مجلة التجارة والتمويل

https://caf.journals.ekb.eg/

كلية التجارة – جامعة طنطا

العدد : الرابع

ديسمبر ٢٠٢١

حوكمة تكنولوجيا المعلومات كمدخل لحماية أمن معلومات الشركات وأثرها على الأداء المالي وغير المالي: دليل من الشركات المصرية

أ.د/ فايزة عبيد الله

أستاذ دكتور بكلية التجارة جامعة دمنهور

fo_user22@yahoo.com

د/ محمد جمعة حراز

دكتور بكلية التجارة جامعة دمنهور

m.haraz424@gmail.com

أماني محمد طلعت حامد إسماعيل

حاصلة على ماجستير محاسبة ومراجعة

AIsmail2021@com.dmu.edu.eg

حوكمة تكنولوجيا المعلومات كمدخل لحماية أمن معلومات الشركات وأثرها على الأداء المالي وغير المالي:
دليل من الشركات المصرية

ملخص:

يهدف هذا البحث إلى دراسة أثر حوكمة تكنولوجيا المعلومات كمدخل لحماية أمن المعلومات على الأداء المالي وغير المالي للشركات في بيئة الأعمال المصرية، من خلال تحليل أثر حوكمة تكنولوجيا المعلومات على تحقيق حماية أمن معلومات الشركات باستخدام إطار COBIT 2019 وإصدارات معيار ISO ذات الصلة، ثم دراسة أثر تطبيق آليات حوكمة تكنولوجيا المعلومات على تحسين الأداء المالي والأداء غير المالي، وكذلك تحليل الأثر الواقع على الأداء المالي وغير المالي للشركات في ظل توافر الحماية الكافية للمعلومات المحاسبية والتي تقدمه أمن المعلومات جراء تطبيق حوكمة تكنولوجيا المعلومات للشركات العاملة بالبيئة المصرية، كما يقدم البحث دليل ميداني يشمل العديد من الشركات العاملة بمجال تكنولوجيا المعلومات كشركات الاتصالات وشركات تكنولوجيا المعلومات، والمؤسسات المالية كالبنوك والاستثمار في تداول الأوراق المالية، والشركات الخدمية كشركات التسويق الإلكتروني العاملة في البيئة المصرية، حيث تم تجميع البيانات اللازمة لاختبار فروض الدراسة باستخدام قائمة الاستبيان والتي تم تحليلها بالاستعانة بالبرنامج الإحصائي SPSS، وتم استخدام العديد من الاختبارات الإحصائية المعلمية واللامعلمية لاختبار الفروض.

وقد توصل البحث إلى العديد من النتائج أهمها أن حوكمة تكنولوجيا المعلومات كأحد مداخل أمن المعلومات لها تأثير جوهري وإيجابي على تحسين الأداء المالي وغير المالي للشركات العاملة في البيئة المصرية، ومن ثم كانت أهم توصيات البحث هي ضرورة اهتمام الشركات بتطبيق حوكمة تكنولوجيا المعلومات واعتبارها من العناصر المهمة في الخطط الاستراتيجية للشركات، والاهتمام بوضع موازنة تُمكن الشركات من مواكبة التحديثات المتلاحقة في التكنولوجيا الحديثة، وكذلك عقد دورات تدريبية لتعريف الكوادر البشرية بالأطر والمعايير الدولية في مجال أمن المعلومات.

Abstract

This paper aims to investigate the impact of information security that results from applying information technology governance on the financial and non-financial performance in Egyptian business environment. This paper analyzes the impact of information technology governance on achieving information security protection in companies using the COBIT 2019 framework and related ISO standards versions. As well as, it illustrates the information technology governance mechanisms and its impact to improve the financial and non-financial performance. Finally, this paper analyzes the impact of protecting accounting information that provided by information security, as a result of information technology governance, on the financial and non-financial performance in the Egyptian business environment.

This paper also provided a field study that included many companies working in the information technology such as telecommunications companies and information technology companies, financial institutions such as banks and investment in securities trading, and service companies such as electronic marketing companies operating in the Egyptian environment. The questionnaire is used to collect the necessary data to test the hypotheses. The SPSS statistical program is used with many parametric and non-parametric statistical tests to test the hypotheses.

This study has many results; the most important is that information technology governance as an approach of information security has a significant and positive impact on improving the financial and non-financial performance in the Egyptian business environment.

This study recommends the companies' management to pay attention to information technology governance as a strategic plans, to set a compatible budget to keep pace with the updates of modern technology, and to give the training courses about international frameworks and standards in information security field more attention.

Keywords: IT governance, information security, financial & non-financial performance, COBIT 2019 framework, ISO standard, Egypt.

١ – مقدمة:

احتلت التكنولوجيا الحديثة أهمية كبيرة في جميع مناحي الحياة، فقد ساهمت بصورة هائلة في تطور العلوم الاقتصادية والسياسية والاجتماعية، حيث جعلت العالم يبدو مختلفاً عن العصور الماضية، وحتما ستجعل من عالم الغد مغايراً عما هو عليه اليوم، وتعتبر تكنولوجيا المعلومات وسيلة لإتمام العديد من المهام التي تتضمن نقل المعلومات والتي تساهم في صناعة القرارات داخل الوحدات الاقتصادية المختلفة، وكذلك تحسين الخدمات المقدمة لأصحاب المصلحة سواء أكانوا متعاملين خارجيين أو داخليين على حد سواء، كما أن التحول الحتمي لبيئة الأعمال التكنولوجية الرقمية أدى إلى ضرورة تنفيذ آليات حوكمة تكنولوجيا المعلومات في الشركات على اختلاف نشاطاتها والتي تتطلب ضرورة تطبيق حوكمة تكنولوجيا المعلومات التي تتضمن القوانين والقواعد والاجراءات التي تحكم الجوانب الاستراتيجية والمؤسسية للمنظمة فيما يخص تكنولوجيا المعلومات.

وقد شهدت الشركات المالية في السنوات الأخيرة ارتفاعًا كبيرًا في عدد الجرائم الإلكترونية كالتزييف والخداع الاحتيالي في متصفحات الإنترنت وسرقة المعلومات المالية الشخصية من خلال اختراق الأجهزة المحمولة التي تؤدي لخسائر فادحة في الشركات على كافة أنواعها، نتيجة لذلك كان ولابد من تفعيل الأطر والمعايير التي تؤدي لحماية أمن المعلومات والتي تؤثر بدورها على الأداء المالي من حيث معدل الربحية ومعدل العائد على الأصول ومعدل العائد على الاستثمار، وكذلك على الأداء غير المالي من حيث المسئولية الاجتماعية والاستدامة، وتحقيق الأهداف الاستراتيجية التي تؤثر على الميزة التنافسية للشركات، وبناء علاقات وطيدة مع أصحاب المصالح، ومن ثم تحقيق التكامل بين الأداء المالي وغير المالي للشركات.

١-١: مشكلة البحث:

يعد الاعتماد على التكنولوجيا كمصدر من مصادر المعلومات عند اتخاذ القرارات أمراً حتمياً ولا غنى عنها في الوقت الحالي، ولحماية أمن المعلومات الناتجة عن هذه التكنولوجيا كان لزاما تطبيق آليات حوكمة تكنولوجيا المعلومات، الأمر الذى قد يترتب عليه تحسين في الأداء المالي للشركات من خلال تحقيق مستوى أمثل للربحية، والوصول لأعلى درجة من الكفاءة الاستثمارية وزيادة حجم الأعمال، فضلاً عن تحسين الأداء غير المالي من خلال جذب عملاء جدد وتحقيق أهداف الاستمرارية والاستدامة. وعلى ذلك، يمكن صياغة مشكلة البحث في الأسئلة الآتية:

١. ما هو الدور الذى تقدمه حوكمة تكنولوجيا المعلومات في تحقيق حماية أمن المعلومات في الشركات باستخدام إطار COBIT 2019، وإصدارات معيار ISO ذات الصلة؟
٢. كيف يؤثر تطبيق آليات حوكمة تكنولوجيا المعلومات على تحسين الأداء المالي والأداء غير المالي للشركات؟
٣. ما هو الأثر الواقع على الأداء المالي وغير المالي للشركات في ظل توافر الحماية الكافية للمعلومات المحاسبية والتي تقدمه أمن المعلومات جراء تطبيق حوكمة تكنولوجيا المعلومات؟

١-٢: أهمية البحث:

تتمثل **الأهمية العلمية** للبحث في وصف وتحليل أثر تطبيق حوكمة تكنولوجيا المعلومات كمدخل لحماية أمن المعلومات على الأداء المالي وغير المالي للشركات، والذي يتمثل في مدى زيادة الربحية وتحقيق الكفاءة الاستثمارية وخلق ميزة تنافسية للشركات في بيئة الأعمال المصرية عند تطبيق آليات حوكمة تكنولوجيا المعلومات كمدخل لحماية أمن المعلومات. **أما الأهمية العملية** لهذا البحث فتتمثل فيما يقدمه للقائمين على إدارة تكنولوجيا المعلومات من دليل عملي على أهمية تطبيق أطر ومعايير دولية منظمة لأمن المعلومات كإطار COBIT ومعايير ISO/IEC-27001 والتي يمكن تطبيقها في الشركات على اختلاف أحجامها وأنشطتها. وكذلك يقدم البحث الآليات التي تعمل على حماية أمن المعلومات _بصفة عامة والمعلومات المحاسبية بصفة خاصة_ ضمن إطار حوكمة تكنولوجيا المعلومات بما يحسن الأداء المالي وغير المالي للشركات. كما يوجه هذا البحث القائمين على إدارة تكنولوجيا المعلومات لوضع موازنة تُمكن الشركات من مواكبة التحديثات المتلاحقة في التكنولوجيا الحديثة، وكذلك يقدم توعية للإدارة العليا بالشركات نحو أهمية توفير كوادر بشرية مدربة لتحديث برامج حماية البيانات والمعلومات من القرصنة والاستخدام غير المصرح به لمعلومات الشركات.

١-٣: منهجية البحث:

يعتمد البحث على المنهج الاستنباطي Deductive Approach والمنهج التحليلي في جانبه النظري حيث تم مسح أهم المصادر العلمية التي تناولت موضوع البحث بهدف التوصل لمدى تأثير حوكمة تكنولوجيا المعلومات كمصدر من مصادر توفير أمن المعلومات على الأداء المالي وغير المالي للشركات. أما الجانب التطبيقي للبحث، فتم الاعتماد على المنهج الوصفي والمنهج الاستقرائي Inductive Approach، حيث أُجريت دراسة ميدانية عن طريق تصميم قائمة استبيان لاختبار صحة فروض البحث، وتحليل وتفسير تلك البيانات من أجل التوصّل إلى نتائج توضح العلاقات بين متغيرات الدراسة.

١-٤: هدف البحث:

يتمثل **الهدف الرئيسي** لهذا البحث في **دراسة واختبار** أثر تطبيق حوكمة تكنولوجيا المعلومات كمدخل لحماية أمن المعلومات على الأداء المالي وغير المالي للشركات، وذلك في عينة من الشركات في بيئة الأعمال المصرية عن طريق اتباع مدخل ميداني تجريبي موثق بطريقة علمية.

١-٥: حدود البحث:

يقتصر البحث على اختبار أثر تطبيق حوكمة تكنولوجيا المعلومات كمدخل لحماية أمن المعلومات على الأداء المالي وغير المالي للشركات العاملة بمجال تكنولوجيا المعلومات وشركات الاتصالات، والشركات الخدمية كشركات التسويق الإلكتروني، والمؤسسات المالية كالبنوك وشركات الاستثمار في الأوراق المالية دون غيرها من الشركات. وتم إجراء دراسة ميدانية من خلال عينة من المديرين الماليين ومسئولي إدارة المخاطر وخبراء تكنولوجيا المعلومات والحوكمة بالمؤسسات المصرية المحددة سابقاً. كما تم استخدام إطار COBIT 2019، ومعيار الـ ISO/IEC-27001 كأطر لحماية أمن المعلومات، ومما لاشك فيه أن

تعميم نتائج البحث مشروط بضوابط اختيار عينات البحث والتي تقتصر على القدر الذى يفي بتحقيق الغرض من الموضوع محل الدراسة.

١-٦: خطة البحث:

ينقسم البحث إلى تسع أجزاء، يتضمن الجزء الأول المقدمة السابق عرضها، ويستعرض الجزء الثاني ماهية حوكمة تكنولوجيا المعلومات من حيث تعريفها وأهميتها وأهداف تطبيقها والمبادئ التي تستند إليها وعوامل نجاحها ومن ثم إلقاء الضوء على العديد من العوامل الهامة التي تؤدي لتحقيق فعالية حوكمة تكنولوجيا المعلومات في بيئة الأعمال المصرية والمعوقات التي تواجه تطبيق حوكمة تكنولوجيا المعلومات ثم تناول أدوات تقييم حوكمة تكنولوجيا المعلومات، أما الجزء الثالث فيستعرض آليات حوكمة تكنولوجيا المعلومات والتي تتكون من الآلية الهيكلية Structure والآليات العلاقية Relational وآلية العمليات Processes لحوكمة تكنولوجيا المعلومات، ويتضمن الجزء الرابع ماهية أمن المعلومات والمعايير الدولية التي تنظمه وماهية أمن المعلومات المحاسبية الالكترونية وإطار COBIT كأحد أطر إدارة المخاطر وأمن المعلومات وكذلك المعيار الدولي لإدارة أمن المعلومات (ISO/IEC-27001) وكيفية تحقيق التكامل بين معيار ISO/IEC-27001 وإطار COBIT لتحقيق فعالية حوكمة تكنولوجيا المعلومات، ويوضح الجزء الخامس الدور الذي تقوم به حوكمة تكنولوجيا المعلومات لتحقيق حماية أمن المعلومات، أما الجزء السادس فيتناول دور تطبيق آليات حوكمة تكنولوجيا المعلومات في تحسين الأداء المالي وغير المالي للشركات، ويتناول الجزء السابع أثر حماية أمن المعلومات الناتجة من تطبيق آليات حوكمة تكنولوجيا المعلومات على تحسين الأداء المالي وغير المالي للشركات، كما يستعرض الجزء الثامن الدراسة الميدانية والذي يتضمن تصميم قائمة الاستبيان وتحديد مجتمع وعينة الدراسة والتحليل الوصفي لعينة الدراسة وقياس صدق الاستبيان Validity ثم قياس ثبات الاستبيان Reliability وتوضيح الأساليب الإحصائية المستخدمة لاختبار فروض الدراسة ويتبع ذلك اختبار فروض البحث الثلاثة، وأخيراً يتناول الجزء التاسع الخلاصة والتوصيات.

٢: ماهية حوكمة تكنولوجيا المعلومات:

فرضت التغيرات الجذرية في العالم والظروف الحياتية الآنية اتخاذ مسلكاً جديداً لم يُعرف من قبل، فالثورة التكنولوجية والتقلبات المناخية وظهور العديد من الأوبئة مثل فيروس كورونا المستجد Covid-19 قد فرض على العالم ضرورة الالتزام بتقنين قوانين جديدة واتباع ارشادات مختلفة تستطيع مواكبة والتعايش مع الواقع الحالي لا سيما القوانين التي تحكم تكنولوجيا المعلومات والتي تسمى بحوكمة تكنولوجيا المعلومات، فقد أصبحت حوكمة تكنولوجيا المعلومات من الدعائم الأساسية التي لا غنى عنها لتحقيق أهداف الشركات باختلاف توجهاتها.

وقد قامت العديد من الدراسات السابقة بوضع **تعريفات لحوكمة تكنولوجيا المعلومات**؛ حيث عرفها معهد حوكمة تكنولوجيا المعلومات ITGI (2003) على أنها "عنصر من عناصر حوكمة الشركات، التي تهدف إلى تحسين الإدارة العامة لتكنولوجيا المعلومات والحصول على قيمة محسنة من الاستثمار في المعلومات والتكنولوجيا، حيث

تضع خطة عمل للمهام التي يقوم بها الأشخاص المنوط بهم حوكمة الشركات في تعاملهم مع تكنولوجيا المعلومات المرتبطة بها وكذلك في مراحل الإشراف والتوجيه والرقابة عليها بما يحقق رؤية الشركة وأهدافها الاستراتيجية ". كما عرفت دراسة Soliman and Zaky (2018) حوكمة تكنولوجيا المعلومات بأنها "هي التي تحدد حقوق اتخاذ القرار وإطار المساءلة لتشجيع السلوك المرغوب في استخدام تكنولوجيا المعلومات". وعرفها أكريم (٢٠١٩) بأنها "عملية استخدام مصادر تكنولوجيا المعلومات بفعالية لتحقيق الأهداف التنظيمية".

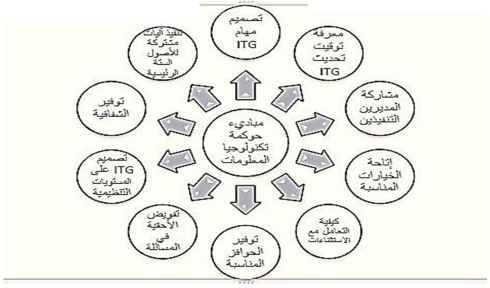
وقد استخلص الباحثون تعريفاً لحوكمة تكنولوجيا المعلومات وهو أنها "جزء أصيل من حوكمة الشركات، التي من خلالها يتم صياغة المبادئ والمعايير والآليات الرقابية ووضع خارطة طريق يجب أن تتبعها إدارات تكنولوجيا المعلومات لتحقيق الأهداف الاستراتيجية للشركة في ضوء التطورات التكنولوجية الحديثة والمتلاحقة بمجال الأعمال، وبما يتفق مع الاستثمارات الموضوعة من قبل الإدارة العليا، ومن ثم توفير نظام جيد لإدارة المخاطر، وتحقيق ميزة تنافسية وخلق قيمة للشركة".

وتكمن أهمية حوكمة تكنولوجيا المعلومات في أنها تعمل على تحديد المخاطر تواجه الشركة، وبالتالي تحدد كيفية إدارة تلك المخاطر وتخفيضها إلى الحد يحقق الاستقرار ويساعد في نجاح الشركة وفتح أسواق جديدة. كما يمكن من خلال حوكمة تكنولوجيا المعلومات متابعة تطبيق القوانين وإحكام الرقابة على إدارة المعلومات بالشركة. ويرجع الاهتمام المتزايد بحوكمة تكنولوجيا المعلومات إلى التكنولوجيا بصفة عامة لخلق الكفاءة وتحسين قيمة الأعمال، فيمكن لهدف ما قد يبدو بسيطًا أن يجعل الاستثمار في التكنولوجيا أحد أهم البنود في الميزانية (Pereira and da Silva, 2012).

ويعتبر تحقيق القدر الكافي من العائد على الاستثمار وزيادة الربحية وزيادة قيمة الشركة وتعزيز قدرتها التنافسية من الأهداف الرئيسية لتطبيق حوكمة تكنولوجيا المعلومات، وتركز أهداف حوكمة تكنولوجيا المعلومات على احتواء التكاليف (بما في ذلك؛ الكفاءة، والتوحيد، والأتمتة Automation) والحد من المخاطر (بما في ذلك؛ الامتثال، والأمن، والتدقيق العام لحماية الفشل في تطبيق تكنولوجيا المعلومات)، علاوة على ذلك تعلمت بعض الشركات كيفية الاستفادة من تكنولوجيا المعلومات في تعزيز الربحية من خلال الاستفادة من الآثار الإيجابية لولاء العملاء، والبيع المتبادل، وخفض التكاليف التسويقية والبيعية، والتي يمكن تعزيزها من خلال إدارة فعالة لتكنولوجيا المعلومات، وبالتالي توفير ربحية أفضل من الشركات الأخرى التي لا تطبقها في صناعاتها (Mithas et al., 2012).

تستند حوكمة تكنولوجيا المعلومات إلى عدة مبادئ، حيث يتطلب تطبيق الحوكمة الفعالة لتكنولوجيا المعلومات الالتزام بالسياسات والإجراءات الواجب اتباعها في مجال تكنولوجيا المعلومات والتى تلبي مبادئ حوكمة تكنولوجيا المعلومات، مثل: الشفافية والمشاركة النشطة وإعادة التصميم المتكرر وإنشاء الحوكمة عند مستويات تنظيمية متعددة ووجود عمليات محددة لمعالجة الاستثناءات ومواءمة أنظمة الحوافز والمكافآت (Sofyani et al., 2020).

