منهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل: دليل تطبيقي

إعداد

د. هبه جمال هاشم علي

أستاذ مساعد المحاسبة والمراجعة

كلية التجارة بالإسماعيلية، جامعة قناة السويس

drhebagamala@gmail.com

المجلة العلمية للدراسات والبحوث المالية والتجارية

كلية التجارة – جامعة دمياط

المجلد الرابع - العدد الثاني – الجزء الثاني - يوليو ٢٠٢٣

التوثيق المقترح وفقاً لنظام APA:

علي، هبه جمال هاشم (٢٠٢٣). منهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل: دليل تطبيقي. **المجلة العلمية للدراسات والبحوث المالية والتجارية**، كلية التجارة، جامعة دمياط، ٤(٢)٢، ١-٥٨.

رابط المجلة: https://cfdj.journals.ekb.eg/

منهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل: دليل تطبيقي

د. هبه جمال هاشم علي

الملخص

استهدفت الدراسة التوصل لمنهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل بالبيئة المصرية، وعلى ذلك تناولت الدراسة النظرية انعكاسات مخاطر الأمن السيبراني على أعمال المراجع الخارجي وخطوات المنهج المقترح ، واعتمدت منهجية الدراسة التطبيقية علي شركات المساهمة المقيدة في البورصة المصرية والعاملة في القطاعات والأنشطة المرتبطة بالتقنيات الحديثة في نظم المعلومات والتكنولوجيا، حيث بلغ عدد الشركات الممثلة لمجتمع الدراسة (٢٠) شركة ، وتوصلت الدراسة إلى أن تقييم مخاطر الأمن السيبراني يعتمد على عمليات المراجعة التي تدرس وتقيم مجموعة من الضوابط المحددة مسبقاً في مجموعة متنوعة من الموضوعات المتعلقة بالأمن السيبراني ، كما أوضحت نتائج التحليل الإحصائي وجود تأثير طردي معنوي لمخاطر هجمات الأمن السيبراني بمنشأة العميل على أعمال المراجع الخارجي، ووجود ارتباط طردي معنوي بين إدارة الإفصاح عن مخاطر الأمن السيبراني والمنهج الإجرائي المقترح لأعمال المراجع الخارجي.

المقدمة

أدى ظهور التقنيات الحديثة في نظم المعلومات والتكنولوجيا الرقمية مثل إنترنت الأشياء (Internet of Things) وسلاسل الكتل (Block Chain) وخدمات الحوسبة السحابية (Cloud Services) إلي ترابط غير مسبوق بين دول العالم والشركات والأفراد؛ وأصبحت شبكة الإنترنت جزء من بيئة الأعمال ومن حياتنا اليومية أيضاً، ومع تزايد عدد الشركات التي تتواجد على مواقع الإنترنت وتستخدمها في تعاملاتها الرقمية وتستفيد منها في جوانبها العملياتية والانتاجية والبيعية وحتى في تحصيل إيراداتها، فقد أصبحت أنظمتها وعملياتها وأنشطتها عرضة للكثير من المخاطر والتهديدات والتحديات، ومنها تهديدات الأمن السيبراني ويشمل ذلك فقدان المعلومات الخاصة والحساسة، والتلاعب واتلاف البيانات والأنظمة والشبكات، وحتى الأصول المادية، وقد تسبب ذلك في تكبد الشركات تكاليف وخسائر كبيرة وتقويض الثقة في تلك المنشآت. وبالتالي فقد برز موضوع الأمن السيبراني (Cyber security)، والذي يشمل أمن المعلومات على أجهزة وشبكات الحاسب الآلي، بما في ذلك العمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو تعطيل قد يحدث، وعليه فقد أصبح الأمن السيبراني ركيزة أساسية في كل المنظمات والمؤسسات بل وحتى الدول لمواجهة الحروب الإلكترونية.

حيث أشار معهد المراجعين الداخليين (IIA. 2022: 2019) إلى أن تهديدات الأمن السيبراني وأمن المعلومات تعد من أكبر المخاطر التي تواجه الشركات في عصرنا الحالي، فيما أشار المنتدى الاقتصادي العالمي (WEF. 2020: 11) في تقريره عن المخاطر الدولية إلى ارتفاع المخاوف من الهجمات السيبرانية وتحريف البيانات وظهرت هذه المخاطر في قائمة أعلى خمسة مخاطر محتملة الحدوث في ٢٠٢٠م، ومؤخراً وفي ظل تفشي جائحة (COVID-19) أشار (PwC. 2020) إلى أنه بدأت بالفعل بعض المنظمات العمل من المنزل من خلال شبكة الانترنت، وبدون اخذ الاحتياطات المناسبة، وهذا يمكن أن يزيد بشكل أساسي من مخاطر الأمن السيبراني.

وعلى ذلك فقد ظهرت تساؤلات كثيرة حول ما إذا كانت مخاطر الأمن السيبراني ترتبط بمهنة المراجعة وتحديداً المراجعة الخارجية للتقارير المالية أم لا (No, W. G., & Vasarhelyi, M. A. (2017:2. واستجابة لتزايد تهديدات مخاطر الأمن السيبراني وتزايد التساؤلات حول مدى ارتباطها بالمراجعة، عقدت الجهات المنظمة لمهنة المحاسبة والمراجعة عدة ندوات ولقاءات لمناقشة موضوع الأمن السيبراني والمشاكل ذات العلاقة، والتحديات التي يثيرها في اسواق المال والشركات، وآثارها المحتملة على إعداد التقارير المالية ومهنة المراجعة وكيفية معالجة تلك القضايا والتحديات (SEC. 2014: 2013: 2018) (PCAOB. 2014: 2016: 2017) (IFAC. 2019) (CAQ. 2014) وأكدت تلك المناقشات على أن تهديدات الأمن السيبراني تعد من أكبر المخاطر التي تواجه الشركات وأن لها انعكاسات على أداء الشركات وإعداد التقارير المالية ومهنة المراجعة. وعليه يمكن اعتبار مخاطر الأمن السيبراني مجال خطر لا يقل أهمية ولا يمكن تجاهله، وبالتالي فإن هذه الدراسة تأتي لتقييم مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل.

أولاً: مشكلة الدراسة

ظهرت المخاطر السيبرانية كتهديد رئيسي لاستقرار منشآت الأعمال في أعقاب الهجمات الأخيرة على المؤسسات المالية، حيث أشار مسح شمل مؤسسات مالية نموذجية عام ٢٠١٧ إلى أن تلك المؤسسات تواجه في المتوسط ٨٥ هجوماً إلكترونياً كل عام ثلثها كانت هجمات ناجحة، وأشار تقرير (IBM, 2020) إلى أن الهجمات السيبرانية كلفت الشركات مبالغ طائلة فمن ناحية بلغ متوسط تكلفة خسائر اختراق البيانات في عام ٢٠١٩مبلغ ٣,٨٦ مليون دولار، ردا على ذلك تركز الشركات بشكل أساسي على تأمين البنية التحتية من خلال الاستثمار في التقنيات الجديدة وتنفيذ معايير وأطر الأمن السيبرانيCurtis, B. (2022) ، حيث تنفق الشركات في المتوسط ١٨,٤ مليون دولار سنوياً على الأمن السيبراني ورغم ذلك لا تزال تتعرض لاختراق بياناتها. وفي عام ٢٠٢١ تم تسجيل هجوم سيبراني على شركةColonial Pipeline الأمريكية، وقد أدى هذا الهجوم إلى تعطل في تدفق ما يقارب نصف إمدادات البنزين ووقود الطائرات، وفي النهاية اضطرت الشركة إلى دفع فدية قيمتها خمسة ملايين دولار لمجموعة القراصنة لاستعادة الشبكة واستعادة البيانات (IIA: 2022)، وأشار (IIA: 2022) إلى أنه لا تزال مخاطر الأمن السيبراني من بين أكبر المخاطر في جميع المنظمات، حيث تعكس الاستطلاعات باستمرار الحاح وكثافة الجهود التي يبذلها مجرمو الإنترنت لاختراق البيانات الحساسة والوصول الى بيانات ومعلومات الشركات الهامة.

وفي ضوء ما سبق كان هناك محاولات عديدة من قبل المنظمات المهنية الناشطة في مجال تكنولوجيا المعلومات لوضع برامج لإدارة الأمن السيبراني وإدارة مخاطره وفق أطر من المعايير والقواعد المناسبة باعتبار مخاطر الأمن السيبراني مخاطر أعمال لا تقل أهمية عن المخاطر المالية والتشغيلية ومخاطر السمعة (2019) .IFAC، كما صاحب ذلك اهتمام كبير من الجهات المنظمة لمهنة المحاسبة والمراجعة والباحثين في مجال الفكر المحاسبي بموضوع الأمن السيبراني، من منطلق امكانية تأثير مخاطر الأمن السيبراني على الشركات وسلامة تقاريرها المالية، وبالتالي على أعمال المراجع الخارجي؛ فقد قام المعهد الأمريكي للمحاسبين المعتمدين AICPA (2016) بإصدار دليل الأمن السيبراني استجابة للحاجة إلى مشاركة مهنة المراجعة، وأكد مركز جودة المراجعة حقيقة أنه يجب على المراجع الانتباه بشكل خاص إلى الحوادث السيبرانية، حيث يمكن أن يلعب المراجع دور مهم في منع أو تخفيف آثار هذه الحوادث من خلال توفير ضمانات إضافية حول ضوابط تكنولوجيا المعلومات لعملائه (CAQ: 2014, 2016, 2017: 2020)، كما أكد تقرير من (:PCAOB 2013,2014, 2018) على ضرورة تقييم المراجعين لمخاطر الأمن السيبراني لعملائهم، وقام AICPA (2016) بإصدار إطار عمل لإعداد التقارير لإبلاغ الإدارة ومجلس الإدارة بمخاطر الأمن السيبراني.

