمار في شبكات المعلومات. لذلك فالحوكمة أصبحت عامل هام من عوامل نجاح أمن المعلومات تطبق على أمن المعلومات والتي تؤدى إلى زيادة تفعيل أمن المعلومات.

والشكل رقم (٣) يوضح العلاقة المتبادلة بين الحوكمة وأمن المعلومات، حيث أن الحوكمة تتطلب ضرورة وضع مجموعة من القوانين والمعايير التي تحدد العلاقة بين إدارة الشركة وحملة الأسهم وأصحاب المصالح والأطراف المرتبطة بالشركة والتي تعد أحد عوامل نجاح برامج أمن نظم المعلومات المحاسبية، حيث أن إيمان الإدارة بضرورة وضع برامج لأمن المعلومات يتطلب حوكمة هذه البرامج وبالتالي إمكانية نجاحها.

٦. عوامل نجاح برامج أمن نظم المعلومات المحاسبية ودورها في تفعيل حوكمة الشركات

تعبر حوكمة الشركات من أحد عوامل نجاح برامج أمن نظم المعلومات المحاسبية، وفى نفس الوقت نجد أن لعوامل نجاح برامج أمن نظم المعلومات المحاسبية دور في تفعيل حوكمة الشركات.



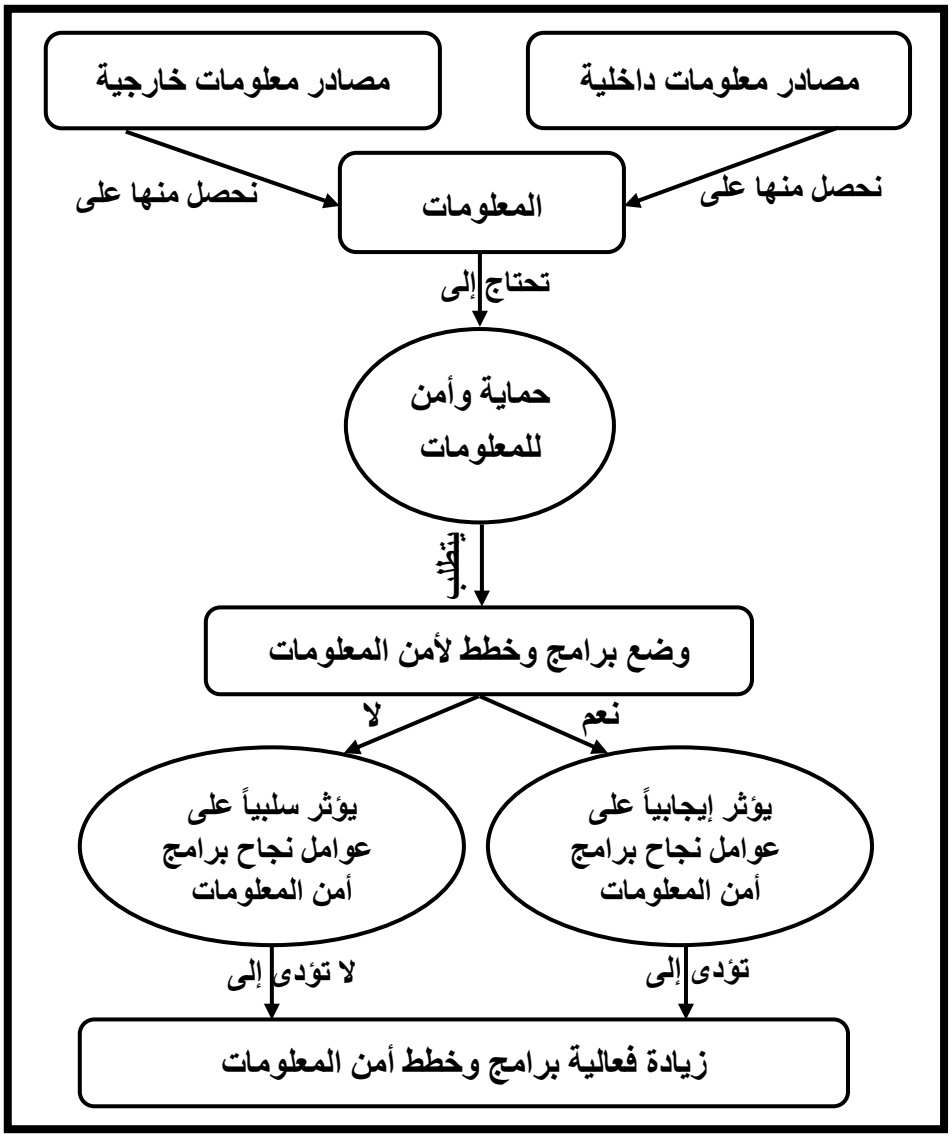
شكل رقم (٣) العلاقة بين الحوكمة وأمن المعلومات

٦-١. دراسة عوامل نجاح برامج أمن نظم المعلومات المحاسبية

إن المعلومات المتعلقة بالمنشأة ما هي إلا أحد الممتلكات الأساسية لها، ويجب على إدارة الشركة بذل كل الجهود ووضع الخطط والبرامج التي تضمن سلامة وأمن تلك المعلومات، ولكي تنجح تلك البرامج والخطط لا بد لها من توافر عوامل النجاح، وبالتالي تظهر أهمية البحث عن مجموعة العوامل التي تضمن نجاح برامج أمن المعلومات. والشكل رقم (٤) يبين ضرورة الحاجة إلى دراسة وتحديد عوامل نجاح برامج أمن نظم المعلومات المحاسبية. ومن الشكل رقم (٤) نلاحظ ما يلي:

(١) **المعلومات:** وهى تمثل أصول وممتلكات للشركة وتتجمع من نوعين من المصادر:

- مصادر معلومات داخلية والتي تتجمع من داخل المنشأة.
- مصادر معلومات خارجية والتي تتجمع من مصادر خارج المنشأة.



شكل رقم (٤) محددات عوامل نجاح برامج أمن المعلومات

(٢) **حماية وأمن المعلومات:** إن أي معلومات تتجمع لدى المنشأة ستحتاج إلى حماية وأمن، وللحفاظ على تلك المعلومات من أي تهديدات محتملة كالسرقة أو التدمير أو التحريف أو التلاعب أو الاستخدام غير المشروع وغيرها من التهديدات والمخاطر المتعلقة بأمن المعلومات، وبالتالي يتطلب الأمر ضرورة وضع الخطط والبرامج اللازمة لحماية أمن المعلومات.

(٣) **وضع برامج وخطط لأمن المعلومات:** إن حماية وأمن المعلومات يتطلب ضرورة وضع برامج وخطط مناسبة لأمن المعلومات. ومن ثم تبدو الحاجة ملحة للإجابة على التساؤل التالي: هل قامت إدارة المنشأة بوضع مجموعة من البرامج والخطط اللازمة لأمن المعلومات ؟

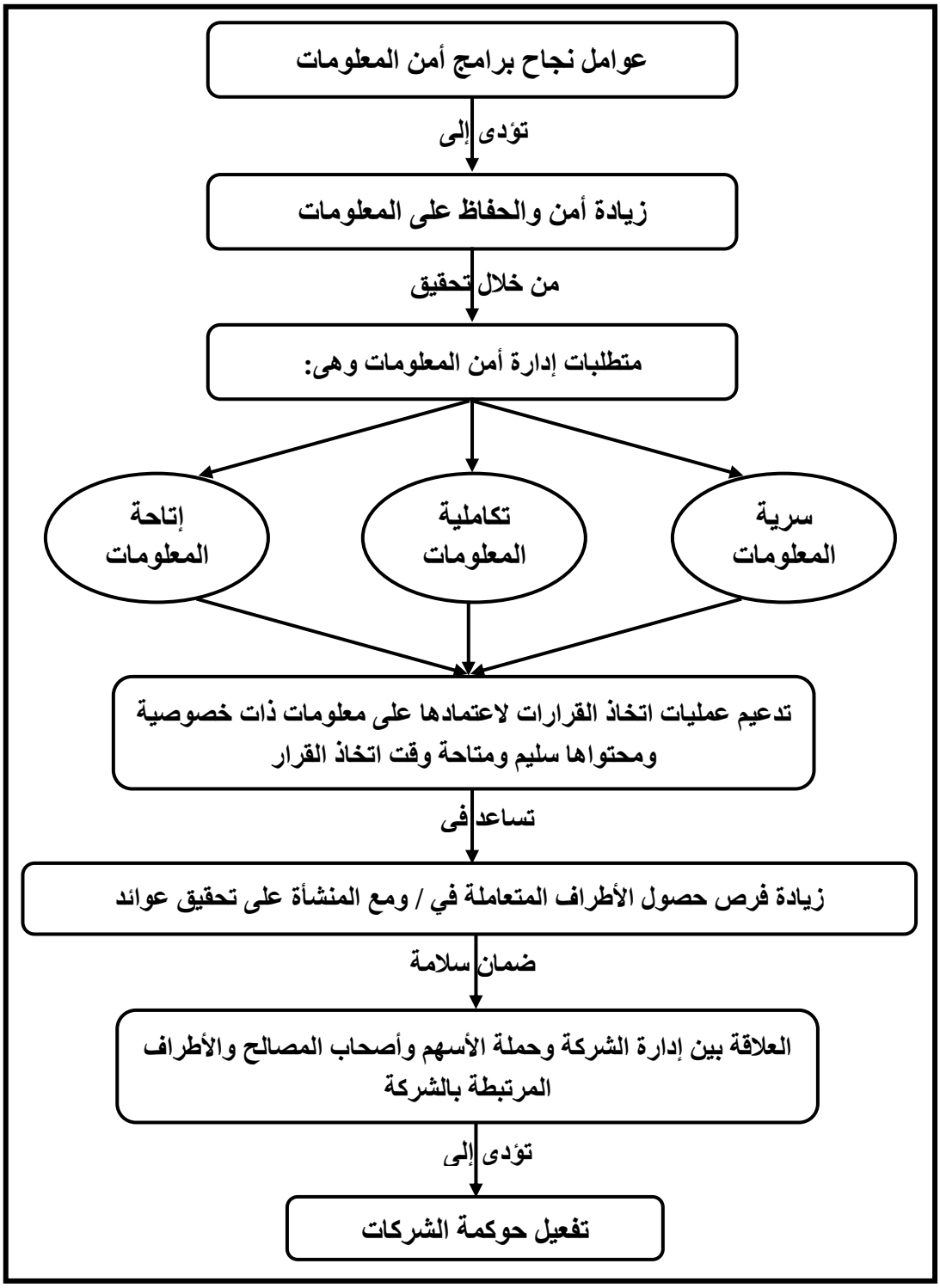
- إذا كانت الإجابة على السؤال السابق "نعم": فانه من المتوقع أن يؤثر إيجابياً على نجاح برامج أمن المعلومات، ومن ثم تظهر الحاجة إلى ضرورة دراسة عوامل نجاح برامج أمن نظم المعلومات المحاسبية.
- إذا كانت الإجابة على السؤال السابق "لا": فانه من المتوقع أن يؤثر ذلك سلبياً على نجاح برامج أمن المعلومات، ومن ثم لا يوجد مجال لدراسة عوامل نجاح لبرامج غير موجودة لأمن المعلومات.

(٤) زيادة فعالية برامج وخطط أمن المعلومات :

- إذا كانت الإجابة على السؤال السابق بالإيجاب فإن ذلك يؤدى إلى زيادة في فعالية برامج أمن المعلومات وخططها.
- إذا كانت الإجابة على السؤال السابق بالنفي فإن ذلك يؤدى إلى الأثير سلبياً على فعالية برامج أمن المعلومات وخططها.

٦-٢. دور عوامل نجاح برامج أمن نظم المعلومات المحاسبية في تفعيل حوكمة الشركات

إن الدراسة والبحث عن مجموعة من عوامل نجاح برامج أمن نظم المعلومات المحاسبية سيؤدى إلى زيادة تحقيق درجات عالية من الحفاظ على المعلومات وتأمينها ضد أي تهديدات قد تواجهها، والتي ستؤدى إلى تحقيق ثلاثة متطلبات رئيسية وهى: سرية المعلومات، تكاملية المعلومات، وإتاحة المعلومات. إن وجود مجموعة من الأدوات التي تضمن الحفاظ على المعلومات، وتضمن صحة محتواها، والتأكد من استمرارية تدفقها، سيساعد في دعم عمليات اتخاذ القرارات مما يؤدى إلى زيادة فرص حصول الأطراف المتعاملة في / ومع المنشأة على تحقيق عوائد مما يساعد في ضمان سلامة العلاقة بين إدارة الشركة وحملة الأسهم وأصحاب المصالح والأطراف المرتبطة بالشركة مما يؤدى إلى تفعيل حوكمة الشركات والشكل رقم (٥) يبين دور عوامل نجاح برامج أمن نظم المعلومات المحاسبية في تفعيل حوكمة الشركات.



شكل رقم (٥) تأثير عوامل نجاح برامج أمن المعلومات في تفعيل حوكمة الشركات

٧. الإطار المقترح لعوامل نجاح برامج أمن نظم المعلومات المحاسبية

يتناول الإطار المقترح لعوامل نجاح برامج أمن نظم المعلومات المحاسبية تجميع أهم العوامل التي تساعد في نجاح برامج وخطط أمن المعلومات ودراستها واختبارها ميدانياً على عينة من شركات الأعمال السعودية، حيث أن غالبية الدراسات التي تناولت عوامل نجاح برامج أمن نظم المعلومات المحاسبية قد تناولت كل منها دراسة عامل واحد أو عدد محدود من عوامل نجاح برامج أمن نظم المعلومات المحاسبية، أما الإطار المقترح فإنه يتضمن مجموعة متكاملة من عوامل النجاح، وبالتالي يتميز الإطار المقترح بالآتي:

- يتضمن مجموعة متكاملة من عوامل نجاح برامج أمن نظم المعلومات المحاسبية.
- تحديد مجموعة من المتغيرات الفرعية داخل كل عامل من عوامل نجاح برامج أمن نظم المعلومات المحاسبية.
- إخضاع عناصر الإطار المقترح بعوامله ومتغيراته للدراسة والتحليل النظري.
- إخضاع عناصر الإطار المقترح بعوامله ومتغيراته للاختبارات الإحصائية من خلال الدراسة الميدانية.
- إمكانية التطبيق الفعلي للإطار المقترح على شركات الأعمال.