ووفقاً لدراسة Weill and Ross (2004) تتكون مبادئ حوكمة تكنولوجيا المعلومات من عشر مبادئ كما هي موضحة بالشكل رقم (١):



الشكل رقم (١): المبادئ العشر لحوكمة تكنولوجيا المعلومات

المصدر: إعداد الباحثون

ولتحقيق فعالية حوكمة تكنولوجيا المعلومات في بيئة الأعمال المصرية فهناك العديد من العوامل الهامة التي يتوقف عليها هذا التطبيق الفعال ومن ثم تحقيق الأهداف الإستراتيجية للشركة وتحقيق مزايا تنافسية يرتبط بالأداء الأمثل لتكنولوجيا المعلومات ، **وهي:** سَّن القوانين والسياسات والإجراءات لحوكمة تكنولوجيا المعلومات والتي تُواءم أوضاعنا الداخلية السياسة والاقتصادية والاجتماعية، لتجعله سهل التطبيق وواقعي، ويكون مرجعاً ومحفزاً للرقابة الداخلية للشركات. وتخصيص الاستثمارات المطلوبة لتوفير البنية التحتية لتكنولوجيا المعلومات، ويعد توفير هذه المخصصات المالية هو التحدي الأكبر في البيئة المصرية. كما يُعتبر الخوف من المساءلة من أهم السلبيات التي تقوِّض أي تقدم في مختلف المجالات، فلابد من وضع مساحة لاتخاذ القرارات من قبل مستخدمي تكنولوجيا المعلومات ولتكن متدرجة علي مستوي الإدارات حتى يتسنى لمتخذي القرارات المضي قدماً ودرء أي معوقات أو تحديات منذ البداية، وتسجيل ذلك للاستفادة منها في سن تشريعات حوكمة تكنولوجيا المعلومات فيما بعد.

ونظراً لأهمية حوكمة تكنولوجيا المعلومات فقد اهتم الباحثون **بأدوات تقييم حوكمة تكنولوجيا المعلومات** باعتبار أن حوكمة تكنولوجيا المعلومات تمثل إطاراً لمساءلة متخذ القرار باستخدام تكنولوجيا المعلومات، بالإضافة إلى أنها تضمن تطابق القرارات المتعلقة بتكنولوجيا المعلومات مع الأهداف الاستراتيجية على مستوى الشركة (Weill and Ross 2004). وقد أعطت دراسة De Haes and Van Grembergen, (2009) مثال على أدوات تقييم حوكمة تكنولوجيا المعلومات وهي بطاقات الأداء المتوازن في تكنولوجيا المعلومات، والتي تمثل عمليات مهمة للشركات التي ترغب في مراقبة وتقييم أدائها مع مواءمة استراتيجيات أعمالها، وفي ذات السياق أشارت دراسة عبيد الله (٢٠٠٥) إلى أن تطبيق نظام القياس المتوازن لتقييم الأداء (Balance Scorecard BSC) له مزايا عديدة حيث يؤدى تطبيقه لخلق قيمة تنافسية وزيادة قيمة الشركة، بالإضافة إلى أنه من أكثر

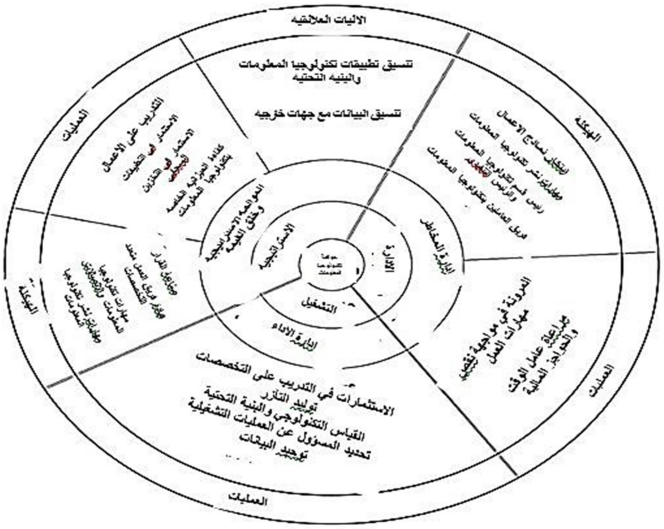
المقاييس التي تساعد على معرفة مدى توافق الاستراتيجيات المطبقة بالشركة مع أهدافها المالية وغير المالية.

٣: آليات حوكمة تكنولوجيا المعلومات:

تقدم تكنولوجيا المعلومات للشركات العديد من الفرص لتحسين منتجاتها وخدماتها وأسواقها وعملياتها وعلاقاتها التجارية وتساعدها في تحقيق أهدافها وزيادة قيمتها السوقية وخلق ميزة تنافسية في الأسواق الحالية مرتفعة الخطر، ولذلك فإن هذه الأنشطة تتطلب تضافر الجهود وتنظيمها بعناية بين المتخصصين في التكنولوجيا والأعمال في الشركة، وكاستجابة لمتطلبات الشركات المختلفة والآخذة إلى اتباع نهجاً أكثر تكيفًا، فقد تطلب تنفيذ حوكمة تكنولوجيا المعلومات استخدام آليات معينة للحفاظ على المواءمة بين وحدات الأعمال وتكنولوجيا المعلومات، هذا يعني وجوب الانتقال من آليات الحوكمة القائمة على الاستقرار والمساءلة، الى آليات الحوكمة التي يجب أن تتوائم مع سياسات وإجراءات حوكمة تكنولوجيا المعلومات (Zuo et al., 2020; Maccani et al., 2020).

يتكون إطار حوكمة تكنولوجيا المعلومات من ثلاثة مجالات وهي؛ المجالات الاستراتيجية والإدارية والتشغيلية، وهذه المجالات الثلاثة لم تأت من فراغ ولكنها تكونت من مجموعة من العناصر المترابطة المُضمَّنة في ثلاث آليات وهي الآليات الهيكلية Structure وآليات العمليات Processes والآليات العلاقية Relationships والتي تضمن أن تكنولوجيا المعلومات في الشركة تدعم وتخدم استراتيجياتها وأهدافها (Wiedenhoft et al., 2017; Tambotoh et al., 2018)

ويلخص الشكل رقم (٢) إطار حوكمة تكنولوجيا المعلومات، ويسلط الضوء على العلاقة بين كل من المجالات والآليات المكونة لإطار حوكمة تكنولوجيا المعلومات ("العجلة").



الشكل رقم (٢): إطار حوكمة تكنولوجيا المعلومات

المصدر بتصرف: [Khalil and Belitski, 2020]

وفيما يلى توضيح للآليات الثلاث لحوكمة تكنولوجيا المعلومات.

٣-١: الآلية الهيكلية لحوكمة تكنولوجيا المعلومات Structure: الآلية الهيكلية كيفية تنظيم وتحديد مكان حوكمة تكنولوجيا المعلومات في الهيكل الهرمي للمؤسسة، وكذلك التعريف الواضح للأدوار والمسؤوليات المنوطة التي يتكون منها هذا الهيكل (De Haes and Van Grembergen, 2009). وتنقسم الآلية الهيكلية لحوكمة تكنولوجيا المعلومات إلى عدة عناصر وهي؛ توزيع الأدوار والمسئوليات لحوكمة تكنولوجيا المعلومات، والهياكل التنظيمية لحوكمة تكنولوجيا المعلومات، واللجان الاستراتيجية لحوكمة تكنولوجيا المعلومات، واللجان التوجيهية لحوكمة تكنولوجيا المعلومات، وتحديد دور مدير قسم تكنولوجيا المعلومات CIO، واللجان التوجيهية للمشروع ككل.

٣-٢: آليات العلاقات التنظيمية لحوكمة تكنولوجيا المعلومات Relational:

تتمثل الآليات العلاقية في التواصل بين مختلف مستويات المديرين والإدارات داخل الشركة Weill and Ross (2004)، أما عن أهمية الآليات العلاقية فقد توصلت دراسة Bermejo et al. (2014) لمزيدٍ من الأدلة فيما يتعلق بتعزيز التوافق بين تكنولوجيا المعلومات والأعمال بما في ذلك الممارسات التي تعزز التآزر بين الإدارة العليا وتكنولوجيا المعلومات والمجالات التنظيمية الأخرى حيث يجب أن تتماشى استراتيجية العمل مع عملية صنع القرار في تكنولوجيا المعلومات، وتناولت دراسة Sjödin et al. (2019) دور استراتيجيات الحوكمة العلاقية والتي اقترحت أربعة شروط لتطبيق حوكمة علاقية فعالة (وهى: ابتكار الخدمة، وتكاليف التحويل المتوقعة، وجاذبية البدائل، والعقود الواضحة) التي يشكل وجودها أو غيابها تأثيراً مباشراً على تحقيق أداء مالي عالي.

٣-٣: آ لية عمليات حوكمة تكنولوجيا ا لمعلومات Processes:

تعرف آلية عمليات حوكمة تكنولوجيا المعلومات بأنها التعامل مع عملية صنع القرار الاستراتيجي، وكيفية التخطيط الاستراتيجي لخدمة عملية الرقابة والتحكم وكيفية إدارة العمليات، والتي تضمن تنفيذ سياسات تكنولوجيا المعلومات في العمليات التنظيمية ومراقبة النتائج، والإفصاح عنها (Weill and Ross, 2004; De Haes and Van Grembergen, 2009; Bradley et al., 2012)، وتتضمن هذه الآلية التخطيط الاستراتيجي للهيكل المعلوماتي للشركة، واقتصاديات المعرفة، واتفاقيات مستوى الخدمة، وتوفير إطار البنية التحتية لتكنولوجيا المعلومات (ITIL).

على الرغم من أن الشركات بدأت في النجاح في تنفيذ آليات حوكمة تكنولوجيا المعلومات الخاصة بها بشكل أفضل، إلا أن آليات الحوكمة وحدها لا يمكن أن تضمن التنفيذ الناجح لسياسات وإجراءات حوكمة تكنولوجيا المعلومات، حيث يجب أن تكون الشركات قادرة على فهم استراتيجيات السوق المعقد وخصائص بيئته التنافسية بشكل أفضل وأن تكون قادرة على تجميع مجموعة موثوقة من التكنولوجيا المنوطة بالحوكمة والتي يمكن مشاركتها وتنفيذها بسهولة من قبل المديرين الذين يتخذون قرارات رئيسية للشركة.

٤: ماهية أمن المعلومات والمعايير الدولية التي تنظمه:

بات عصرنا الحالي معتمداً اعتماداً مباشراً على التكنولوجيا الحديثة، والتي أصبحت من أهم العناصر التي توفر الجهد وتختصر الوقت بشكل فائق، كما أنها أصبحت ضرورة لإتمام التعاملات في بيئة الأعمال التكنولوجية بين الأفراد والشركات بكافة أنواعها وأحجامها، ومع الاعتماد المباشر والمتزايد على تكنولوجيا المعلومات أصبحت قضية أمن المعلومات محل الكثير من الجدل.

٤-١: ماهية أمن المعلومات المحاسبية الالكترونية:

يعد أمن المعلومات المحاسبية الالكترونية جزء من أمن المعلومات الذى يجب أن تهتم به الشركات، وقد عرفت منظمة الأيزو ISO **أمن المعلومات** أنه "حماية المعلومات من مجموعة واسعة من التهديدات من أجل ضمان استمرارية وتقليل مخاطر الأعمال، وزيادة العائد على الاستثمارات وفرص العمل (ISO, 2005). كذلك أوضحت دراسة Whitman and Mattord (2011) أن أمن المعلومات هو "حماية سرية وسلامة وتوافر المعلومات، بما في ذلك البرامج والأجهزة التي تستخدم وطرق تخزين ومعالجة ونقل تلك المعلومات من خلال تطبيق السياسات وتوافر الوعي بالتكنولوجيا مما يؤثر بالإيجاب على أداء الشركة".

وفي عصر يكون فيه الاعتماد على أنظمة المعلومات مرتفعًا بشكل كبير، فإن الحوادث التي قد تتعرض لها المعلومات المالية تعد تهديد خطير لأمن المعلومات، حيث تشير الدراسات المختلفة، مثل دراسات Abu-Musa (2006); Otero (2015); Zaydi and Nassereddine (2019) إلى أن القصور في ممارسات أمن المعلومات والافتقار إلى طرق حماية أمن المعلومات المالية القيمة والحساسة يقود الشركة إلى؛ (١) الاحتيال و/أو التلاعب و/أو إساءة استخدام البيانات، (٢) ظهور عوائق متعلقة بالأمن، (٣) وجود صفقات مزيفة للحصول على أرباح أو لإخفاء الخسائر، (٤) عمل قيود يومية محاسبية غير صحيحة، (٥) انتهاكات أمن الحاسب الآلي، (٦) تزوير المعاملات المالية للتهرب من المسائلة القانونية لمجلس الإدارة.

تعد ثقافة أمن المعلومات المحاسبية في ضوء هذه التطورات التكنولوجية ليست سهلة، فأمن المعلومات كمفهوم شامل يحتوي على؛ أمن الشبكات، وأمن الأجهزة المستخدمة، والأمن التنظيمي والأمن القانوني، كما يجب الأخذ في الاعتبار السياسة الأمنية المطبقة حيث تعتبر بمثابة الغطاء الأمني لجميع الجوانب الأمنية السالف ذكرها، وحتى يتم توفير المتطلبات الأساسية لتحقيق الأمن يجب أن تُبنى على المتطلبات وليس على الاعتبارات الفنية كما يجب أن تكون الأهداف الأساسية لأي سياسة أمنية هي الحفاظ على السرية والنزاهة والكمال وتوافر جميع أصول الثروة المعلوماتية للشركات، كما أنه يجب تحقيق السرية فلا يجب أن تُعرض المعلومات على جميع المتعاملين بل تقتصر على بعض المستخدمين المحددين من قبل، وتشير السلامة والكمال إلى أن بيانات ومعلومات الشركة يجب أن تكون دقيقة وحديثة للغاية وتوفر التكامل والأمان الذي يحمي المعلومات من التعديل غير المصرح به، كما يجب أن تضمن المعلومات الإتاحة والوصول للبيانات الموثوقة متى دعت الحاجة لذلك (Hamdan, 2017).

إلى جانب المخاطر المتعلقة بالتكنولوجيا فيُنظر إلى السلوك البشري على أنه أكبر تهديد لنظام تكنولوجيا المعلومات حيث يتسبب المستخدمون بشكل منتظم في حوادث نظم المعلومات من خلال سلوك المخاطرة المتعمد أو غير المتعمد، مثل خطأ التعامل مع

المعلومات المالية، أو تصفح صفحات الويب والتعامل مع البيانات غير الآمنة (Crossler et al., 2013; Lebek et al., 2014; Siponen and Vance, 2010). ونظراً للتهديدات التى تحيط أمن المعلومات المحاسبية الإلكترونية، فإن الشركات تستثمر جزء كبير من ميزانياتها للحد من هذه التهديدات، ولتأمين أنظمة المعلومات المادية لديها، وإنشاء سياسات أمنية لخلق بيئة من الوعي الأمني. وفى ضوء محدودية موازنات تلك الشركات فيجب عليها فحص هذه التهديدات بشكل تفصيلي (Hwang et al., 2019).

من السرد السابق يمكن استخلاص أن مكونات أمن المعلومات المحاسبية الالكترونية تتمثل في النقاط التالية:

- توفير كل الاحتياطات لحماية المعلومات المحاسبية السرية والتي تمر عبر أوساط ومواقع عديدة قبل أن تصل للموقع النهائي من ذوي النوايا السيئة والذي يمكنهم من الاختراق الأمني بهدف تغيير تلك المعلومات بما يضر بالشركة ويساهم في اتخاذ قرارات خاطئة للمستثمرين ومن ثم الإضرار بسمعة الشركة مما يؤثر سلباً على الأداء المالي وغير المالي للشركات.
- تخصيص موازنة مالية كافية للتغلب على الثغرات الأمنية في الأنظمة المعلوماتية وذلك بتوفير أدوات التحكم والأساليب المتقدمة التي تستطيع من خلالها الشركات اكتشاف تلك الثغرات الموجودة في أنظمتها.
- تجهيز وحدة إدارية آمنة متخصصة لحماية الأجهزة والسيرفرات الخاصة بنقل المعلومات من أي تهديد بيئي، كارتفاع درجات الحرارة الهائلة التي تهدد سلامة الأجهزة، واشتعال الحرائق، والتلف الناتج عن التغيرات في الترددات الكهربية.
- الاستعانة بمجموعة من المتخصصين لدرء أي تهديد لأمن المعلومات المحاسبي والذي يتمثل في محاولة الاختراق، أو تصحيح الأخطاء البرمجية، وتحميل برامج متخصصة وتحديثها باستمرار لمواجهة الفيروسات التي تصيب الأجهزة بالعطب، وتغيير كلمات السر باستمرار لمجابهة الدخول غير المسموح به للمعلومات، وتوفير البرامج التي تضمن الاسترجاع الآمن للمعلومات في حال تلفها أو ضياعها.

٤-٢: إطار COBIT كأحد أطر إدارة المخاطر وأمن المعلومات:

يعتبر إطار (COBIT) من أفضل الأطر في إدارة مخاطر تكنولوجيا المعلومات وتحقيق فعالية حوكمة تكنولوجيا المعلومات فهو عبارة عن مجموعة من أفضل الممارسات (إطار العمل) لحوكمة تكنولوجيا المعلومات (IT) التي أنشأتها جمعية مراجعة ومراقبة نظم المعلومات (ISACA) ومعهد حوكمة تكنولوجيا المعلومات (ITGI) في عام ١٩٩٢، وقد تم إطلاق إطار COBIT لأول مرة في عام ١٩٩٦، حيث يُعد هو الإطار المنوط بمساعدة القائمين بالعمل في الشركات المتعددة على جعل تكنولوجيا المعلومات ذات الصلة تحقق استثمارات أفضل (Hamid et al. 2016).

وقد تناولت العديد من الدراسات السابقة تعريف إطار (COBIT)، والتى استخلص منها الباحثون **تعريفاً شاملاً لإطار COBIT** بأنه "إطار يحتوي على المعايير والضوابط التي يؤدي تطبيقها للوصول لمستوى رقابة مقبولة على عمليات الشركة المتعلقة بتكنولوجيا المعلومات، ومن ثم التوصل للطريقة المثلي التي سيتم بها تطبيق تكنولوجيا المعلومات من

قبل الإدارة وأصحاب المصالح، والذي يؤدي بالتالي إلى تحقيق الأهداف المرجوة والتي على رأسها تحقيق أعلى أرباح، والوصول لأدنى درجات المخاطرة".

ويتمثل الهدف الأساسي من تطبيق إطار عمل COBIT في التحكم بالمعلومات والتكنولوجيا ذات الصلة لتوفير سياسة واضحة وممارسات جيدة عند تطبيق حوكمة تكنولوجيا المعلومات، والغرض من وضع هذه السياسة هو مساعدة الإدارة والمستخدم على فهم وإدارة المخاطر المرتبطة بحوكمة تكنولوجيا المعلومات، وكذلك توفير المعلومات الضرورية والتي تهدف لسد الفجوة بين مخاطر الأعمال واحتياجات الرقابة والقضايا الفنية (Abu-Musa, 2009; ITGI, 2007). كما يؤدى تطبيق إطار COBIT إلى رفع كفاءة أنظمة الرقابة الداخلية ويحسن من أداء الشركات ويخفض التكاليف، ويساعد أيضاً على ضمان كفاءة العمل وتوافقه مع الأهداف الاستراتيجية للمنظمة (الدليمي والشرع، ٢٠١٨).

وتُعد حوكمة تكنولوجيا المعلومات من صميم عمل إطار COBIT كما تساعد على ضمان التوافق مع متطلبات العمل، كما أن بناء إطار COBIT يمكِّن المراجعين من تحديد ومعرفة الإصدارات والنشرات التنظيمية للبنية التحتية لتكنولوجيا المعلومات، فضلاً عن مساعدتهم على تعزيز نتائج تقاريرهم (Haouam, 2020).

ومن ثم تتمثل أهداف تطبيق إطار COBIT الرئيسية فى توفير آلية صنع للقرار أكثر فعالية من خلال تحديد خطة استراتيجية لتكنولوجيا المعلومات، وتعزيز توافق تكنولوجيا المعلومات مع احتياجات العمل، والمساعدة في الرقابة على البنية التحتية لتكنولوجيا المعلومات، والمساعدة في إدارة مخاطر تكنولوجيا المعلومات، والعمل على رصد مدى نجاح تطبيق تكنولوجيا المعلومات.