كما أكدت لجنة الأوراق المالية والبورصة (4 :2014) :SECعلى ضرورة اتخاذ الشركات جميع الإجراءات اللازمة والمطلوبة لإبلاغ المستثمرين بشأن مخاطر وحوادث الأمن السيبراني في الوقت المناسب، بما في ذلك الشركات التي تعرضت لبعض مخاطر الأمن السيبراني المادي ولكن لم تكن هدفاً بعد للهجوم السيبراني، ووفقاً للمبادرة الوطنية لمهن ودراسات الأمن السيبراني ( ).NICCS 2017، يشير مصطلح مخاطر الأمن السيبراني إلى أي حدث يهدد أو يشكل تهديداً لنظام المعلومات أو المعلومات التي يقوم النظام بمعالجتها أو تخزينها أو نقلها، كما تشير إدارة مخاطر الأمن السيبراني إلى مستوى عملية الشركة في تنفيذ وتشغيل الضوابط وأنشطة إدارة المخاطر الأخرى لحماية معلوماتها وأنظمتها. AICPA. (2017a)

وعليه يجب تبني مدخل شامل لإدارة المخاطر للتعامل مع التغير المستمر في الأعمال التجارية، والتهديدات والمخاطر التي تتطور باستمرار والتي تمتد إلى الأفراد والعمليات والتكنولوجيا عبر الشركة. كما يجب إشراك جميع المستويات الادارية في إدارة المخاطر بحيث يساعد ذلك على ضمان وجود إطار يفهمه الجميع وأن تدار خطوط الدفاع المختلفة بشكل جماعي وتخفف من مخاطر الأمن السيبراني على أساس مستمر Sylvia Tsen. (2019 :7)، حيث يعد تحديد المخاطر والأولويات أمراً ضرورياً للإدارة الفعالة للمخاطر، إذا فشلت الشركة في تحديد مخاطر معينة أو إعطاء الأولوية للمخاطر الخاطئة ، فإن إدارة المخاطر لا بد أن تفشل وتؤدي إلى عواقب سلبية كبيرة، وهذا ما ينطبق تماماً على الأمن السيبراني، حيث توجد تهديدات لا حصر لها وهي متغيرة باستمرار. Eaton, T. V., et al (2019)

وفي الحقيقة ومن وجهه نظر الباحثة فإن تقييم المخاطر يعد جزءً مهماً من تخطيط المراجعة، حيث تشير معايير المراجعة إلى أن المراجع مطالب بفهم مخاطر الأعمال التي قد تؤدي إلى مخاطر الأخطاء أو التحريفات الجوهرية في التقارير المالية، وبالتالي فإن مخاطر الأمن السيبراني هي مجال مخاطر لا يقل أهمية عن مخاطر الأعمال ولا يمكن تجاهلها، وعليه فإن هذه الدراسة تأتي لتحليل

ودراسة مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل باعتبار الأمن السيبراني ومخاطره من الناحية النظرية والعملية من الموضوعات الحديثة التي تحتاج مزيد من البحث والدراسة خاصة في البيئة المصرية، وعلى ذلك يمكن صياغة مشكلة الدراسة من خلال التساؤلات البحثية التالية:

١. ماهي انعكاسات مخاطر الأمن السيبراني على نطاق ومسئوليات المراجع الخارجي؟
٢. ما هي محددات درجة استجابة المراجع الخارجي للحوادث والتهديدات السيبرانية الحاصلة والمكتشفة في منشأة عميل المراجعة؟
٣. هل هناك إمكانية لصياغة منهج إجرائي مقترح لمراجعة وتقييم عملية إدارة مخاطر الأمن السيبراني؟

ثانياً: أهمية الدراسة

لقد ساهم انتشار أنظمة تكنولوجيا المعلومات في ظهور أنواع جديدة من المخاطر، حيث سمح الترابط بين مجالات التكنولوجيا التشغيلية (OT) مع مجالات تكنولوجيا المعلومات (IT) وتكنولوجيا الأمن (ST) بانتقال المخاطر من مجال إلى الآخر مما أدى إلى تزايد المخاطر الناشئة عن الهجمات السيبرانية، وسمحت لمجرمي الإنترنت بتهديد الأمن السيبراني للمنشآت Eaton, T. V., et al (2019)، الأمر الذى دفع الباحثة نحو دراسة العلاقة بين مخاطر الأمن السيبراني ومدى استجابة المراجع الخارجي لهذه المخاطر، حيث تتمثل الأهمية العلمية في ندرة الدراسات الاكاديمية- من وجه نظر الباحثة - حول موضوع استجابة المراجع الخارجي لحوادث الأمن السيبراني التي يتعرض لها عميله، وما إذا كان ينظر إلى مخاطر الأمن السيبراني قبل التحقق من المخاطر ، وفي المقابل هناك اهتمام متزايد من قبل الهيئات المنظمة للمهنة بالأمن السيبراني، وبالتالي يمكن تحديد أهمية الدراسة فيما يلي:

١- تضييق الفجوة في الأدبيات السابقة من خلال التأطير النظري للعلاقة بين عملية المراجعة والحوادث السيبرانية، كما تتمثل أهمية الدراسة من الناحية العلمية في أن تأثيرات الأمن السيبراني على أعمال المراجعة تأتي استجابة للدعوات من قبل المنظمات المهنية بإجراء مزيد من النقاش والبحث في هذا المجال.
٢- وفي الجانب العملي تساهم هذه الدراسة في البحث حول مدى استجابة المراجع الخارجي للحوادث والتهديدات السيبرانية في منشأة عميل المراجعة، إضافة إلى تطوير البحث حول الأمن السيبراني في المجال المحاسبي من خلال محاولة تحليل انعكاسات مخاطر الأمن السيبراني على إجراءات المراجعة.

ثالثاً: أهداف الدراسة

يعتبر الأمن السيبراني أحد أكثر القضايا أهمية لدى إدارات ومجالس ادارة كل شركة في العالم تقريباً كبيرها وصغيرها، عامها وخاصها AICPA. (2018a: .10)، ولهذا هدفت الدراسة بشكل رئيسي إلى التوصل لمنهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل ، ويمكن تقسيم هذا الهدف إلى الأهداف الفرعية التالية:

١- تحليل انعكاسات مخاطر الأمن السيبراني على نطاق ومسئوليات المراجع الخارجي.
٢- طرح المحددات المؤثرة على درجة استجابة المراجع الخارجي للحوادث والتهديدات السيبرانية الحاصلة والمكتشفة في منشأة عميل المراجعة.
٣- تقييم آليات التبرير للمراجع الخارجي لمراجعة مخاطر الأمن السيبراني من خلال منهج إجرائي مقترح.

رابعاً: فروض الدراسة

بناءً على مشكلة وأهداف الدراسة يمكن صياغة الفروض البحثية على النحو التالي:

الفرض الأول: لا يوجد تأثير معنوي لمخاطر هجمات الأمن السيبراني بمنشأة العميل على أعمال المراجع الخارجي.

الفرض الثاني: لا توجد علاقة ذات دلالة معنوية بين إدارة الإفصاح عن مخاطر الأمن السيبراني والمنهج الإجرائي المقترح لأعمال المراجع الخارجي.

خامساً: الدراسات والأدبيات السابقة

نظراً لاعتماد الشركات بشكل متزايد على البيانات التي تم جمعها ومعالجتها وتخزينها، فقد زادت احتمالية حدوث ضرر ناتج عن حوادث الأمن السيبراني بشكل كبير، بينما تبلغ وسائل الإعلام عن الأضرار الناجمة عن هجمات القراصنة على أساس يومي، فهي ليست النوع الوحيد من حوادث الأمن السيبراني. وعلى ذلك اهتمت الدراسات المحاسبية بدراسة العلاقة بين مخاطر الأمن السيبراني وعملية المراجعة، حيث استهدفت دراسة Li, B, et. Al,(2022) قياس مدى استجابة المراجعون لمخاطر الأمن السيبراني من خلال الاستثمار بشكل أكبر في رأس المال البشري للأمن السيبراني، كما حققت الدراسة في دور المراجعين في مساعدة عملائهم غير المخترقين في زيادة الوعي بالأمن السيبراني والاستثمار في موظفي الأمن السيبراني، وتوصلت الدراسة إلى أن طلب مكاتب المراجعة على موظفي الأمن السيبراني قد ارتفع بعد أن واجهت شركات عملائهم لأحداث اختراق بياناتها الإلكترونية، كما ظهرت هذه التأثيرات فقط للمراجعين الموجودين في الولايات التي تعرضت فقط بشكل متقطع لخروقات البيانات.

بينما تناولت دراسة (فرج: ٢٠٢٢) اختبار العلاقة بين توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكتروني (الأمن السيبراني) وقرار الاستثمار بالأسهم، وكذلك اختبار أثر تأهيل وخبرة المستثمرين على العلاقة محل الاختبار، ولقد اعتمدت الدراسة على إجراء دراسة تجريبية على عينة من ٦٥ من المستثمرين المؤسسيين والذين يتمثلون في أمناء الاستثمار في البنوك التجارية المصرية، وتوصلت الدراسة إلى وجود تأثير لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكتروني إيجاباً ومعنوياً على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية، وتم استخدام متغيرات معدلة تمثلت في مستوى التأهيل العلمي للمستثمر، ومستوى خبرة المستثمر، وخلصت الدراسة إلى عدم وجود تأثير معنوي لمتغيري التأهيل والخبرة، كل على حده، على قرار الاستثمار بالأسهم، وكذلك عدم وجود تأثير معنوي لمتغيري التأهيل والخبرة معاً على قرار الاستثمار بالأسهم.

وركزت دراسة Slapničar, S., et al. (2022) على تحليل فعالية المراجعة الداخلية للأمن السيبراني، واعتمدت على تطوير مؤشر لمراجعة الأمن السيبراني يتكون من ثلاثة أبعاد (التخطيط والأداء وإعداد التقارير)، حيث افترضت الدراسة أن فعالية مراجعة الأمن السيبراني ترتبط ارتباطاً إيجابياً بإدارة المخاطر الإلكترونية وسلبياً باحتمال حدوث هجوم إلكتروني ناجح، واعتمدت منهجية الدراسة الإحصائية على استطلاع تم إجرائه مع المراجعين والرؤساء التنفيذيين للمراجعين من مختلف الدول والصناعات. وتوصلت نتائج الدراسة إلى أن درجات مؤشر مراجعة الأمن السيبراني تختلف اختلافًا كبيراً، بمتوسط ٥٨ على مقياس من ٠ إلى ١٠٠، وفي حين أن مرحلتي التخطيط والأداء مترابطتان بشكل إيجابي إلا أنهما أقل ارتباطاً بالتقرير عن فعالية إدارة المخاطر الإلكترونية لمجلس الإدارة، كما توصلت الدراسة إلى أن مؤشر مراجعة الأمن السيبراني يرتبط بشكل إيجابي بمدى فعالية إدارة المخاطر، ولا يرتبط باحتمالية هجوم إلكتروني ناجح.