٧-١. متغيرات الإطار المقترح

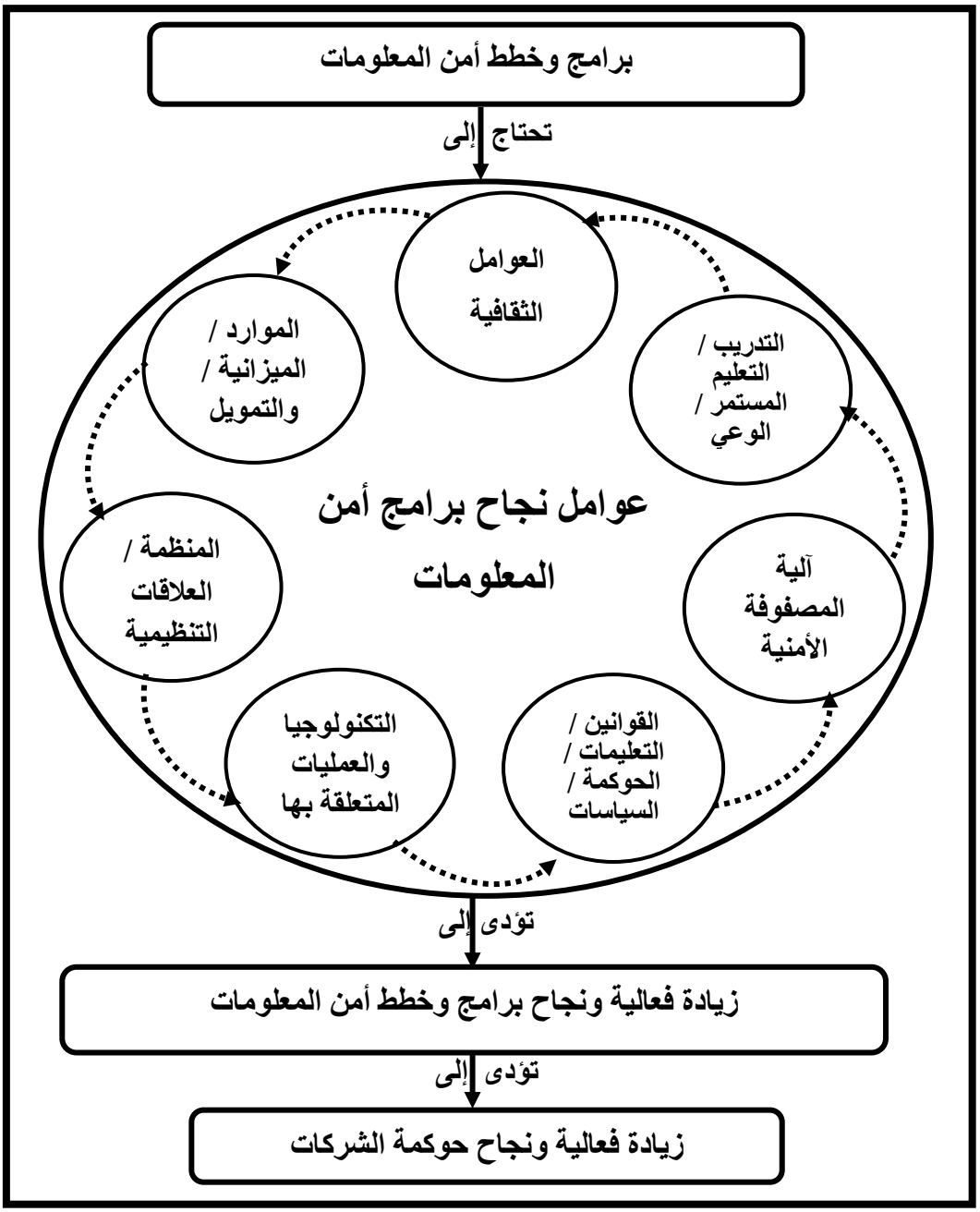
يمكن تقسيم متغيرات الإطار المقترح إلى عدة متغيرات على النحو التالي:

- برامج وخطط أمن المعلومات.
- عوامل نجاح برامج أمن نظم المعلومات المحاسبية.
  - العوامل الثقافية.
  - الموارد / الميزانية.
  - المنظمة/ العلاقات التنظيمية والتمويل.
  - التكنولوجيا والعمليات المتعلقة بها.
  - القوانين والتعليمات والحوكمة والسياسات.
  - آلية المصفوفة الأمنية.
  - التدريب والتعليم المستمر وتنمية المهارات والوعي.
- فعالية ونجاح برامج وخطط أمن المعلومات.

٧-٢. الإطار العام لعوامل نجاح برامج أمن نظم المعلومات المحاسبية

يوضح الشكل رقم (٦) الإطار العام المقترح لعوامل نجاح برامج أمن نظم المعلومات المحاسبية والذي يتضمن مجموعة من عوامل نجاح برامج أمن نظم المعلومات المحاسبية المختارة والتي تمثل علاقة دائرية تكاملية Integrated مع بعضها البعض، حيث أن كل عامل يعتمد في نجاحه على العوامل السابقة له كما أنه يسهم في تعزيز ونجاح العامل الذي يليه، ومن ثم فإن كل

عامل يسهم بنصيب معين في فعالية ونجاح برامج وخطط أمن المعلومات، بحيث أن تبنى وتطبيق تلك العوامل مجتمعة يمكن إن يصل ببرامج أمن المعلومات إلى أعلى درجة ممكنه من الحماية والأمان.



شكل رقم (٦) الإطار العام المقترح لعوامل نجاح أمن المعلومات

٧-٣. الإطار التفصيلي المقترح لعوامل نجاح برامج أمن نظم المعلومات المحاسبية

من الإطار العام المقترح في شكله الإجمالي السابق يتضح أن تكامل عوامل نجاح برامج أمن نظم المعلومات المحاسبية يؤدى إلى زيادة فعالية ونجاح تلك البرامج، وأن كل عامل سوف يسهم بدور معين في تحقيق ذلك النجاح، أما الإطار المقترح في شكله التفصيلي سيتناول بالدراسة والتحليل للمتغيرات التفصيلية لكل عامل من عوامل نجاح برامج أمن نظم المعلومات المحاسبية.

٧-٣-١. العوامل الثقافية

تتمثل العوامل الثقافية لنجاح برامج أمن المعلومات في غرس مفاهيم وقيم أمن المعلومات داخل كل فرد من أفراد المنشأة وجعلها جزء من ثقافة العاملين على كافة المستويات التنظيمية والإدارية بالمنشأة (شكل ٧). ومن ثم يمكن تحديد مجموعة من المتغيرات الفرعية المتعلقة بالعوامل الثقافية وهي:

٧-٣-١-١. أهمية وأولوية أمن المعلومات

يجب على كل فرد بالمنشأة أن يعطى أهمية كبيرة وأولوية مسبقة لأمن المعلومات وأن يكون ذلك جزء من ثقافته وتكوينه.

٧-٣-١-٢. الرقابة على مخاطر أمن المعلومات

يجب على كل فرد بالمنشأة أن يعلم أن هناك مخاطر مستمرة تهدد أمن وسلامة المعلومات، وأن يعمل على مساندة المسئولين عن أمن المعلومات في اكتشاف تلك التهديدات والرقابة عليها والحد منها ومنعها وتخفيض أثارها السلبية المحتملة في حالة حدوثها.

٧-٣-١-٣. وضع أمن المعلومات على قائمة جدول أعمال الإدارة بصورة منتظمة

يجب على الإدارة العليا بالمنشأة أن تضع على قائمة جدول أعمالها موضوع أمن المعلومات بصورة منتظمة في كل اجتماعاتها، ومناقشة ذلك الموضوع الهام وإعطائه الأولوية المناسبة على جدول الأعمال.

٧-٣-١-٤. تطبيق ورقابة والتقرير عن أمن المعلومات

يجب تطبيق مجموعة من الوسائل والأساليب والأفكار الحديثة في أمن المعلومات والرقابة على كيفية تطبيقها مع إعطاء تقرير بصورة مستمرة عن الحالة التي وصلت إليها المنشأة في مجال أمن المعلومات.

٧-٣-٢. الموارد/ التمويل والميزانية

يجب على الإدارة أن تضع ميزانية مناسبة لأمن المعلومات وأن تقوم بتدبير مصادر التمويل الكافية للصرف على مجالات حماية وأمن المعلومات، لأن أي خطة يراد لها النجاح لا بد من وضع ميزانية وتمويل بدرجة كافية لضمان هذا النجاح، وأمن المعلومات من أهم برامج وخطط المنشآت في العصر الحديث والذي يتميز بالتطورات التكنولوجية السريعة في وسائل الاتصال

والمعلومات، لذلك يجب على الإدارة وضع التمويل الكافي على مستوى الأجل القصير والطويل (شكل ٧).

٧-٣-٢-١. وجود تمويل كافي وميزانية مناسبة ومفعلة لأمن المعلومات

يجب وضع ميزانية كافية لأمن المعلومات، ويجب أن تكون تلك الميزانية متناسبة مع حجم المنشأة وحجم المعلومات المراد حمايتها، مع ضرورة مراقبة أوجه الصرف من هذه الميزانية حتى لا يصرف على أغراض أخرى غير الأغراض المخصصة للصرف، مما يجعلها مفعلة بدرجة كبيرة.

٧-٣-٢-٢. وجود ميزانية لإستراتيجية أمن المعلومات والخطط التكتيكية

يجب وضع ميزانية طويلة الأجل لأمن المعلومات حتى نضمن مصادر التمويل اللازمة لتنفيذ الأهداف والخطط الإستراتيجية لأمن المعلومات. وكذلك ضمان الصرف على الخطط التكتيكية التفصيلية لأمن المعلومات في الأجل القصير.

٧-٣-٣. المنظمة/ العلاقات التنظيمية

تمثل المنظمة والعلاقات التنظيمية أحد عوامل نجاح برامج أمن نظم المعلومات المحاسبية، والتي تتكون من مجموعة من المتغيرات الداخلية وهى:

٧-٣-٣-١. تحديد مسئوليات الاتصال بالزبون

يجب أن يكون هناك تحديد واضح للمسئوليات الخاصة بالاتصال بالزبون مع ضرورة التحديد الواضح للمسئوليات عن الخسارة الناتجة عن الالتزامات المرتبطة باستخدام الوسائل التكنولوجية في إجراء الصفقات مع الزبون.

٧-٣-٣-٢. التزام الإدارة العليا بمبادرات أمن المعلومات

يجب على الإدارة العليا أن تبادر دائما بالحديث عن أمن المعلومات وأن تبحث في إيجاد حلول ووسائل متطورة في مجال أمن المعلومات وأن تشجع الأفكار الحديثة في هذا المجال وتكلف المتخصصين في البحث في ذلك.

٧-٣-٣-٣. تأثير وتدخل الإدارة العليا وإيمانها بأهمية أمن المعلومات

يجب على الإدارة العليا بالمنشأة أن تتدخل بصورة مباشرة وتؤثر في اختيار أفضل البدائل والحلول الممكنة لحل المشاكل المتعلقة بأمن المعلومات، وأن تبذل الجهد المناسب من أجل ذلك، وأن تكلف من له الخبرة الكبيرة والوعي الكافي لحل مشاكل الأمن في الوقت المناسب.

٧-٣-٣-٤. تناسق وتناغم أهداف الشركة مع أهداف أمن المعلومات

إن من أهم المتغيرات التي تساعد في نجاح برامج أمن المعلومات هو ضرورة اتساق أهداف الشركة مع أهداف أمن المعلومات، بمعنى أن جميع العاملين بالمنشأة يعملون من أجل تحقيق الأهداف الرئيسية للشركة والتي تتضمن ضرورة الحفاظ على أمن وسلامة المعلومات المهمة بالمنشأة.

٧-٣-٣-٥. تكامل أنشطة الشركة مع أشطة أمن المعلومات

يجب أن تتكامل أشطة أمن المعلومات مع الأنشطة الأخرى الموجودة بالشركة وأن تعمل ضمن إطار متكامل من أجل تحقيق الأهداف والخطط الإستراتيجية للمنشأة.

٧-٣-٣-٦. توصيف الهيكل الإداري والتحديد الواضح للمسئوليات

بمعنى توضيح مسئوليات كل إدارة في الهيكل الإداري بصورة واضحة، والتركيز على انجازات كل إدارة ودورها في المساهمة في حماية وأمن المعلومات.

٧-٣-٣-٧. منع حدوث مشاكل أمن المعلومات في الأجل الطويل

إن أمن المعلومات غالبا ما يواجه بالعديد من المشاكل سواء في الأجل الطويل أو الأجل القصير، وقد تركز العديد من الشركات على منع حدوث مشاكل أمن المعلومات في الأجل القصير وتتجاهل مدى خطورة مشاكل أمن المعلومات في الأجل الطويل، إلا أنه من الواجب على الإدارة وضع خطة طويلة الأجل لمنع حدوث أي تهديدات لأمن المعلومات في الأجل الطويل وتخفيض أثارها السلبية على المنشأة إلى أدنى حد ممكن في حالة حدوثها.

٧-٣-٣-٨. تعريف واضح لأمن المعلومات مرتبط برؤية وأهداف الشركة

يجب على إدارة الشركة أن تضع تعريف واضح لأمن المعلومات بناء على رؤية واضحة للشركة تبين اتجاهاتها نحو هذا المجال.

٧-٣-٣-٩. احتلال أمن المعلومات لمكانة مناسبة في الهيكل الإداري والتنظيمي

يجب أن يحتل موضوع أمن المعلومات المكانة المناسبة في الهيكل الإداري والتنظيمي، وذلك من خلال وضع إدارة في الهيكل التنظيمي مسئولة عن أمن المعلومات وأن تكون تلك الإدارة لها صلاحيات وتسهيلات واسعة بدون قيود.

٧-٣-٣-١٠. تكامل أمن المعلومات مع إجراءات وسياسات الأمن التقليدية

أن بعض الشركات قد تقوم بإحلال أساليب أمن المعلومات التقليدية بأساليب تكنولوجية أكثر تطورا، إلا أن البقاء على أساليب الأمن التقليدي وتكاملها مع أساليب أمن المعلومات الحديثة قد يفيد أكثر ويزيد من نجاح برامج أمن المعلومات.