تتكون الأهداف الرقابية لإطار COBIT من أربعة أبعاد أساسية، وهى بُعد التخطيط والتنظيم، وبُعد الاستحواذ والتنفيذ، وبُعد التوصيل والدعم، وأخيراً بُعد المتابعة والتقييم (Mataracioglu and Ozkan, 2011; Al Skafy et al. 2012; Motii and Semma, 2017; Bouayad et al. 2017; Alotaibi et al. 2021).

يعتمد إطار COBIT على مجموعة من المبادئ تبدأ من تحديد متطلبات العمل التي تقود إلى اعتماد الاستثمارات في مصادر تكنولوجيا المعلومات، والتي تستخدم بدورها في عمليات تكنولوجيا المعلومات، ومن ثم تقود في نهاية الأمر إلى إتاحة معلومات للشركة والتي تستجيب بالتالي لمتطلبات العمل، ويوضح الشكل رقم (٣) هذه المبادئ ITGI (2007) .

الشكل رقم (٣): المبادئ الأساسية لإطار COBIT

المصدر بتصرف: [ITGI, 2007]

وتوجد ستة **إصدارات من إطار COBIT**، صدرت الأولى في عام ١٩٩٦ بينما صدرت الأخيرة عام ٢٠١٩، حيث يتوافق التحديث الأخير مع التغيرات الخاصة بهيكلة ومحتوى إطار العمل في الوقت الحاضر، ويضيف مميزات جديدة مثل عوامل التصميم Design factors التي تسمح بتكييف أنظمة الحوكمة مع الظروف الحالية، حيث قدم COBIT 2019 العديد من عوامل التصميم التي يمكن أن تُطور تصميم نظام حوكمة تكنولوجيا المعلومات للشركة (على سبيل المثال؛ استراتيجية الشركة، وتعريف المخاطر، ودور تكنولوجيا المعلومات، وطرق نشر تكنولوجيا المعلومات، وتحديد التهديدات). وسيتم الاعتماد على **COBIT 2019** فى هذا البحث لما له من مزايا تدعم **حوكمة تكنولوجيا المعلومات**، وهى أن إطار COBIT 2019 يعتبر من أفضل الأطر الذي يقوم بالتقييم والرقابة لحوكمة تكنولوجيا المعلومات ويساعد في تنفيذها. كما يعد كإطار عمل من أفضل الممارسات الداعمة حيث يساعد في توفير بيئة تكنولوجيا معلومات مرنة ومُدارة جيدًا. وهو يساعد على مراقبة كافة الأنشطة المرتبطة بحوكمة تكنولوجيا المعلومات. كما يحاول اطار COBIT 2019 ربط الأهداف الرئيسية للشركة مع منظومات العمل مع أهداف قسم تكنولوجيا المعلومات. فضلاً عن أن تطبيق أطر الرقابة والتقييم كإطار COBIT 2019 يخدم نظام الرقابة الداخلية بالشركة من خلال توفيره للمبادئ المقبولة عالمياً، وبالتالي يؤدي لتوفير الممارسات التحليلية التي تساعد بدورها على زيادة الثقة في قيمة المعلومات المقدمة للأطراف الداخليين والخارجيين مما يؤدي للتوسع في أعمال الشركة وزيادة ربحيتها. وأخيراً أنه يساعد الشركات أن تصل للهدف الرئيسي لها وهو زيادة الأداء الكلي من خلال اتباع أنظمة الرقابة والمساعدة في إدارة المخاطر بشكل مناسب، مما يؤدي لتحقيق الربح المستهدف، وأيضاً تحقيق الميزة التنافسية في الأسواق المختلفة سواء داخلياً وخارجياً.

٤-٣: المعيار الدولى لإدارة أمن المعلومات (ISO/IEC 27001):

تتكون معايير الأيزو من مجموعة من الإصدارات المختلفة التى تم إصدارها بواسطة المنظمة الدولية للمعايير (ISO) [١]. حيث وضعت المنظمة الدولية للمعايير ISO أنظمة توضح كيفية حماية البيانات والمعلومات من التهديدات المختلفة، فمن خلال وضع معايير لإدارة أمن المعلومات يمكن حماية البيانات الهامة الخاصة بالشركة بما سيؤدى قطعاً إلى زيادة ثقة العملاء الحاليين وجذب العملاء المحتملين، كذلك كسب ثقة أصحاب المصلحة ومن ثّمَّ إلى زيادة الأرباح ورفع المستوى التنافسى للشركة محلياً وعالمياً، لذلك ظهرت الحاجة جلية لوجود معايير محددة لقياس الكفاءة والفعالية لأمن المعلومات فى الشركات المختلفة، ويأتى ذلك من خلال ربط الأهداف الخاصة بأمن المعلومات والتى تتمثل فى مثلث أمن المعلومات Confidentiality, Integrity and Availability (CIA) وهو سرية

(١) المنظمة العالمية للتوحيد القياسي أو (أيزو) (ISO: International Organization for Standardization)، هي منظمة تعمل على وضع المعايير، وتضم هذه المنظمة ممثلين من عدة منظمات قومية للمعايير حيث وصل عدد أعضائها إلى ١٦٣، وتأسست في ٢٣ فبراير ١٩٤٧ ودورها هو إصدار معايير تجارية وصناعية عالمية، ومقرها في جنيف سويسرا، وبالرغم من أن الأيزو تعرف نفسها كمنظمة غير حكومية، ولكن قدرتها على وضع المعايير التي تتحول عادة إلى قوانين تجعلها أكثر قوة من معظم المنظمات. المصدر: https://www.iso.org

المعلومات، والتكامل وسلامة وصحة المحتوى، وتوفر واستمرارية المعلومات بالتوافق مع المعيار الدولي لأمن المعلومات ISO/IEC-27001 (نصيف، ٢٠١٢).

وقد بدأ تطوير مجموعة المعايير لعائلة (ISO/IEC-27001) والتي تخص نظام إدارة أمن المعلومات (ISMS) المشار إليها بشكل شائع في عام ٢٠٠٥ مع اثنين من معايير ISO الأكثر تطبيقاً في العالم وهما (ISO/IEC-27001) و(ISO/IEC-27002) والتي وضعت قواعد تطبيق إدارة أمن المعلومات، ومنذ ذلك الحين تم إضافة معايير أخرى إلى العائلة، كالمبادئ التوجيهية التي تدعم ISO / IEC 27001، والمعايير المتعلقة بالاعتماد والتصديق ومراجعة أدوات ISMS، والمعايير الخاصة بتطبيق (ISO / IEC) / (ISO / IEC 27001) (27002) المخصصة لقطاعات الخدمات والتطبيقات مثل الاتصالات والخدمات السحابية وحوكمة تكنولوجيا المعلومات (Humphreys, 2018).

وتهدف هذه المعايير **الدولية التي تنظم أمن المعلومات** إلى إعداد خطة تنفيذ توضح فيها كيفية تطبيق تلك المعايير والوقت المطلوب لتنفيذها. ووضع نطاق عمل للمعيار وسياساته والإجراءات التي يجب اتباعها. وتحديد الأدوار والمسئوليات الخاصة بأمن المعلومات في الشركة. وتوفير تدريب مناسب للكوادر البشرية القائمة بالعمل وذلك لتحقيق أقصى قدر من المردود المطلوب جراء تطبيق معايير ISO. بالإضافة إلى إعداد الموظفين للقيام بمهمة أمن المعلومات على أكمل وجه. والحصول على الاعتماد الدولي والذي يساعد في تحقيق نتائج هادفة. وتحديد الثغرات الأمنية الموجودة بإدارة أمن المعلومات. وكذلك التأكد من وجود نظام أمن معلومات يقوم بالعمل بكفاءة لإدارة الأعطال الأمنية. والحفاظ على سلامة المعلومات السرية. وتحقيق سيولة البيانات والمعلومات بشكل ثابت ومستمر. والتوصل لتحقيق ميزة تنافسية محلية وعالمية نتيجة للحصول على شهادات الأيزو. وأخيراً إدارة المخاطر المتعلقة بإدارة أمن المعلومات، والتى تنقسم إلى: تقييم المخاطر، ومعالجة تلك المخاطر.

يعتمد هذا البحث على معيار ISO/IEC-27001 الذى يدعم توفير أمن حوكمة تكنولوجيا المعلومات للعديد من الأسباب أهمها أنه يمكن لمزودي تكنولوجيا المعلومات توثيق مطابقة عملياتهم الأمنية مع معيار معترف به، حيث أن الحصول على شهادة الايزو تعمل بمثابة ختم جودة من هيئة مستقلة بشأن تطبيق التدابير الأمنية المناسبة. ونظراً لمرونة معيار الأيزو فإنه يتم استخدامه من قبل جميع الشركات في جميع أنحاء العالم بما فيها الصغيرة والمتوسطة ومنظمات الأعمال الكبيرة، مما أدى به ليصبح لغة مشتركة لإدارة أمن المعلومات. وقد تم تقنين متطلبات ISO/IEC-27001 وشرحها في ISO/IEC-27002 في شكل دليل حيث أوجب توثيق العمليات الروتينية المثالية في دليل يسمى بإجراءات التشغيل القياسية، وكذلك أوجب توثيق الحوادث الأمنية وتحليلها وتقييمها من أجل تطوير التحسينات الممكنة والأساسية على نظام أمن المعلومات. أخيرًا، وضع المعيار كيفية تنفيذ التدابير المناسبة للوفاء بمتطلبات الامتثال، على وجه الخصوص حقوق الطبع والنشر وحقوق الاستغلال، وتم الاستشهاد بمتطلبات أمان البيانات، وتوضيح طريقة تنظيمها وضمانها بطريقة يمكن التحقق منها.

ونظراً لأن معايير الـ ISO تقدم المبادئ الأساسية التي توجه مديري الشركات ذات الأنشطة المختلفة لكيفية استخدام تكنولوجيا المعلومات بطريقة فعالة، وكذلك فإن هدفها

الرئيسي التحقق من الجودة وتوافر أمن المعلومات بالشركة، والذي تنعكس بالتالي على الأداء المالي وغير المالي بالشركة، فسيكون أحد محاور الدراسة في هذا البحث.

٤-٤: تكامل معيار ISO/IEC-27001 مع إطار COBIT لتحقيق فعالية حوكمة تكنولوجيا ا لمعلومات:

يمكن أن يدعم تكامل COBIT 2019 مع ISO/ IEC-27001/27002 في زيادة فعالية حوكمة تكنولوجيا المعلومات حيث (١) يساعد تطبيق إطار COBIT 2019 الإدارة في وضع خطط واستراتيجيات عمليات حوكمة تكنولوجيا المعلومات أما معيار ISO/IEC-27001/27002 فهدفه هو إدارة المخاطر وتنفيذ الضوابط الأمنية. (٢) يوفر دمج إطار COBIT 2019 مع معيار ISO/IEC-27001 مزايا مختلفة لتحقيق الأهداف الاستراتيجية للشركة، فسيكون COBIT 2019 بمثابة خط إرشادي لأمن المعلومات لمعالجة قياس مستوى قدرة أمن المعلومات على توجيه الأعمال، بينما سيكون ISO/IEC-27001/27002 معيارًا دوليًا لتقييم أداء النظام من حيث موثوقيته ودقته والتي تحمي أمن معلومات بالشركة، ويوفر دمجهما مزايا أكثر تفصيلاً في قياس قدرات أمن المعلومات وما يتبعها من تأثير على فعالية تطبيق حوكمة تكنولوجيا المعلومات. (٣) هناك حاجة لقياس أثر تطبيق إطار COBIT 2019، ومعيار ISO/IEC-27001/27002 على مستوى دقة أمن المعلومات والذي يؤثر بالتالي على أصول المعلومات حيث تعتبر القوة الدافعة للعمليات التجارية داخل الشركة لتحقيق أهداف العمل. (٤) يتم إجراء قياس أثر تطبيق إطار COBIT 2019، ومعيار ISO/IEC-27001/27002 لتقديم توصيات لتحسين نظام إدارة أمن المعلومات بحيث يمكن لأصحاب المصلحة اتخاذ القرارات المناسبة للاستثمار وتحسين ظروف العمل بالشركة. (٥) يخلق أمن المعلومات القدرة على قياس مستوى التحسن في الإدارة، وبالتالي يوفر فرصة لتحسين أداء المنشأة بهدف الحفاظ على الخدمة وتحسينها للعملاء ومواجهة المنافسة على مستوى السوق المحلي والعالمي.

٥: دور حوكمة تكنولوجيا ا لمعلومات في تحقيق حماية أمن المعلومات:

من خلال المعايير التي تنظم حماية أمن المعلومات يمكن تحليل العلاقة بين حوكمة تكنولوجيا المعلومات وتحقيق حماية أمن المعلومات واشتقاق الفرض الأول للدراسة. فقد أوضحت دراسة بركات وآخرون (٢٠١٢) أن استخدام إطار COBIT للرقابة على حوكمة تكنولوجيا المعلومات يقوم بمساعدة المديرين والمراجعين على فهم حوكمة تكنولوجيا المعلومات بالشركة مما يؤدي لحماية أصولها وتحقيق مستوى الأمن المطلوب ومن ثم تحقيق الفائدة المرجوة من تكنولوجيا المعلومات والتي تنعكس بشكل إيجابي على تحسين أجواء العمل والوصول لرضا العملاء وزيادة ثقتهم في الخدمات المقدمة بالشركة، كذلك سعت دراسة Alkhaldi et al. (2017) لفهم فوائد حوكمة تكنولوجيا المعلومات في الشركات المطبقة لإطار COBIT، حيث أشارت نتائج البحث إلى أن إدارة مخاطر حوكمة تكنولوجيا المعلومات هي المؤشر الرئيسي لشرح سلوك تطبيق حوكمة تكنولوجيا المعلومات، وقامت دراسة King et al., (2017) باختبار العلاقة بين حوكمة تكنولوجيا المعلومات وأمن المعلومات المتوافقة مع معيار الأيزو (ISO/27002-27001) وأثرها على إدارة المخاطر، وتوصلت لوجود علاقة إيجابية بين الحوكمة الفعالة لتكنولوجيا المعلومات وإدارة مخاطر تكنولوجيا المعلومات باستخدام معيار (ISO/27002-27001)،

وقامت دراسة Mayer and De Smet (2017) باختبار كيفية التعامل بشكل أفضل مع التكامل بين حوكمة تكنولوجيا المعلومات وإدارة المخاطر وذلك باستخدام معايير الـ ISO ذات الصلة، وقد أظهرت نتائج هذا البحث أن الاهتمام بالتنسيق بين آليات الحوكمة وعناصر إدارة مخاطر تكنولوجيا المعلومات يؤثر إيجابيا على تنفيذ حوكمة تكنولوجيا المعلومات، أما دراسة Motii and Semma (2017) فقامت باختبار وضع منهج جديد لدمج إطار COBIT مع ISO/IEC-27002 من أجل استخدام أفضل لحوكمة تكنولوجيا المعلومات في البرلمان المغربي، وأوضحت أهمية استخدام COBIT لتقييم عوامل النجاح الحاسمة وأوصت بتطبيق معيار ISO/IEC-27002 في تكنولوجيا المعلومات لحل قضايا أمن وحوكمة تكنولوجيا المعلومات، وفي ذات النهج قامت دراسة البلقاسي (٢٠١٨) بإيضاح مفهوم حوكمة تكنولوجيا المعلومات ودراسة إمكانية استخدام COBIT كأحد الأطر الرقابية على الحوكمة، ودراسة التأثير الناتج من تطبيق مفهوم الحوكمة على تخفيض فجوة المخاطر في نظم المعلومات الالكترونية، كما درس Fathoni et al. (2020) حالة بنك XYZ بأندونيسيا وقام بتحليل إجراءات نظام حوكمة أمن المعلومات عند تنفيذ تطبيقات خدمات الائتمان باستخدام مزيج من إطار COBIT ومعيار ISO/IEC-27001، حيث أوضح أنه من حق أصحاب المصلحة في شركة ما معرفة أفضل طريقة لحوكمة تكنولوجيا المعلومات والذي يمكن أن يؤثر على أداء الشركة وسمعتها، وركز التقييم على تقسيم عنصر الأمن في نظام أمن تكنولوجيا المعلومات إلى خمسة عناصر وهي؛ قبول الحد الأمثل من المخاطر، إدارة المخاطر، إدارة الأمن، إدارة التغيير، وإدارة خدمات الأمن، أما دراسة Khusna and Ali (2020) فقامت بتقييم حوكمة تكنولوجيا المعلومات القائم على استخدم إطار COBIT في الشركات الصغيرة وأظهرت نتائج البحث أن إطار COBIT قد ساعد الشركات على إنشاء قيمة مثالية من تكنولوجيا المعلومات من خلال الحفاظ على التوازن بين تحقيق الربح وتحسين مستوى المخاطر والموارد المستخدمة. **وعليه يمكن اشتقاق الفرض الأول للدراسة على النحو التالي:**

الفرض الأول (H_1): توجد علاقة ذات دلالة احصائية بين تطبيق حوكمة تكنولوجيا المعلومات وتحقيق حماية أمن المعلومات باستخدام إطار COBIT 2019، وإصدارات معيار ISO ذات الصلة.

وسيتم الاعتماد في هذا البحث على قياس متغيرات الدراسة فى الفرض الأول من خلال طرح عدد (١٦) سؤال مدرج في قائمة استبيان موجهة لعينة الدراسة.

٦: دور تطبيق آليات حوكمة تكنولوجيا المعلومات في تحسين الأداء المالي وغير المالي للشركات:

الأداء المالي للشركات هو الإنجاز المالي للشركة ويمكن قياسه من خلال مالية مختلفة يتم اسخراجها من القوائم المالية لقياس الأداء المالي مثل نسب السيولة، ومعدل العائد على الأصول، معدل العائد على حقوق الملكية كمؤشرات للربحية (Alber and Nabil 2015; Fatihudin and Mochklas 2018; Yang et al., 2018; Mulyono et al., 2020)

أما **الأداء غير المالي للشركة** فهو عبارة عن معلومات غير محاسبية ليس مكانها القوائم المالية، وللأداء غير المالي ستة جوانب؛ **الجانب الأول** والمتعلق بالمفهوم يحتوى على

المسئولية الاجتماعية والاستدامة، أما **الجانب الثاني** فهو يحتوي على الأهداف الاستراتيجية للشركة والتي تعزز فكرة تحقيق ميزة تنافسية، و **الجانب الثالث** ويشمل الدافع الذي يجعل الإدارة تقوم بدورها وهو تحقيق الربحية، و**الجانب الرابع** وهو بناء علاقات وطيدة مع أصحاب المصالح، أما **الجانب الخامس** فهو الإفصاح الاختياري عن المعلومات غير المالية، و**الجانب السادس** والأخير فهو تحقيق التكامل بين المعلومات المالية والمعلومات غير المالية (Sridhar, 2012).