فيما اقترحت دراسة Antunes, M., et al (2022) نظام معلومات عام لمراجعة الأمن السيبراني، وأشارت الدراسة إلى أن إدارة الأمن السيبراني تلعب دوراً رئيسياً في المؤسسات الحديثة، وأن هناك عدد كبير من المعايير والأطر والأدوات لتنفيذ إطار عمل الأمن السيبراني، فعلى الصعيد العالمي يتم تنفيذ هذه المعايير من خلال أدوات مخصصة لجمع وتحليل المزيد من مراجعة الأمن السيبراني الذي يتم تنفيذه في المؤسسة، حيث أن الهدف العام للمراجعة يتمثل في تقييم مخاطر الأمن السيبراني والتخفيف من حدتها، واعتمدت منهجية الدراسة الإحصائية على اختبار النظام المقترح في خمسين شركة صغيرة ومتوسط الحجم ، وتوصلت الدراسة إلى أن تقييم مخاطر الأمن السيبراني يعتمد على عمليات المراجعة التي تدرس وتقيم مجموعة من الضوابط المحددة مسبقاً في مجموعة متنوعة من الموضوعات المتعلقة بالأمن السيبراني، وأنه يتم تطبيق قائمة مرجعية بالإجراءات لكل عنصر رقابة ويقترح مجموعة من الإجراءات التصحيحية، من أجل التخفيف من العيوب وزيادة مستوى الامتثال للمعايير المستخدمة.

وتناولت دراسة Rosati, P., et al (2022) أن حوادث الأمن السيبراني تمثل عوامل خطر كبيرة لجودة التقارير المالية كإشارات على نقاط ضعف الرقابة الداخلية ، حيث اعتمدت الدراسة بشكل تجريبي على تقييم الآثار المترتبة على جودة المراجعة لانتهاكات البيانات لعينة كبيرة من الشركات الأمريكية، وتوصلت الدراسة إلى عدم وجود أي دليل على أن حوادث الأمن السيبراني تؤدي إلى انخفاض جودة المراجعة، كما أشارت النتائج إلى أن المراجعين قد عوضوا بشكل فعال الزيادات في مخاطر المراجعة من خلال زيادة الاختبارات الجوهرية وجهد المراجعة.

فيما أشارت دراسة Shaikh, F. A., & Siponen, M. (2022) إلى تركيز أبحاث نظم المعلومات (IS) حول الاستجابة الإدارية لانتهاكات الأمن السيبراني إلى حد كبير على الإجراءات الموجهة خارجياً فقط مثل معالجة العملاء والاستجابة للأزمات، وأن التركيز الضيق المنفصل قد يؤدي إلي إصلاح المشكلات العاجلة فقط، كما أشارت الدراسة إلى أن تقييمات مخاطر أمن المعلومات (ISRA) قد تساعد في الكشف عن نقاط الضعف الأخرى بعد الاختراق، وأكدت على دور الحوكمة في تقييم مخاطر أمن المعلومات، وتوصلت الدراسة إلى أن تكاليف الاختراق المرتفعة تؤدي إلى زيادة اهتمام الإدارة العليا بالأمن السيبراني، مع زيادة احتمالية قيام الشركات بتنفيذ تقييمات مخاطر أمن المعلومات، كما توصلت إلى أن اهتمام الإدارة بالأمن السيبراني يتوسط جزئياً في العلاقة بين تكاليف الاختراق وقرار تنفيذ ISRA.

وركزت دراسة Blakely, B., et al (2022) على حوادث اختراقات البيانات، وهي نوع خاص من الحوادث السيبرانية، والتي قد تؤدي إلى فقدان المعلومات السرية من خلال استخدام إطار الرقابة الداخلية COSO ERM لفحص ما إذا كانت تقارير الاختراق الإلكتروني الحالية تحتوي على معلومات قد تؤثر على قدرة الشركة على إجراء تغيير جوهري داخل صناعتها بسبب قوى خارجية (COSO ERM Principle 15)، حيث أشارت الدراسة إلى أن صناع القرار السيبراني يعتمدوا على هذا النوع من المعلومات لتقييم برامج أمن المعلومات لضمان تغطية التهديدات ذات الصلة والاستخدام الفعال للأموال المتاحة، كما يمكن استخدام هذه التقارير لأغراض تقييم مخاطر الأمن السيبراني والتخطيط الاستراتيجي، وتشير النتائج إلى أن تقارير نتائج عينة الدراسة تحتوى على القليل من المعلومات التي يمكن دمجها لتحسين ملف مخاطر المؤسسة.

وهدفت دراسة Al-Matari, O. M., et al (2021) تكوين إطار مقترح لإجراء دراسة مقارنة لأدوات مراجعة الأمن السيبراني وأطر المراجعة المتعارف عليها، وتمثل الهدف الرئيسي للدراسة في تنفيذ أداة متكاملة للأمن السيبراني لمراجعة نظم المعلومات والأمن السيبراني بهدف جعل عملية مراجعة الأمن السيبراني أسهل وأكثر شمولاً، حيث يمكن للأداة المتكاملة أيضاً قياس مقدار الوقت والجهد الموفر لتحقيق العمليات اليومية، وتوصلت الدراسة إلى أن مستويات المراجعة تزيد من احتمالية اكتشاف نقاط ضعف الرقابة الداخلية وتوفر المزيد من الضوابط والتوازنات للمنظمات، من خلال مواءمة هذا الإطار المتكامل مع التقنيات والوظائف الحديثة والقضايا ذات الصلة بالأمن السيبراني.

فيما تناولت دراسة Tosun, O. K. (2021) تحليل طبيعة استجابة الأسواق المالية للهجمات السيبرانية للشركات على المدى القصير أو الطويل، أشارت النتائج إلى أن الإفصاح العلني عن أحداث اختراق الأمن السيبراني للشركات للمرة الأولى يؤدي إلى انخفاض العوائد اليومية وزيادة حجم التداول، وتشير الأدلة إلى أن حجم التداول يزداد بسبب ضغوط البيع وتدهور السيولة، كما أشارت النتائج إلى أن الاختراقات للأمن السيبراني تؤثر على سياسات الشركات على المدى الطويل وحتى خمس سنوات بعد الإعلان عن خروقات الأمن السيبراني وتتفق هذه النتائج مع الفرضية القائلة بأن الخروقات الأمنية تمثل صدمات سلبية غير متوقعة لسمعة الشركات مما يدفع المستثمرين إلى التصرف بغض النظر عن الأساسيات الاقتصادية.

واختبرت دراسةRosati, P.,et al(2019) العلاقة بين جودة المراجعة وحوادث الأمن السيبراني من خلال دراسة اختراق بيانات لعينة ٣٢٩ من الشركات الأمريكية باستخدام نهج الاختلاف في الفروق المستند إلى عينة مطابقة من الشركات المخترقة وغير المخترقة. لم تجد الدراسة أي دليل على أن حوادث الأمن السيبراني تؤدي إلى انخفاض جودة المراجعة، بدلاً من ذلك وجدت تحولات إيجابية في أربعة مؤشرات مستخدمة على نطاق واسع لجودة المراجعة، وثقت الدراسة أن الشركات المخالفة تواجه انخفاضاً في الاستحقاقات غير العادية، وتكون أقل احتمالاً للإفصاح عن الأرباح أو الزيادات البسيطة في الأرباح، من المحتمل أن تصدر تقرير استمرارية. كما أشارت النتائج إلى أن المراجعين عوضوا بشكل فعال الزيادات في مخاطر المراجعة من خلال الاختبارات الجوهرية وجهد المراجعة، وهذ يدعم وجهة النظر القائلة بأن المراجعين قد زادوا من وعيهم بمخاطر المراجعة ووضعوا إجراءات مناسبة للتعامل مع اثآر حوادث الأمن السيبراني.

كما تناولت دراسة Frank, M. L., et al (2019) إلى قياس تأثير الإفصاح عن هجوم سيبراني سابق على فعالية الإفصاح عن إدارة مخاطر الأمن السيبراني والتأكيد المستقل على تصورات المستثمرين حول جاذبية الاستثمار، انتهت الدراسة إلى أن غياب تقرير التأكيد المستقل حول إدارة مخاطر الأمن السيبراني يكون أكثر فاعلية عندما لا تفصح الشركة عن هجوم إلكتروني سابق نظراً لأن المستثمرين غير المحترفين أقل عرضة للتشكيك في موثوقية تقارير الإدارة حول الأمن السيبراني،

ومع ذلك فإن إصدار تقرير تأكيد مستقل مع تقرير الإدارة حول إدارة مخاطر الأمن السيبراني يوفر فائدة إضافية أكبر للشركات التي افصحت مقابل التي لم تفصح عن هجوم الكتروني سابق حيث أن هذه الشركات تستفيد أكثر من خلال تعزيز موثوقية التأكيد المستقل، وانتهت الدراسة إلى أنه يمكن تعزيز جاذبية الاستثمار في الشركة من خلال إصدار تقرير تأكيد مستقل عن مخاطر الأمن السيبراني.

وتناولت دراسة Perols, R. R. (2019) قياس تأثير حادثة الأمن السيبراني اللاحقة على تصورات المستثمرين اعتماداً على ما إذا كانت مراجعة الأمن السيبراني تتم من خلال اشتراك مراجعة القوائم المالية ومراجعة الأمن السيبراني في عملية المراجعة أو تتم بشكل منفصل، وتناولت الدراسة أثر وجود حادثة للأمن السيبراني على الرغبة في الاستثمار بأسهم الشركات في حالتي حدوث حادثة الأمن السيبراني بعد الافصاح عن مراجعة الأمن السيبراني أو حدوثها قبل الافصاح عن مراجعة الأمن السيبراني، وأشارت النتائج إلى أنه في حالة عدم وجود حادث للأمن السيبراني فإن المراجعة المشتركة مقارنة بالمراجعة المنفصلة لها تأثير سلبي على تصورات المستثمرين لاستقلالية المراجع وتأثير إيجابي على كفاءة مراجعة الأمن السيبراني أو كفاءة المراجعة الخارجية، كما أن تأثير حادثة الأمن السيبراني على تصورات المستثمرين لكفاءة المراجعة كانت سلبية بشكل كبير على المراجعة المشتركة مقارنة بالمراجعة المنفصلة وتظهر النتائج كذلك أن جودة مراجعة الأمن السيبراني تخفف من التأثير السلبي لحادث الأمن السيبراني على رغبة المستثمرين في الاستثمار.