٧-٣-٤. التكنولوجيا والعمليات المتعلقة بها

تتمثل التكنولوجيا والتسهيلات المتعلقة بها أحد عوامل نجاح/ أو فشل برامج أمن المعلومات. والشكل رقم (٧) يوضح المتغيرات الفرعية لعامل التكنولوجيا والعمليات المتعلقة بها.

٧-٣-٤-١. التخطيط لأمن العمليات قبل اقتناء التقنية الجديدة

على الرغم من أن التغيير شيء لا بد منه لملاحقة التطورات الحديثة، إلا أنه قبل إجراء أي تغيير لا بد من وضع تخطيط جيد يضمن أن اقتناء التكنولوجيا الجديدة لن يؤثر سلبياً على سلامة أمن المعلومات ومدى الاستفادة منها.

٧-٣-٤-٢. وضع إجراءات مناسبة لإدارة التغيير

نظراً للتطور التكنولوجي المستمر فإن التغيير يعد أمراً هاماً بالمنشأة، ومن ثم لا بد من وجود إدارة مسئولة عن إدارة برنامج التغيير، ولكي تنجح تلك الإدارة في تحقيق ذلك الهدف يجب أن ترسم إجراءات وخطوات ملائمة لإدارة ذلك التغيير.

٧-٣-٤-٣. القدرة على التعامل مع عمليات القرصنة ومحاولات اختراق النظام

من متغيرات نجاح برامج أمن المعلومات أن يكون لدى المسئولين عن أمن المعلومات القدرة على الاستجابة والرد على أي عمليات قرصنة وسرقة المعلومات، وأن يكون لديهم من الأسلحة والقدرات التفكيرية والعقلية ما يساعدهم في فهم تلك العمليات التي قد تدمر نظام المعلومات وحمايته.

٧-٣-٤-٤. دراسة الجدوى الفنية من استخدام الحلول الآلية

إن اقتناء تكنولوجيا جديدة في المعلومات تتطلب تكلفة مرتفعة، ونظير هذه التكنولوجيا المقتناة يتوقع تحقيق عائد معين وإن كان غير ملموس، ولتحقيق نجاح في برامج أمن المعلومات يجب أن تكون المنفعة من اقتناء وتطبيق تكنولوجيا حديثة تفوق التكاليف المرتبطة بهذه التكنولوجيا.

٧-٣-٥. القوانين/التعليمات/الحوكمة/السياسات/المعايير

تمثل مجموعة القوانين والتعليمات وأساليب الحوكمة والسياسات والمعايير أحد عوامل نجاح برامج أمن نظم المعلومات المحاسبية، حيث أن تطبيق معايير حوكمة الشركات في مجال أمن المعلومات سيفرض معايير وأساليب معينة تساعد بدرجة كبيرة فيما تتبناه الشركة من عوامل لنجاح برامج أمن المعلومات، ويوضح الشكل رقم (٧) متغيرات عامل القوانين والتعليمات والحوكمة والسياسات والمعايير، حيث أن المتغيرات الرئيسية لهذا العامل تتكون من:

٧-٣-٥-١. الالتزام بالقوانين

إن البيئة التي تعمل بها الشركة تفرض قوانين معينة وعلى الشركة الالتزام بمتطلبات تلك القوانين المتعددة والتي تتعلق بعمليات الشركة.

٧-٣-٥-٢. تبنى لوائح وتعليمات أمنية معينة

إن تطبيق أساليب الحوكمة في مجال أمن المعلومات يتطلب وضع مجموعة من القوانين واللوائح والتعليمات التي تلتزم بها الشركات، ويجب أن لا يكون هناك تعارض داخلي بين تلك

القوانين واللوائح والتعليمات أو بينها وبين إستراتيجية المنشأة وأهدافها وسياستها العامة حتى نضمن الالتزام بمعايير الجودة في مجال أمن المعلومات.

٧-٣-٥-٣. تنفيذ سياسات ومعايير أمن المعلومات

يجب على إدارة الشركة وضع مجموعة من السياسات والمعايير والقواعد التي تحكم كيفية تنفيذ آليات أمن المعلومات، وعلى المسئولين عن برامج أمن المعلومات تنفيذ تلك السياسات والمعايير بدقة وكفاءة.

٧-٣-٥-٤. التنفيذ الثابت لسياسات أمن المعلومات

إن مجرد تنفيذ مجموعة السياسات والمعايير التي تحكم أمن المعلومات ليس كافيا، وإنما يجب الثبات في تنفيذ تلك السياسات والمعايير حتى لا تضيع معلومات هامة نتيجة التغيير من سياسة لأخرى، ويجب أن لا يحدث تغيير إلا في حالات الضرورة، وأن يخضع ذلك التغيير للدراسة والتحليل الكافي.

٧-٣-٦. آلية المصفوفة الأمنية

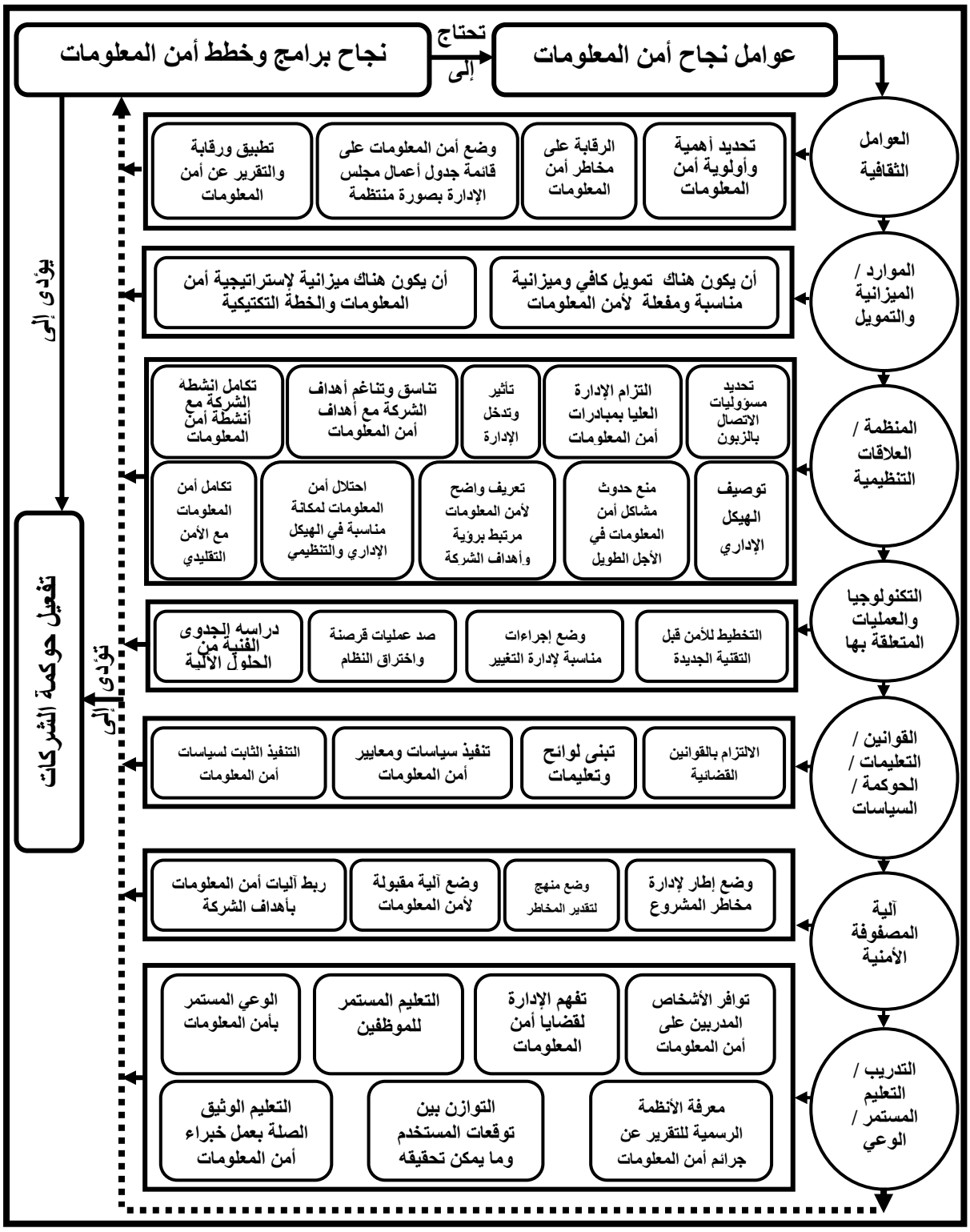
يتمثل هذا العامل في كيفية التعامل مع مخاطر أمن المعلومات وتقدير المخاطر الأمنية وتحديد آلية مقبولة لإدارة مخاطر أمن المعلومات مع ربطها بأهداف الشركة، والشكل رقم (٧) يبين متغيرات عامل آلية المصفوفة الأمنية.

٧-٣-٦-١. وضع إطار محدد لإدارة مخاطر المشروع

إن أي مشروع يتعرض من قريب أو من بعيد للمخاطر، وبالتالي يجب تكليف إدارة مختصة لدراسة تلك المخاطر والرقابة عليها، وهذه الإدارة يجب أن تعمل في ظل إطار يحدد كيفية إدارة تلك المخاطر والتعامل معها، ولكي تنجح برامج أمن المعلومات لا بد من أن يتكامل ذلك الإطار الخاص بإدارة المخاطر مع إستراتيجية وسياسات أمن المعلومات بالمنشأة.

٧-٣-٦-٢. وضع منهج لتقدير المخاطر

إن هناك العديد من المناهج العلمية لإدارة مخاطر أمن المعلومات، ولا بد من الاتفاق على منهج علمي لتقدير وتقييم المخاطر حتى تساعد في نجاح برامج أمن المعلومات.



شكل رقم (٧) الإطار المقترح لعوامل نجاح أمن المعلومات

٧-٣-٦-٣. وضع آلية مقبولة لأمن المعلومات

هناك العديد من الممارسات والسياسات والآليات التي تستخدم في مجال أمن المعلومات، ويجب على إدارة الشركة الاتفاق على آلية معينة لأمن المعلومات تكون مقبولة من القائمين على أمن المعلومات لتحقيق أفضل الممارسات الخاصة بأمن المعلومات.

٧-٣-٦-٤. ربط آليات أمن المعلومات بأهداف الشركة

إن الاتفاق على آلية معينة لأمن المعلومات يعد هاماً وضرورياً لنجاح برامج أمن المعلومات، ولكن من المهم أيضا ربط تلك الآلية بأهداف الشركة التي يجب تحقيقها حتى تزداد فعالية ونجاح برامج أمن المعلومات.

٧-٣-٧. التدريب/ التعليم المستمر/ الوعي

يمثل التدريب والتعليم المستمر وزيادة الوعي المتعلق بأمن المعلومات عوامل هامة لنجاح برامج أمن المعلومات في المنشأة. ويشمل هذا العامل مجموعة من المتغيرات الداخلية كما يوضحها الشكل رقم (٧).

٧-٣-٧-١. توافر الأشخاص المدربين على أمن المعلومات

يجب أن يتوافر لدي المنشأة الأشخاص المدربين ذوى الخبرة المهنية في مجال أمن المعلومات، وعلى إدارة الشركة البحث عن هؤلاء الأشخاص ذوى الخبرة وجذبهم للعمل في الشركة وتشجيعهم على الاستمرار في العمل بالمنشأة.

٧-٣-٧-٢. تفهم الإدارة لقضايا أمن المعلومات

يجب على الإدارة العليا أن تحدد نوعية القضايا الهامة التي تواجه أمن المعلومات بالمنشأة، وأن تدرسها بعناية شديدة وتتفهم طبيعة المشاكل المتعلقة بكل قضية حتى تستطيع تجنب تلك المشاكل في المستقبل وتقديم الحلول المناسبة لها.

٧-٣-٧-٣. التعليم المستمر للموظفين

تدريب الموظفين وسيلة ضرورية لخلق كوادر ذات خبرة ومعرفة بالقضايا التي يتدربون عليها، كما أن الاستمرار في تدريبهم على ما يحدث من مستجدات أصبح من أهم الضروريات، لذلك على إدارة الشركة إيجاد برامج ومناهج للتدريب على أمن المعلومات، مع تحديث تدريبهم كل فترة لمواكبة التطورات التي تظهر في هذا المجال.

٧-٣-٧-٤. الوعي المستمر بأمن المعلومات

إن من أهم المتغيرات التي تساعد في نجاح برامج أمن المعلومات هو ضرورة تنمية وتطوير وعى العاملين بالمنشأة في كافة المستويات الإدارية بصورة مستمرة بأمن المعلومات.

٧-٣-٧-٥. معرفة الأنظمة الرسمية للتقرير عن جرائم أمن المعلومات

إن التقرير عن الحوادث والجرائم المتعلقة بأمن المعلومات بمعرفة المسئولين عن أمن المعلومات يعد أحد المتغيرات الهامة لنجاح برامج أمن المعلومات، وذلك للتبليغ عما يحدث للمعلومات من سرقة أو تدمير أو عمليات قرصنة وسوء استخدام وخلافه لكي يمكن تفادى تلك الجرائم في المستقبل.

٧-٣-٧-٦. التوازن بين توقعات المستخدم وما يمكن تحقيقه

يتطلب هذا المتغير ضرورة إحداث توازن بين ما يتوقعه مستخدم المعلومات، وما يمكن تحقيقه عمليا وتقنيا من تطبيق آليات وسياسات معينة لأمن المعلومات.

٧-٣-٧-٧. التعليم الوثيق الصلة بعمل خبراء أمن المعلومات

إن التعليم الوثيق الصلة بعمل خبراء أمن المعلومات يمثل أحد المتغيرات الهامة لنجاح برامج أمن المعلومات، حيث أن إعداد برامج تدريبية تعليمية بصورة مستمرة للخبراء في مجال أمن المعلومات يجب أن يركز على موضوعات حماية وأمن المعلومات حتى تزيد من معرفتهم وتعليمهم السابق دراسته.