ومن ثم لابد من وجود تكامل وتضافر بين الأداء المالي والأداء غير المالي حتى يتحقق الإفصاح عن الأداء الكلي بشفافية ومصداقية تساعد أصحاب المصالح في اتخاذ القرارات المختلفة بالاستثمارات في الشركة. وفى هذ السياق قامت دراسة Lunardi et al. (2014) باختبار مؤشرات الأداء المختلفة من الشركات التي اعتمدت رسميا على حوكمة تكنولوجيا المعلومات بالمقارنة بأداء الشركات الأخرى التي لم تعتمدها، وقد توصلت إلى أن الشركات التي تبنت حوكمة تكنولوجيا المعلومات تظهر تحسن ملحوظ في أدائها بالمقارنة بالشركات الأخرى التي لا تتبناها، كما أن آليات حوكمة تكنولوجيا المعلومات قد تم استخدامها من قبل الشركات بشكل أساسي من أجل تحقيق كفاءة أكبر مثل خفض التكلفة وزيادة الربحية. كما اهتمت دراسة Kong et al. (2015) بتحليل علاقة حوكمة أمن المعلومات بالأداء الكلي للشركات العاملة بالأوراق المالية، واستنتج هذا البحث أن الاستثمار في أمن المعلومات يؤدي إلى تعزيز استقرار المعاملات. وقد بحثت دراسة Ahmad and Zabri (2016) في مدى استخدام شركات التصنيع الماليزية لمجموعة محددة من مقياس الأداء غير المالي، وهي (مراقبة الجودة ، الكفاءة الداخلية، المقاييس المستندة إلى العملاء والموظفين)، وأظهرت النتائج أن تسليم السلعة أو الخدمة في الوقت المحدد ورضا العملاء هما أكثر مقاييس الأداء غير المالي استخدامًا. وألقت دراسة Chi, et al. (2017) الضوء على كيفية خلق قيمة من خلال استخدام تكنولوجيا المعلومات في الشركات المتعددة الجنسيات وكذلك تأثير استراتيجيات حوكمة تكنولوجيا المعلومات على تعزيز الأداء الكلي للشركات، وتوصل البحث إلى أن كلا من استراتيجيات حوكمة تكنولوجيا المعلومات والتي تتكون من استراتيجيات التوازن واستراتيجيات التنفيذ يمكن أن تساعد في زيادة الأداء الكلي للشركة، كما أن حوكمة تكنولوجيا المعلومات الجيدة يمكن أن يكون لها تأثيراً إيجابياً على اختيار استراتيجيات الحوكمة التي تطبقها الشركات. وفي مجال تقديم الخدمات الصحية فقد اهتمت دراسة Wang et al. (2018) باختبار الارتباط بين نفقات تكنولوجيا المعلومات الصحية والعمليات التجارية والعائد على الأصول والإنتاجية والأداء المالي للمستشفى بعد تطبيق معايير وقوانين حوكمة تكنولوجيا المعلومات، واستنتجت أن نفقات تكنولوجيا المعلومات الصحية بما في ذلك نفقات تطبيق حوكمة تكنولوجيا المعلومات مرتبطة بشكل إيجابي بعائد المستشفيات على الأصول والإنتاجية. وفي نفس السياق أشارت دراسة Hapsari (2018) أن حوكمة تكنولوجيا المعلومات ظهرت كمتغير معدل في العلاقة السببية بين أثر الميزة التنافسية على الأداء المالي حيث سيؤدي زيادة الميزة التنافسية للشركة إلى رفع مستوى رضا أصحاب المصلحة وبالتالي تحقيق أداء مالي أفضل، كما قامت دراسة Ashsifa and Ali (2019) بعمل دراسة حالة عن تأثير الاستثمار في حوكمة تكنولوجيا المعلومات على أداء تكنولوجيا المعلومات والأداء الكلي للشركة، واعتمد البحث على عدد

من المديرين الماليين بالجامعات وتوصل إلى أن الاستثمار في حوكمة تكنولوجيا المعلومات هي أحد العوامل التي تحفز أداء حوكمة تكنولوجيا المعلومات. وفحصت دراسة Mulyono et al. (2020) أثر تطبيق حوكمة تكنولوجيا المعلومات والتجارة الإلكترونية والابتكار على الميزة التنافسية وتداعياتها على الأداء المالي للشركة، ووجدت أن لتطبيق الحوكمة في مجال تكنولوجيا المعلومات والتي يتم التعامل بها في التجارة الالكترونية تؤثر تأثيراً إيجابياً على الأداء المالي، كما دعمت التجارة الإلكترونية الميزة التنافسية للشركة مما أدى بالتالي لتحسين الأداء المالي للشركة، وقد أوصت الدراسة بتطبيق حوكمة تكنولوجيا المعلومات لما لها من أثر ايجابي على أداء الشركة الكلي. كذلك أوضحت دراسة Mikalef et al. (2020) كيف يمكن لتكنولوجيا المعلومات أن تساعد الشركات على البقاء والازدهار في بيئات العمل المضطربة والمتغيرة باستمرار، وطورت هذه الدراسة فكرة أن اللامركزية في حوكمة تكنولوجيا المعلومات تعزز العلاقة بين مرونة تطبيق حوكمة تكنولوجيا المعلومات والحفاظ على الأداء التنافسي لا سيما في ظل الظروف البيئية الخارجية غير المؤكدة. واستهدفت دراسة Khalil and Belitski (2020) اختبار القدرات الديناميكية لأداء الشركة تحت إطار حوكمة تكنولوجيا المعلومات، وقد توصلت هذه الدراسة إلى أن آليات حوكمة تكنولوجيا المعلومات المختلفة تعمل كقدرات ديناميكية وترتبط بشكل ايجابي بأداء الشركة. وحللت دراسة Salehi et al. (2021) تأثير الحوكمة الفعالة لتكنولوجيا المعلومات والأداء الكلي في قطاع تكنولوجيا المعلومات والاتصالات الكندية، وقد أظهرت النتائج أنه يمكن لحوكمة تكنولوجيا المعلومات الفعالة أن تؤدي لاستقرار الصناعة وإمكانية التنبؤ وتحسين أداء الشركة وبالتالي زيادة النمو الاقتصادي. أما في البيئة المصرية فقد اختبرت دراسة غنيمي (٢٠١٦) علاقة تطبيق حوكمة تكنولوجيا المعلومات على أداء البنوك المصرية، حيث ركز بشكل أساسي على تنفيذ الأنشطة وتقديم الخدمات الالكترونية المصرفية للعملاء عن طريق الانترنت في البنوك التجارية، وتوصلت هذه الدراسة إلى عدة نتائج من أهمها أن حوكمة تكنولوجيا المعلومات تساهم في الحد من المخاطر المصاحبة لاستخدام تكنولوجيا المعلومات، وأنها تدعم تحسين الأداء المالي وزيادة القدرة التنافسية للبنوك التجارية. وألقت دراسة مراد (٢٠١٦) الضوء على تأثير حوكمة تكنولوجيا المعلومات على الأداء المالي والقدرة التنافسية في الشركات المساهمة المصرية، وتوصلت الدراسة إلى أن هناك أثر إيجابي لتطبيق آليات حوكمة تكنولوجيا المعلومات على الأداء المالي والميزة التنافسية. أما دراسة بخيت وعز الدين (٢٠١٨) فقد أكدت على تأثير فاعلية حوكمة المعلومات الالكترونية على مؤشرات الربحية وإدارة المخاطر في البنوك التجارية المقيدة بالبورصة المصرية، ووجدت أن البنوك اتفقت بالإجماع على ضرورة أن يتسم نظام المعلومات بالدقة والملائمة والأمن والسرعة للتوصل لفعالية حوكمة تكنولوجيا المعلومات. وتناولت دراسة Joshi et al., (2018) دور حوكمة تكنولوجيا المعلومات في تحقيق عوائد إضافية من الاستثمار في تكنولوجيا المعلومات، وتحليل العلاقة بين تكاليف الاستثمار في التكنولوجيا والإيرادات المتوقعة من ذلك الاستثمار تطبيقاً على الشركات المصرية، وتوصلت إلى أنه يوجد ارتباط مباشر بين تطبيق آليات حوكمة تكنولوجيا المعلومات وتحقيق عوائد إضافية من الاستثمار في تكنولوجيا المعلومات، وكذلك يوجد ارتباط مباشر بين تكاليف الاستثمار في تكنولوجيا

المعلومات والعوائد المتوقعة من هذا الاستثمار. وعلى ذلك يمكن **اشتقاق الفرض** للدراسة على النحو التالي:

الفرض الثاني(H_2): توجد علاقة ذات دلالة احصائية بين تطبيق آليات حوكمة تكنولوجيا المعلومات وتحسين الأداء المالي والاداء غير المالي للشركات

وسيتم الاعتماد في البحث على قياس متغيرات الدراسة فى الفرض الثاني من خلال عدد (٩) سؤال مدرج فى قائمة الاستبيان وموجه لعينة الدراسة.

٧: أثر حماية أمن المعلومات الناتجة من تطبيق آليات حوكمة تكنولوجيا المعلومات على تحسين الأداء المالي وغير المالي للشركات:

نظراً لما حدث من طفرة حضارية ومعلوماتية استلزمت استخدام تكنولوجيا المعلومات في كافة نواحي الحياة العملية أصبح أمن المعلومات من المصادر التي تجلب القلق لمستخدمي تكنولوجيا المعلومات لأن الخسائر التي قد تتكبدها أي منظمة حال تعرضها لأى اختراق أمنى أمراً لا يستهان به، لذلك باتت من الأمور الحساسة التي يجب أن تُشحذ لها كافة الموارد المادية والبشرية. خاصةً أن تكنولوجيا المعلومات باتت تلعب دورًا حيويًا في مختلف الشركات بما لا يمكن الاستغناء عنها، وزادت تكنولوجيا المعلومات بشكل كبير من فرص الأعمال التجارية عبر الإنترنت، لكن هذه الفرص أوجدت أيضًا مخاطر جسيمة فيما يتعلق بأمن المعلومات، مما أدى لاهتمام الباحثين لاكتشاف دور حوكمة تكنولوجيا المعلومات في إدارة أمن المعلومات، وكان لزاماً على مجتمع الأعمال التوصل إلى مزيج من الأدوات الرقابية لتحقيق المستوى المعقول من الأمن المعلوماتي جراء استخدام تكنولوجيا المعلومات وذلك باستخدام أُطر معينة لمساعدة الشركات على تقييم مخاطر الأمان وتنفيذ الضوابط الأمنية المناسبة، مثل إطار COBIT وإصداراته المختلفة لتحقيق درجة معقولة من أمن المعلومات، وكذلك معيار ISO/IEC-27001 لتحقيق السرية والنزاهة.

وفي هذا الصدد تناولت دراسة Yayla and Hu (2011) ردود فعل سوق الأوراق المالية على الأحداث المتعلقة بأمن المعلومات، وتوصلت هذه الدراسة إلى اختبار تأثير عدد من العوامل منها نوع النشاط ونوع الصناعة حيث وُجد أن شركات التجارة الإلكترونية شهدت ارتفاعًا في ردود فعل السوق السلبية بانخفاض قيمة الشركة السوقية في حالة الاعلان عن الخرق الأمني، أما نوع الانتهاك فقد وجدت أن هجمات رفض الخدمة كان لها تأثير سلبي أعلى من الأنواع الأخرى من الخروقات الأمنية، أما بالنسبة لسنة الحدث فقد تبين أن أحداث الخروقات الأمنية التي وقعت في السنوات الأخيرة كان لها تأثير أقل أهمية من تلك التي حدثت في وقت سابق مما يشير إلى أن المستثمرين ربما أصبحوا أقل حساسية، كما اختبرت الدراسة تأثير هذه الأحداث على قيمة أسهم الشركات حيث توصلت إلى أن الأسهم قصيرة الأجل تأثرت بشكل واضح بتلك الخروقات الأمنية.

واختبرت دراسة Selamat and Babatunde (2014) أثر أمن المعلومات كمتغير وسيط على العلاقة بين أنشطة أمن المعلومات والأداء المصرفي في دولة نيجيريا، وتوصلت إلى أن عدم الامتثال للمعايير الأمنية الدولية أدى لارتكاب الاحتيال داخل الإدارة وبالتالي لوجود تأثير سلبى على أداء الشركة، كما يوجد تأثير إيجابي لتحديد مخاطر أمن المعلومات ووضع قيود لكيفية مواجهتها على أداء الشركات، كما أثبتت الدراسة حقيقة أنه لا يمكن تنفيذ

ثقافة أمن المعلومات بكفاءة دون الاهتمام بمعلومات الأنشطة الأمنية وإرساء ثقافة أمن المعلومات.

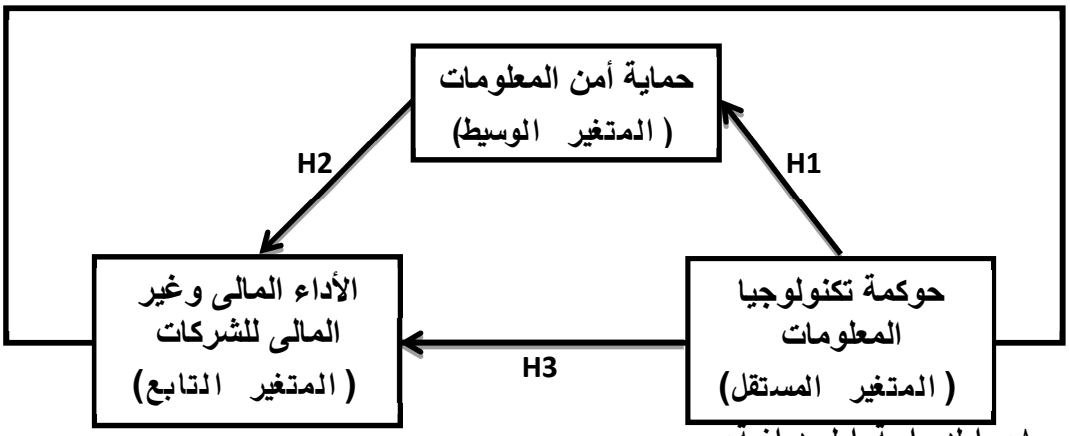
كما تناولت دراسة Herath and Herath (2014) مراجعة أمن تكنولوجيا المعلومات كنموذج لتقييم الأداء، وأثبتت أن الامتثال لقوانين الخصوصية هي أولوية قصوى للشركات المختلفة وتضمنت عملية مراجعة أمن المعلومات لتقييم فعالية حوكمة تكنولوجيا المعلومات والأنظمة الخاصة بها وتحديد توقيت وجوب الزامية إجراء مراجعة لأمن تكنولوجيا المعلومات وأثر دفع الحوافز للمديرين على تحسين أداء الشركات، وتحديد الحالات التي من الأفضل عدم إجراء المراجعة وفقاً لجدواها الاقتصادية. وقامت دراسة Avery and Chandraskaren (2016) أيضاً بدراسة الأثر السلبي للاختراقات الأمنية للمعلومات على الأداء المالي، حيث وجدا أنه يمكن أن تؤثر هذه الاختراقات على سمعة الشركة بالسلب مما يؤدي لانخفاض القيمة السوقية للشركة. وأوضحت دراسة Martin et al. (2017) أنه على الرغم من أن التسويق الإلكتروني يعتمد بشكل متزايد على بيانات العملاء، إلا أن مجرد الوصول إلى البيانات الشخصية للعملاء يضخم مشاعر الانتهاك ويقلل ثقة العملاء في الشركة مما يؤدي يؤثر سلباً على الأداء الكلي للشركة، كما يؤدي ذلك لسهولة الاختراق لمعلومات الشركة مما تساعد الشركات المنافسة الحصول على تلك المعلومات وبالتالي الاضرار بقيمتها التنافسية في السوق.

أما دراسة Dwivedi and Wang (2018) فقد حاولت اكتشاف منهجًا لعلم البيانات بهدف تقييم مدى تأثر العلاقات التجارية بانتهاكات أمن المعلومات بالشركات، وتوصلت إلى أن العلاقات العامة للشركات قد تأثرت إيجابياً بالأخطار الأمنية الناتجة من خروقات أمن المعلومات لتلك الشركات. ووضعت دراسة Heyasat et al. (2019) إطاراً لإدارة أمن المعلومات في أسواق رأس المال يمكن أن يتصدى بفعالية لتحديات ومتطلبات حوكمة تكنولوجيا المعلومات، واستنتجت أنه يوجد أثر إيجابي بين تحسين أمن المعلومات وأداء الشركة. وفي ذات السياق، هدفت دراسة Juma'h and Alnsour (2020) إلى التحقق من تأثير خرق البيانات على الأداء الكلي للشركات المتضررة، وتحليل تأثير انتهاكات البيانات المالية المحاسبة وآثارها القانونية والاجتماعية والاقتصادية على الأداء الكلي للشركات، وتوصلت أن الشركات المخترَقة أمنياً عانت من حيث الأداء، كما يمكن اعتبار المعلومات التي تم اصدارها طواعية من قبل الشركات فيما يتعلق بانتهاكات البيانات وحوادث الأمن السيبراني مؤشرا على أدائها. وعليه فيمكن **اشتقاق الفرض الثالث** للدراسة، على النحو التالي:

الفرض الثالث (H_3): تؤثر حماية أمن المعلومات الناتجةمن تطبيق آليات حوكمة تكنولوجيا المعلومات على تحسين الأداء المالي والأداء غير المالي للشركات.

وسيتم الاعتماد في هذا البحث على قياس متغيرات الدراسة في الفرض الثالث من خلال عدد (٩) سؤال مدرج في قائمة الاستبيان وموجه لعينة الدراسة.

ويوضح الشكل رقم (٤) نموذج الدراسة والعلاقة بين المتغيرات:



٨: الدراسة الميدانية:

تهدف الدراسة الميدانية إلى تحقيق هدف الدراسة وهو **دراسة واختبار** أثر تطبيق حوكمة تكنولوجيا المعلومات كمدخل لحماية أمن المعلومات على الأداء المالي وغير المالي للشركات، وذلك في عينة من الشركات في بيئة الأعمال المصرية من خلال اختبار فروض الدراسة الثلاثة التي تم اشتقاقها في الجانب النظري للبحث.

٨-١: تصميم قائمة الاستبيان:

اعتمد البحث على توزيع استمارة الاستبيان كأحد أدوات جمع البيانات، وتم صياغة الأسئلة بدقة حيث تنقسم أسئلة الاستبيان إلى مجموعتين:

١- أسئلة تتعلق بالمعلومات العامة (الديموغرافية) التي تخص أفراد العينة الذين قاموا بالإجابة على أسئلة الاستبيان من حيث جهة العمل، والمسمى الوظيفي، وعدد سنوات الخبرة، والمؤهل الدراسي، والشهادات المهنية الحاصلين عليها، وعدد المتخصصين الذين يعملون في قسم تكنولوجيا المعلومات في الشركات المختلفة.

٢- أسئلة الاستبيان التي تم إعدادها بناء على الدراسة النظرية وتتكون من ثلاثة محاور حيث تم الاعتماد على مقياس ليكرت الخماسي لقياس إستجابات مفردات العينة فيشير رقم (٥) إلى موافق بشدة، ورقم (٤) إلى موافق، ورقم (٣) إلى محايد، ورقم (٢) إلى غير موافق، وتتدرج حتى تصل إلى رقم (١) غير موافق بشدة.

٨-٢: مجتمع وعينة الدراسة:

لتحقيق هدف البحث تم الاعتماد على أسلوب العينة الحُكمية في اختيار العينة والمكونة من (٨٥) فرد، حيث تم توزيع استمارات الاستبيان على مفردات العينة والتي شملت العديد من الشركات العاملة بمجال تكنولوجيا المعلومات كشركات الاتصالات وشركات تكنولوجيا المعلومات، والشركات الخدمية كشركات التسويق الإلكتروني، والمؤسسات المالية كالبنوك والاستثمار في تداول الأوراق المالية العاملين في البيئة المصرية. ولقد تم مراعاة أن تكون مفردات العينة من الشركات التي تهتم بأمن المعلومات، ويوضح الجدول رقم (١) عدد استمارات الاستبيان التي وُزعت والتي تم استلامها ويمكن خضوعها للتحليل الإحصائي.

جدول (١): فئات عينة الدراسة وعدد استمارات الاستبيان التي وُزِعت وتم استلامها ويمكن خضوعها للتحليل الإحصائي

العينة	الاستمارات المُوزعة	الاستمارات المستلمة	نسبة الاستمارات المُوزعة إلى المستلمة	الاستمارات المستبعدة	الاستمارات الصحيحة	الاستمارات الخاضعة للتحليل الاحصائي	
						العدد	النسبة%
بنك	٣٢	٢٧	%٨٤,٤	٢	٢٥	٢٥	%٢٩,٤
شركة تكنولوجيا معلومات	١٧	١٥	%٨٨,٢	٢	١٣	١٣	%١٥,٣
شركة تداول أوراق مالية	١٨	١٧	%٩٤,٤	١	١٦	١٦	%١٨,٨
شركة اتصالات	٢٦	٢٣	%٨٨,٤	٢	٢١	٢١	%٢٤,٧
شركة تسويق الكتروني	١٧	١٣	%٧٦,٤	٣	١٠	١٠	%١١,٧
الاجمالي	**١١٠**	**٩٥**	**%٨٦,٥**	**١٠**	**٨٥**	**٨٥**	**%١٠٠**

ملحوظة: يدخل ضمن عدد الاستمارات الموضحة بالجدول الاستمارات المستلمة إلكترونياً والبالغ عددها (٣٠) استمارة.

٨-٣: التحليل الوصفي لعينة الدراسة:

توضح الجداول أرقام (٢أ) وحتى (٢هـ) التكرارات والنسبة المئوية لتوزيع عينة الدراسة تبعاً للمسمى الوظيفي، وعدد سنوات الخبرة، والمؤهل الدراسي، والشهادات المهنية، وعدد المتخصصين بقسم تكنولوجيا المعلومات.