وتناولت دراسة Islam, M. S., et al (2018) العوامل المرتبطة بمدى مراجعة الأمن السيبراني من قبل وظيفة المراجعة الداخلية (IAF) للشركة وعلى وجه التحديد ركزت الدراسة على ما إذا كانت خصائص المراجعة الداخلية (مدير المراجعة المعتمد) ومشاركة مجلس الإدارة، ودور لجنة المراجعة ومدير إدارة المخاطر والعلاقة بين مسئولية المراجع الداخلي في إدارة مخاطر المنشأة (ERM) ودوره في مراجعة الأمن السيبراني، وانتهت الدراسة إلى أن هناك علاقة تأثيرية بين قدرات كفاءة المراجعة الداخلية المتعلقة بالحوكمة والمخاطر والرقابة عليها ودوره في مراجعة الأمن السيبراني، حيث إن دعم مجلس الإدارة بشأن الحوكمة هو أيضا مهم وإيجابي ومع ذلك فإن لجنة المراجعة لم يكن لها دور كبير في جميع الشركات محل الدراسة، التقييم الشامل للمخاطر من قبل المراجع الداخلي له تأثير إيجابي على دوره في مراجعة سلامة الأمن السيبراني.

واستكشفت دراسة Amir, E., Levi, S., & Livne, T. (2018) قياس مدى افصاح شركات أسواق رأس المال الأمريكية عن تهديدات الأمن السيبراني وذلك بالرجوع إلى بيانات الشركات التي لها أسهم متداولة في البورصة الأمريكية والمتوافرة في قاعدة البيانات vc veris community database حيث اعتمدت الدراسة على تصنيف الهجمات الإلكترونية إلى مجموعتين رئيسيتين تتمثل في الهجمات الإلكترونية التي تعرضت لها الشركات وافصحت عنها، والهجمات الإلكترونية التي لم يتم الإفصاح عنها وتم اكتشافها في وقت لاحق بشكل مستقل من قبل مصادر خارجية. وانتهت الدراسة إلى أن الهجمات الإلكترونية هي واحدة من المخاطر الرئيسية التي يجب على الشركات إدارتها، كما أن مديري الشركات يفصحون فقط عن الهجمات الأقل شدة ويخفون عن المستثمرين المعلومات عن الهجمات التي قد تتسبب في الكثير من الضرر أن المديرين لا يفصحون عن الهجمات السيبرانية إلا عند وجود مستوى معين من الشك لدى المستثمرون بتعرض الشركة لهجوم سيبراني أو عندما يكون هناك احتمال كبير باكتشاف تلك الهجمات من قبل طرف خارجي مستقل بشكل عام. كما أشارت النتائج إلى أن الإفصاح الطوعي عن الهجمات السيبرانية أمر نادر الحدوث إذا رغب المنظمون في ضمان وصول المعلومات المتعلقة بالهجمات السيبرانية إلى المستثمرين فعليهم أن يفكروا في فرض قواعد للإفصاح الإلزامي وبشكل أكثر صرامة فيما يتعلق بالهجمات السيبرانية وتحديد درجات الاهمية المادية بوضوح.

وفى ضوء ما سبق وتعقيباً على الدراسات السابقة تقدم الباحثة تحليلاً شاملاً للدراسات والأدبيات السابقة في مجال الدراسة حيث تناولت دراسة Li, B, et. Al,(2022) قياس مدى استجابة

المراجعون لمخاطر الأمن السيبراني من خلال الاستثمار بشكل أكبر في رأس المال البشري للأمن السيبراني، بينما تناولت دراسة (فرج: ٢٠٢٢) اختبار العلاقة بين توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكتروني، وفى هذا السياق تناولت دراسة Perols, R. R. (2019) قياس تأثير حادثة الأمن السيبراني اللاحقة على تصورات المستثمرين اعتماداً على ما إذا كانت مراجعة الأمن السيبراني تتم من خلال اشتراك مراجع القوائم المالية ومراجع الأمن السيبراني في عملية المراجعة أو تتم بشكل منفصل، واتفقت الدراسات على فعالية دور مراجعي الحسابات في مساعدة عملائهم غير المخترقين في زيادة الوعي بالأمن السيبراني والاستثمار في موظفي الأمن السيبراني.

كما اتفقت دراسة بعض الدراسات Al-Matari, O. M., et al (2021) & Rosati, P., et al (2022) Slapničar, S., et al. (2022) على أن حوادث الأمن السيبراني تمثل عوامل خطر كبيرة لجودة التقارير المالية كإشارات على نقاط ضعف الرقابة الداخلية، وأن مستويات المراجعة تزيد من احتمالية اكتشاف نقاط ضعف الرقابة الداخلية ذات الصلة بالأمن السيبراني، حيث ركزت دراسة Slapničar, S., et al. (2022) على تحليل فعالية المراجعة الداخلية للأمن السيبراني، واعتمدت على تطوير مؤشر مراجعة الأمن السيبراني يتكون من ثلاثة أبعاد (التخطيط والأداء وإعداد التقارير)، حيث أكدت بعض الدراسات أن المراجع يستجيب للمخاطر السيبرانية وبخاصة في حالة حدوث اختراق للأمن السيبراني لمنشأة العميل، وأكدت تلك الدراسات على ضرورة أن يأخذ المراجع الخارجي في اعتباره لمخاطر وتهديدات الامن السيبراني خلال عملية المراجعة .

وعلى ذلك يمكن القول أن معظم الدراسات قد تناولت مخاطر الأمن السيبراني وخلصت إلى أنه من أهم المخاطر التي تواجهها منشآت الأعمال وتساهم في تحمل الشركات لتكاليف عالية عند وجود تهديدات أو اختراقات سيبرانية وأن لها تأثيرات على التقارير المالية، كما أشارت بعض الدراسات إلى أن مخاطر الأمن السيبراني والإفصاح عن اختراقات الأمن السيبراني للشركات يؤثر على الأداء المالي، مما يؤثر على أسعار أسهم الشركة المتداولة وبالتالي تخفيض حجم الاستثمار. وعليه فقد أكدت تلك الدراسات على ضرورة اتخاذ الشركات الخطوات اللازمة نحو الأمن السيبراني لحماية نفسها من الهجمات السيبرانية وأنه يجب القيام بالرقابة المنتظمة لنظم المعلومات ويجب القيام بأي أنشطة أخرى لحماية الأمن السيبراني إدارة مخاطره.

وفي ضوء الدراسات السابقة تلاحظ الباحثة غياب أو ندرة الدراسات العربية التي تتناول العلاقة بين مخاطر الامن السيبراني والمراجعة الخارجية للقوائم المالية لعملاء المراجعة، باستثناء دراسة (فرج: ٢٠٢٢) التي ركزت على العلاقة بين توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن السيبراني وقرار الاستثمار بالأسهم، وبالتالي لم تتناول استجابة المراجع للمخاطر السيبرانية في إطار مراجعته للقوائم المالية للعميل، وعليه فقد جاءت الدراسة الحالية لسد الفجوة البحثية في مجال البحث، وتوافقاً مع الاهتمام العالمي والدعوات إلى إجراء مزيد من الدراسات حول موضوع المخاطر والتهديدات الناشئة عن الأمن السيبراني ودور المراجع الخارجي في الاستجابة لها خلال عملية المراجعة للقوائم المالية.

سادساً: خطة الدراسة

تستعرض الباحثة في المحور الأول تعريف ومخاطر الأمن السيبراني، وانعكاسات مخاطر الأمن السيبراني على أعمال المراجع الخارجي، وتحليل تأثيرات مخاطر الأمن السيبراني على عملية المراجعة، فيما يستهدف المحور الثاني الدراسة التطبيقية، ويختتم البحث بعرض النتائج والتوصيات والأبحاث المستقبلية.

المحور الأول: الدراسة النظرية

لقد جذب موضوع الأمن السيبراني في السنوات الأخيرة الكثير من الاهتمام من قبل المجتمع المحاسبي والمنظمات المهنية ومنشآت الأعمال نتيجة القلق من التهديدات الإلكترونية المتزايدة والتي قد تتسبب في فقدان معلومات مهمة وحساسة للمنشآت أو تعطيل الأعمال أو سرقة الأسرار التجارية (Li, H,(2017:12 ولقد أشار تقرير PwC عام ٢٠١٦ أن متوسط عدد الحوادث السيبرانية المكتشفة زاد بنسبة ٣٨ ٪ وسرقة الملكية الفكرية بنسبـــة ٥٦ ٪ في عام ٢٠١٥ مـقارنة بعام ٢٠١٤ وأن أكثر من ٢٠ ٪ من الشركات المخالفـة تعرضت لـخسائر كـبيرة في الإيرادات وفي عدد العملاء وفرص العمل وأنفقت معظم الشركات التي تم اختراقها ملايين الدولارات لتحسين تقنيات الدفاع وتوسيع الإجـراءات الأمنيـة بعد الهجمات (Cisco Annual Internet Report (2018–2023) White:2020 Paper)، مما ساهم في زيادة تركيز المنظمين والمهتمين بمهنة المحاسبة والمراجعة على كيفية وصف هذه المخاطر وتأثيراتها على عمليات الشركات ونتائج أعمالها وبالتالي على أعمال المراجعة الخارجية.

وتنظر دراسة No, W. G., & Vasarhelyi, M. A. (2017:1) إلى الأمن السيبراني على أنه مفهوم شامل يتضمن أمن وضمان المعلومات حيث يرتبط أمن المعلومات بالحفاظ على سرية وسلامة وتوافر المعلومات ويرتبط ضمان المعلومات بإعطاء الثقة أو اليقين في المعلومات وطمأنة المستخدمين بأنه يمكن الإعتماد عليها من خلال توفير وسائل لحماية الأعمال بهدف تقليل المخاطر المرتبطة بالمعلومات ونظم المعلومات من خلال وضع استراتيجية شاملة للإجراءات الأمنية. بينما توضح دراسة Li, H. (2017: 13) أن الأمن السيبراني مختلف عن أمن المعلومات بمعنى أن الأمن السيبراني يتعلق بالمخاطر الأمنية المتعلقة بالهجمات الإلكترونية، ونتيجة لذلك ظهرت مجموعة متنوعة من المصطلحات والتعريفات المتباينة في الأدب. أثارت جدل كبيراً حول الأمن السيبراني وأمن المعلومات.