والشكل رقم (٧) يبين الإطار المقترح من خلال تجميعه لعوامل نجاح برامج أمن نظم المعلومات المحاسبية وما يحتويه كل عامل من مجموعة من المتغيرات التي ستزيد من فعالية ونجاح برامج أمن المعلومات، وتأثيرها في تفعيل حوكمة الشركات. ومما سبق يلاحظ أن حوكمة الشركات تلعب دوراً مزدوجاً في مجال أمن المعلومات، حيث تعتبر عامل رئيسي من عوامل نجاح أمن المعلومات، فهي تساهم في زيادة تفعيل برامج وخطط أمن المعلومات، وفى الوقت نفسه نجد أن مجموعة عوامل نجاح برامج أمن نظم المعلومات المحاسبية ستساهم في زيادة تفعيل حوكمة الشركات.

٨. الدراسة الميدانية على عينة من منشآت الأعمال السعودية

٨-١. أداة جمع البيانات

اعتمد الباحثان على قائمة الاستقصاء كوسيلة لجمع البيانات اللازمة لتحقيق أهداف البحث. وقد تم تصميم استمارة الاستقصاء على أساس مقياس ليكرت الخماسي Five- Point Likert Scale من أجل تحديد إجابات أفراد عينة البحث بحيث تشير الدرجة (٥) إلى القبول بدرجة عالية جداً، والدرجة (٤) إلى القبول بدرجة عالية، والدرجة (٣) إلى الحياد، والدرجة (٢) إلى عدم القبول، والدرجة (١) إلى عدم القبول بدرجة عالية.

٨-٢. عينة البحث

تم اختيار عينة البحث من مجموعة من الشركات السعودية، حيث تم توزيع عدد ٢٥٠ استمارة استقصاء على عينة عشوائية من المنشآت السعودية. ولقد شملت عينة البحث عدداً من المنشآت الصناعية؛ البنوك؛ الصحة؛ الوحدات الحكومية؛ تجارة الجملة؛ تجارة التجزئة؛ الخدمات العامة؛ البترول والغاز؛ الدعاية والإعلان؛ شركات التأمين وغيرها من المنشآت الأخرى؛ وذلك في عدد من المدن السعودية الرئيسية. وقد تم الحصول على عدد ٦٧ قائمة استقصاء صالحة للتحليل والتي تمثل ٣٤٪ من إجمالي عدد استمارات الاستقصاء التي تم توزيعها على مفردات العينة. ويعد هذا المعدل للردود معقولاً مقارنة بالأبحاث المماثلة التي تمت في هذا المجال. ولقد تم تحليل البيانات التي تم تجميعها باستخدام حزمة البرامج الجاهزة للعلوم الاجتماعية SPSS؛ الطبعة السادسة عشرة (SPSS, Version 16)

ولقد روعي في اختيار عينة البحث أن تكون عينة غير متحيزة Unbiased وأن تكون ممثلة Representative للمجتمع الذي سحبت منه. حيث تم اختيار عينة عشوائية من المنشآت السعودية من مختلف أنواع النشاطات والقطاعات من عدة مدن مختلفة في المملكة العربية السعودية. فلقد شملت عينة البحث ٩ منشآت صناعية تمثل ١٣.٤٪ من إجمالي الردود و١٣ منشأة تجارية و١٣ بنكا و١٣ وحدة حكومية (تمثل كل منها ١٩.٤٪ من إجمالي الردود)؛ كما اشتملت عينة البحث أيضا على منشأتين من المنشآت الخدمية وشركتين تأمين (تمثل كل منها ٣٪ من إجمالي الردود). كما تضمنت عينة الدراسة عدد سبعة منشآت صحية تمثل ١٠.٤٪ وعدد ثمانية شركات أخرى معظمها من شركات مقاولات والتي تمثل ١١.٩٪ جدول رقم (١).

جدول رقم (١) عينة البحث

عينة البحث حسب نوع الصناعة			عينة البحث حسب الوظيفة		
نوع المنشأة	العدد	النسبة	الوظيفة	العدد	النسبة
منشأة صناعية	9	13.4	محاسب مالي	14	20.9
منشأة تجارية	13	19.4	مراجع داخلي	8	11.9
بنك	13	19.4	محاسب تكاليف	6	9
منشأة خدمية	2	3	مراقب عام	5	7.5
شركة تأمين	2	3	مراجع لنظم المعلومات	5	7.5
وحدة حكومية	13	19.4	الإلكترونية	24	35.8
منشأة صحية	7	10.4	رئيس قسم	5	7.5
أخرى	8	11.9	مدير عام	-	-
الإجمالي	67	100.0		67	100.0

وتجدر الإشارة إلى أن ١٤ من المشاركين في الاستقصاء (٢٠.٩٪ من إجمالي الردود) كانوا يعملون محاسبون ماليون؛ وأن ثمانية من المشاركين في الاستقصاء (١١.٩٪ من إجمالي

الردود) كانوا يعملون كمراجعين داخليين. بينما ستة من المشاركين (٩٪ من إجمالي الردود) كانوا يعملون كمحاسبي تكاليف. بينما خمسة من المشاركين (٧.٥٪ من إجمالي الردود) ونسبة مماثلة يعملون كمراجعي لنظم المعلومات الإلكترونية، ونسبة أخرى مماثلة كمديرين عموميين. بينما ٢٤ من المشاركين (٣٥.٨٪ من إجمالي الردود) كانوا يعملون كرؤساء أقسام. ومن ثم فإنه يمكن القول بأن عينه البحث تعد عينة ممثلة للهيكل الوظيفي في عينة المنشآت السعودية جدول رقم (١). وسوف يتم عرض ومناقشة نتائج الدراسة في الأقسام التالية.

٨-٣. أسلوب تحليل البيانات

اعتمد الباحثان على حزمة البرامج الإحصائية SPSS Version (16) في تحليل البيانات المجمعة من استمارات الاستقصاء لتحقيق أهداف البحث. من خلال استخدام الاختبارات الآتية:-

(١) اختبار ألفا- كرونباخ Cronbach's Alpha لأغراض تحليل مدى التجانس بين البنود المستخدمة في قياس المتغيرات.

(٢) الاختبارات اللامعلمية لاختبار فروض البحث.

ولقد قام الباحثان بإجراء التحليل الوصفي Descriptive Analysis (مثل معدل التكرارات والنسب) للبيانات التي تم تجميعها للتعرف على الخصائص الأساسية لعينة البحث ومتغيرات الدراسة. كما تم إجراء بعض الاختبارات اللامعلمية Non-Parametric Tests (مثل اختبار كارسوكال - ولاس Krsukal-Wallis وكذلك اختبار تحليل التباين ANOVA) لاختبار فروض البحث والتعرف على الفروق الجوهرية بين المنشآت المختلفة فيما يتعلق بمحددات وعوامل نجاح برامج أمن نظم المعلومات المحاسبية.

٨-٤. نتائج الدراسة الميدانية

٨-٤-١. اختبار تحليل المصداقية Reliability Analysis

ويتم هذا الاختبار عن طريق استخدام اختبار ألفا- كرونباخ Cronbach's Alpha الذي يبين مدى تجانس بنود المتغيرات المستخدمة في قياس ظاهرة معينة، وفى ضوء هذا الاختبار تتوافر المصداقية Reliability لأداه جمع البيانات، ويكون هناك تجانس واتساق كبير بين المتغيرات كلما اقتربت قيمة Alpha من الواحد الصحيح، بينما يكون هناك عدم تجانس كلما اقتربت قيمة Alpha من الصفر.

جدول قم (٢) اختبار تحليل المصداقية

عوامل نجاح برامج أمن نظم المعلومات المحاسبية	اختبار ألفا- كرونباخ
العوامل الثقافية	0.735
الموارد البشرية / الميزانية والتمويل	0.264
المنظمة / العلاقات التنظيمية	0.776
التكنولوجيا والعمليات المتعلقة بها	0.742
القوانين / التعليمات / الحوكمة / السياسات والمعايير	0.560

عوامل نجاح برامج أمن نظم المعلومات المحاسبية	اختبار ألفا- كرونباخ
آلية المصفوفة الأمنية	0.625
التدريب / التعليم المستمر / الوعى	0.881
الإجمالي	0.917

ويوضح الجدول رقم (٢) أن اختبار ألفا- كرونباخ لعوامل النجاح كلها تقترب من الواحد الصحيح باستثناء عامل الموارد البشرية / الميزانية والتمويل، وقد يرجع ذلك إلى أن عدد متغيرات ذلك العامل كان صغيراً نسبياً (متغيران فقط).

٨-٤-٢. تحليل نتائج الاختبارات اللامعلمية

٨-٤-٢-١. العوامل الثقافية

لقد أوضحت نتائج الدراسة أن الغالبية العظمى من المشاركين في الاستقصاء (٩٤٪) يرون أن مجالس الإدارات والإدارات التنفيذية بمنشآتهم لديهم اعتقاد بأهمية وأولوية أمن المعلومات، وأنهم يقومون بالرقابة على مخاطر أمن المعلومات (٨٥.١٪). وأن أمن المعلومات يعد من الموضوعات الهامة التي تدرج بصفة منتظمة ومستمرة على جدول أعمال مجلس الإدارة (٨٥.١٪) في المنشآت التي يعملون بها. كما تشير نتائج الدراسة إلى أن غالبية المشاركين في الاستقصاء (٨٩.٦٪) يؤكدون على أن الإدارات العليا والإدارات التنفيذية بمنشأتهم تقوم بمسؤوليتها كاملة فيما يتعلق بتطبيق ورقابة والتقرير عن أمن المعلومات جدول رقم (٣).

ولقد أظهرت نتائج اختبارات كلاً من كارسوكال – ولاس وتحليل التباين جدول رقم (٤) وجود اختلافات جوهرية بين المنشآت السعودية فيما يتعلق باعتبار أمن المعلومات من الموضوعات الهامة التي تدرج بصفة منتظمة ومستمرة على قائمة جدول أعمال مجلس الإدارة عند مستوى معنوية P = 0.05. **ومن ثم يمكن قبول الفرض الإحصائي الأول بأنه لا توجد اختلافات جوهرية بين المنشآت السعودية في القطاعات الاقتصادية المختلفة فيما يتعلق بمدى إدراكها *<u>للعوامل الثقافية</u>* الهامة اللازمة لنجاح برامج أمن نظم المعلومات المحاسبية** إلا فيما يتعلق باعتبار أمن المعلومات من الموضوعات الهامة التي تدرج بصفة منتظمة ومستمرة على قائمة جدول أعمال مجالس الإدارات، حيث أوضحت الدراسة أن البنوك وشركات التأمين وشركات الخدمات تولى الموضوعات المتعلقة بأمن المعلومات اهتماماً خاصاً، حيث تعد من الموضوعات الهامة المدرجة بصفة منتظمة ومستمرة على جدول أعمال مجلس الإدارة. ولم تظهر نتائج الاختبارات الإحصائية وجود اختلافات جوهرية بين المنشآت السعودية فيما يختص بمتغيرات العوامل الثقافية الأخرى.

وتجدر الإشارة إلى أن نتائج اختبارات كارسوكال – ولاس وكذلك نتائج اختبارات تحليل التباين جدول رقم (٤) لم تفصح عن وجود اختلافات جوهرية بين آراء الوظائف المختلفة بالمنشآت السعودية فيما يتعلق بأهمية وتطبيق العوامل الثقافية كمحددات هامة ورئيسية لنجاح برامج أمن المعلومات عند مستوى معنوية P = 0.05. **وبالتالي يمكن قبول الفرض الإحصائي الثاني القائل بعدم**

وجود اختلافات جوهرية بين إدراك الوظائف المختلفة داخل المنشآت السعودية فيما يتعلق *بالعوامل الثقافية* الهامة اللازمة لنجاح برامج أمن نظم المعلومات المحاسبية.

بينما أظهرت نتائج اختبارات تحليل التباين جدول رقم (٤) وجود اختلافات جوهرية فيما يتعلق بقيام مجالس الإدارات والإدارات التنفيذية بالرقابة على مخاطر أمن المعلومات بين المنشآت السعودية التي تستخدم نظماً محاسبية مختلفة عند مستوى معنوية P = 0.05 جدول رقم (٤). **وبناء عليه يمكن قبول الإحصائي الثالث بأنه لا توجد اختلافات جوهرية بين المنشآت السعودية التي تستخدم نظماً محاسبية مختلفة فيما يتعلق بمدى إدراكها *للعوامل الثقافية* الهامة اللازمة لنجاح برامج أمن نظم المعلومات المحاسبية إلا فيما يتعلق بقيام مجالس الإدارات والإدارات التنفيذية بالرقابة على مخاطر أمن المعلومات**، حيث أوضحت الدراسة أن المنشآت التي لديها نظم محاسبية إلكترونية تعتمد بدرجة كبيرة على الكمبيوتر قد أظهرت اهتماماً كبيراً بالرقابة على مخاطر أمن المعلومات مقارنة بمثيلتها من المنشآت التي لديها نظم محاسبية يدوية أو نظم محاسبية إلكترونية تعتمد على خليط من العمل اليدوي والتشغيل الإلكتروني.

٨-٤-٢-٢. الموارد والميزانية والتمويل

فيما يتعلق بمدى توافر الموارد البشرية والميزانية والتمويل، تشير نتائج الدراسة إلى أن ٨٠.٦٪ من المشاركين في الاستقصاء يرون أنه يوجد تمويل كافي وميزانية مناسبة ومفعّلة لأمن المعلومات، وأن ٧٢.١٪ من المشاركين في الاستقصاء يؤكدون وجود ميزانيات لإستراتيجيات أمن المعلومات والخطط التكتيكية المتعلقة بها في المنشآت السعودية جدول رقم (٣).