جدول (٢أ): نتائج التحليل الوصفي لعينة الدراسة تبعاً للمسمى الوظيفي

التكرارات والنسبة المئوية لوصف خصائص عينة الدراسة تبعاً للمسمى الوظيفي												
الفئات	محاسب		مراجع IT مهندس برمجة		مراقب عام		رئيس قسم		مدير عام		الاجمالي	
	العدد	النسبة٪	العدد	النسبة٪	العدد	النسبة ٪	العدد	النسبة٪	العدد	النسبة ٪	العدد	النسبة ٪
الاجمالي	٣٢	٪٣٧.٦	١٢	٪١٤.١	٧	٪٨.٣	٢٨	٪٣٣	٦	٪٧	٨٥	٪١٠٠

يتضح من الجدول رقم (٢أ) أن نسبة ٣٧,٦% من حجم العينة يعملون كمحاسبين، ونسبة ١٤,١% من حجم العينة يعملون كمراجعين IT (مهندس برمجة)، ونسبة ٨,٣% من حجم العينة يعملون كمراقبين، ونسبة ٣٣% من حجم العينة يعملون كرؤساء أقسام، وأخيراً فإن نسبة ٧% من حجم العينة يعملون كمديرين، ويدل ذلك على وجود إلمام كافي لمتغيرات الدراسة من قبل المستجيبين في عينة الدراسة.

جدول (٢ب): نتائج التحليل الوصفي لعينة الدراسة تبعاً لعدد سنوات الخبرة

التكرارات والنسبة المئوية لوصف خصائص عينة الدراسة تبعاً لعدد سنوات الخبرة

الفئات	أقل من ٥ سنوات		٥ سنوات وأقل من ١٠ سنوات		١٠ سنوات وأقل من ١٥ سنة		١٥ سنه أو أكثر		الاجمالي	
	العدد	النسبة %	العدد	النسبة %	العدد	النسبة%	العدد	النسبة%	العدد	النسبة %
الاجمالي	١٥	١٧,٤ %	١٨	٢١,٧ %	٢٤	٢٨,١%	٢٨	٣٢,٨%	٨٥	١٠٠%

يتضح من الجدول رقم (٢ب) أن نسبة ٦٠.٩% من حجم العينة لديهم خبرة تزيد عن عشر سنوات مما يدل على أن العينة مأخوذة من الأفراد الذين تتوافر لديهم الخبرة العلمية والعملية، والتي تساعدهم على فهم الأسئلة الواردة في استمارة الاستبيان فهماً جيداً وبالتالي الحصول على إجابات موضوعية لتلك الأسئلة.

جدول (٢ جـ): نتائج التحليل الوصفي لعينة الدراسة تبعاً للمؤهل الدراسي

التكرارات والنسبة المئوية لوصف خصائص عينة الدراسة تبعاً للمؤهل الدراسي

الفئات	بكالوريوس		دبلوم دراسات عليا		ماجستير		الاجمالي	
	العدد	النسبة %	العدد	النسبة %	العدد	النسبة%	العدد	النسبة %
الاجمالي	٥٢	٦١,٢ %	١٧	٢٠%	١٦	١٨,٨%	٨٥	١٠٠%

يوضح الجدول رقم (٢جـ) توزيع عينة الدراسة وفقاً المؤهل الدراسي حيث يتضح أن نسبة ٦١,٢% من حجم العينة حاصلين على بكالوريوس، ونسبة ٢٠% من حجم العينة حاصلين على دبلوم دراسات عليا، وأخيراً نسبة ١٨,٨% من حجم العينة حاصلين على

ماجستير، ويدل ذلك على أن أفراد العينة من ذوي التعليم العالي وهم قادرون على استيعاب أسئلة الاستبيان والاجابة عليها بدقة لما لهم من مستوى عالي من التعليم الجامعي وما بعد الجامعي.

جدول (٢د): نتائج التحليل الوصفي لعينة الدراسة تبعاً للشهادات المهنية

التكرارات والنسبة المئوية لوصف خصائص عينة الدراسة تبعاً للشهادات المهنية											
العدد	شهادة CPA		شهادة CMA		شهادة CFA		شهادات أخرى		لا يوجد شهادات مهنية		الاجمالي	
	العدد	النسبة %	العدد	النسبة %	العدد	النسبة %	العدد	النسبة %	العدد	النسبة %	العدد	النسبة
الاجمالي	٣	٣,٥%	١٠	١١,٨ %	٣	٣,٥ %	٣١	٣٦,٥ %	٣٨	٤٤,٧ %	٨٥	١٠٠ %

كذلك يتضح من الجدول رقم (٢د) أن نسبة ٣,٥% من حجم العينة لديهم شهادة محاسب قانوني معتمد CPA، ونسبة ١١,٨% من حجم العينة لديهم شهادة محاسب إداري معتمد CMA، ونسبة ٣,٥% من حجم العينة لديهم شهادة محلل مالي CFA، ونسبة ٣٦,٥% من حجم العينة لديهم شهادات أخرى كشهادة MBA ، وشهادة CCNA، وشهادة Microsoft، وشهادة من أكاديمية التسويق الالكترونية، وأخيراً فإن نسبة ٤٤,٧% من حجم العينة ليس لديهم شهادات مهنية، ويدل ذلك على الاهتمام المتزايد من أفراد هذا المجال بالحصول على شهادات لشحذ قدراتهم المهنية كما يدل على أن أفراد العينة لهم القدرة على فهم أسئلة الاستبيان والإجابة عليها بكفاءة.

جدول (٢ هـ): نتائج التحليل الوصفي لعينة الدراسة تبعاً لعدد المتخصصين في قسم تكنولوجيا المعلومات

التكرارات والنسبة المئوية لوصف خصائص عينة الدراسة تبعاً لعدد المتخصصين في قسم تكنولوجيا المعلومات										
العدد	أقل من ٥		٥ وأقل من ١٠		١٠ وأقل من ١٥		١٥أوأكثر		الاجمالي	
	العدد	النسبة%	العدد	النسبة%	العدد	النسبة%	العدد	النسبة%	العدد	النسبة%
الاجمالي	١١	١٣%	٤	٤,٧%	٦	٧,١%	٦٤	٧٥,٢%	٨٥	١٠٠%

وأخيراً يوضح الجدول رقم (٢هـ) أن النسبة الأكبر من عينة الدراسة (وهى ٧٥,٢% من حجم العينة) هي لشركات يحتوي فيها قسم تكنولوجيا المعلومات على مجموعة كبيرة من المتخصصين (يزيد عن ١٥ موظف) مما يعني أن العينة من المتوقع أن يكون لديهم المعرفة المطلوبة لاستيعاب والرد على أسئلة الدراسة.

٨-٤: قياس صدق الاستبيان (Validity):

يساعد الصدق والثبات في التحليل الإحصائي على التأكد من صحة النتائج التي توصل إليها الباحثون، ومن ثم إمكانية تعميم النتائج على مجتمع البحث. حيث يعطى صدق الاستبيان دليلاً على أن عينة البحث قد مثلت مجتمع الدراسة بشكل جيد، وأن اجابات أفراد العينة قد أعطت المعلومات التي هدفت أسئلة الاستبيان الحصول عليها، ويحتوي مقياس الصدق على عدة أنواع وهي؛ الصدق الظاهري، صدق الاتساق الداخلي، الصدق البنائي.

وقد تم استيفاء الصدق الظاهرى بعرض قائمة الاستبيان على عدد من أصحاب الخبرة لإبداء رأيهم حول صحة صياغة العبارات المدرجة باستمارة الاستبيان وتم إجراء التعديلات المناسبة.

أما **صدق الاتساق الداخلي** وهو ما يعرف بصدق المحتوى أو مدى اتساق سؤال من أسئلة الاستبيان مع المحور الذي ينتمي إليه هذا السؤال، وذلك من خلال حساب معاملات الارتباط بين كل سؤال من أسئلة محاور الاستبيان والدرجة الكلية للمحور نفسه، وتم اختبار الاتساق الداخلي باستخدام معامل الارتباط بيرسون Pearson correlation coefficient، وجاءت النتائج بما توضح أن معامل الارتباط للمحور الأول عند مستوى معنوية ٠,٠١ قوي ويعنى ذلك أن المحور الأول بقائمة الاستبيان (بشأن فحص أثر حوكمة تكنولوجيا المعلومات على تحقيق حماية أمن المعلومات باستخدام إطار COBIT 2019، وإصدارات معيار ISO ذات الصلة) والمُصمم بغرض اختبار الفرض الأول للدراسة يؤدي الغرض الذي صُمم من أجله.

كما أن معامل الارتباط للمحور الثاني للاستبيان عند مستوى معنوية ٠,٠١ قوي ويعنى ذلك أن المحور الثاني بقائمة الاستبيان (بشأن أثر تطبيق آليات حوكمة تكنولوجيا المعلومات على تحسين الأداء المالي والأداء غير المالي للشركات) والمُصمم بغرض اختبار الفرض الثاني للدراسة يؤدي الغرض الذي صُمم من أجله. كذلك فإن معامل الارتباط للمحور الثالث للاستبيان عند مستوى معنوية ٠,٠١ قوي ويعنى ذلك أن المحور الثالث بقائمة الاستبيان (بشأن الدور الذي يقوم به حماية أمن المعلومات الناتجة من تطبيق حوكمة تكنولوجيا المعلومات على تحسين الأداء المالي وغير المالي) والمُصمم بغرض اختبار الفرض الثالث للدراسة يؤدي الغرض الذي صُمم من أجله.

ولقياس الصدق البنائي وهو مدى قدرة أسئلة الاستبيان على تحقيق الأهداف التي تريد الدراسة الوصول إليها، ومدى ارتباط كل محور من محاور الدراسة بجميع أسئلة المحور، فقد تم استخدام معامل ارتباط بيرسون لقياس درجة الصدق البنائي لأسئلة الاستبيان ككل، وذلك على النحو الموضح بالجدول (٣).

جدول (٣): قياس الصدق البنائى لأسئلة الاستبيان

م	محاور الاستبيان	معامل ارتباط	تفسير النتيجة
١	المحور الأول	٠,٩٢٨ (**)	يوجد ارتباط قوي ذو دلالة احصائية عند مستوى معنوية ٠,٠١
٢	المحور الثاني	٠,٩٠١ (**)	يوجد ارتباط قوي ذو دلالة احصائية عند مستوى معنوية ٠,٠١
٤	المحور الثالث	٠,٩٤١ (**)	يوجد ارتباط قوي ذو دلالة احصائية عند مستوى معنوية ٠,٠١

تعنى علامة (**) أن الارتباط ذو دلالة احصائية عن مستوى معنوية ٠,٠١

يتضح من الجدول رقم (٣) أن معامل الارتباط بين محاور الاستبيان قوي جداً ويعنى ذلك أن قائمة الاستبيان المُصممة بغرض اختبار فروض الدراسة تؤدي الغرض الذي صُممت من أجله.

٨-٥: قياس ثبات الاستبيان (Reliability):

عرف Crowder et al. (1994) الثبات بأنه قدرة الأداة التي يستخدمها الباحث على إعطاء نتائج مطابقة في كل مرة يقوم بها بإعادة نفس تطبيق الأداة تحت نفس الشروط وفي ظروف مشابهة لو تم إعادة توزيعه على أفراد العينة عدة مرات خلال فترات زمنية معينة، وقد تم قياس الثبات باستخدام معامل ألفا كرونباخ Cronbach's Alpha، وتعد نسبة ٦٠% مقبولة للحكم على مدى ثبات الاستبيان. ويوضح الجدول رقم (٤) أن المحاور الثلاثة تمتع بدرجة ثبات عالية جداً، كما أن نسبة الثبات لجميع محاور الاستبيان هي ٨٥% تقريبا ويشير ذلك إلى أن الترابط بين أسئلة الاستبيان عالي جداً، مما يعنى أن أسئلة الاستبيان قادرة على إعطاء نتائج مطابقة في كل مرة لو تم إعادة توزيعها على أفراد العينة عدة مرات خلال فترات زمنية معينة.

جدول (٤): قياس الثبات باستخدام معامل الفا كرونباخ Cronbach's Alpha Method

م	المحور	عدد الأسئلة	معامل الثبات ألفا كرونباخ
١	المحور الأول	١٦	٠,٨٨١
٢	المحور الثاني	٩	٠,٨٧٨
٣	المحور الثالث	٩	٠,٩٠٤
إجمالي المحاور		٣٤	٠,٨٩٤

٨-٦: الأساليب الإحصائية المستخدمة لاختبار فروض الدراسة:

لتحديد الأسلوب الإحصائي المناسب لطبيعة الدراسة الميدانية التي تختبر أثر حوكمة تكنولوجيا المعلومات كمدخل لحماية أمن المعلومات على الأداء المالي وغير المالي للشركات يتطلب ذلك حساب التوزيع الإحصائي لعينة الدراسة، وقد تم الإستعانة باختبار Kolmogorov-Smirnov Test لمعرفة درجة التوزيع الطبيعي لبيانات الدراسة، عند مستوى معنوية (α) يساوي ٠,٠٥ وكانت النتائج كما هي موضحة بالجدول رقم (٥).

جدول (٥): تحديد الأسلوب الإحصائي المناسب لطبيعة الدراسة الميدانية باستخدام Kolmogorov-Smirnov Test

المحور	Kolmogorov-Smirnov	مستوى الدلالة الاحصائية Asymp Sig	القرار	الاختبارات المستخدمة
الأول	٠,٠٤٦	٠,٢٠٠	التوزيع طبيعي	- التحليل الوصفي. - T -Test. - تحليل التباين أحادي الاتجاه. - اختبار المقارنات البعدية شيفيه.
الثاني	٠,١١٥	٠,٠٠٧	التوزيع غير طبيعي	- التحليل الوصفي. - اختبار الإشارة. - تحليل التباين كروسكال واليس. - تحليل مان ويتني لاختبار الفروق البعدية
الثالث	٠,٠٩١	٠,٠٧٧	التوزيع طبيعي	- التحليل الوصفي. - تحليل المسار - معامل الارتباط بيرسون - اختبار التأثير الوسيط باستخدام Bootstrapping - تحليل التباين أحادي الاتجاه. - اختبار المقارنات البعدية شيفيه.

يتضح من الجدول رقم (٥) بالنسبة للمحور الأول والثالث أن مستوى الدلالة الاحصائية **Sig** على التوالى (٠,٢٠٠) و (٠,٠٧٧) > مستوى المعنوية α (٠,٠٥) مما يعني أن مجتمع العينة يتبع التوزيع الطبيعي ويعنى ذلك أنه يمكن الاعتماد على الأساليب الإحصائية ذات الإختبارات المعلمية Parametric Tests. وبالنسبة للمحور الثاني فإن مستوى الدلالة الاحصائية **Sig** (٠,٠٠٧) < مستوى المعنوية α (٠,٠٥) مما يدل على أن مجتمع العينة لا يتبع التوزيع الطبيعي، ويعنى ذلك أنه يمكن الاعتماد على الأساليب الإحصائية ذات الإختبارات اللامعلمية Non-Parametric Tests. ويوضح العمود الأخير بالجدول رقم (٥) الاساليب الإحصائية المستخدمة مع كل فرض من فروض البحث.

٨-٧: اختبار فروض البحث:

سيتم اختبار فروض البحث على مستوى ثقة ٩٥% حيث تكون نسبة الشك في البيانات ٥% أي أن مستوى المعنوية α يساوي (٠,٠٥).

٨-٧-١: اختبار الفرض الأول للبحث:

ينص الفرض الأول على أنه: "توجد علاقة ذات دلالة احصائية بين تطبيق حوكمة تكنولوجيا المعلومات وتحقيق حماية أمن المعلومات باستخدام إطار COBIT 2019، وإصدارات معيار ISO ذات الصلة".

ولاختبار الفرض الأول تم صياغة عدد (١٦) سؤال تشمل أسئلة المحور الأول من قائمة الاستبيان، ويوضح الجدول رقم (٦) نتائج التحليل الوصفي لإجابات عينة الدراسة على المحور الأول.

جدول (٦): نتائج التحليل الوصفي لأسئلة المحور الأول

رقم السؤال	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	الوسط الحسابي	الانحراف المعياري	الاتجاه العام	الترتيب
	العدد	العدد	العدد	العدد	العدد				
	%	%	%	%	%				
١	٣٤	٤٥	٢	٤	-	٤,٢٨	٠,٧٣٣٧	موافق بشدة	٤
	٤٠%	٥٢,٩%	٢,٤%	٤,٧%	-				
٢	٣٥	٤٦	٤	-	-	٤,٣٦	٠,٥٧٤٢	موافق بشدة	٢
	٤١,٢%	٥٤,١%	٤,٧%	-	-				
٣	٢٩	٤٤	١١	١	-	٤,١٩	٠,٦٩٨٥	موافق	٦
	٣٤,١%	٥١,٨%	١٢,٩%	١,٢%	-				
٤	٣٠	٣٨	١٢	٤	١	٤,٠٨	٠,٨٨٩٢	موافق	١٢
	٣٥,٣%	٤٤,٧%	١٤,١%	٤,٧%	١,٢%				
٥	٢٦	٤٨	١٠	١	-	٤,١٦	٠,٦٦٩٨	موافق	٧
	٣٠,٦%	٥٦,٥%	١١,٨%	١,٢%	-				
٦	٢٨	٣٠	٢١	٦	-	٣,٩٤	٠,٩٣٠٣	موافق	١٦
	٣٢,٩%	٥٣,٣%	٢٤,٧%	٧,١%	-				
٧	٣٢	٤١	١١	١	-	٤,٢٢	٠,٧١٣٤	موافق بشدة	٥
	٣٧,٦%	٤٨,٢%	١٢,٩%	١,٢%	-				
٨	٢٨	٣٨	١٥	٢	٢	٤,٠٤	٠,٩٠٥٦	موافق	١٣
	٣٢,٩%	٤٤,٧%	١٧,٦%	٢,٤%	٢,٤%				
٩	٢٦	٤٧	١٠	٢	-	٤,١٤	٠,٧٠٩٧	موافق	٨
	٣٠,٦%	٥٥,٣%	١١,٨%	٢,٤%	-				
١٠	٢٧	٤٤	١٢	٢	-	٤,١٣	٠,٧٣٦٦	موافق	١٠
	٣١,٨%	٥١,٨%	١٤,١%	٢,٤%	-				
١١	٢٢	٤١	١٩	٢	١	٣,٩٥	٠,٨٢٩٦	موافق	١٤
	٢,٤%	٥٢,٩%	٢,٤%	٤,٧%	١,٢%				
١٢	٣١	٤٠	٩	٥	-	٤,١٤	٠,٨٣٣١	موافق	٩
	٣٦,٥%	٤٧,١%	١٠,٦%	٥,٩%	-				
١٣	٢٤	٤٧	١٤	-	-	٤,١٢	٠,٦٦٢١	موافق	١١
	٢٨,٢%	٥٥,٣%	١٦,٥%	-	-				
١٤	٣٧	٣٦	١٢	-	-	٤,٢٩	٠,٧٠٤١	موافق بشدة	٣
	٤٣,٥%	٤٢,٤%	١٤,١%	-	-				
١٥	٤٩	٣٢	٣	١	-	٤,٥٢	٠,٦٢٨٩	موافق بشدة	١
	٥٧,٦%	٣٧,٦%	٣,٥%	١,٢%	-				
١٦	٣٢	٢٢	٢٣	٨	-	٣,٩٥	١,٠١٤٣	موافق	١٥
	٣٧,٦%	٢٥,٩%	٢٧,١%	٩,٤%	-				
الوسط الحسابي المرجح للمحور الأول					٤,١٥٥٩	٠,٤٦٣٣		موافق	

يتضح من الجدول رقم (٦) أن المتوسط العام لهذا المحور هو (**٤,١٥٥٩**) عند درجة انحراف معياري (**٠,٤٦٣٣**)، مما يدل على أن آراء عينة الدراسة تتجه للموافقة على الأسئلة التي تختبر الفرض الأول والتي تتعلق بدراسة أثر تطبيق حوكمة تكنولوجيا

المعلومات على تحقيق حماية أمن المعلومات باستخدام إطار COBIT 2019 وإصدارات معيار ISO ذات الصلة.