١/١مخاطر الأمن السيبراني وفقاً للإصدارات المهنية الدولية

أوضح AICPA, (2017b) أن الأمن السيبراني يمثل "عملية تطبيق الإجراءات الأمنية لضمان سرية البيانات وتكاملها وتوافرها" وبالتالي فإن الأمن السيبراني عبارة عن مجموعة من التقنيات والعمليات والممارسات التي تحمي وتضمن حماية أصول المنظمة مثل المعلومات والأنظمة. كما يوضح المعهد الوطني للمعايير والتكنولوجيا (NIST, 2018) بأن الأمن السيبرانى" وسيلة لحماية المعلومات عن طريق منع الهجمات وكشفها والاستجابة لها". كما تعرف المبادرة الوطنية لمهنة ودراسات الأمن السيبراني (NICCS: 2017) الأمن السيبراني بأنه " النشاط أو العملية أو القدرة أو الحالة التي يتم بموجبها حماية أنظمة المعلومات والاتصالات والمعلومات الواردة فيها والدفاع عنها ضد التعطيل أو الاستخدام غير المصرح به أو التعديل أو الاستغلال" ، وأوضحت دراسة كلاً من No, W. G., & Vasarhelyi, &Haapamäki, E., & Sihvonen, J. (2019 :810) M. A. (2017:1) أن الأمن السيبراني يشمل "التقنيات والعمليات والضوابط المصممة لحماية الأنظمة والشبكات والبيانات من الهجمات السيبرانية، يقلل الأمن السيبراني الفعال من مخاطر الهجمات السيبرانية ويحمي المجتمعات والمنظمات والأفراد من الاستغلال غير المصرح به للأنظمة والشبكات والتكنولوجيات.

وتناولت دراسة Hasanefendioglu., B., (2018:73) الأمن السيبراني على اعتباره "مجموعة استباقية من ردود الفعل التي تحتوي على العمليات التي أنشأتها المنشأة باستخدام أدوات تكنولوجيا المعلومات لمنع التهديدات السيبرانية الناتجة عن استغلال نقاط الضعف في نظام المعلومات الخاص بالمنشأة والتي قد تتسبب في خسائر مالية نتيجة التأثيرات السلبية على سمعة المنشأة مما يتسبب في مواجهة المنشأة لمشاكل في تحقيق أهدافها الاستراتيجية وفقدان سمعتها وتكبدها لمبالغ مالية، كما أشارت دراسة (Althonayan, A., & Andronache, A. (2018:69 إلى الأمن السيبراني " مجموعة من الأدوات والسياسات ومفاهيم الأمن والضمانات الأمنية والمبادئ التوجيهية وأساليب إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمان والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمة والمستخدمين.

وأوضحت دراسة Möller D.P.., Haas R.E. (2019:377) أن الأمن السيبراني عبارة عن "مجموعة من التقنيات والعمليات والممارسات المصممة لحماية أجهزة الكمبيوتر والبيانات والشبكات والبرامج من الاختراق أو التلف أو الوصول غير المصرح به من الهجمات الإلكترونية، وأشارت دراسة Ursillo, S., & Arnold, C. (2019) إلى الأمن السيبراني بأنه" وسيلة لضمان أمن بيانات المنشأة من الهجمات الداخلية والخارجية الخبيثة ويشمل مجموعة من التقنيات والعمليات والهياكل والممارسات المستخدمة لحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الوصول غير المصرح به أو منع أو تخفيف الأضرار الناتجة عن الوصول غير المصـــرح". ومع تعدد تعريفات الأمن السيبراني واختلافها في بعض الأحيان فإن الأمن السيبراني وفق لتلك التعريفات تشير من وجهه نظر الباحثة إلى الأنشطة والمصادر المشتركة التي تمكن الأفراد والمنشآت والحكومات من الوصول إلى أهدافهم الخاصة في معالجة البيانات بشكل آمن وخاص وموثوق.

هذا وتشير الدراسات والتقارير إلى أن مخاطر الأمن السيبراني خلال السنوات الأخيرة قد زادت لتصبح من أهم وأخطر التحديات التي تواجه المجتمعات والحكومات والدول وكافة منشآت الأعمال WEF, (2020: 11)&IIA. 2019& Li, H,(2017:12) وغالباً ما ينظر إلى الأمن السيبـراني علـى أنـه مصـدر قلق عـالي المستـوى للمنظمات والمـؤسسات والحـكومات، والحقيقة أن لهذا القلق ما يبرره؛ فبحلول عام ٢٠٢١ ، زادت الهجمات الإلكترونية من كل نوع تقريباً بمعدلات مرتفعة ، فبحسب تقرير SonicWall: (2022: 5)، ارتفع عدد التهديدات المشفرة في عام ٢٠٢١ بنسبة ١٦٧٪ (١٠,٤ مليون هجوم)، ارتفعت فيروسات الفدية بنسبة ١٠٥٪ (٦٢٣,٣ مليون هجوم) ، وارتفعت هجمات Cryptojacking (الهجمات على أجهزة الكمبيوتر لتعدين العملات المشفرة) بنسبة ١٩٪ (٩٧,١ مليون هجوم) ، وارتفعت محاولات التسلل بنسبة ١١٪ (٥,٣ تريليون هجوم) والبرامج الضارة الموجهة إلى إنترنت الأشياء (IoT) ارتفعت بنسبة ٦٪ (٦٠,١ مليون هجوم). إضافة إلى ذلك فإن كل هذه الهجمات تحمل تكلفة كبيرة للأضرار التي تسببها إجمالي التكاليف السنوية للهجمات الإلكترونية ومن المتوقع أن تصل إلى ١٠,٥ تريليون دولار بحلول عام ٢٠٢٥، بمتوسط نمو يبلغ ١٥٪ على أساس سنوي.

ووفقاً (للهيئة الوطنية للأمن السيبراني، ٢٠١٨) فإن المخاطر السيبرانية تمثل المخاطر التي تمس أعمال المنشأة بما في ذلك رؤيتها أو رسالتها أو إداراتها أو صورتها أو سمعتها أو أصولها أو الأفراد أو الجهات الأخرى أو الدولة، بسبب إمكانية الوصول غير المصرح به أو الاستخدام أو الإفشاء أو التعطيل أو التعديل أو تدمير المعلومات أو نظم المعلومات. وأوضحت دراسة (Florackis, C., et al (2020: 2 مخاطر الأمن السيبراني بأنها " مخاطر احتمال حدوث خسارة مالية أو الاضطراب أو الإضرار بسمعة الشركة نتيجة عطل في أنظمة تكنولوجيا المعلومات الخاصة بها بسبب الهجمات الخارجيةK حيث تشمل مخاطر الأمن السيبراني مخاطر فقدان البيانات الحساسة، وتعطيل شبكة الشركة، والأضرار بالأنظمة والخدمات الإلكترونية.

وتشير دراسة Hartmann, C. C., &Carmenate, J. (2021: 9-23) إلى أن المخاطر السيبرانية يقصد بها المخاطر التشغيلية على أصول المعلومات والتكنولوجيا التي لها عواقب تؤثر على سرية وسلامة ونظم المعلومات ومقارنة بفئات المخاطر التي يغطيها التأمين فإن المخاطر السيبرانية تتفق من حيث الخصائص والمسئولية مع مخاطر كل من الممتلكات والخصوم وكذلك المخاطر الكارثية والتشغيلية، ومما لاشك فيه أن تكنولوجيا المعلومات والاتصالات تتيح إمكانات هائلة وغير مسبوقة لإنتاجية أفضل في جميع القطاعات وللتواصل عبر القارات إلا أن البنية التحتية لهذه التقنيات تمثل ارتباطا بين مصالح متعددة وخدمات مختلفة ودول عديدة الأمر الذي يجعل الأخطار في المجال السيبراني أخطارا عالمية فلا يمكن لأي جهة أن تضمن بقاءها بعيدة عن الأخطار ما دامت سلامة الآخرين معرضة للخطر.

وتختلف الهجمات الإلكترونية باختلاف أهدافها فيمكن أن تهدف إلى السرقة والابتزاز أو تدمير الأصول المالية أو سرقة الملكية الفكرية أو سرقة المعلومات الحساسة الأخرى التي تخص الشركات أو عملائها أو شركائها التجاريين، وقد تهدف الهجمات الإلكترونية أيضاً إلي تعطيل عمليات الشركات أو عمليات شركائها التجاريين، ويشمل الاستهداف أيضاً الشركات التي تعمل في الصناعات المسؤولة عن البنية التحتية الحيوية لتكنولوجيا المعلومات والاتصالات (SEC. 2018 :4).

وبشكل عام تصنف مخاطر التهديدات السيبرانية إلى ثلاثة أنواع رئيسية تتمثل أولهما في المخاطر المالية والتشغيلية فبغض النظر عن حجم الصناعة أو المنظمة أو نوع الهجوم، فإن اختراق بيانات الشركة يتسبب في تحملها لتكاليف كبيرة، وتشمل هذه التكاليف كل من تكاليف الاستثمار في التكنولوجيا والغرامات والرسوم القانونية وتكاليف الخطر وفقدان المبيعات (Moreira: 2019). فقد تؤدي الحوادث السيبرانية إلى انخفاض التدفقات النقدية المستقبلية مما يؤدي الى انخفاض قيمة بعض الأصول بما في ذلك الشهرة والأصول غير الملموسة المتعلقة بالعملاء والعلامة التجارية أو براءات الاختراع أو البرمجيات أو الأصول الأخرى طويلة الأجل المرتبطة بالأجهزة أو البرامج والمخزون (SEC'. 2011). ولقد أشارت دراسة أجريت في عام ٢٠١٦ إلى أن (٦٤) شركة تعرضت لاختراق بياناتها وبلغ متوسط التكلفة لكل اختراق مبلغ وقدره ٧ ملايين دولار (Mordor Intelligence: 2020)، ويقدر العديد من المراقبين أن التكلفة الإجمالية للأضرار المتعلقة بجرائم الإنترنت قد تجاوزت حتى الآن تريليون دولار سنوياً (Li, H., et. al.: 2018 :41) وبلغ حجم سوق الأمن السيبراني العالمي إلى ١٦١,٠٧ مليار دولار أمريكي خلال عام (٢٠١٩م) ومن المتوقع أن ينمو حجم هذا السوق إلى ٣٦٣,٠٥ مليار دولار أمريكي بحلول عام ٢٠٢٥. (Mordor Intelligence. (2020