وتجدر الإشارة إلى أن نتائج اختبار كارسوكال – ولاس جدول رقم (٤) لم تظهر أي اختلافات جوهرية بين المنشآت السعودية حسب طبيعة نشاطها أو حسب وظيفة المشاركين بالاستقصاء أو طبيعة النظام المحاسبي المطبق بتلك المنشآت عند مستوى معنوية P= 0.05. **ومن ثم يمكن قبول الفرضين الإحصائيين الأول والثاني بأنه لا توجد اختلافات جوهرية بين المنشآت السعودية في القطاعات الاقتصادية المختلفة و كذلك عدم جود اختلافات جوهرية بين إدراك الوظائف المختلفة داخل تلك المنشآت فيما يتعلق بمدى إدراكها لأهمية وضرورة توافر تمويل كافي و ميزانية ومفعّلة مناسبة لنجاح برامج أمن نظم المعلومات المحاسبية.** بينما أظهرت نتائج اختبارات تحليل التباين جدول رقم (٤) وجود اختلافات جوهرية (عند مستوى معنوية P = 0.05) فيما يتعلق بوجود ميزانيات لإستراتيجيات أمن المعلومات والخطط التكتيكية بين المنشآت السعودية ذات الطبيعة المختلفة. **ومن ثم يمكن رفض الفرضية الإحصائية المتعلقة بالفرض الثالث بأنه لا توجد اختلافات جوهرية بين المنشآت السعودية التي تستخدم نظماً محاسبية مختلفة فيما يتعلق بمدى إدراكها بوجود تمويل كافي و ميزانيات مناسبة ومفعّلة لأمن المعلومات في المنشآت السعودية.**

٨-٤-٢-٣. المنظمة والعلاقات التنظيمية

أظهرت نتائج الدراسة أن نسبة عالية من المنشآت السعودية التي شاركت في الاستقصاء (٧٩.١٪) لديها تحديد واضح لمسؤوليات الاتصال بالزبون وكذلك مسؤولية الخسارة الناتجة عن

الالتزامات المرتبطة باستخدام التكنولوجيا في العمليات والصفقات مع العملاء. وأن الإدارات العليا لديها التزام فيما يتعلق بمبادرات أمن المعلومات (٧٧.٧٪). كما تشير نتائج الدراسة إلى أن معظم المشاركين في الاستقصاء يؤكدون على وجود تناسق وتناغم بين أهداف الشركة وأهداف أمن المعلومات (٨٩.٦٪)، وأن هناك تكامل بين أنشطة وعمليات الشركة وأمن المعلومات (٨٠.٦٪) بالمنشآت التي يعملون فيها.

كما تشير نتائج الدراسة إلى أن ٧٤.٤٪ من المنشآت المشاركة في الاستقصاء يوجد لديها توصيف واضح للهيكل الإداري والتنظيمي، غير أن أمن المعلومات يحتل المكان المناسب في الهيكل الإداري والتنظيمي في ٦٧.١٪ فقط من تلك المنشآت جدول رقم (٣). ولقد أوضحت نتائج الدراسة جدول رقم (٣) أن غالبية المشاركين في الاستقصاء (٧٩.١٪) يعتقدون أنه يوجد تعريفات واضحة لأمن المعلومات وأنها مرتبطة بشكل ملائم وكاف برؤية وإستراتيجية المنشآت التي يعملون بها، وان تلك المنشآت تركز على تحقيق الأهداف المرسومة لأمن المعلومات في الأجل القصير وذلك لمنع حدوث أي مشاكل محتملة لأمن المعلومات في الأجل الطويل.

ومن ناحية أخرى فإن ٥٩.٧٪ من المشاركين في الاستقصاء يرون أن تدخل الإدارة لا يعطي أفضل الحلول للمشكلات المتعلقة باختيار منتج أو خدمة معينة في منشأتهم جدول رقم (٣). وأن نسبة ٤١.٧٪ فقط من المشاركين في الاستقصاء يعتقدون أن هناك تكاملاً بين الوسائل التكنولوجية الحديثة لأمن المعلومات والترتيبات التقليدية لأمن المعلومات في المنشآت السعودية.

ولقد أظهرت نتائج اختبار كارسوكال – ولاس جدول رقم (٤) عدم وجود فروق جوهرية بين المنشآت السعودية فيما يختص بمتغيرات العلاقات التنظيمية عند مستوى معنوية P = 0.05. كما أظهرت نتائج اختبارات تحليل التباين جدول رقم (٤) عدم وجود فروق جوهرية بين المنشآت السعودية (عند مستوى معنوية P = 0.05) إلا فيما يتعلق بوجود تكامل بين أنشطة وعمليات الشركة وأمن المعلومات. **وبناءً على ذلك، يمكن قبول الفرض الإحصائي الأول بأنه لا توجد اختلافات جوهرية بين المنشآت السعودية في القطاعات الاقتصادية المختلفة فيما يتعلق بمدى إدراكها لمتغيرات العلاقات التنظيمية الهامة واللازمة لنجاح برامج أمن نظم المعلومات المحاسبية إلا فيما يختص بوجود تكامل بين أنشطة وعمليات الشركة وأمن المعلومات.** بينما تشير نتائج اختبار كارسوكال – ولاس جدول رقم (٤) إلى وجود فروق جوهرية بين آراء الأشخاص في الوظائف المختلفة فيما يتعلق بالتزام الإدارات العليا بمبادرات أمن المعلومات في المنشآت السعودية عند مستوى معنوية P = 0.05. بينما تشير نتائج اختبارات تحليل التباين جدول رقم (٤) إلى عدم وجود فروق جوهرية بين أراء المشاركين في الاستقصاء ذوى الوظائف المختلفة فيما يختص بمتغيرات العلاقات التنظيمية عند مستوى معنوية P = 0.05. **ومن ثم يمكن قبول الفرض الإحصائي الثاني القائل بعدم وجود اختلافات جوهرية بين إدراك الوظائف المختلفة في المنشآت السعودية فيما يتعلق بمتغيرات العلاقات التنظيمية الهامة اللازمة لنجاح برامج أمن نظم المعلومات المحاسبية إلا فيما يختص بالتزام الإدارات العليا بمبادرات أمن المعلومات.** كما أظهرت نتائج اختبارات كارسوكال – ولاس جدول رقم (٤) وجود فروق جوهرية بين المنشآت السعودية التي تستخدم نظماً محاسبية الكترونية

وتلك التي لديها نظماً محاسبية يدوية بأن تدخل الإدارة في اختيار المنتج أو الخدمة لا يعطي أفضل الحلول الممكنة لمشاكل أمن المعلومات، وكذلك وجود تكامل بين أنشطة وعمليات الشركة وأمن المعلومات عند مستوى معنوية P = 0.05. بينما أظهرت نتائج اختبارات تحليل التباين جدول رقم (٤) وجود اختلافات جوهرية بين المنشآت السعودية التي تطبق نظم محاسبية مختلفة في درجة الآلية فيما يختص بمدى التزام الإدارات العليا بمبادرات أمن المعلومات عند مستوى معنوية P = 0.05. **وبالتالي يمكن قبول الفرض الإحصائي الثالث القائل بعدم وجود اختلافات جوهرية بين المنشآت السعودية التي تطبق نظم محاسبية مختلفة في درجة الآلية لمتغيرات العلاقات التنظيمية الهامة اللازمة لنجاح برامج أمن نظم المعلومات المحاسبية إلا فيما يتعلق بتدخل الإدارة في اختيار المنتج أو الخدمة لا يعطي أفضل الحلول الممكنة لمشاكل أمن المعلومات، مدى التزام الإدارات العليا بمبادرات أمن المعلومات، وكذلك وجود تكامل بين أنشطة وعمليات الشركة وأمن المعلومات.**

٨-٤-٢-٤. التكنولوجيا والعمليات المتعلقة بها

فيما يتعلق بالتكنولوجيا والعمليات المتعلقة بها تشير نتائج الدراسة إلى أن ٨٦.٦٪ من المشاركين في الاستقصاء يرون أن وجود تخطّيط كافي للأمن قبل اقتناء وتطبيق التقنيات الجديدة تمثل أحد العوامل الهامة لنجاح برامج أمن المعلومات في المنشآت السعودية. وان نسبة كبيرة من المشاركين في الاستقصاء (٧٩.١٪) يعتقدون بوجود إجراءات وإمكانيات ملائمة ومناسبة لإدارة التغيير بالمنشآت التي يعملون بها، وأن المنشآت السعودية (٧٧.٦٪) لديها القدرة على الاستجابة والرد على عمليات القرصنة والعمليات المتعلقة باختراق النظم واستخدامها بطريقة غير مشروعة جدول رقم (٣). كما تشير نتائج الدراسة إلى أن ٧٤.٦٪ من المنشآت المشاركة في الاستقصاء يعتقدون أن تحقيق موازنة بين التوقّعات من استخدام الحلول الآلية مع الجدوى الفنية لمشاكل أمن المعلومات تمثل أحد عوامل النجاح الهامة لبرامج أمن المعلومات في المنشآت السعودية جدول رقم (٣).

وتجدر الإشارة إلى أن نتائج اختبارات كارسوكال – ولاس وكذلك نتائج اختبارات تحليل التباين جدول رقم (٤) لم تفصح عن وجود اختلافات جوهرية بين المنشات ذات الأنشطة الاقتصادية المختلفة أو بين الوظائف المختلفة عند درجة معنوية P = 0.05. **ومن ثم يمكن قبول الفرضين الإحصائيين الأول والثاني بأنه لا توجد اختلافات جوهرية بين المنشآت السعودية في القطاعات الاقتصادية المختلفة و كذلك عدم جود اختلافات جوهرية بين إدراك الوظائف المختلفة في تلك المنشآت فيما يتعلق بالتكنولوجيا والعمليات المتعلقة بها كعوامل نجاح حاسمة لبرامج أمن نظم المعلومات المحاسبية في المنشآت السعودية.**

جدول رقم (٣) التكرارات والنسب لعوامل نجاح برامج أمن نظم المعلومات المحاسبية

عوامل نجاح برامج أمن نظم المعلومات المحاسبية	أوافق بشدة		أوافق		محايد		لا أوافق		لا أوافق بشدة	
العوامل الثقافية	عدد	٪	عدد	٪	عدد	٪	عدد	٪	عدد	٪
١. اعتقاد مجلس الإدارة / الإدارة التنفيذية بأهمية وأولوية أمن المعلومات	48	71.6	15	22.4	2	3	2	3	-	-
٢. يقوم مجلس الإدارة / الإدارة التنفيذية بالرقابة على مخاطر أمن المعلومات	42	62.7	15	22.4	8	11.9	2	3	-	-
٣. يعد أمن المعلومات من الموضوعات الهامة المدرجة بصفة منتظمة ومستمرة على جدول أعمال مجلس الإدارة	37	55.2	22	32.8	6	9	2	3	-	-
٤. تقوم الإدارة العليا والإدارة التنفيذية بمسؤوليتها فيما يتعلق بتطبيق ورقابة والتقرير عن أمن المعلومات	29	43.3	31	46.3	5	7.5	2	3	-	-
الموارد البشرية / الميزانية والتمويل										
٥. يوجد تمويل كافي وميزانية مناسبة ومفعّلة لأمن المعلومات	25	37.3	29	43.3	8	11.9	4	6	1	1.5
٦. توجد ميزانية لإستراتيجية أمن المعلومات والخطة التكتيكية	21	31.3	28	41.8	13	19.4	5	7.5	-	-
المنظمة / العلاقات التنظيمية										
٧. تحديد مسؤوليات الاتصال بالزبون وكذلك مسؤولية الخسارة الناتجة عن الالتزامات المرتبطة باستخدام التكنولوجيا في عمليات الصفقات مع الزبون.	23	34.3	30	44.8	12	17.9	2	3	-	-
٨. التزام الإدارة العليا فيما يتعلق بمبادرات أمن المعلومات	20	29.9	32	47.8	11	16.4	3	4.5	1	1.5
٩. تأثير وتدخل الإدارة يؤدّي إلى اختيار منتج / خدمة لا يعطي أفضل حل للمشكلة	16	23.9	24	35.8	17	25.4	7	10.4	3	4.5
١٠. يوجد تناسق وتناغم بين أهداف الشركة وأهداف أمن المعلومات	41	61.2	19	28.4	4	6	2	3	1	1.5
١١. يوجد تكامل بين أنشطة وعمليات الشركة وأمن المعلومات	34	50.7	20	29.9	5	7.5	7	10.4	1	1.5
١٢. يوجد توصيف واضح للهيكل الإداري بالشركة	35	52.2	10	22.2	9	13.4	5	7.5	1	1.5
١٣. التركيز على الأهداف القصيرة الأجل لمنع مشاكل ضعف أمن المعلومات في الأجل الطويل	35	52.2	18	26.9	8	11.9	5	7.5	1	1.5
١٤. يوجد تعريف واضح لأمن المعلومات مرتبط بشكل ملائم وكافي برؤية وإستراتيجية الشركة.	22	32.8	31	46.3	8	11.9	6	9	-	-
١٥. أمن المعلومات يحتل المكان المناسب في الهيكل الإداري والتنظيمي للشركة	24	35.8	21	31.3	17	25.4	5	7.5	-	-
١٦. تكامل أمن تكنولوجيا المعلومات مع وسائل وترتيبات الأمن التقليدي	18	26.9	28	14.8	13	19.4	5	7.5	3	4.5
التكنولوجيا والعمليات المتعلقة بها										
١٧. يوجد تخطّيط كافي للأمن قبل تطبيق التقنيات الجديدة	33	49.3	25	37.3	7	10.4	2	3	-	-
١٨. توجد إجراءات ملائمة ومناسبة لإدارة التغيير	22	32.8	26	38.8	15	22.4	2	3	2	3