وبإجراء T-Test لدراسة للفرض الأول، نظراً لأن عينة الدراسة تتبع التوزيع الطبيعي فيما يخص المحور الأول، لذلك فسوف يتم تطبيق الاختبارات المعلمية على الفرض الأول لاختبار أثر تطبيق حوكمة تكنولوجيا المعلومات على تحقيق حماية أمن المعلومات باستخدام إطار COBIT 2019 وإصدارات معيار ISO ذات الصلة، ويوضح الجدول رقم (٧) نتائج T-Test.

جدول (٧): نتائج اختبار الفرض الأول باستخدام T-Test

الفرض الأول	قيمة T المحسوبة	درجات الحرية df	مستوى الدلالة الإحصائية Sig	متوسط الفروق	فترة الثقة إلى الفرق	
					الحد الأدنى	الحد الأعلى
أثر تطبيق حوكمة تكنولوجيا المعلومات على تحقيق حماية أمن المعلومات باستخدام إطار COBIT 2019، وإصدارات معيار ISO ذات الصلة.	١٦,٧٩٥	٨٤	٠,٠٠٠	٠,٨٤٤١١	٠,٩٤٤٠٦	٠,٧٤٤١٧

يتضح من الجدول رقم (٧) أن مستوى الدلالة الاحصائية sig (٠,٠٠) < مستوى المعنوية α (٠,٠٥) لذلك يمكن قبول الفرض الأول والذي يفترض أن تطبيق حوكمة تكنولوجيا المعلومات تؤثر إيجابياً على تحقيق حماية أمن المعلومات باستخدام إطار COBIT 2019، وإصدارات معيار ISO ذات الصلة، بدرجة ثقة ٩٥%.

ولمزيد من التحليل تم إجراء **تحليل التباين أحادي الاتجاه (One-Way Test)** لقياس مستوى معنوية الفرق بين آراء العينة المشتركة في الدراسة من حيث جهة العمل، والمسمى الوظيفي، وعدد سنوات الخبرة، والمؤهل الدراسي، والشهادات المهنية الحاصل عليها عينة الدراسة، وعدد المتخصصين في قسم تكنولوجيا المعلومات، حيث يساعد قياس المعنوية فى التعرف على الإستعدادات الخاصة الكامنة لدى أفراد الفئات ومن ثم التركيز عليها وتطويرها، كما تساعد القائمين على إعداد القوانين والمعايير أن يراعى إستعدادات وقدرات العاملين في مجال تكنولوجيا المعلومات ومراعاة حاجاتهم الأساسية لتحقيق حماية كافية لأمن المعلومات. فقد أوضحت نتائج تحليل التباين الأحادي ANOVAللفرض الأول تبعاً للمسمى الوظيفي، وعدد سنوات الخبرة، والمؤهل الدراسي، والشهادات المهنية، وعدد المتخصصين بقسم تكنولوجيا المعلومات وجود فروق ذات دلالة إحصائية

لدى أفراد عينة الدراسة تبعاً لجهة العمل حيث كانت مستوى الدلالة الإحصائية Sig (٠,٠٠) < مستوى المعنوية α (٠,٠٥) وعندها قيمة (ف) المحسوبة تساوي ٥,٦٧٨، وأنه لا توجد فروق ذات دلالة إحصائية لدى أفراد عينة الدراسة تبعاً للمسمى الوظيفي حيث أن مستوى الدلالة الإحصائية Sig (٠,٦٨٤) > مستوى المعنوية α (٠,٠٥) وعندها قيمة (ف) المحسوبة تساوي ٠,٥٧٢ والسبب في ذلك تقارب قيمة المتوسطات، كما أنه توجد فروق ذات دلالة إحصائية لدى أفراد عينة الدراسة تبعاً لسنوات الخبرة حيث أن مستوى الدلالة الإحصائية Sig (٠,٠٢٥) < مستوى المعنوية α (٠,٠٥) وعندها قيمة (ف) المحسوبة تساوي ٣,٢٨٧، كما أنه لا توجد فروق ذات دلالة إحصائية لدى أفراد عينة الدراسة تبعاً للمؤهل الدراسي حيث أن مستوى الدلالة الإحصائية Sig (٠,١٤٨) > مستوى المعنوية α (٠,٠٥) وعندها قيمة (ف) المحسوبة تساوي ١,٩٥٦ والسبب في ذلك تقارب قيمة المتوسطات، وكذلك لا توجد فروق ذات دلالة إحصائية لدى أفراد عينة الدراسة تبعاً للشهادات المهنية حيث أن مستوى الدلالة الإحصائية Sig (٠,٥١١) > مستوى المعنوية α (٠,٠٥) وعندها قيمة (ف) المحسوبة تساوي ٠,٨٢٨ والسبب في ذلك تقارب قيمة المتوسطات، وأخيرا توجد فروق ذات دلالة إحصائية لدى أفراد عينة الدراسة تبعاً نسبة لعدد المتخصصين بقسم تكنولوجيا المعلومات حيث أن مستوى الدلالة الإحصائية Sig (٠,٠٠) < مستوى المعنوية α (٠,٠٥) وعندها قيمة (ف) المحسوبة تساوي ٨,٢١٤.

ولمعرفة سبب الفروقات في نتائج تحليل التباين لمفردات العينة من حيث جهة العمل وسنوات الخبرة وعدد المتخصصين بقسم تكنولوجيا المعلومات تم استخدام اختبار المقارنات البعدية Multiple Comparisons (Scheffe) الذي يوضح سبب وماهية الفروق الدالة إحصائياً، حيث أوضحت نتائج التحليل البعدي شيفيه أن الفرق في المتوسطات بين العاملين بشركة تداول أوراق مالية والعاملين بشركة التسويق الالكتروني بفارق معنوي ٠,٥٩٢٩٧، والعاملين بشركة الاتصالات والعاملين بشركة التسويق الالكتروني بفارق معنوي ٠,٧٠٦٢٥ ، وجاءت القيم الاحتمالية (٠,٠٠٦)، (٠,٠٠) على التوالي < قيمة α (٠.٠٥) مما يوضح أنه دال إحصائياً، أما سبب الفروق فترجع إلى العاملين بشركة الاتصالات حيث لديهم أكبر متوسط حسابي ٤,٣٧٥٠ بقيمة احتمالية ٠,٠٣٥ < قيمة α (٠.٠٥) دال احصائياً، وأن الفرق بين من لديهم (١٠) سنوات وأقل من (١٥) سنة خبرة والذين لديهم (١٥) سنه خبرة أو أكثر بفارق معنوي ٠,٣٤٢٦٦ وقيمة احتمالية ٠,٠٣٥ ، ويرجع سبب الفروق إلى من لديهم خبرة (١٥) سنه وأكثر حيث لديهم أكبر متوسط حسابي ٤,٢٧٤٦ بقيمة احتمالية ٠,٠٣٥ < قيمة α (٠.٠٥) مما يوضح أنه دال احصائياً، كما أن الفرق بين المتوسطات في الشركات التي لديها عدد المتخصصين العاملين بقسم تكنولوجيا المعلومات (٥) وأقل من (١٠) والتي لديها (١٥) أو أكثر بفارق معنوي ٠,٧٨٠٢٧، وعدد المتخصصين العاملين بقسم تكنولوجيا المعلومات (١٠) وأقل من (١٥) والتي لديها (١٥) أو أكثر بفارق معنوي ٠,٦٠٨٤٠، وجاءت القيم الاحتمالية (٠,٠٠٢)، (٠,٠٠٥) على التوالي < قيمة α (٠.٠٥)، أما سبب الفروق فترجع إلى الشركات التي لديها عدد المتخصصين العاملين بقسم تكنولوجيا المعلومات (١٥) أو أكثر متخصص حيث لديهم أكبر متوسط حسابي ٤,٢٦٤٦ بقيمة احتمالية ٠,٠٠٥ < قيمة α (٠.٠٥) مما يوضح أنه دال احصائياً.

توضح النتائج السابقة قبول الفرض الأول للدراسة حيث يؤثر تطبيق حوكمة تكنولوجيا المعلومات إيجابياً وبشكل جوهري على حماية أمن المعلومات باستخدام إطار COBIT 2019، وإصدارات معيار ISO ذات الصلة، بدرجة ثقة ٩٥%.

٨-٧-٢: اختبار الفرض الثاني للبحث:

ينص الفرض الثاني على أنه: "توجد علاقة ذات دلالة احصائية بين تطبيق آليات حوكمة تكنولوجيا المعلومات وتحسين الأداء المالي وغير المالي للشركات".

ولاختبار الفرض الثاني تم صياغة عدد (٩) أسئلة تشمل أسئلة المحور الثاني من قائمة الاستبيان، ويوضح الجدول رقم (٨) نتائج التحليل الوصفي لإجابات عينة الدراسة على المحور الثاني والتي توضح التكرارات والوسط الحسابي والانحراف المعياري والنسب المئوية الخاصة بدراسة أثر تطبيق آليات حوكمة تكنولوجيا المعلومات على تحسين الأداء المالي وغير المالي للشركات.

رقم السؤال	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	الوسط الحسابي	الانحراف المعياري	الاتجاه العام	الترتيب
	العدد	العدد	العدد	العدد	العدد				
	%	%	%	%	%				
١٧	٣٠	٣٦	١٩	-	-	٤,١٣	٠,٧٥٢٥	موافق	٥
	%٣٥,٣	%٤٢,٢	%٢٢,٤	-	-				
١٨	٢٠	٤٦	١٥	٤	-	٣,٩٦	٠,٧٧٨٣	موافق	٨
	%٢٣,٥	%٥٤,١	%١٧,٦	%٤,٧	-				
١٩	٢٦	٤٦	١٣	-	-	٤,١٥	٠,٦٦٣٧	موافق	٤
	%٣٠,٦	%٥٤,١	%١٥,٣	-	-				
٢٠	٣٣	٤٠	٩	٣	-	٤,٢١	٠,٧٧٢٩	موافق بشدة	٢
	%٣٨,٨	%٤٧,١	%١٠,٦	%٣,٥	-				
٢١	٢٥	٣٧	٢٣	-	-	٤,٠٢	٠,٧٥٥٥	موافق	٧
	%٢٩,٤	%٤٣,٥	%٢٧,١	-	-				
٢٢	٣٢	٤٠	١١	٢	-	٤,٢٠	٠,٧٥٢٧	موافق بشدة	٣
	%٣٧,٦	%٤٧,١	%١٢,٩	%٢,٤	-				
٢٣	٣٣	٣٩	١٢	١	-	٤,٢٢	٠,٧٢٩٩	موافق بشدة	١
	%٣٨,٨	%٤٥,٩	%١٤,١	%١,٢	-				
٢٤	١٩	٤٤	١٦	٦	-	٣,٨٩	٠,٨٣١٢	موافق	٩
	%٢٢,٤	%٥١,٨	%١٨,٨	%٧,١	-				
٢٥	٢٧	٤٣	١٢	٢	١	٤,٠٩	٠,٨١٠٩	موافق	٦
	%٣١,٨	%٥٠,٦	%١٤,١	%٢,٤	%١,٢				
الوسط الحسابي المرجح للمحور الثاني				٤,٠٩٩٣	٠.٥٤١٩		موافق		

جدول (٨): نتائج التحليل الوصفي لأسئلة المحور الثاني

يتضح من الجدول رقم (٨) أن المتوسط العام لهذا المحور هو (**٤,٠٩٩٣**) عند درجة انحراف معياري (**٠,٥٤١٩**)، مما يدل على أن آراء عينة الدراسة تتجه للموافقة على الأسئلة التي تختبر الفرض الثاني والتي تتعلق بدراسة أثر تطبيق آليات حوكمة تكنولوجيا

المعلومات على تحسين الأداء المالي وغير المالي للشركات، بمعنى أنه يوجد أثر إيجابي لتطبيق آليات حوكمة تكنولوجيا المعلومات على تحسين الأداء المالي وغير المالي للشركات.

وتم استخدام اختبار الإشارة Sign Test لاختبار **الفرض الثاني للدراسة**. نظراً لأن عينة الدراسة لا تتبع التوزيع الطبيعي فيما يخص المحور الثاني، فتم اختيار أحد الاختبارات اللامعلمية المناسبة وهو اختبار الإشارة لاختبار أثر تطبيق آليات حوكمة تكنولوجيا المعلومات على تحسين الأداء المالي وغير المالي للشركات ويوضح الجدول رقم (٩) نتائج اختبار الإشارة Sign Test.

جدول (٩): اختبار الإشارة Sign Test للفرض الثاني

المحور	المجموعات	الفئات	حجم العينة	النسبة المشاهدة	نسبة الاختبار	مستوى الدلالة الإحصائية Sig
أثر تطبيق آليات حوكمة تكنولوجيا المعلومات على تحسين الأداء المالي وغير المالي للشركات	المجموعة ١	< أو = ٣,٤	٧٧	٠,٩١	٠,٥٠	٠,٠٠٠
	المجموعة ٢	> ٣,٤ =	٨	٠,٠٩		
	الكلي		٨٥	١,٠٠		

يتضح من الجدول رقم (٩) أن مستوى الدلالة الاحصائية sig (٠,٠٠٠) < مستوى المعنوية α (٠,٠٥) لذلك يمكن قبول الفرض الثاني للدراسة والذي يفترض أن تطبيق آليات حوكمة تكنولوجيا المعلومات يؤثر إيجابياً على تحسين الأداء المالي والأداء غير المالي للشركات، بدرجة ثقة ٩٥%.

ولقياس مستوى معنوية الفرق بين آراء العينة المشتركة في الدراسة بشأن الفرض الثانى، فقد تم استخدام **اختبار كروسكال واليس** (Kruskal-Wallis Test) اللامعلمي وهو اختبار بديل للاختبار المعلمي ANOVA، حيث يساعد قياس المعنوية في التعرف على الإستعدادات الكامنة لدى أفراد الفئات الخاصة ومن ثم التركيز عليها وتطويرها، كما تساعد القائمين على إعداد القوانين والمعايير بما يراعى إستعدادات وقدرات العاملين في مجال تكنولوجيا المعلومات ومراعاة حاجاتهم الأساسية لتحقيق حماية كافية لأمن المعلومات. وقد أوضحت نتائج اختبار كروسكال واليس (Kruskal-Wallis Test) للفرض الثاني تبعاً للمسمى الوظيفي، وعدد سنوات الخبرة، والمؤهل الدراسي، والشهادات المهنية، وعدد المتخصصين بقسم تكنولوجيا المعلومات وجود فروق ذات دلالة إحصائية لدى أفراد عينة الدراسة تبعاً لجهة العمل حيث أن مستوى الدلالة

الإحصائية Sig (٠,٠٥) = مستوى المعنوية α (٠,٠٥) وعندها قيمة كروسكال واليس تساوي ٩,٤٧٤٥، وأنه لا توجد فروق ذات دلالة إحصائية لدى أفراد عينة الدراسة تبعاً للمسمى الوظيفي حيث أن مستوى الدلالة

الإحصائية Sig (٠,٤٥٧) > مستوى المعنوية α (٠,٠٥) وعندها قيمة كروسكال واليس تساوي ٣,٦٤٠ والسبب في ذلك تقارب قيمة المتوسطات، كما أنه لا توجد فروق ذات دلالة إحصائية لدى أفراد عينة الدراسة تبعاً لسنوات الخبرة حيث أن مستوى الدلالة الإحصائية Sig (٠,٢٨١) > مستوى المعنوية α (٠,٠٥) وعندها قيمة كروسكال واليس تساوي ٣,٨٢١ والسبب في ذلك تقارب قيمة المتوسطات، كما أنه لا توجد فروق ذات دلالة إحصائية لدى أفراد عينة الدراسة تبعاً للمؤهل الدراسي حيث أن مستوى الدلالة الإحصائية Sig (٠,٢٨١) > مستوى المعنوية α (٠,٠٥) وعندها قيمة كروسكال واليس تساوي ٢,٥٤٠ والسبب في ذلك تقارب قيمة المتوسطات، وكذلك لا توجد فروق ذات دلالة إحصائية لدى أفراد عينة الدراسة تبعاً للشهادات المهنية حيث أن مستوى الدلالة الإحصائية Sig (٠,٠٧٤) > مستوى المعنوية α (٠,٠٥) وعندها قيمة كروسكال واليس تساوي ٨,٤٤٧ والسبب في ذلك تقارب قيمة المتوسطات، وأخيرا لا توجد فروق ذات دلالة إحصائية لدى أفراد عينة الدراسة تبعاً نسبة لعدد المتخصصين بقسم تكنولوجيا المعلومات حيث أن مستوى الدلالة الإحصائية Sig (٠,١٨٦) > مستوى المعنوية α (٠,٠٥) وعندها قيمة كروسكال واليس تساوي ٤,٨١٦ والسبب في ذلك تقارب قيمة المتوسطات.

ولمعرفة سبب الفروقات في نتائج التباين لمفردات العينة من حيث جهة العمل الذي يوضح سبب وماهية الفروق الدالة إحصائياً تم اختبار المقارنات البعدية Mann Whitney الذي يعقد مقارنة ثنائية بين كل جهتين عمل، وتوضح نتائج التحليل البعدي مان ويتني أن القيمة الاحتمالية للعاملين بالبنك نسبة إلى العاملين بشركة التسويق الالكتروني ٠,٠٠٥، والقيمة الاحتمالية للعاملين بشركة تكنولوجيا المعلومات نسبة إلى العاملين بشركة التسويق الالكتروني ٠,٠٤٨، والقيمة الاحتمالية للعاملين بشركة تداول الأوراق المالية نسبة إلى العاملين بشركة التسويق الالكتروني ٠,٠٣٠، والقيمة الاحتمالية للعاملين بشركة الاتصالات نسبة إلى العاملين بشركة التسويق الالكتروني ٠,٠٠٩ < مستوى المعنوية α (٠,٠٥) مما يوضح أنه دال إحصائياً، ويوضح التحليل السابق أن السبب في الفروق في الدلالة الإحصائية يرجع إلى العاملين بشركة التسويق الالكتروني.

يتضح من النتائج السابقة قبول الفرض الثاني للدراسة حيث يؤثر تطبيق آليات حوكمة تكنولوجيا المعلومات إيجابياً وبشكل جوهري على تحسين الأداء المالي والأداء غير المالي للشركات، بدرجة ثقة ٩٥%.

٨-٧-٣: اختبار الفرض الثالث للبحث:

ينص الفرض الثالث على أنه: "تؤثر حماية أمن المعلومات الناتجة من تطبيق آليات حوكمة تكنولوجيا المعلومات على تحسين الأداء المالي والأداء غير المالي للشركات".

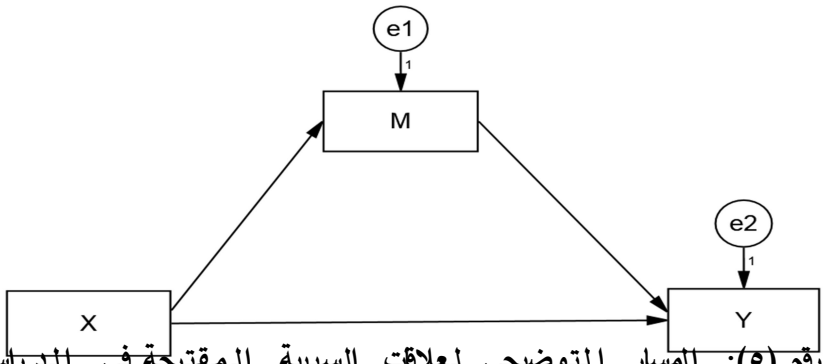
ولاختبار الفرض الثالث تم صياغة عدد (٩) أسئلة تشمل أسئلة المحور الثالث من قائمة الاستبيان، ويوضح الجدول رقم (١٠) نتائج التحليل الوصفي لإجابات عينة الدراسة على المحور الثالث.