وبالنسبـــة للمخاطر التشغيلية يمكن أن تشمل الاحتيال والأمن وحماية الخصوصية والمخاطر القانونية والمخاطر المادية (مثل تعطيل البنية التحتية)، والمخاطر البيئية، وتؤثر المخاطر التشغيلية على رضاء العملاء وسمعة الشركة وحقوق المساهمين مع زيادة المخاطر الشاملة للمنشأة Lawrence, A., et al (2018:140) ، وبشكل عام فإن الشركات التي تقع ضحية للهجمات السيبرانية الناجحة أو التي تعاني من ضعف في أمنها السيبراني قد تتحمل تكاليف وخسائر كبيرة، وتعاني من أثار سلبية أخرى. Nick Eubanks (2017)

ويتطلب هذا الأمر ضرورة التعرف على موقف المراجع الخارجي من تكاليف الإصلاح والتي تتمثل في التكاليف الناتجة عن المسئولية عن الأصول أو المعلومات المسروقة وتكاليف إصلاح تلف النظام والحوافز الممنوحة للعملاء أو شركاء العمل في محاولة للحفاظ على العلاقات بعد الهجوم السيبراني، إضافة إلى زيادة تكاليف حماية الأمن السيبراني وقد تشمل تكاليف التغييرات التنظيمية وتوفير المزيد من الموظفين أو تدريب الموظفين الحاليين وتكاليف الحصول على تقنيات الحماية وإشراك خبراء واستشاريين. وتكاليف التقاضي والمخاطر القانونية بما في ذلك الإجراءات التنظيمية من قبل الدولة والسلطات الحكومية والسلطات الأخرى وضرر السمعة الذي يؤثر سلباً على ثقة العملاء أو المستثمرين، والإضرار بالقدرة التنافسية للشركة وسعر السهم وقيمة الاستثمارات طويل الأجل. Nick Eubanks (2017)

وثانيهما مخاطر السمعة والتي تتمثل في أنه قد يكون للهجمات الإلكترونية تداعيات وتأثيرات ترتبط بعلاقات المنشأة مع عملائها أو موردیها فمن المحتمل أن تلحق الهجمات السيبرانية الضرر بسمعة الشركة والسبب في ذلك أن الضرر يمكن أن يلحق بالعملاء فيصبحون ضحايا للهجمات السيبرانية لأن المعلومات المسروقة عادةً تعرض العملاء لسرقة الهوية أو حتى الخسائر المالية DiStaso, M. W. (2018)، ولقد أشار أحد الاستطلاعات أن٨٦ % من العملاء من غير المحتمل أن يتعاملوا مع الشركة التي تتعرض لاختراق قواعد بياناتها الحساسة.

فقد أشارت دراسة مشتركة IBM Security and Ponemon Institute.(2019: 5) إلى أن فقدان الأعمال يمثل أكبر عامل يساهم في ارتفاع تكاليف اختراق البيانات إذ أن فقدان ثقة العملاء ينتج عنه مخاطر مالية كبيرة وخسارة الأعمال هي أكبر فئات التكاليف الرئيسية الخارجية التي تساهم في إجمالي تكلفة اختراق البيانات، قد بلغ متوسط تكلفة الأعمال المفقودة للمنشآت في دراسة (٢٠١٩) مبلغ ١,٤٢ مليون دولار وهو ما يمثل ٣٦ % من إجمالي متوسط التكلفة البالغة ٣,٩٢ مليون دولار. وأشارت الدراسة إلى أن الاختراقات تسببت في معدل دوران غير طبيعي للعملاء بنسبة بلغت ٣,٩ % في عام٢٠١٩، وانتهت دراسة Kamiya, S., et al (2020:1) إلى أن الهجمات السيبرانية الناجحة تؤثر سلباً على أسعار أسهم الشركات في صناعة معينة، إضافة إلى أن الهجمات الناجحة التي يترتب عليها فقدان المعلومات المالية الشخصية للعملاء، توفر إشارات سلبية عن إدارة المخاطر السيبرانية للشركات المستهدفة وأصحاب المصلحة فيها والمنافسين مما يؤثر سلباً على سمعة الشركات، كما توصلت الدراسة أن الهجوم السيبراني الناجح والذي ينتج عنه فقدان المعلومات المالية للأفراد والمنظمات، يقلل من ثروة المساهمين بنسبة ١,٠٩٪ خلال ثلاثة أيام بعد الهجوم السيبراني.

وثالثهما مخاطر الامتثال – القانونية حيث كان ظهور التهديدات السيبرانية حافزاً لمعظم الدول لوضع قوانين وقواعد صارمة للأمن السيبراني بهدف الحفاظ على سرية وسلامة وتوافر نظم المعلومات في الفضاء السيبراني، كما كانت الدافع الرئيسي وراء معظم الجهود التنظيمية Deelman, E., et. al. ,(2019 :13-15) &Cojocaru, I., & Cojocaru, I. (2019) ، ويتطلب حماية الأمن السيبراني تنفيذ الضمانات أو الإجراءات المناسبة لمواجهة أي مخاطر تتعلق بالأمن السيبراني والتي منها إمتثال المنظمات بمتطلبات السلامة من خلال تدريب الموظفين والحصول على معدات الحماية المناسبة لحماية الأمن السيبراني، كما تتطلب تلك المتطلبات اعتماد إجراءات للحماية مثل الجدران النارية وبرامج مكافحة الفيروسات وإجراءات التشفير، وأنظمة كشف التسلل وما إلى ذلك، حيث يؤدي عدم الامتثال إلى تعرض المنشآت للدعاوى القضائية والإجراءات العقابية وعلى سبيل المثال لا الحصر، رفع دعوى قضائية ضد المنشأة نتيجة فشلها في حماية المعلومات الحساسة للعملاء أو الأطراف الأخرى ذات العلاقة، كما أصبحت الدعاوى القضائية التي يرفعها المستهلكون والموظفون على الشركات والمرتبطة بالمخاطر السيبرانية شيئاً وارداً. Marotta, A., & Madnick, S. (2020:2)

٢/١ انعكاسات مخاطر الأمن السيبراني بمنشأة العميل على أعمال المراجع الخارجي

تؤدي الحوادث السيبرانية إلى تحمل المنشآت لأعباء مالية، تؤثر على التقارير المالية ويمكن أن يكون التأثير المالي على الشركات كبيراً وأن يتسبب في أضرار بالغة على مستوى جميع نواحي المنشأة ويمكن أن تستمر تلك الهجمات دون أن تكتشف مما يترتب عليه آثار مالية على المنشأة قد لا تعكس في التقارير المالية، على هذا الأساس تعتبر مخاطر الأمن السيبراني موضوعاً أساسياً في عملية مراجعة التقارير المالية وبالتالي يجب على المراجع أن ينظر ويقيم أثر هذه المخاطر على التقارير المالية ومن ثم مدى الاستجابة لمعالجة تلك المخاطر . ISCA(2018)

فمن منظور المراجعة تؤثر إدارة مخاطر المنشأة محل المراجعة على تقدير مخاطر التحريفات على مستوى تأكيدات التقارير المالية والتي تؤثر على تخطيط عملية المراجعة وترتبط مخاطر الأمن السيبراني بكافة الشركات باستثناء الشركات التي تقوم بأعمالها كاملة بشكل يدوي أي بدون استخدام أي وسائل تكنولوجية أو اتصالات عبر الإنترنت ويعد ذلك نادر جداً في وقتنا الحالي، وخلاف ذلك فإن الفضاء السيبراني سوف يجعل المخاطر السيبرانية أمراً واقعاً وإن كان بدرجات متفاوتة. Cohen, J., et al (2017)

ولقد أشارت دراسة No, W. G., & Vasarhelyi, M. A. (2017:2) إلى أن مخاطر الأمن السيبراني يمكن أن تؤثر بشكل واضح على الحالة الاقتصادية للمنشأة، فمتوسط خسائر الهجمات السيبرانية تكون مرتفعة جداً، وحول مسئوليات المراجع الخارجي طرحت الباحثة تساؤلً مهمً للغاية، إذ لم يكن للمراجع دور في ربط المعلومات المالية والمعلومات المتعلقة بالمخاطر السيبرانية في شكل من أشكال الضمانات التي يمكن تقديمها للمساهمين فمن الذي يجب أن يأخذ هذا الدور؟ وفي ضوء ذلك ومن خلال تحليل الدراسات الأكاديمية ومناقشات المنظمات المهتمة بالمهنة والإصدارات ذات العلاقة، فإنه يمكن القول أن هناك عدة أسباب تستدعي انتباه المراجع الخارجي لمخاطر الأمن السيبراني من منطلق إمكانية تأثيرها على سلامة التقارير المالية لعملائهم ومن أهمها:

١- تقييم تكاليف الحوادث السيبرانية، وتقييم أثرها النهائي على التقارير المالية وجودة الإفصاح عنها:

أشارت دراسة Haapamäki, E., & Sihvonen, J. (2019:811) أنه عند حدوث هجمات الأمن السيبراني، يكون المراجع الخارجي مسئول عن تقييم أسلوب العميل في المحاسبة عن الخسائر والمطالبات والالتزامات المتعلقة بالحادثة وتقييم أثرها النهائي على التقارير المالية؛ حيث أنه عادةً ما تتحمل المنشآت التي تتعرض لمخاطر الأمن السيبراني تكاليف مباشرة وغير مباشرة عديدة وغير متوقعة وتشمل التكاليف المباشرة تكاليف إصلاح الاضرار والرسوم القانونية والغرامات وفقدان المعاملات وفقدان المبيعات وتشمل التكاليف غير المباشرة فقدان الإيرادات الحالية والمستقبلية بالإضافة إلى تدهور ثقة العملاء والمساهمين، هذه التكاليف بحكم تعريفها عادة يصعب تقديرها لذلك فإنها إلى حد ما تخضع للتقدير والحكم الشخصي والذي يزيد في الأخير من مخاطر المراجعة الخارجية.

وتشير دراسة Ursillo, S., & Arnold, C. (2019) إلى أن فقدان المنشآت لبيانات عملائها، قد يؤدي إلى اتخاذ إجراءات قانونية أو تنظيمية ضد المنشأة، فقد يرفع طرف ثالث دعوى قضائية ضد المنشأة نتيجة الأضرار التي تعرضوا لها، وقد تخضع المنشأة أيضاً لعقوبات أو إجراءات قانونية ناتجة عن الانتهاكات لقوانين الخصوصية، وبهذا الخصوص فقد أشار الاتحاد الدولي للمحاسبين (ISA:250) بعنوان "مراعاة القوانين واللوائح عند مراجعة قوائم مالية" أن عدم الإمتثال للقوانين واللوائح قد يؤدي إلى فرض غرامات أو دعاوى قضائية أو عقوبات أخرى على المنشأة وقد يكون لها تأثير جوهري على مستوى تأكيدات القوائم المالية.