عوامل نجاح برامج أمن نظم المعلومات المحاسبية	أوافق بشدة		أوافق		محايد		لا أوافق		لا أوافق بشدة	
١٩. القدرة على الاستجابة والرد على عمليات القرصنة والعمليات المتعلقة باختراق النظام واستخدامه بطريقة غير مشروعة.	29	43.3	23	34.3	7	10.4	5	7.5	3	4.5
٢٠. موازنة التوقّعات مع الجدوى الفنية من الحلول الآلية	23	34.3	27	40.3	11	16.3	4	6	1	1.5
القوانين / التعليمات / الحوكمة / السياسات والمعايير										
٢١. الالتزام بمتطلبات القوانين القضائية المتعدّدة والمتعلقة بعمليات الشركة	31	46.3	22	32.8	11	16.4	3	4.5	-	-
٢٢. تبني القوانين واللوائح والتعليمات الملائمة وغير المتعارضة	26	38.8	31	46.3	9	13.4	-	-	1	1.5
٢٣. الالتزام بتنفيذ سياسات ومعايير أمن المعلومات	26	38.8	23	34.4	14	20.9	3	4.5	1	1.5
٢٤. التنفيذ الثابت والمستمر للسياسات والمعايير المتعلقة بأمن المعلومات	28	41.8	23	34.3	9	13.4	5	7.5	2	3
آلية المصفوفة الأمنية										
٢٥. وضع إطار لإدارة مخاطر المشروع والذي يتكامل مع أمن المعلومات	35	52.2	21	31.3	6	9	3	4.5	2	3
٢٦. الاتفاق على منهج عالميا لتقدير وتقييم المخاطر	24	35.8	28	14.8	12	17.9	2	3	1	1.5
٢٧. الاتفاق على أليه لأمن المعلومات مقبولة قبولا عاما طبقا لأفضل الممارسات لأمن المعلومات	30	44.8	25	37.3	8	11.9	2	3	2	3
٢٨. ربط آليات وتقارير أمن المعلومات مع أهداف وإستراتيجيات الشركة	32	47.8	23	34.3	7	10.4	3	4.5	2	3
التدريب / التعليم المستمر/ الوعي										
٢٩. توافر الأشخاص المدرّبين ذوي الخبرة المهنية في مجال أمن المعلومات	37	55.2	19	28.4	8	11.9	2	3	1	1.5
٣٠. تفهم الإدارة للقضايا والموضوعات المتعلقة بأمن المعلومات	24	35.8	27	40.3	6	9	8	11.9	2	3
٣١. تعليم الموظفين، وتحديث تعليمهم ومعلوماتهم فيما يختص بحماية المعلومات	38	56.7	14	20.9	7	10.4	6	9	2	3
٣٢. الوعي المستمر لأمن المعلومات	32	47.8	21	31.3	10	14.9	2	3	2	3
٣٣. معرفة الأنظمة الرسمية للتقرير عن الحوادث والجرائم المتعلقة بأمن المعلومات	26	38.8	20	29.9	15	22.4	4	6	2	3
٣٤. إحداث التوازن بين توقّعات المستخدم وما يمكن تحقيقه عمليا وتقنيا	29	43.3	23	34.3	7	10.4	6	9	2	3
٣٥. التعليم الوثيق الصلة بعمل خبراء أمن المعلومات، مثل التعليم المهني المستمر	32	47.8	15	22.4	9	13.4	6	9	5	7.5

وعلى الرغم من نتائج اختبارات تحليل التباين جدول رقم (٤) لم تظهر وجود أي اختلافات جوهرية بين المنشات ذات النظم المحاسبية المختلفة عند درجة معنوية P = 0.05، إلا أن نتائج اختبارات كارسوكال – ولاس قد أظهرت اختلافات جوهرية بين المنشات ذات النظم المحاسبية المختلفة يتعلق بوجود إجراءات ملائمة ومناسبة لإدارة التغيير في المنشات التي تستخدم نظماً محاسبية شديدة الآلية مقارنة بغيرها من المنشآت التي تطبق نظماً محاسبية يدوية أو خليطاً من العمل اليدوي والتشغيل الإلكتروني عند درجة معنوية P = 0.05 . **ومن ثم يمكن قبول الفرض الإحصائي الثالث بأنه لا توجد اختلافات جوهرية بين المنشآت السعودية التي تستخدم نظماً محاسبية مختلفة إلا فيما يتعلق بوجود إجراءات ملائمة ومناسبة لإدارة التغيير.**

٨-٤-٢-٥. الالتزام بالقوانين والسياسات والمعايير ومبادئ الحوكمة

تشير نتائج الدراسة إلى أن غالبية المنشآت المشاركة في الاستقصاء يرون أن تبني مجموعة ملائمة وغير متعارضة من القوانين واللوائح والسياسات والتعليمات ٨٥.١٪، وأن الالتزام بمتطلبات القوانين القضائية المتعدّدة والمتعلقة بعمليات الشركة ٧٩.١٪ تمثل أحد عوامل النجاح الهامة لبرامج أمن المعلومات في عينة المنشآت السعودية. ولقد أشارت نتائج الدراسة إلى أن ٧٣.٢٪ من المشاركين في الاستقصاء أكدوا الالتزام بتنفيذ سياسات ومعايير أمن المعلومات، وأن هناك ثبات نسبى ومستمر في تنفيذ وتطبيق السياسات والمعايير المتعلقة بأمن المعلومات (٧٩.١٪) في المنشآت السعودية.

وتشير نتائج اختبارات كلاً من كارسوكال – ولاس وتحليل التباين جدول رقم (٤) إلى عدم وجود اختلافات جوهرية بين المنشآت السعودية فيما يتعلق بالالتزام بمتطلبات القوانين القضائية المتعدّدة والمتعلقة بعمليات الشركة، وتبني القوانين واللوائح والتعليمات الملائمة وغير المتعارضة، والالتزام بتنفيذ سياسات ومعايير أمن المعلومات، والتنفيذ الثابت والمستمر لتلك السياسات والمعايير المتعلقة بأمن المعلومات المنشآت السعودية عند مستوى معنوية P = 0.05. وتجدر الإشارة إلى أن نتائج اختبارات تحليل التباين جدول رقم (٤) قد أظهرت وجود اختلافات جوهرية بين المنشات السعودية في القطاعات الاقتصادية المختلفة فيما يتعلق بالتنفيذ الثابت والمستمر للسياسات والمعايير المتعلقة بأمن المعلومات. **وطبقاً لنتائج الاختبارات الإحصائية فإنه يمكن قبول الفرض الإحصائي الأول بأنه لا توجد اختلافات جوهرية بين المنشآت السعودية في القطاعات الاقتصادية المختلفة فيما يتعلق بالالتزام بالقوانين والسياسات والمعايير ومبادئ الحوكمة إلا فيما يتعلق بالتنفيذ الثابت والمستمر للسياسات والمعايير المتعلقة بأمن المعلومات كأحد عوامل النجاح الهامة لبرامج أمن نظم المعلومات المحاسبية. كما يمكن أيضا قبول الفرضين الإحصائيين الثاني والثالث بعدم وجود اختلافات جوهرية بين المنشآت السعودية ذات النظم المحاسبية المختلفة و كذلك عدم جود اختلافات جوهرية بين إدراك الوظائف المختلفة في تلك**

المنشآت فيما يتعلق بالالتزام بالقوانين والسياسات والمعايير ومبادئ الحوكمة كعوامل نجاح حاسمة لبرامج أمن نظم المعلومات المحاسبية في المنشآت السعودية .

٨-٤-٢-٦. آلية المصفوفة الأمنية

تشير نتائج الدراسة إلى أن ٨٣.٥٪ من المنشآت المشاركة في الاستقصاء قد عبروا عن رأيهم بوجود إطار لإدارة المخاطر والذي يتكامل مع أمن المعلومات بالمنشآت التي يعملون بها، وأسفرت نتائج الدراسة عن أن ٨٢.١٪ من المشاركين في الاستقصاء يؤكدون على ربط آليات وتقارير أمن المعلومات مع أهداف وإستراتيجيات الشركة بالمنشآت التي يعملون بها، وأن هناك اتفاق على وجود آلية لأمن المعلومات مقبولة قبولا عاما طبقا لأفضل الممارسات لأمن المعلومات في المنشآت السعودية. بينما نجد أن نسبة ضئيلة من المشاركين في الاستقصاء (٥٠.٦٪ من إجمالي الردود) يعتقدون بوجود اتفاق على منهج عالمي لتقدير وتقييم المخاطر المتعلقة بأمن المعلومات في المنشآت السعودية.

وتجدر الإشارة إلى أن نتائج اختبارات كارسوكال – ولاس وكذلك اختبارات تحليل التباين جدول رقم (٤) لم تفصح عن وجود أي فروق جوهرية بين أنواع المنشآت المختلفة فيما يتعلق بمتغيرات آلية المصفوفة الأمنية المتعلقة بوضع إطار لإدارة مخاطر المشروعات والتي تتكامل مع السياسات وأفضل الممارسات لأمن المعلومات، الاتفاق على آلية منهجية لتقدير وتقييم تلك المخاطر، بالإضافة إلى ربط آليات وتقارير أمن المعلومات مع أهداف وإستراتيجيات تلك المنشآت عند مستوى معنوية P = 0.05. **وطبقاً لنتائج الاختبارات الإحصائية فإنه يمكن قبول الفروض** الإحصائية الثلاثة القائلة بعدم وجود **اختلافات جوهرية بين المنشآت السعودية بالقطاعات الاقتصادية المختلفة، ذات النظم المحاسبية المختلفة، وكذلك عدم وجود اختلافات جوهرية الوظائف المختلفة فيما يتعلق بمتغيرات آلية المصفوفة الأمنية كعوامل نجاح حاسمة لبرامج أمن نظم المعلومات المحاسبية في المنشآت السعودية.**

٨-٤-٢-٧. التدريب / التعليم المستمر/ الوعي

تشير نتائج الدراسة إلى أن ٨٣.٦٪ من المشاركين في الدراسة يعتقدون بتوافر الأشخاص المدرّبين ذوي الخبرة المهنية في مجال أمن المعلومات، بينما يؤكد ٧٠.٢٪ من المشاركين في الاستقصاء على حرص منشآتهم على التعليم المهني المستمر الوثيق الصلة بعمل خبراء أمن المعلومات. وأن ٧٦.١٪ من المشاركين في الاستقصاء يؤكدون تفهم الإدارة للقضايا والموضوعات المتعلقة بأمن المعلومات، وحرصها على تعليم الموظفين وتحديث تعليمهم ومعلوماتهم فيما يختص بحماية المعلومات (٧٧.٦٪)، وكذلك تنمية الوعي العام والمستمر بأهمية أمن المعلومات (٧٨.١٪) من خلال الاشتراك في الندوات والدورات المتعلقة بحماية وتأمين المعلومات.

بينما تشير نتائج الدراسة إلى أن نسبة عالية من المشاركين في الاستقصاء (٧٧.٢٪) قد أشاروا إلى وجود توازن بين توقّعات المستخدم من آليات أمن المعلومات وما يمكن تحقيقه عمليا

وتقنيا في هذا المجال، وأن الإدارة لديها معرفة بالأنظمة الرسمية للتقرير عن الحوادث والجرائم المتعلقة بأمن المعلومات (٦٨.٧٪) بالمنشآت السعودية.

ولقد أظهرت نتائج اختبارات كلاً من كارسوكال – ولاس وتحليل التباين جدول رقم (٤) وجود اختلافات جوهرية بين المنشآت السعودية فيما يتعلق بالتعليم المهني المستمر الوثيق الصلة بعمل خبراء أمن المعلومات، وكذلك معرفة الأنظمة الرسمية للتقرير عن الحوادث والجرائم المتعلقة بأمن المعلومات عند مستوى معنوية $P = 0.05$. **ومن ثم يمكن رفض الفرض الإحصائي الأول بأنه لا توجد اختلافات جوهرية بين المنشآت السعودية في القطاعات الاقتصادية المختلفة فيما يتعلق بالتعليم المهني المستمر الوثيق الصلة بعمل خبراء أمن المعلومات، وكذلك معرفة الأنظمة الرسمية للتقرير عن الحوادث والجرائم المتعلقة بأمن المعلومات.** وعلى الجانب الأخر لم تظهر نتائج اختبارات كلاً من كارسوكال – ولاس وتحليل التباين جدول رقم (٤) أي اختلافات جوهرية بين آراء المشاركين في الاستقصاء في الوظائف المختلفة وكذلك المنشآت ذات النظم ذات درجات الآلية المختلفة عند درجة معنوية $P = 0.05$. **وبناء على ذلك يمكن قبول الفرضين الإحصائيين الثاني والثالث بعدم وجود اختلافات جوهرية بين المنشآت السعودية ذات النظم المحاسبية المختلفة وكذلك عدم جود اختلافات جوهرية بين إدراك الوظائف المختلفة في تلك المنشآت لأهمية التدريب والتعليم المستمر كعوامل نجاح حاسمة لبرامج أمن نظم المعلومات المحاسبية في المنشآت السعودية.** ويعرض الجدول رقم (٥) ملخصاً لنتائج اختبارات الفروض الإحصائية للدراسة.

٩. خلاصة البحث

تناول البحث كيفية الحفاظ على أمن المعلومات من خلال تحديد ودراسة مجموعة من عوامل نجاح برامج أمن نظم المعلومات المحاسبية، ودورها في تفعيل حوكمة الشركات، واختبارها ميدانيا على مجموعة من شركات الأعمال السعودية، وذلك بتناول أهمية أمن المعلومات وضرورة الحفاظ عليها، والتعرف على دور حوكمة الشركات في تعزيز وتفعيل أمن المعلومات، ودراسة عوامل نجاح برامج أمن نظم المعلومات المحاسبية بشكل تفصيلي، وبيان دور عوامل نجاح برامج أمن نظم المعلومات المحاسبية في تفعيل حوكمة الشركات. ولقد قدم البحث إطاراً مقترحاً لتحديد ودراسة عوامل نجاح برامج أمن نظم المعلومات المحاسبية، ودورها في تفعيل حوكمة الشركات واختبار هذه العوامل من خلال دراسة ميدانية في بيئة الأعمال السعودية.