جدول (١٠): نتائج التحليل الوصفي لأسئلة المحور الثالث

رقم السؤال	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	الوسط الحسابي	الانحراف المعياري	الاتجاه العام	الترتيب
	العدد	العدد	العدد	العدد	العدد				
	%	%	%	%	%				
٢٦	٣٠	٤٤	٩	٢	-	٤,٢٠	٠,٧٢٠٤	موافق بشدة	٥
	%٣٥,٣	%٥١,٨	١٠,٦ %	%٢,٤	-				
٢٧	٣٥	٣٣	٨	٨	١	٤,٠٩	٠,٩٩٥٥	موافق	٨
	%٤١,٢	%٣٨,٨	%٩,٤	%٩,٤	%١,٢				
٢٨	٢٩	٤١	١٥	-	-	٤,١٦	٠,٧٠٤٥	موافق	٦
	%٣٤,١	%٤٨,٢	١٧,٦ %	-	-				
٢٩	٣٦	٣٩	١٠	-	-	٤,٣١	٠,٦٧٣٠	موافق بشدة	٢
	%٤٢,٤	%٤٥,٩	١١,٨ %	-	-				
٣٠	٤٦	٢٩	٧	٣	-	٤,٣٩	٠,٧٨٨٢	موافق بشدة	١
	%٥٤,١	%٣٤,١	%٨,٢	%٣,٥	-				
٣١	٣٤	٣٢	١٠	٩	-	٤,٠٧	٠,٩٧٣٣	موافق	٩
	%٤٠,٠	%٣٧,٦	١١,٨ %	١٠,٦ %	-				
٣٢	٢٨	٣٩	١٧	١	-	٤,١١	٠,٧٥٦٢	موافق	٧
	%٣٢,٩	%٤٥,٩	٢٠,٠ %	%١,٢	-				
٣٣	٣٣	٤٤	٨	-	-	٤,٢٩	٠,٦٣٢٩	موافق بشدة	٣
	%٣٨,٨	%٥١,٨	%٩,٤	-	-				
٣٤	٣٤	٤٠	٨	٣	-	٤,٢٤	٠,٧٦٦٠	موافق بشدة	٤
	%٤٠,٠	%٤٧,١	%٩,٤	%٣,٥	-				
الوسط الحسابي المرجح للمحور الثالث				٤,٢٠ ٦٥	٠,٥٩٢ ٧	موافق بشدة			

يتضح من الجدول (١٠) أن المتوسط العام لهذا المحور هو **(٤,٢٠٦٥)** عند درجة انحراف معياري **(٠,٥٩٢٧)**، مما يدل على أن آراء عينة الدراسة تتجه للموافقة بشدة على الأسئلة التي تختبر الفرض الثالث والتي تتعلق بدراسة أثر حماية أمن المعلومات الناتجة من تطبيق آليات حوكمة تكنولوجيا المعلومات على تحسين الأداء المالي والأداء غير المالي للشركات.

بإجراء تحليل المسار Path analysis لبيان العلاقة السببية بين حوكمة تكنولوجيا المعلومات (X) كمتغير مستقل، والأداء المالي وغير المالي للشركات كمتغير تابع (Y) وحماية أمن المعلومات كمتغير وسيط (M). ويوضح الشكل رقم (٥) المسار التوضيحي لعلاقات السببية المقترحة في الدراسة.



الشكل رقم (٥): المسار التوضيحي لعلاقات السببية المقترحة في الدراسة

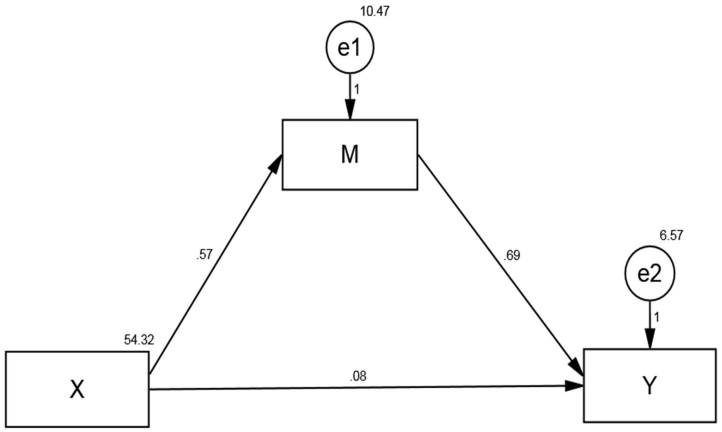
ولإيجاد تحليل المسار بين المتغيرات الثلاثة تم أولاً إيجاد معامل الارتباط البسيط بين متغيرات الدراسة، ويوضح الجدول رقم (١١) نتائج معامل الارتباط البسيط لبيرسون بين المتغير المستقل والمتغير التابع (X,Y) حيث يساوي (٠,٧١٤) بمستوى دلالة إحصائية Sig (٠,٠٠٠) < مستوى المعنوية α (٠,٠١) ونستنتج من ذلك وجود علاقة طردية قوية بين المتغيرين. كما يتضح أن معامل الارتباط بين المتغيرين (X,M) يساوي (٠,٧٩٢) بمستوى دلالة إحصائية Sig (٠,٠٠٠) < مستوى المعنوية α (٠,٠١) ونستنتج من ذلك وجود علاقة طردية قوية بينهما. كذلك يتضح أن معامل الارتباط بين المتغيرين (Y,M) يساوي (٠,٨٤٦) بمستوى دلالة إحصائية Sig (٠,٠٠٠) < مستوى المعنوية α (٠,٠١) ونستنتج من ذلك وجود علاقة طردية قوية بين المتغيرين.

جدول رقم (١١): معامل الارتباط بيرسون بين المتغيرات الثلاثة

م	مسار الارتباط	قيمة معامل الارتباط	تفسير النتيجة
١	الارتباط بين (X) و(Y)	٠,٧١٤ (**)	يوجد ارتباط قوي ذو دلالة احصائية عند مستوى معنوية ٠,٠١
٢	الارتباط بين (X) و(M)	٠,٧٩٢ (**)	يوجد ارتباط قوي ذو دلالة احصائية عند مستوى معنوية ٠,٠١
٣	الارتباط بين (M) و (Y)	٠,٨٤٦ (**)	يوجد ارتباط قوي ذو دلالة احصائية عند مستوى معنوية ٠,٠١

تعنى علامة (**) أن الارتباط ذو دلالة احصائية عند مستوى معنوية ٠,٠١

ويوضح الشكل رقم (٦) الرسم التخطيطي بعد إيجاد قيم المسارات باستخدام برنامج (IBM-SPSS-AMOS25).



الشكل رقم (٦): نتائج تحليل المسار

ويتضح من تحليل المسار السابق أن المتغير المستقل (X) يؤثر في المتغير الوسيط (M) بمعدل (٠,٥٧) ويعني ذلك أنه كلما زاد (X) بوحدة واحدة زاد (M) بمقدار (٠,٥٧)، كما يؤثر في المتغير التابع (Y) بمعدل (٠,٨) ويعني ذلك أنه كلما زاد (X) بوحدة واحدة زاد (Y) بمقدار (٠,٨)، وكذلك يؤثر (M) في (Y) بمعدل (٠,٦٩) ويعني ذلك أنه كلما زاد (M) بوحدة واحدة زاد (Y) بمقدار (٠,٦٩). كما يتضح من تحليل المسار أن CMNI = (٠,٠٠٠)، وقيمة RMSEA = ٠,٨٦٢ وتشير هذه النتائج إلى أن هذا النموذج يتمتع بدرجة عالية من القوة.

وقد تم **تحليل تأثير المتغير الوسيط باستخدام Bootstrapping In Mediation Effect**. ويوضح الجدول رقم (١٢) تحديد تأثير المتغير الوسيط سواء أكان تأثيراً كلياً Full Mediation ، أم تأثيراً جزئياً Partial Mediation في العلاقة بين المتغيرات.

جدول (١٢): التأثير المباشر وغير المباشر للمتغير الوسيط

التأثير المباشر		التأثير غير المباشر		التأثير الكلي		الدلالة الإحصائية			
M	X		M	X		M	X		
٠,٠٠٠	٠,٥٧٠	M	٠,٠٠٠	٠,٠٠٠	M	٠,٥٧٠	٠,٠٠٠	M	M
٠.٦٨٩	٠,٠٧٧	Y	٠,٠٠٠	٠,٣٩٣	Y	٠,٦٨٩	٠.٤٦٩	Y	Y

توضح النتائج أن التأثير المباشر بين (X) ، (Y) يساوي ٠,٤٦٩، والتأثير غير المباشر ٠,٣٩٣ أما مستوى الدلالة الإحصائية Sig (٠,٠٠٧) < مستوى المعنوية α (٠,٠٥) أي أنه دال إحصائيا، وهذا يعني أن المتغير الوسيط يؤثر تأثيراً جزئيا Partial Mediation مما يوضح أن المتغير الوسيط لم يحمل كل تأثير المتغير المستقل على المتغير التابع وله تأثير ذو دلالة إحصائية.

ولمزيد من التحليل تم إجراء تحليل التباين أحادي الاتجاه (One-Way ANOVA Test)

لقياس مستوى معنوية الفرق بين آراء العينة المشتركة في الدراسة من حيث جهة العمل، والمسمى الوظيفي، وعدد سنوات الخبرة، والمؤهل الدراسي، والشهادات المهنية الحاصل عليها عينة الدراسة، وعدد المتخصصين في قسم تكنولوجيا المعلومات، حيث يساعد قياس المعنوية في التعرف على الإستعدادات الكامنة لدى أفراد الفئات ومن ثم التركيز عليها وتطويرها، كما تساعد القائمين على إعداد القوانين والمعايير بما يراعى إستعدادات وقدرات العاملين في مجال تكنولوجيا المعلومات ومراعاة حاجاتهم الأساسية لتحقيق حماية كافية لأمن المعلومات. وأوضحت نتائج تحليل التباين الأحادي ANOVA للفرض الثالث تبعاً للمسمى الوظيفي، وعدد سنوات الخبرة، والمؤهل الدراسي، والشهادات المهنية، وعدد المتخصصين بقسم تكنولوجيا المعلومات وجود فروق ذات دلالة إحصائية لدى أفراد عينة الدراسة تبعاً لجهة العمل حيث أن مستوى الدلالة الإحصائية Sig (٠,٠٢٣) < مستوى المعنوية α (٠,٠٥) وعندها قيمة (ف) المحسوبة تساوي ٣,٠٠٢، وأنه لا توجد فروق ذات دلالة إحصائية لدى أفراد عينة الدراسة تبعاً للمسمى الوظيفي حيث أن مستوى الدلالة الإحصائية Sig (٠,٢٧٤) > مستوى المعنوية α (٠,٠٥) وعندها قيمة (ف) المحسوبة تساوي ١,٣٠٩ والسبب في ذلك تقارب قيمة المتوسطات، كما أنه لا توجد فروق ذات دلالة إحصائية لدى أفراد عينة الدراسة تبعاً لسنوات الخبرة حيث أن مستوى الدلالة الإحصائية Sig (٠,٠٨٧) > مستوى المعنوية α (٠,٠٥) وعندها قيمة (ف) المحسوبة تساوي ٢,٢٧١ والسبب في ذلك تقارب قيمة المتوسطات، كما أنه توجد فروق ذات دلالة إحصائية لدى أفراد عينة الدراسة تبعاً للمؤهل الدراسي حيث أن مستوى الدلالة الإحصائية Sig (٠,٠٤٣) < مستوى المعنوية α (٠,٠٥) وعندها قيمة (ف) المحسوبة تساوي ٣,٢٦٩، وكذلك لا توجد فروق ذات دلالة إحصائية لدى أفراد عينة الدراسة تبعاً للشهادات المهنية حيث أن مستوى الدلالة الإحصائية Sig (٠,١١٠) > مستوى المعنوية α (٠,٠٥) وعندها قيمة (ف) المحسوبة تساوي ١,٩٥٠ والسبب في ذلك تقارب قيمة المتوسطات، وأخيرا لا توجد فروق ذات دلالة إحصائية لدى أفراد عينة الدراسة تبعاً نسبة لعدد المتخصصين بقسم تكنولوجيا المعلومات حيث أن مستوى الدلالة الإحصائية Sig (٠,١٨٩)

> مستوى المعنوية α (٠,٠٥) وعندها قيمة (ف) المحسوبة تساوي ١,٦٣١ والسبب في ذلك تقارب قيمة المتوسطات.

ولمعرفة سبب الفروقات في نتائج تحليل التباين لمفردات العينة من حيث جهة العمل والمؤهل الدراسي تم اختبار المقارنات البعدية Multiple Comparisons (Scheffe) الذي يوضح سبب وماهية الفروق الدالة إحصائياً. وقد أوضحت نتائج التحليل البعدي شيفيه أن الفرق في المتوسطات بين العاملين بالبنك والعاملين بشركة التسويق الالكتروني بفارق معنوي ٠,٦٦٨٨٩، والعاملين بشركة تداول أوراق مالية والعاملين بشركة التسويق الالكتروني بفارق معنوي ٠,٦٨٦١١ ، والعاملين بشركة اتصالات والعاملين بشركة التسويق الالكتروني بفارق معنوي ٠,٦٥٢٣٨، وجاءت القيم الاحتمالية (٠,٠١٩)، (٠,٠٢٩)، (٠,٠٢٨) على التوالي < مستوى المعنوية α (٠,٠٥)، أما سبب فروق الدالة إحصائياً يرجع للعاملين بشركة تداول الأوراق المالية حيث لديهم أكبر متوسط حسابي ٤,٣١٩٤ بقيمة احتمالية ٠,٠٢٩ < مستوى المعنوية α (٠,٠٥) مما يوضح أنه دال احصائياً.

كما أن الفرق بين الحاصلين على درجة بكالوريوس والحاصلين على دبلوم دراسات عليا بفارق معنوي ٠,٤٠٥٤٨، وجاءت القيمة الاحتمالية ٠,٠٣٧، ويرجع سبب الفروق إلى الحاصلين على درجة بكالوريوس حيث لديهم أكبر متوسط حسابي ٤,٣٢٠٥ بقيمة احتمالية ٠,٠٣٧ < مستوى المعنوية α (٠,٠٥) مما يوضح أنه دال احصائياً.

توضح النتائج السابقة قبول الفرض الثالث للدراسة حيث تؤثر حماية أمن المعلومات الناتجة من تطبيق آليات حوكمة تكنولوجيا المعلومات إيجابياً وبشكل جوهري على تحسين الأداء المالي والأداء غير المالي للشركات، بدرجة ثقة ٩٥%.

٩: الخلاصة والتوصيات:

يتمثل الهدف الرئيسي للدراسة في **دراسة واختبار** أثر حوكمة تكنولوجيا المعلومات كمدخل لحماية أمن المعلومات على الأداء المالي وغير المالي للشركات، وذلك في عينة من الشركات العاملة في بيئة الأعمال المصرية، ولتحقيق هذا الهدف تناول البحث ماهية الدور الذى تقدمه حوكمة تكنولوجيا المعلومات في تحقيق حماية أمن المعلومات في الشركات باستخدام إطار COBIT 2019، وإصدارات معيار ISO ذات الصلة. وأثر تطبيق آليات حوكمة تكنولوجيا المعلومات على تحسين الأداء المالي والأداء غير المالي للشركات. ثم تناول البحث الأثر الواقع على الأداء المالي وغير المالي للشركات في ظل توافر الحماية الكافية للمعلومات المحاسبية والتي تقدمه أمن المعلومات جراء تطبيق حوكمة تكنولوجيا المعلومات.

وقد توصل البحث فى شقه النظري إلى أن المعطيات الحالية للمتغيرات الحادثة في العالم ألزم الدول والمجتمعات بالتوجه بشكل كامل للاستثمار في المجال التكنولوجي والاعتماد على تكنولوجيا المعلومات والذي بدونه لا تستطيع أي شركة على اختلاف نشاطاتها الاستمرار في الأسواق المختلفة سواء أكانت محلية أو عالمية. وأن عدم تطبيق مبادئ وأهداف حوكمة تكنولوجيا المعلومات وكذلك عدم تحديد السياسات الأمنية فيما يتعلق بحماية المعلومات ربما يؤدي لتفاقم المخاطر التي تتعرض لها المعلومات المحاسبية الالكترونية، وينجم عن ذلك انحسار درجة الأمان التي يجب أن تتواجد بالمعلومات

المحاسبية الالكترونية المقدمة من الشركات لأصحاب المصالح والتي تساعدهم في اتخاذ القرارات الاستثمارية بالشركات المختلفة.

ويعد تطبيق آليات حوكمة تكنولوجيا المعلومات (الآلية الهيكلية والآليات العلاقية وآلية العمليات) من المميزات التي من الممكن أن تنقل الشركات التي تطبقها إلى مستوى أعلى من الشركات الأخرى المنافسة في السوق، ويتبع ذلك ارتفاع في الربحية وتحقيق ميزة تنافسية وقيمة مضافة. كما تلعب حوكمة تكنولوجيا المعلومات دوراً قوياً ولا يستهان به في تطوير العمليات التشغيلية، فهو يؤدي إلى فعالية اتخاذ القرارات مما يترتب عليه تحسين الأداء المالي وغير المالي للشركات.

وتعد أمن المعلومات المحاسبية من أهم العناصر التي تحرص عليها جميع الشركات بمجالاتها المختلفة، ويمثل العاملين في تلك الشركات من أهم العناصر التي يجب اختيارهم وتدريبهم لمواجهة الاختراقات وسرقة البيانات. ويؤدي التطبيق الجيد للمنهجية والمبادئ والقواعد التي تتبعها حوكمة تكنولوجيا المعلومات إلى الوصول لحماية أمن المعلومات. فقد تحولت إجراءات أمن المعلومات التكنولوجية السياسة الأمنية إلى إجراءات تشغيلية على أرض الواقع حيث أنها عبارة عن إجراءات للسيطرة على المخاطر التي تحدق بالمعلومات المحاسبية الإلكترونية من تهيئة الأجهزة الالكترونية وتثبيط البرامج المضادة للفيروسات، والجدار الناري المضاد للقرصنة الإلكترونية.

وقد أوجب الأهمية الكبيرة لمواجهة إدارة مخاطر تكنولوجيا المعلومات وضع أطر لمواجهة تلك المخاطر، وقد وضعت جمعية مراجعة ومراقبة نظم المعلومات (ISACA) إطار COBIT والذي دوره هو تحديد الخطة الاستراتيجية لتكنولوجيا المعلومات لضمان الخدمة المستمرة ومراقبة أداء حوكمة تكنولوجيا المعلومات، وتطبيق آليات حوكمة تكنولوجيا المعلومات بشكل يؤدي في النهاية لنجاح أهداف الشركة. كما يعمل معيار ISO/IEC-27001 كمعيار لإدارة أمن المعلومات على وضع الضوابط الأمنية، والمساعدة على إدارة مخاطر تكنولوجيا المعلومات.

وقد أجرى هذا البحث دراسة ميدانية اعتمدت على آراء عينة مكونة من (٨٥) فرد من العاملين بالشركات العاملة بمجال تكنولوجيا المعلومات كشركات الاتصالات، والشركات الخدمية كشركات التسويق الإلكتروني، والمؤسسات المالية كالبنوك والاستثمار في تداول الأوراق المالية العاملين في البيئة المصرية، وكانت النتائج كالتالى:

١. توجد علاقة إيجابية وجوهرية بين تطبيق حوكمة تكنولوجيا المعلومات وتحقيق حماية أمن المعلومات باستخدام إطار COBIT 2019، وإصدارات معيار ISO ذات الصلة بدرجة ثقة ٩٥%.
٢. توجد علاقة إيجابية وجوهرية بين تطبيق آليات حوكمة تكنولوجيا المعلومات وتحسين الأداء المالي والأداء غير المالي للشركات بدرجة ثقة ٩٥%.
٣. تؤثر حماية أمن المعلومات الناتجة من تطبيق حوكمة تكنولوجيا المعلومات إيجابياً وبشكل جوهري على تحسين الأداء المالي والأداء غير المالي للشركات بدرجة ثقة ٩٥%.

ومما سبق عرضه من نتائج يتضح مدى أهمية موضوع البحث في الواقع العملي، ومن ثم يمكن التوصية بما يلي:

١- ضرورة اهتمام الإدارة العليا بوضع ميزانية متوافقة لمواكبة التحديثات الدائمة للتكنولوجيا الحديثة وترقية البنية التحتية لتكنولوجيا المعلومات وفقاً لتلك التطورات.

٢- أهمية عقد دورات تدريبية لتعريف الكوادر البشرية بالأطر والمعايير الدولية وكيفية تطبيقها والاستفادة منها استفادة قصوى في الواقع العملي بالشركات المختلفة.

٣- ضرورة اهتمام الإدارة العليا بالشركات بوضع خطط لحماية البيانات والمعلومات من القرصنة من خلال توفير الكوادر البشرية المدربين لتحديث برامج الحماية، وتغيير كلمات المرور، وبرامج الفيروسات، واستخدام الجدار الناري لمواجهة القرصنة الالكترونية.