٢- تقييم نظام الرقابة الداخلية على التقارير المالية:

تنشئ الشركات أنظمة رقابة داخلية لتوفير ضمان معقول حول تحقيق الأهداف بالفعالية والكفاءة التشغيلية المطلوبة وإعداد التقارير المالية الموثوقة والامتثال للقانون واللوائح (COSO,2004) وقد تؤثر حادثة الأمن السيبراني بشكل مباشر على الضوابط الداخلية وعلى التقارير المالية للشركة المتضررة وتضعفها وفي هذه الحالة قد يتم تحريف دفاتر وسجلات الشركة مما قد يؤدي إلى التلاعب بالبيانات المالية(Rosati, P., et al. (2020: 3 . وبالتالي قد تشير حوادث الأمن السيبراني أيضاً إلى حالات فشل محتملة في الرقابة الداخلية ويكون المراجع الخارجي مسئول قانوناً عن اكتشاف أوجه القصور في ضوابط الرقابة الداخلية ، ويمكن أن يكون لتهديدات الأمن السيبراني آثار كبيرة على فعالية الرقابة الداخلية حالياً أو في المستقبل وبالتالي قد يكون المراجع ملزماً بالتحقيق فيما إذا كانت الإدارة قد نفذت الضوابط المناسبة لتهديد معروف وما إذا كانت الضوابط التي تم تنفيذها من شأنه أن يقلل من مخاطر التحريفات الجوهرية المستقبلية في البيانات المالية للعميل Calderon, T. G., & Gao, L. (2021:26)

ونظراً للاستخدام المتزايد لتكنولوجيا المعلومات في إعداد التقارير المالية وكذلك في القيام بأنشطة الأعمال المختلفة، والطبيعة المترابطة لأنظمة تكنولوجيا المعلومات الحديثة بالأعمال على طول سلسلة القيمة فإن المراجع مطالب عملياً بتوسيع مراجعته لتشمل أنظمة أخرى يمكن استغلالها في الوصول غير المصرح به وبغض النظر عما إذا كان هذا النظام يتعلق مباشرة بإعداد التقارير المالية والمحاسبة

أو بالأنشطة التشغيلية حيث قد يؤثر ضعف عنصر معين على العناصر الأخرى Lawrence, A., et al (2018:140). ويشير دليل الرقابة على المخاطر الإلكترونية لمجالس الشركات في أوروبا الصادر عن NACD. (2020. :14) إلى أن الترابط الهائل بين أنظمة معلومات المنشأة وبين الأطراف على طول سلسلة التوريد كبائعين أو موردين أو شركاء أو عملاء أو موظفين أو أي طرف مرتبط بالمنشأة إلكترونياً يمكن أن يصبح نقطة ضعف يتسلل منها المهاجمين حيث قد يتمكن المهاجمين من التسلل بعمق إلى شبكات الشركات ومهاجمة طبقات مختلفة من الأنظمة بما في ذلك أنظمة تخطيط موارد المؤسسات (ERP) ودفتر الأستاذ العام، ونظراً للوظائف المركزية لنظم المعلومات المحاسبية للشركة فمن المحتمل أن تكون تشكل البيانات المخزنة على تلك الأنظمة ثروة ذات أهمية كبيرة لمجرمي الإنترنت، ويجب على المراجعين الخارجيين النظر في المخاطر المحتملة التي تأتي من تهديدات الأمن السيبراني لهذه البيانات (Li, H. :(2017: 13-18.

وفي اتجاه آخر يعد الارتباط بين إدارة مخاطر المنشأة وعملية إعداد التقارير المالية أمراً مهماً لأنه من الضروري أن تعكس التقارير المالية الوضع المالي للشركة بشكل مناسب إلى جانب المخاطر التي كشفت عنها إدارة مخاطر المنشأة، فعندما يكون نظام العميل الخاص بإدارة المخاطر غير فعال فإنه قد يترتب على ذلك وجود قصور في عملية تحديد وتقييم أو الافصاح عن المخاطر الهامة التي تؤثر على التقارير المالية، فقد لا يتم أخذ المخاطر في الإعتبار بشكل صحيح عند وضع التقديرات المحاسبية أو عند الإفصاح، وتؤثر إدارة مخاطر المنشأة على فعالية وكفاءة الرقابة على المخاطر وضوابطها مما يؤثر على ضوابط الرقابة الداخلية وكذلك على تقييمات المراجع لمخاطر المراجعة وتخطيط عملية المراجعة. Cohen, J., et al (2017)

حيث أكدت دراسة(Masoud, N., & Al-Utaibi, G.(2022 على أهمية إعداد التقارير المالية عند تقييم الآثار المترتبة على حوادث الأمن السيبراني والتي قد تشير إلى أوجه القصور في إعداد التقارير المالية في المستقبل، ومؤشرات مخاطر الأمن السيبراني، وتحديداً فإن الأسئلة المتعلقة بكيفية تأثير الإفصاح عن مخاطر الأمن السيبراني على تقييم الشركة بسبب التغيير في تصورات المخاطر تؤثر على أوجه القصور في التقارير المالية، ويشير هذا الأمر بطبيعة الحال إلى وجود نقاط الضعف المادية للرقابة الداخلية في إعداد التقارير المالية، وبالتالي يمكن أن يمثل عوامل خطر كبيرة على جودة التقارير المالية الواردة في التقارير السنوية للشركات، حيث يمكن أن تؤدي حوادث مخاطر الأمن السيبراني في المؤسسات الكبرى إلى إلحاق أضرار جسيمة بالشركات المخالفة من حيث تكاليف العلاج والغرامات والسمعة لسنوات(Rosati, P.,et al (2019 وفى هذا السياق ناقشت المجموعة الاستشارية الدائمة لمجلس الرقابة على شركات المحاسبة العامة (PCAOB) أيضاً أن الآثار المحتملة لمخاطر الأمن السيبراني والهجمات الإلكترونية قد تكون كبيرة على التقارير المالية وعملية المراجعة.

٣- الاستجابة للضغوط المتزايدة من المنظمين والمهتمين بالمهنة:

نظراً لأهمية الأمن السيبراني وتعاظم مخاطره، فقد تزايدت ضغوط المنظمين والمهتمين بالمهنة على المراجع الخارجي فيما يتعلق بضرورة الإنتباه إلى موضوع الأمن السيبراني، فقد أكد مركز جودة المراجعة (CAQ. 2014, 2016, 2017) حقيقة أنه يجب على المراجع الانتباه بشكل خاص إلى المخاطر والتهديدات السيبرانية، حيث يمكن أن يلعب المراجع دوراً مهماً في منع أو تخفيف

آثار تلك الحوادث من خلال توفير ضمانات إضافية حول ضوابط تكنولوجيا المعلومات لمنشأة العميل، كما أكد (PCAOB, 2013) على ضرورة تقييم المراجعين لمخاطر الأمن السيبراني لعملائهم بغض النظر عن ما إذا كانوا قد تأثروا فعلاً بتهديد أو هجوم سيبراني معين أم لا وأنه يجب تضمين مخاطر الأمن السيبراني كجزء من تقييم المراجع لمخاطر تكنولوجيا المعلومات في منشأة العميل وعلى هذا النحو يجب أن تكون مخاطر الأمن السيبراني جزءاً من عملية التقييم الشامل لمخاطر المراجعة، ومؤخراً شدد (PCAOB, 2018) على أن الأمن السيبراني يمثل خطراً متنامياً للمراجعين ويتطلب تركيزاً مستمراً ويظل هذا الخطر قائماً حتى لو لم تؤثر حادثة سابقة على الرقابة الداخلية لأنها قد تسلط الضوء على نقاط ضعف محتملة.

وأشارت تعديلات معيار المراجعة الدولي رقم (ISA: 315) بعنوان " التعرف على مخاطر التحريف الجوهري وتقييمها" وهو المعيار الذي ذكر صراحة الأمن السيبراني والذي بدأ سريانه اعتباراً من ١٥ ديسمبر ٢٠٢٢ إلى أنه قد يتضمن نظر المراجع في مخاطر الأمن السيبراني التحقق من الوصول غير المصرح به والمخاطر المتعلقة بالوصول غير المصرح به من قبل الأطراف الداخلية أو الخارجية، وقد لا تؤثر هذه المخاطر بالضرورة على التقارير المالية، وإنما تشير إلى وجود اختلالات في نظام الرقابة الداخلية.

فبينما تمثل حوادث الأمن السيبراني تهديداً واضحاً للشركات المخترقة، فإنها تحمل أيضاً مخاطر للمراجعة الخارجية، خاصةً مع اعتبار أن تقارير المراجعة الخارجية تمثل ضماناً موضوعياً ومستقلاً عن جودة التقارير المالية لعملائهم، والمراجع الخارجي مسئول عن مراجعة القوائم المالية والرقابة الداخلية عليها وبالتالي فإنه يوفر ضماناً لأصحاب المصلحة الخارجيين حول جودة وموثوقية المعلومات الواردة في تلك التقارير المالية (Kajüter,p., et. al. (2017 :24).وشددت لجنة الأوراق المالية (SEC, 2014, 2015, 2018) على أهمية الإفصاح عن مخاطر الأمن السيبراني بشكل صريح في التقارير المالية للشركات المسجلة في البورصة الأمريكية حيث يتوجب الإفصاح عن أي معلومات حول المخاطر المادية وتطوراتها ضمن تقاريرهم السنوية، وتواجه الشركات تحديات خاصة في الإفصاح عن تهديدات الأمن السيبراني بشكل علني ويرجع ذلك جزئياً إلى الحاجة إلى الإفصاح عن المعلومات المادية مع الاحتفاظ بالمعلومات الحساسة المحتملة بعيداً عن أي تهديدات.

كما يشير مركز جودة المراجعة (CAQ. 2016) ومجلس معايير المراجعة والتأكيد (AUASB: 2021) ومعيار المراجعة الدولي (ISA:315) المتعلق بالأمن السيبراني ومسئوليات المراجع الخارجي إلى أن مسئولية المراجع الخارجي عن مخاطر وضوابط الأمن السيبراني تقع ضمن نطاق مسئوليته عن تأثيراتها المادية والجوهرية في التقارير المالية وأصول الشركة. وتتطلب معايير المراجعة للقيام بمراجعة القوائم المالية للعميل والحصول على فهم بكيفية إستخدام الشركة لتقنية المعلومات وتأثير تكنولوجيا المعلومات على البيانات المالية، وفهم مدى صلة الضوابط الإلكترونية بالتقارير المالية وبما في ذلك الضوابط العامة لتكنولوجيا المعلومات ومدى التشغيل الفعال لتلك الضوابط وموثوقية البيانات والتقارير محل المراجعة والتي تم إعدادها من قبل الشركة.