جدول رقم (٤) نتائج الاختبارات الإحصائية لعوامل نجاح برامج أمن نظم المعلومات المحاسبية

عوامل نجاح برامج أمن نظم المعلومات المحاسبية	كارسوكال والاس طبقاً لنوع المنشأة		كارسوكال والاس طبقاً للوظيفة		كارسوكال والاس طبقاً للنظام المحاسبي		ANOVA طبقاً لنوع المنشأة		ANOVA طبقاً للوظيفة		ANOVA طبقاً للنظام المحاسبي	
العوامل الثقافية	**Chi**	**Sig**	**Chi**	**Sig**	**Chi**	**Sig**	**F**	**Sig**	**F**	**Sig**	**F**	**Sig**
١. اعتقاد مجلس الإدارة / الإدارة التنفيذية بأهمية وأولوية أمن المعلومات	9.62	0.21	3.79	0.71	0.05	0.98	1.16	0.34	0.89	0.51	0.16	0.86
٢. يقوم مجلس الإدارة / الإدارة التنفيذية بالرقابة على مخاطر أمن المعلومات	4.05	0.78	7.95	0.24	5.75	0.06	0.62	0.74	1.57	0.17	5.14	0.01
٣. يعد أمن المعلومات من الموضوعات الهامة المدرجة بصفة منتظمة ومستمرة على جدول أعمال مجلس الإدارة	13.52	0.06	6.93	0.33	0.32	0.85	2.49	0.03	1.09	0.38	0.73	0.49
٤. تقوم الإدارة العليا والإدارة التنفيذية بمسؤوليتها فيما يتعلق بتطبيق ورقابة والتقرير عن أمن المعلومات	8.37	0.30	5.37	0.50	4.39	0.11	1.34	0.25	0.64	0.70	1.40	0.25
الموارد البشرية / الميزانية والتمويل												
٥. يوجد تمويل كافي و ميزانية مناسبة ومفعّلة لأمن المعلومات	7.01	0.43	2.24	0.90	0.5	0.78	1.16	0.34	0.91	0.50	0.02	0.98
٦. توجد ميزانية لإستراتيجية أمن المعلومات والخطة التكتيكية	11.90	0.10	3.77	0.71	2.81	0.25	2.15	0.05	0.75	0.61	1.11	0.34
المنظمة / العلاقات التنظيمية												
٧. تحديد مسؤوليات الاتصال بالزبون وكذلك مسؤولية الخسارة الناتجة عن الالتزامات المرتبطة باستخدام التكنولوجيا في عمليات الصفقات مع الزبون.	14.70	0.40	3.13	0.79	3.80	0.15	3.09	0.01	0.65	0.69	2.61	0.08
٨. التزام الإدارة العليا فيما يتعلق بمبادرات أمن المعلومات	11.47	0.12	12.81	0.05	3.32	0.19	1.70	0.13	1.63	0.15	1.56	0.22
٩. تأثير وتدخل الإدارة يؤدّي إلى اختيار منتج / خدمة لا يعطي أفضل حل للمشكلة	8.66	028	3.72	0.72	9.52	0.01	1.16	0.34	0.63	0.71	4.79	0.01
١٠. يوجد تناسق وتناغم بين أهداف الشركة وأهداف أمن المعلومات	8.70	0.28	6.02	0.42	0.07	0.97	1.32	0.26	0.87	0.53	0.10	0.90
١١. يوجد تكامل بين أنشطة وعمليات الشركة وأمن المعلومات	15.60	0.30	3.53	0.74	5.59	0.06	2.40	0.03	0.72	0.63	2.79	0.07
١٢. يوجد توصيف واضح للهيكل الإداري بالشركة	12.32	0.90	5.73	0.45	0.23	0.89	1.55	0.17	0.63	0.70	0.09	0.91
١٣. التركيز على الأهداف القصيرة الأجل لمنع مشاكل ضعف أمن المعلومات في الأجل الطويل	3.33	0.85	3.70	0.72	0.25	0.88	0.41	0.89	0.79	0.58	0.02	0.98
١٤. يوجد تعريف واضح لأمن المعلومات مرتبط بشكل ملائم وكافي برؤية وإستراتيجية الشركة.	12.57	0.08	5.75	0.45	1.12	0.57	1.90	0.09	0.97	0.46	0.57	0.57
١٥. أمن المعلومات يحتل المكان المناسب في الهيكل الإداري والتنظيمي للشركة	5.28	0.63	7.85	0.25	0.31	0.86	0.70	0.67	1.15	0.35	0.10	0.90
١٦. تكامل أمن تكنولوجيا المعلومات مع وسائل وترتيبات الأمن التقليدي	9.61	0.21	6.05	0.42	0.01	0.99	1.42	0.21	0.68	0.67	0.08	0.93

التكنولوجيا والعمليات المتعلقة بها												
١٧. يوجد تخطّيط كافي للأمن قبل تطبيق التقنيات الجديدة	5.31	0.62	3.98	0.68	1.05	0.59	0.89	0.52	0.67	0.67	1.29	0.28
١٨. توجد إجراءات ملائمة ومناسبة لإدارة التغيير	11.64	0.11	5.77	0.45	5.92	0.05	1.55	.17	0.94	0.47	2.01	0.14
١٩. القدرة على الاستجابة والرد على عمليات القرصنة والعمليات المتعلقة باختراق النظام واستخدامه بطريقة غير مشروعة.	7.17	0.41	1.13	0.98	0.004	0.99	1.25	0.29	0.37	0.90	0.08	0.93
٢٠. موازنة التوقّعات مع الجدوى الفنية من الحلول الآلية	11.72	0.11	3.27	0.77	1.67	0.43	1.59	0.16	0.41	0.87	1.04	0.36
القوانين / التعليمات / الحوكمة / السياسات والمعايير												
٢١. الالتزام بمتطلبات القوانين القضائية المتعدّدة والمتعلقة بعمليات الشركة	0.64	0.99	10.22	0.12	0.43	0.81	0.09	0.99	1.58	0.17	0.57	0.57
٢٢. تبني القوانين واللوائح والتعليمات الملائمة وغير المتعارضة	5.09	0.65	5.94	0.43	0.63	0.73	0.48	0.85	0.54	0.78	0.30	0.74
٢٣. الالتزام بتنفيذ سياسات ومعايير أمن المعلومات	6.91	0.44	2.71	0.84	0.27	0.87	1.10	0.37	0.44	0.85	0.20	0.82
٢٤. التنفيذ الثابت والمستمر للسياسات والمعايير المتعلقة بأمن المعلومات	11.57	0.12	2.10	0.91	0.12	0.94	1.99	0.07	0.39	0.88	0.22	0.81
آلية المصفوفة الأمنية												
٢٥. وضع إطار لإدارة مخاطر المشروع والذي يتكامل مع أمن المعلومات	6.90	0.44	2.67	0.85	0.08	0.96	1.00	0.44	0.40	0.88	0.25	0.78
٢٦. الاتفاق على منهج عالميا لتقدير وتقييم المخاطر	10.65	0.16	3.67	0.72	0.99	0.61	1.71	0.12	0.55	0.77	0.50	0.61
٢٧. الاتفاق على آلية لأمن المعلومات مقبولة قبولا عاما طبقا لأفضل الممارسات لأمن المعلومات	7.87	0.34	6.20	0.40	0.22	0.90	1.41	0.22	0.61	0.72	0.16	0.85
٢٨. ربط آليات وتقارير أمن المعلومات مع أهداف واستراتيجيات الشركة	7.75	0.36	4.73	0.85	5.68	0.06	1.08	0.39	0.58	0.75	1.79	0.18
التدريب / التعليم المستمر/ الوعي												
٢٩. توافر الأشخاص المدرّبين ذوي الخبرة المهنية في مجال أمن المعلومات	9.13	0.24	6.14	0.41	0.19	0.91	1.42	0.22	0.90	0.50	0.12	0.89
٣٠. تفهم الإدارة للقضايا والموضوعات المتعلقة بأمن المعلومات	13.22	0.07	3.98	0.68	0.41	0.81	1.93	0.08	0.59	0.74	0.21	0.81
٣١. تعليم الموظفين، وتحديث تعليمهم ومعلوماتهم فيما يختص بحماية المعلومات	11.37	0.12	0.70	.99	0.07	0.97	2.12	0.06	0.23	0.97	0.02	0.99
٣٢. الوعي المستمر لأمن المعلومات	11.50	0.12	9.21	0.16	0.56	0.76	1.83	0.10	1.07	0.39	0.36	0.70
٣٣. معرفة الأنظمة الرسمية للتقرير عن الحوادث والجرائم المتعلقة بأمن المعلومات	15.13	0.03	4.53	0.61	0.64	0.73	2.14	0.05	0.55	0.77	0.41	0.67
٣٤. إحداث التوازن بين توقّعات المستخدم وما يمكن تحقيقه عمليا وتقنيا	11.59	0.12	1.41	0.97	0.46	0.79	1.74	0.12	0.22	097	0.36	0.70
٣٥. التعليم الوثيق الصلة بعمل خبراء أمن المعلومات، مثل التعليم المهني المستمر	24.05	0.001	1.06	0.98	1.08	0.58	4.03	0.00	0.16	0.99	1.24	0.30

جدول رقم (٥) نتائج اختبارات الفروض الإحصائية لعوامل نجاح برامج أمن نظم المعلومات المحاسبية

الفروض الإحصائية	الفروض الإحصائية الفرعية	نتائج الفروض الإحصائية	الاستثناءات
الفرض الأول: لا توجد اختلافات جوهرية بين المنشآت السعودية في القطاعات الاقتصادية المختلفة فيما يتعلق بمدى إدراكها لعوامل النجاح الهامة لبرامج أمن نظم المعلومات المحاسبية.	العوامل الثقافية	قبول الفرض الإحصائي	• اعتبار أمن المعلومات من الموضوعات الهامة التي تدرج بصفة منتظمة ومستمرة على قائمة جدول أعمال مجالس الإدارات
	الموارد البشرية / الميزانية والتمويل	قبول الفرض الإحصائي	• لا توجد استثناءات
	المنظمة / العلاقات التنظيمية	قبول الفرض الإحصائي	• وجود تكامل بين أنشطة وعمليات الشركة وأمن المعلومات
	التكنولوجيا والعمليات المتعلقة بها	قبول الفرض الإحصائي	• لا توجد استثناءات
	القوانين / التعليمات / الحوكمة / السياسات والمعايير	قبول الفرض الإحصائي	• التنفيذ الثابت والمستمر للسياسات والمعايير المتعلقة بأمن المعلومات
	آلية المصفوفة الأمنية	قبول الفرض الإحصائي	• لا توجد استثناءات
	التدريب / التعليم المستمر/ الوعي	قبول الفرض الإحصائي	• التعليم المهني المستمر الوثيق الصلة بعمل خبراء أمن المعلومات • معرفة الأنظمة الرسمية للتقرير عن الحوادث والجرائم المتعلقة بأمن المعلومات
الفرض الثاني: لا توجد اختلافات جوهرية بين إدراك الوظائف المختلفة داخل المنشآت السعودية فيما يتعلق بعوامل النجاح الهامة لبرامج أمن نظم المعلومات المحاسبية.	العوامل الثقافية	قبول الفرض الإحصائي	• لا توجد استثناءات
	الموارد البشرية / الميزانية والتمويل	قبول الفرض الإحصائي	• لا توجد استثناءات
	المنظمة / العلاقات التنظيمية	قبول الفرض الإحصائي	• التزام الإدارات العليا بمبادرات أمن المعلومات
	التكنولوجيا والعمليات المتعلقة بها	قبول الفرض الإحصائي	• لا توجد استثناءات
	القوانين / التعليمات / الحوكمة / السياسات والمعايير	قبول الفرض الإحصائي	• لا توجد استثناءات
	آلية المصفوفة الأمنية	قبول الفرض الإحصائي	• لا توجد استثناءات
	التدريب / التعليم المستمر/ الوعي	قبول الفرض الإحصائي	• لا توجد استثناءات
الفرض الثالث: لا توجد اختلافات جوهرية بين المنشآت السعودية التي تستخدم نظماً محاسبية مختلفة فيما يتعلق بمدى إدراكها لعوامل النجاح الهامة لبرامج أمن نظم المعلومات المحاسبية	العوامل الثقافية	قبول الفرض الإحصائي	• قيام مجالس الإدارات والإدارات التنفيذية بالرقابة على مخاطر أمن المعلومات
	الموارد البشرية / الميزانية والتمويل	قبول الفرض الإحصائي	• يوجد تمويل كافي و ميزانية مناسبة ومفعّلة لأمن المعلومات
	المنظمة / العلاقات التنظيمية	قبول الفرض الإحصائي	• تدخل الإدارة في اختيار المنتج أو الخدمة لا يعطي أفضل الحلول الممكنة لمشاكل أمن المعلومات • مدى التزام الإدارات العليا بمبادرات أمن المعلومات • وجود تكامل بين أنشطة وعمليات الشركة وأمن المعلومات
	التكنولوجيا والعمليات المتعلقة بها	قبول الفرض الإحصائي	• وجود إجراءات ملائمة ومناسبة لإدارة التغيير
	القوانين / التعليمات / الحوكمة / السياسات والمعايير	قبول الفرض الإحصائي	• لا توجد استثناءات
	آلية المصفوفة الأمنية	قبول الفرض الإحصائي	• لا توجد استثناءات
	التدريب / التعليم المستمر/ الوعي	قبول الفرض الإحصائي	• لا توجد استثناءات

ولقد تم تحديد عوامل نجاح برامج أمن نظم المعلومات المحاسبية تحت سبعة عوامل رئيسية تتمثل في: العوامل الثقافية؛ الموارد البشرية/ الميزانية والتمويل؛ المنظمة/ العلاقات التنظيمية؛ التكنولوجيا والعمليات المتعلقة بها؛ القوانين/ التعليمات/ الحوكمة/ السياسات؛ آلية المصفوفة الأمنية؛ والتدريب/ التعليم المستمر/ الوعي، ولقد تم عرض تلك العوامل والمتغيرات الفرعية المكونة لكل عامل في الإطار المقترح واختبارها ميدانيا على عينة عشوائية من المنشآت السعودية من مختلف أنواع النشاطات والقطاعات من عدة مدن مختلفة في المملكة العربية السعودية. ولقد أشارت نتائج الدراسة الميدانية إلى أهمية تلك العوامل ودورها الفعال في تعزيز وتفعيل حوكمة الشركات في المنشآت السعودية. ولقد أظهرت نتائج الدراسة أن البنوك والمنشآت المالية و شركات التأمين قد أولت اهتماماً كبيراً لعوامل نجاح برامج أمن نظم المعلومات المحاسبية مقارنة بغيرها من المنشآت. كما أن مديري الشركات ومراجعي نظم المعلومات الإلكترونية والمراجعين الداخليين قد اظهروا اهتماماً أكبر لأهمية عوامل نجاح برامج أمن نظم المعلومات المحاسبية ودورها في تعزيز وتفعيل حوكمة الشركات مقارنة بالوظائف الأخرى في عينة الدراسة. ولقد أوصت الدراسة بضرورة أخذ هذه العوامل في الحسبان وحث الإدارة العليا والمستويات الإدارية الأخرى بالمنشأة وكل العاملين بها على تبنى هذه العوامل وجعلها جزء من ثقافة العاملين بالمنشأة. وحث إدارة المنشآت على البحث المستمر عن عوامل أخرى لضمان نجاح برامج أمن نظم المعلومات كلما تغيرت بيئة الأعمال والظروف الاقتصادية والاجتماعية المحلية والعالمية.