٤- توعية الإدارة العليا بالشركات بأهمية حوكمة تكنولوجيا المعلومات وتطبيقها في جميع الشركات واعتبارها من العناصر المهمة عند وضع خططها الاستراتيجية.

٥- ضرورة تدخل الجهات الرقابية كالهيئة العامة للرقابة المالية لمراقبة تطبيق حوكمة تكنولوجيا المعلومات ومتابعة التطورات التكنولوجية المعاصرة.

٦- ضرورة إضافة موضوع حوكمة تكنولوجيا المعلومات إلى المناهج الدراسية بكليات التجارة.

١٠: مقترحات أبحاث مستقبلية:

١- وضع إطار مقترح لحوكمة تكنولوجيا المعلومات تطبيقاً على بيئة الأعمال المصرية.

٢- دراسة أثر جائحة فيروس كورونا على فعالية نظام أمن المعلومات المحاسبي.

٣- دراسة أثر الاستثمار في تكنولوجيا المعلومات على الأداء المالي وغير المالي للشركات في البيئة المصرية.

ا لمر اجع:

أولاً: ا لمر اجع ا لعربية:

اكريم، حمزة محمد محمود، (٢٠١٩)، أهمية حوكمة تكنولوجيا المعلومات في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية بالقطاع المصرفي: دراسة تطبيقية على المصارف التجارية الليبية، المجلة العلمية للدراسات التجارية والبيئية: كلية التجارة، جامعة قناة السويس، المجلد ١٠، العدد١ ، ص ص ١ – ٣٥.

البلقاسى، منال صبحى على، (٢٠١٨)، أثر تطبيق حوكمة تكنولوجيا المعلومات وفقا لـ Cobit5على مخاطر نظم المعلومات الالكترونية: دراسة ميدانية على المعاهد العالية الخاصة، المجلة المصرية للدراسات التجارية، كلية التجارة جامعة المنصورة، المجلد ٤٢، العدد١، ص ص ٧٨ – ١١٩.

الدليمى، خليل ابراهيم، وحمزة فتحى الشرع، (٢٠١٨)، أثر تطبيق نظام كوبيت Cobit فى كفاءة أنظمة الرقابة الداخلية فى الشركات الصناعية المساهمة العامة الأردنية، مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع، كلية الإمارات للعلوم التربوية، العدد ٢٧، ص ص ٣٥٩ – ٣٧٦.

بخيت، محمد بهاء الدين محمد، عز الدين، أسر حسن يوسف، (٢٠١٨)، تأثير نظم المعلومات المحاسبية الإلكترونية على الربحية – دراسة تطبيقية على الشركات الصناعية النشطة فى البورصة المصرية خلال الفترة من ٢٠٠٧–٢٠١٧، مجلة الاسكندرية للبحوث المحاسبية، كلية التجارة، جامعة الاسكندرية، العدد ٢، المجلد ٢.

بركات، عبد الله، وآخرون، (٢٠١٢)، قياس مستوى حاكمية تكنولوجيا المعلومات فى الشركات الصناعية باستخدام إطار عمل "أهداف الرقابة للمعلومات والتكنولوجيا المرتبطة بها": دراسة تطبيقية على الشركات الصناعية الأردنية، مجلة جامعة الملك سعود للعلوم الإدارية، جامعة الملك سعود، الرياض، المجلد ٢٤، العدد ٢، ص ص ١٨٣ – ٢١٣.

عبيد الله، فايزة محمود محمد، (٢٠٠٥)، إطار مقترح لتحسين جودة التقارير الخارجية عن أعمال المنشأة في ظل استخدام نظام قياس الأداء المتوازن: مع دراسة تطبيقية، رسالة دكتوراه غير منشورة، كلية التجارة، جامعة الاسكندرية، فرع دمنهور.

غنيمى، سامى محمد أحمد، (٢٠١٦)، دور حوكمة تكنولوجيا المعلومات فى تحسين جودة الأداء المالى وزيادة القدرة التنافسية بالبنوك المصرية: دراسة ميدانية، مجلة البحوث المحاسبية، كلية التجارة، جامعة طنطا، المجلد ١، العدد١، ص ص ١٦١ – ٢٠٢.

مراد، ممدوح هاشم محمد، (٢٠١٦)، تأثير حوكمة تكنولوجيا المعلومات على الأداء المالي والقدرة التنافسية في الشركات المساهمة المصرية: دراسة إمبريقية. مجلة البحوث التجارية: كلية التجارة، جامعة الزقازيق المجلد ٣٨، العدد٢، ص ص ٢٦٩ – ٣٠٢.

نصيف، عمر بن عبدالله عمر، (٢٠١٢)، دور المعيار الدولى (أيزو ٢٧٠٠١) فى تعزيز كفاءة وفعالية أمن المعلومات بمنظمات الأعمال: دراسة استطلاعية على منظمات الأعمال بالمملكة العربية السعودية، المجلة العلمية للإدارة، كلية إدارة الأعمال، جامعة الملك سعود، العدد ٧، ص ص ٦٧ – ١٠٨.

ثانياً: المراجع الأجنبية:

Abu-Musa, A. A. (2006). Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations. *Journal of King Saud University - Computer and Information Sciences*, *18*, 1–30. https://doi.org/10.1016/S1319-1578(06)80001-7

——————— (2009), Exploring COBIT Processes for ITG in Saudi Organization: An Empirical Study, The International journal of Digital Accounting Research, Vol. 9, Iss.15, pp.99-126.

Ahmad, K., & Zabri, S. M. (2016). The Application of Non-Financial Performance Measurement in Malaysian Manufacturing Firms. *Procedia Economics and Finance*, *35*(October 2015), 476–484. https://doi.org/10.1016/s2212-5671(16)00059-9

Al Skafy, H., Abdel, Z., & Al-Theebeh, H. (2012). The level of information technology governance in KULACOM-Jordan Company. In *Basic Research Journal of Business Management and Accounts* (Vol. 1, Issue 5).

Alber, N., & Nabil, M. (2015). The Impact of Information Security on Banks' Performance in Egypt. *International Journal of Economics and Finance*, *7*(9). https://doi.org/10.5539/ijef.v7n9p219

Alkhaldi, F. M., Hammami, S. M., & Uddin, M. A. (2017). Understating value characteristics toward a robust IT governance application in private organizations using COBIT framework. *International Journal of Engineering Business Management*, *9*, 1–8. https://doi.org/10.1177/1847979017703779

Alotaibi, M. Z. M., Alotibi, M. F. E., & Zraqat, O. M. F. (2021). The Impact of Information Technology Governance in Reducing Cloud Accounting Information Systems Risks in Telecommunications Companies in the State of Kuwait. *Modern Applied Science*, *15*(1), 143. https://doi.org/10.5539/mas.v15n1p143

Alreemy, Z., Chang, V., Walters, R., & Wills, G. (2016). Critical success factors (CSFs) for information technology governance (ITG). *International Journal of Information Management*, *36*(6). https://doi.org/10.1016/j.ijinfomgt.2016.05.017

Ashsifa, I., & Ali, S. (2019). The Effect of Information Technology Investment Governance on Information Technology Performance and Organizational Performance: a Case Study. *The Indonesian Journal of Accounting Research*, *22*(02). https://doi.org/10.33312/ijar.468

Avery, A., & Chandraskaren, R. (2016). Financial Performance Impacts of Information Security Breaches. *WISP 2016 Proceedings*.

Aziz, N. M., Salleh, H., & Mustafa, N. K. F. (2012). People critical success factors (CSFs) in Information Technology / Information System (IT / IS) implementation. *Journal of Design + Built*, *5*(1).

Bermejo, P. H. de S., Tonelli, A. O., Zambalde, A. L., Santos, P. A. dos, & Zuppo, L. (2014). Evaluating IT Governance Practices and Business and IT Outcomes: A quantitative Exploratory Study in Brazilian Companies. *Procedia Technology*, *16*, 849–857. https://doi.org/10.1016/j.protcy.2014.10.035

Bouayad, H., Benabbou, L., & Berrado, A. (2017). Towards an information technology governance framework selection: Criteria determination. *Proceedings of the International Conference on Industrial Engineering and Operations Management*, *1*, 2366–2377.

Bradley, R. V., Byrd, T. A., Pridmore, J. L., Thrasher, E., Pratt, R. M. E., & Mbarika, V. W. A. (2012). An empirical examination of antecedents and consequences of IT governance in US hospitals. *Journal of Information Technology*, *27*(2), 156–177. https://doi.org/10.1057/jit.2012.3

Chi, M., Zhao, J., George, J. F., Li, Y., & Zhai, S. (2017). The influence of inter-firm IT governance strategies on relational performance: The moderation effect of information technology ambidexterity. *International Journal of Information Management*, *37*(2), 43–53. https://doi.org/10.1016/j.ijinfomgt.2016.11.007

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers and Security*, *32*(June), 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Crowder, M. J., Kimber, A., Sweeting, T., & Smith, R. (1994). Statistical analysis of reliability data (Vol. 27). CRC Press. *Available at*: https://books.google.com.eg/books

De Haes, S., & van Grembergen, W. (2009). An Exploratory Study into IT Governance Implementations and its Impact on Business/IT Alignment. *Information Systems Management*, *26*(2), 123–137. https://doi.org/10.1080/10580530902794786

Dwivedi, R., & Wang, J. (2018). *Breaching Together : A Data Science Approach on Firms ' Correlated Risk in Information Security Breaching Together : A Data Science Approach on Firms ' Correlated Risk in Information Security*.

Fathoni, Putra, P., & Dinna, Y. H. (2020). *Information Security: Credit Service Application Analysis at Bank Indonesia*. *172*(Siconian 2019), 146–154. https://doi.org/10.2991/aisr.k.200424.022

Fatihudin, D., Jusni, & Mochklas, M. (2018). How measuring financial performance. *International Journal of Civil Engineering and Technology*, *9*(6), 553–557.

Hamdan, M. N. (2017). The Relationship between Network Security Policies and Audit Evidence Documentation: The Accounting Information Security Culture as a Mediator. *International Journal of Business and Management*, *12*(12), 168. https://doi.org/10.5539/ijbm.v12n12p168

Hamid, Z. A., & Sulaiman, H. (2016). COBIT benchmarking of system development governance for a government agency in Malaysia. *Journal of Theoretical and Applied Information Technology*, *89*(1), 1–10.

Haouam, D. (2020). IT governance impact on financial reporting quality using COBIT framework. *Global Journal of Computer Sciences: Theory and Research*, *10*(1), 1–10. https://doi.org/10.18844/gjcs.v10i1.4143

Hapsari, I. (2018). The Effect of Competitive Advantage Toward Financial Performance With Good Information Technology Governance As Moderating Variable *(An Empirical Studies on Commercial Banking Listed in Indonesia Stock Exchange)*. *XVII*(2), 1–9. http://jurnalnasional.ump.ac.id/index.php/kompartemen/

Herath, H. S. B., & Herath, T. C. (2014). IT security auditing: A performance evaluation decision model. *Decision Support Systems*, *57*(1), 54–63. https://doi.org/10.1016/j.dss.2013.07.010

Heyasat, H., Mubarak, S., & Evans, N. (2019). A framework for information security management in capital markets. *Proceedings of the 23rd Pacific Asia Conference on Information Systems: Secure ICT Platform for the 4th Industrial Revolution, PACIS 2019*, *NetDiligence 2016*.

Humphreys, E. (2018). The Future Landscape of ISMS Standards. *Datenschutz und Datensicherheit-DuD*, *42*(7), 421-423.

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2019). Security Awareness: The First Step in Information Security Compliance Behavior. *Journal of Computer Information Systems*, *0*(00), 1–12. https://doi.org/10.1080/08874417.2019.1650676

Information Systems Audit and Control Association. (2011). COBIT 5: A business framework for the governance and management of enterprise IT. Rolling Meadows, IL: ISACA. Available at: https://www.isaca.org/resources/cobit

International Organization for Standardization, ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls, Available at: https://www.iso.org.

ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements Available at: https://www.iso.org/standard/42103.html

IT Governance Institute. (2007). IT Governance Status Report. Available at: http://www.itgi.org/template_ITGI.cfm?Section=About_IT_Governance1&Templ

ITGI, I. (2003). Board Briefing on IT Governance,(2nded.). United States of America. Available at: http://www.itgi.org

Joshi, A., Bollen, L., & Hassink, H. De Haes, S., & Van Grembergen, W. (2018). Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role. *Information and Management*, *55*(3), 368–380. https://doi.org/10.1016/j.im.2017.09.003

Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. *International Journal of Accounting and Information Management*, *28*(2), 275–301. https://doi.org/10.1108/IJAIM-01-2019-0006

Khalil, S., & Belitski, M. (2020). Dynamic capabilities for firm performance under the information technology governance framework. *European Business Review*, *32*(2), 129–157. https://doi.org/10.1108/EBR-05-2018-0102

Khusna, Z., & Ali, S. (2020). Information Technology Governance in a Sharia Microfinance Institution: an Evaluation Based on Cobit 5 Framework. *Share: Jurnal Ekonomi Dan Keuangan Islam*, *9*(1), 22–47. https://doi.org/10.22373/share.v9i1.6288

King, K. E., Kenneth, K., & King, K. E. (2017). Examine The Relationship Between Information Technology Governance, Control Objectives For Information and Related Technologies, ISO 27001/27002, and Risk Management. *Dissertation*, *February*, 24.

Kong, H., Jung, S., Lee, I., & Yeon, S. J. (2015). Information security and organizational performance: Empirical study of Korean securities industry. *ETRI Journal*, *37*(2), 428–437. https://doi.org/10.4218/etrij.15.0114.1042.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Management Research Review Information security awareness and behavior: a theory-based literature review) " Information security awareness and behavior: a theory-based literature

review" Information security awareness and behavior: a theory-based. *Management Research Review*, *37*(4), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085.

Lunardi, G. L., Becker, J. L., Maçada, A. C. G., & Dolci, P. C. (2014). The impact of adopting IT governance on financial performance: An empirical analysis among Brazilian firms. *International Journal of Accounting Information Systems*, *15*(1), 66–81. https://doi.org/10.1016/j.accinf.2013.02.001

Maccani, G., Connolly, N., McLoughlin, S., Puvvala, A., Karimikia, H., & Donnellan, B. (2020). An emerging typology of IT governance structural mechanisms in smart cities. *Government Information Quarterly*, *37*(4), 101499. https://doi.org/10.1016/j.giq.2020.101499

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

Mataracioglu, T., & Ozkan, S. (2011). Governing information security in conjunction with COBIT and ISO 27001. arXiv preprint arXiv:1108.2150

Mayer, N., & De Smet, D. (2017). Systematic Literature Review and ISO Standards analysis to Integrate IT Governance and Security Risk Management. *International Journal for Infonomics*, *10*(1), 1255–1263. https://doi.org/10.20533/iji.1742.4712.2017.0154

Mikalef, P., Pateli, A., & van de Wetering, R. (2020). IT architecture flexibility and IT governance decentralisation as drivers of IT-enabled dynamic capabilities and competitive performance: The moderating effect of the external environment. *European Journal of Information Systems*, *00*(00), 1–29. https://doi.org/10.1080/0960085X.2020.1808541

Mithas, S., Tafti, A., Bardhan, I., & Goh, J. M. (2012). Information Technology and Firm Profitability. *MIS Quarterly*, *36*(1), 205–224. https://misq.org/information-technology-and-firm-profitability-mechanisms-and-empirical-evidence.html

Motii, M., & Semma, E. (2017). Towards a new approach to pooling COBIT 5 and ITIL V3 with ISO/IEC 27002 for better use of ITG in the Moroccan parliament. *International Journal of Computer Science Issues*, *14*(3), 49–58. https://doi.org/10.20943/01201703.4958

Mulyono, Manurung, A. H., Alamsjah, F., & Hamsal, M. (2020). The effect of corporate governance, E-Business and innovation on competitive advantage and implication on financial performance. *Pertanika Journal of Social Sciences and Humanities*, *28*(January), 1–13.

Otero, A. R. (2015). An information security control assessment methodology for organizations' financial information. *International Journal of Accounting Information Systems*, *18*, 26–45. https://doi.org/10.1016/j.accinf.2015.06.001

Pereira, R., & da Silva, M. (2012). IT Governance Implementation: The Determinant Factors. *Communications of the IBIMA*. https://doi.org/10.5171/2012.970363

Salehi, F., Abdollahbeigi, B., & Sajjady, S. (2021). *Impact of Effective IT Governance on Organizational Performance and Economic Growth in Canada*. *3*(2), 14–19.

Selamat, M. H., & Babatunde, D. A. (2014). Mediating Effect of Information Security Culture on the Relationship between Information Security Activities and Organizational Performance in the Nigerian Banking Setting. *International Jour*nal of Business and Management, 9(7), 33–38. https://doi.org/10.5539/ijbm.v9n7p33

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS quarterly, 487-502.

Sjödin, D., Parida, V., & Kohtamäki, M. (2019). Relational governance strategies for advanced service provision: Multiple paths to superior financial performance in servitization. *Journal of Business Research*, *101*(March), 906–915. https://doi.org/10.1016/j.jbusres.2019.02.042

Sofyani, H., Riyadh, H. A., & Fahlevi, H. (2020). Improving service quality, accountability and transparency of local government: The intervening role of information technology governance. *Cogent Business and Management*, *7*(1). https://doi.org/10.1080/23311975.2020.1735690

Soliman, M., & Zaky, A. H. M. (2018). The Mediating Role of IT Governance Effectiveness between ITG and Financial/ Non-Financial Performance: Empirical Research on Egyptian Banking Sector. *SSRN Electronic Journal*, *9*(2), 77–89. https://doi.org/10.2139/ssrn.3119507

Sridhar, K. (2012). Is the Triple Bottom Line a restrictive framework for non-financial reporting? In *Asian Journal of Business Ethics* (Vol. 1, Issue 2). https://doi.org/10.1007/s13520-011-0010-4

Steuperaert, D. (2019). Cobit 2019: a Significant Update. *Edpacs*, *59*(1), 14–18. https://doi.org/10.1080/07366981.2019.1578474

Tambotoh, J. J. C., Kosala, R., Ranti, B., Prabowo, H., Supangkat, S. H., Isa, S. M., & Pudjianto, B. W. (2018). A conceptual model for creating effective public value through key practices in information technology governance mechanisms. *Proceedings of 2017 International Conference on Information Management and*

Technology, ICIMTech 2017, *2018-January*(November), 128–132. https://doi.org/10.1109/ICIMTech.2017.8273524

Van Grembergen, W., & De Haes, S. (2012). A Research Journey into Enterprise Governance of IT, Business/IT Alignment and Value Creation. *Business Strategy and Applications in Enterprise IT Governance*, 1–13. https://doi.org/10.4018/978-1-4666-1779-7.ch001

Wang, T., Wang, Y., & McLeod, A. (2018). Do health information technology investments impact hospital financial performance and productivity? *International Journal of Accounting Information Systems*, *28*(December 2017), 1–13. https://doi.org/10.1016/j.accinf.2017.12.002

Weill, P., & Ross, J. W. (2004). IT governance: How top performers manage IT decision rights for superior results. Harvard Business Press. *Available at*: https://books.google.com.eg/books

Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security Fourth Edition. *Learning*, 269, 289. *Available at*: https://books.google.com.eg/books

Wiedenhoft, G. C., Luciano, E. M., & Magnagnagno, O. A. (2017). Information Technology Governance in Public Organizations: Identifying Mechanisms That Meet Its Goals While Respecting Principles. *Journal of Information Systems and Technology Management*, *14*(1), 69–87. https://doi.org/10.4301/s1807-17752017000100004

Yang, S., Li, Z., Ma, Y., & Chen, X. (2018). Does Electronic Banking Really Improve Bank Performance? Evidence in China. *International Journal of Economics and Finance*, *10*(2), 82. https://doi.org/10.5539/ijef.v10n2p82

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, *26*(1), 60–77. https://doi.org/10.1057/jit.2010.4

Zaydi, M., & Nassereddine, B. (2019). A new comprehensive solution to handle information security governance in organizations. *ACM International Conference Proceeding Series*, *Part F1481*, 1–5. https://doi.org/10.1145/3320326.3320382

Zuo, M., Ma, D., & Yu, Y. (2020). Contextual determinants of IT governance mechanism formulation for senior care services in local governments. *International Journal of Information Management*, *53*(April 2019), 102125. https://doi.org/10.1016/j.ijinfomgt.2020.102125