قائمة المراجع

مراجع عربية

أحمد عبد السلام أبو موسى (٢٠٠٤)، "أهمية مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة ميدانية على المنشآت السعودية"، ***الإدارة العامة***، معهد الإدارة العامة، الرياض– المملكة العربية السعودية، المجلد الرابع والأربعون، العدد الثالث، ص ص ٥٠٩ – ٥٧٠.

أحمد عبد السلام أبو موسى (٢٠٠٥)،""الربط بين حوكمة تكنولوجيا المعلومات وتفعيل حوكمة الشركات: نموذج مقترح من سياق المحاسبة الإدارية"، ***مجلة التجارة والتمويل***، المجلة العلمية لكلية التجارة – جامعة طنطا، المجلد الأول للعدد الثاني، ص ص ٥٥– ١١٨.

سمير رياض هلال (١٩٩٢)، "محددات إعادة استخدام البرامج في نظم المعلومات المحاسبية: حالة عملية في الوحدات الحكومية بدولة الإمارات العربية"، ***مجلة التجارة والتمويل***، المجلة العلمية لكلية التجارة – جامعة طنطا، العدد الملحق الأول للعدد الثاني، ص ص٤٩–٧٤.

مراجع أجنبية

Abu-Musa, A. A. (2003) “The Perceived Threats to the Security of Computerized Accounting Information Systems”, ***The Journal of American Academy of Business, Cambridge, USA***, Vol. 3, No.1, September, pp. 9- 20.

Abu-Musa, Ahmad A. (2007) “Exploring Information Technology Governance (ITG) in Developing Countries: AN Empirical Study” ***The International Journal of Digital Accounting Research***, Vol. 7, Iss.13, pp. 71- 117.

Abu-Musa, Ahmad A. (2009 a) “Exploring the Importance and Implementation of COBIT Processes in Developing Countries: An Empirical Study”, ***Information Management & Computer Security***, Bradford, Vol. 17, No. 2, pp. 73-95..

Abu-Musa, Ahmad A. (2009 b) “Exploring COBIT Processes for ITG in Saudi Organizations: An Empirical Study”, ***The International Journal of Digital Accounting Research***, Vol. 9, Iss.15, pp.99 - 126.

Chang, Shuchih Ernest and Chienta Bruce Ho (2006) "Organizational Factors to the Effectiveness of Implementing Information Security Management ", ***Industrial Management & Data Systems***, vol. 106, No. 3, PP. 345- 361.

Chang, Shuchih Ernest and Chin-Shien Lin (2007) "Exploring Organizational Culture for Information Security Management ", ***Industrial Management & Data Systems***, vol. 107, No. 3, PP. 438-458.

Gerber, Mariana and Rossouw Van Solms (2008) "Information Security Requirements- Interpreting the Legal Aspects ", ***Computers & Security***, Oct., Vol. 27, PP. 124- 125.

Davis, C. E. (1996) “Perceived Security Threats to Today’s Accounting Information Systems: A Survey of CISAs”, ***IS Audit & Control Journal,*** (Vol. 3), pp. 38 - 41.

Davis, C. E. (1997) “An Assessment of Accounting Information Security”, ***The CPA Journal,*** New York (Vol. 67, Iss. 3), pp. 28 - 34.

FFIEC (1996) ***IS Examination Handbook, Chapter, 14, Security- Physical And Data.***

Haugen S. and J. R. Selin (1999) “Identifying and Controlling Computer Crime and Employee Fraud”, ***Industrial Management and Data Systems,*** (Vol. 99, Iss. 8).

Henry, Laurie (1997), “A Study of the Nature and Security of Accounting Information Systems: The Case of Hampton Roads, Virginia”, ***The Mid-Atlantic Journal of Business,*** (Vol. 33, Iss. 63), pp. 171 - 189.

ISACA (2005) "Critical Elements of Information Success", ***Information Systems Audit and Control Association.***

ISACA (2008) "Model Curriculum for Information Security Management", ***Information Systems Audit and Control Association.***

Jenster, P. V. (1987) "Organization Performance and Monitoring of Critical Success Factors in Strategic Contexts", ***Journal of Management Information Systems***, Vol. 3, No. 3, PP. 17-33.

Kokolakis, S.A.; A.J. Demopoulos and E.A. Kiountouzis (2000) "The Use of Business Modelling in Information Systems Security Analysis and Design", ***Information Management & Computer Security***, vol. 8, Iss. 3, PP. 107-110.

Loch, K. D., Houston H. C. and M. E. Warkentin (1992) "Threats to Information Systems: Today's Reality, Yesterday's Understanding", ***MIS Quarterly,*** (June), pp. 173 - 186.

McFadzean, Elspeth; Jean-Noel Ezingeard and David Birchall (2007) "Perception of Risk and the Strategic Impact of Existing IT on Information Security Strategy at Board Level ", ***Online Information Review***, vol. 31, No. 5, PP. 622- 660.

OECD (Organization for Economic Co-operation and Development) (1992) ***Guidelines for the Security of Information Systems***, The Council of the OECD, 26 November.

Rotvold, Glenda (2008) "How to Create a Security Culture in your Organization" , ***Information Management Journal***, Nov/ Dec, PP. 32- 38.

Schweitzer, J. A. (1987) ***Computers, Business, and Security,*** Butterworth Publishers, London.

Shah, Mahmood Hussain; Ashley Braganza and Vincenzo Morabito (2007), "A Survey of Critical Success factors in E-Banking an Organizational Perspective" , ***European Journal of Information Systems***, PP. 511- 524.

Tang, Lenn (2008) "The Implementation of Deming's System Model to Improve Security Management: A Case Study ", ***International Journal of Management,*** March, PP. 54- 68.

Tondel, Inger Anne; Mortin Gilje Jaatun and Per Hakon Meland (2008) "Security Requirements for the Rest of Us: A Survey", ***IEEE Software***, January/ February, PP. 20- 27.

ملاحق البحث

(ملحق ١: استمارة الاستقصاء)

جمهورية مصر العربية
وزارة التعليم العالي
جامعة طنطا
كلية التجارة – قسم المحاسبة

Arab Republic of Egypt
Ministry Of Higher Education
Tanta University
Accounting Department

عوامل نجاح برامج أمن نظم المعلومات المحاسبية ودورها في تفعيل حوكمة الشركات: دراسة ميدانية على السعودية

الأستاذ الفاضل/ الأستاذة الفاضلة/

أحيطكم علماً بأننا نقوم بدراسة استكشافية للتعرف على أهم عوامل نجاح أو فشل برامج أمن نظم المعلومات المحاسبية في الشركات السعودية. برجاء التكرم بالإجابة على أسئلة الاستبيان المرفق، ويتعهد الباحثان بأن إجابتكم علي أسئلة الاستبيان سوف تظل سرية ولن تستخدم إلا في أغراض هذا البحث العلمي. ونظراً لأن إجاباتكم سوف تكون على قدر عالٍ من الأهمية بالنسبة لهذا البحث، لذا نرجو التكرم بمراعاة الدقة في استيفاء بيانات هذا الاستبيان. ونشكر لكم مشاركتكم وحسن تعاونكم معنا.

الباحثان

دكتور / أحمد أبوموسى — **أستاذ مساعد**

دكتور / محمد خطاب — **مدرس**

قسم المحاسبة – كلية التجارة – جامعة طنطا

Email: ahmadabumusa@gmail.com

معلومات عامة

من فضلك ضع علامة " √" على المربع الذي تختاره لكل سؤال على حدة

١- هل تعمل حالياً في:-

❐ منشأة صناعية	❐ منشأة تجارية
❐ بنك	❐ منشأة خدمية
❐ شركة تأمين	❐ وحدة حكومية
❐ منشأة صحية	❐ أخرى. من فضلك حددها.....

٢- كم عدد المحاسبين الذين يعملون حالياً بالمنشأة؟

❐ ١ - ٥	❐ ٦ - ١٠
❐ ١١ - ١٥	❐ ١٦ - ٢٠
❐ أكثر من٢٠	

٣- كم عدد المتخصصين في نظم المعلومات الذين يعملون حالياً بالمنشأة؟

❐ ١ - ٥	❐ ٦ - ١٠
❐ ١١ - ١٥	❐ ١٦ - ٢٠
❐ أكثر من٢٠	

٤- ما هو المسمى الوظيفي لعملك الحالي بالمنشأة؟

❐ محاسب مالي	❐ مراجع لنظم المعلومات الإلكترونية
❐ مراجع داخلي	❐ رئيس قسم
❐ محاسب تكاليف	❐ مدير عام
❐ مراقب عام	

٥- كم عدد سنوات الخبرة التي قضيتها في مزاولة عملك الحالي؟

❐ أقل من سنة	❐ أكثر من ١٠ سنوات - و أقل من ١٥ سنوات
❐ أكثر من سنة - و أقل من ٥ سنوات	❐ أكثر من ١٥ سنوات - و أقل من ٢٠ سنة
❐ أكثر من ٥ سنوات - و أقل من ١٠ سنوات	❐ أكثر من ٢٠ سنة

٦- النظام المحاسبي في المنشأة التي تعمل فيها:

❐ يدوى لا يستخدم الحاسبات الآلية

❐ خليط من العمل اليدوي، والتشغيل الإلكتروني بالكمبيوتر

❐ يعتمد بدرجة كبيرة على الكمبيوتر (شديد الآلية)

عوامل نجاح برامج أمن نظم المعلومات المحاسبية

من فضلك ضع علامة " √" على المربع المناسب الذي تختاره لكل سؤال على حدة.

عوامل نجاح برامج أمن نظم المعلومات المحاسبية	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
العوامل الثقافية					
١. اعتقاد مجلس الإدارة / الإدارة التنفيذية بأهمية وأولوية أمن المعلومات					
٢. يقوم مجلس الإدارة / الإدارة التنفيذية بالرقابة على مخاطر أمن المعلومات					
٣. يعد أمن المعلومات من الموضوعات الهامة المدرجة بصفة منتظمة ومستمرة على جدول أعمال مجلس الإدارة					
٤. تقوم الإدارة العليا والإدارة التنفيذية بمسؤوليتها فيما يتعلق بتطبيق ورقابة والتقرير عن أمن المعلومات					
الموارد البشرية / الميزانية والتمويل					
٥. يوجد تمويل كافي و ميزانية مناسبة ومفعّلة لأمن المعلومات					
٦. توجد ميزانية لأمن المعلومات الإستراتيجية وتنفيذ الخطة التكتيكية					
المنظمة / العلاقات التنظيمية					
٧. تحديد مسؤوليات الاتصال بالزبون وكذلك مسؤولية الخسارة الناتجة عن الالتزامات المرتبطة باستخدام التكنولوجيا في عمليات الصفقات مع الزبون.					
٨. التزام الإدارة العليا فيما يتعلق بمبادرات أمن المعلومات					
٩. تأثير وتدخل الإدارة يؤدّي إلى اختيار منتج / خدمة لا يعطي أفضل حل للمشكلة					
١٠. يوجد تناسق وتناغم بين أهداف الشركة وأهداف أمن المعلومات					
١١. يوجد تكامل بين أنشطة وعمليات الشركة وأمن المعلومات					
١٢. يوجد توصيف واضح للهيكل الإداري بالشركة					
١٣. التركيز على الأهداف القصيرة الأجل لمنع مشاكل ضعف أمن المعلومات في الأجل الطويل					
١٤. يوجد تعريف واضح لأمن المعلومات مرتبط بشكل ملائم وكافي برؤية واستراتيجية الشركة.					
١٥. أمن المعلومات يحتل المكان المناسب في الهيكل الإداري و التنظيمي للشركة					
١٦. تكامل أمن تكنولوجيا المعلومات مع وسائل وترتيبات الأمن التقليدي					
التكنولوجيا والعمليات المتعلقة بها					
١٧. يوجد تخطّيط كافي للأمن قبل تطبيق التقنيات الجديدة					
١٨. توجد إجراءات ملائمة ومناسبة لإدارة التغيير					

عوامل نجاح برامج أمن نظم المعلومات المحاسبية	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
١٩. القدرة على الاستجابة والرد على عمليات القرصنة والعمليات المتعلقة باختراق النظام واستخدامه بطريقة غير مشروعة.					
٢٠. موازنة التوقّعات مع الجدوى الفنية من الحلول الآلية					
القوانين / التعليمات / الحوكمة / السياسات والمعايير					
٢١. الالتزام بمتطلبات القوانين القضائية المتعدّدة والمتعلقة بعمليات الشركة					
٢٢. تبني القوانين واللوائح والتعليمات الملائمة وغير المتعارضة					
٢٣. الالتزام بتنفيذ سياسات ومعايير أمن المعلومات					
٢٤. التنفيذ الثابت والمستمر للسياسات والمعايير المتعلقة بأمن المعلومات					
آلية المصفوفة الأمنية					
٢٥. وضع إطار لإدارة مخاطر المشروع والذي يتكامل مع أمن المعلومات					
٢٦. الاتفاق على منهج عالميا لتقدير وتقييم المخاطر					
٢٧. الاتفاق على آلية لأمن المعلومات مقبولة قبولا عاما طبقا لأفضل الممارسات لأمن المعلومات					
٢٨. ربط آليات وتقارير أمن المعلومات مع أهداف وإستراتيجيات الشركة					
التدريب / التعليم المستمر/ الوعي					
٢٩. توافر الأشخاص المدرّبين ذوي الخبرة المهنية في مجال أمن المعلومات					
٣٠. تفهم الإدارة للقضايا والموضوعات المتعلقة بأمن المعلومات					
٣١. تعليم الموظفين، وتحديث تعليمهم ومعلوماتهم فيما يختص بحماية المعلومات					
٣٢. الوعي المستمر لأمن المعلومات					
٣٣. معرفة الأنظمة الرسمية للتقرير عن الحوادث والجرائم المتعلقة بأمن المعلومات					
٣٤. إحداث التوازن بين توقّعات المستخدم وما يمكن تحقيقه عمليا وتقنيا					
٣٥. التعليم الوثيق الصلة بعمل خبراء أمن المعلومات، مثل التعليم المهني المستمر					