يتضح مما سبق أن مخاطر الأمن السيبراني وبغض النظر عن طبيعتها فإنها تؤثر من نواحي عدة على أعمال المراجعة؛ فعند وقوع حادثة للأمن السيبراني فإن المراجع الخارجي يقيم عناصر الضعف في الرقابة الداخلية والآثار المترتبة للحادثة على التقارير المالية للشركة، والسعي لتخفيض مخاطر المراجعة. فتؤكد دراسة Hamm, K. (2019) على أن المراجع الخارجي في الوقت الحالي يلعب دوراً مهماً ولكن محدوداً حيث لا يقوم المراجع بتقييم مخاطر الأمن السيبراني للشركة بشكل عام أو بتقييم تصميم وفعالية تشغيل الضوابط غير المالية المعتمدة من قبل الشركة للتخفيف من تلك المخاطر، إنما يركز المراجع على تكنولوجيا المعلومات التي تستخدمها الشركة لإعداد البيانات المالية، ويركز أيضاً على الضوابط الإلكترونية المتعلقة بالتقارير المالية، مثل الضوابط التي تتعلق بموثوقية البيانات والتقارير الأساسية. وعند إجراء عمليات المراجعة المتكاملة، يقوم المراجع أيضاً بتقييم الرقابة الداخلية على التقارير المالية بشكل منفصل.

حيث قد تؤدي الحوادث إلى إنخفاض التدفقات النقدية المستقبلية مما يتطلب النظر في مدى انخفاض قيمة بعض الأصول بما في ذلك الشهرة والأصول غير الملموسة المتعلقة بالعملاء أو العلامات التجارية أو براءات الاختراع أو البرمجيات الرأسمالية أو الأصول الأخرى طويلة الأجل المرتبطة بـالأجهزة أو البرامج والمخزون، وفى هذا السياق تتمثل نطاق مسئولية المراجع الخارجي عن الأمن السيبراني في إطار مراجعة التقارير المالية والرقابة الداخلية على التقارير المالية في ضوء المعايير والإصدارات والدراسات (AUASB: 2021) (CAQ. 2014, 2016, 2017, 2020) فيما يلي:

١- أن يحصل المراجع على الفهم الكافي لبيئة تكنولوجيا المعلومات والعمليات المرتبطة بتدفق المعاملات ومعالجة المعلومات في نظام المعلومات ويقوم المراجع بجمع معلومات حول طبيعة وخصائص تطبيقات تكنولوجيا المعلومات المستخدمة بالإضافة إلى البنية التحتية الداعمة لتكنولوجيا المعلومات وتقييم تأثير تكنولوجيا المعلومات على التقارير المالية (IFA. ISA 315:2019) ، حيث يساعد فهم المراجع لأعمال المنشأة وكيفية إستخدامها لتكنولوجيا المعلومات على فهم مخاطر الأعمال التي تواجهها منشأة العميل وخصوصاً تلك المخاطر التي تؤدي إلى نشوء أخطاء جوهرية في التقارير المالية وعليه فإن الأمن السيبراني يشكل خطراً على معظم المنشآت إلا أن هذا الخطر لا يؤدي دائماً إلى تحريفات جوهرية في التقارير المالية، وقد لا يتطلب من المراجع تصميم وتنفيذ أي إجراءات إستجابة. فوفقاً لمعيار المراجعة الدولي (IFA. ISA315:2019) يجب تحديد وتقييم مخاطر التحريفات الجوهرية سواء كانت ناتجة عن الإحتيال أو الأخطاء بناءً على فهم بيئة منشأة العميل ويتطلب ذلك تقييم مخاطر التحريفات الجوهرية في التقارير المالية وبما في ذلك مخاطر الأمن السيبراني الناتجة عن الوصول غير المصرح به.

٢- إعتبار الأمن السيبراني جزء من عملية تقييم المخاطر من خلال الإستفسار من المراجعين عن ما إذا كان قد حدث هجوم سيبراني ومدى نجاحه وقدرة ذلك الإختراق في التأثير على التقارير المالية، فإذا كانت المعلومات حول وجود إختراق في أحد عناصر الأمن السيبراني فإن المراجع سيحتاج إلى النظر في تأثير ذلك الإختراق على الرقابة الداخلية وإنعكاس ذلك على التقارير المالية وعليه يقرر المراجع فهم عناصر الرقابة ذات العلاقة واختبارها لتحديد التأثير المحتمل أو نطاق التحريفات المحتملة في التقارير المالية أو تقييم مدى كفاية الإفصاح الإدارة في التقارير المالية حول هذا الإختراق الأمني . (ISA:315)

٣- يستخدم المراجع منهج من أعلى إلى أسفل لمراجعة وتحديد ضوابط الرقابة الداخلية على التقارير المالية فيبدأ المراجع وفق هذا المنهج بتقييم المخاطر على مستوى التقارير المالية ومع فهم المراجع للمخاطر الكلية يمكن أن يركز على ضوابط الرقابة على مستوى المنشأة ومن ثم يعمل على الحسابات والإفصاحات الهامة والتأكيدات المرتبطة بها. يوجه هذا المنهج انتباه المراجع إلى الحسابات والإفصاحات والتأكيدات التي تقدم إمكانية معقولة للكشف عن الأخطاء الجوهرية في البيانات والإفصاحات ذات العلاقة (PCAOB, AS. No. 5, 2017) ويرى Rosati, P., et al (2019A) أن المراجع الخارجي يلعب دوراً مهماً في تحديد مدى كفاية الإفصاحات في التقارير المالية وأنها تعكس جميع الحقائق التي تؤثر على أداء الشركة أو قد تقلل من قيمة أصولها وعليه يجب علي المراجع الخارجي تحليل التقارير المالية والتحقق من حجم إستثمارات العميل في مجال الأمن السيبراني قبل وبعد إختراق الأمن السيبراني، والتحقق من إنه تم إبلاغ المستثمرين بذلك وبشكـــل مناسب وكافي.

وبناء على ما سبق أوضحت دراسة (Li, B, et. Al(2022 أهمية استجابة مكاتب وشركات المراجعة لمخاطر الأمن السيبراني من خلال الاستثمار بشكل أكبر في رأس المال البشري للأمن السيبراني من خلال استقطاب موظفين متخصصين في مجال الأمن السيبراني ومراجعين كفء في هذا المجال إضافة إلى دعم وتشجيع المراجعين على التدريب في هذا المجال لمواجهة المسئوليات الملقاة على عاتقهم في ضمان عدالة وسلامة التقارير المالية لعملائهم ، بالإضافة إلى دور المراجعين في مساعدة عملائهم غير المخترقين في زيادة الوعي بالأمن السيبراني والاستثمار في موظفي الأمن السيبراني.

٣/١ مراجعة الإفصاح عن مخاطر الأمن السيبراني (منهج إجرائي مقترح)

لقد فرضت التقنيات الناشئة ومخاطرها على المراجع الخارجي مواجهة العديد من التحديات الجديدة التي ظهرت مع اتجاه الرقمنة، ومع ذلك لا يستطيع المراجع الخارجي وحده التعامل مع تلك المشاكل والتحديات، لذلك فهو بحاجة إلى مشاركة خبراء تكنولوجيا المعلومات لإبداء رأي حول بيئة الرقابة في أنظمة تكنولوجيا المعلومات للتصدي بشكل مناسب للمخاطر الناشئة عن الاستخدام وتشغيل الحلول التكنولوجية التي لها تأثير واسع على اكتمال ودقة البيانات المالية(Barta, G. (2018 ووفقاً لإرشادات (PCAOB AS 2201.09) فإنه يجب على المراجع النظر فيما إذا كان من الأهمية الاستعانة بمهارات متخصصة لتحديد تأثير التقنيات الجديدة وللمساعدة في تقييم المخاطر وفهم تصميم وتنفيذ وفعالية تشغيل الضوابط، فإذا قرر بأهمية المهارات المتخصصة فإنه يعمل على الاستعانة بخبير في الموضوع، وفي هذا الإطار يجب أن يحصل المراجع أيضاً على فهم كافٍ بمجال العميل لتقييم مدى كفاية العمل لأغراض عملية المراجعة.

حيث أكدت دارسة Kelton, A. S., & Pennington, R. R. (2020) أنه استجابةً للمخاوف من أن أصحاب المصلحة ليس لديهم معلومات كافية في الوقت المناسب بشأن مخاطر الأمن السيبراني للشركات وجهود إدارة المخاطر أولى المنظمون وواضعو معايير المحاسبة اهتماماً متزايداً لتعزيز إفصاحات الأمن السيبراني للشركات، فقد أصدرت هيئة البورصات الأمريكية إرشادات بشأن إفصاح الشركات عن مخاطر الأمن السيبراني، توضح العوامل والإفصاحات الموصي به بشأن المسائل الجوهرية، مثل وقوع حوادث الأمن السيبراني السابقة ، واحتمال وحجم الأحداث المستقبلية للأمن

السيبراني، وأي تكاليف تقاضي ومعالجة مرتبطة بحوادث الأمن السيبراني السابقة. وأشارت الدراسات السابقة (Frank, M. L ., et al ,(2019 &Yang, L.et al. (2020 أن المعهد الأمريكي للمحاسبين القانونيين المعتمدين (AICPA,2017) قام بتطوير إطار عمل لإعداد تقارير إدارة مخاطر الأمن السيبراني لتوجيه الشركات في تعزيز عمليات الإفصاح المتعلقة بالأمن السيبراني، ويمكن استخدامها للإفصاح عن المعلومات المفيدة لأصحاب المصلحة حول برنامج إدارة مخاطر الأمن السيبراني وفعاليته، على وجه التحديد اقترح إطار العمل ثلاث أجزاء رئيسية من المعلومات تهدف إلى مساعدة أصحاب المصلحة في مراقبة برنامج إدارة مخاطر الأمن السيبراني للشركة:

١- وصف الإدارة لبرنامج إدارة مخاطر الأمن السيبراني للشركة، حيث تستخدم الإدارة معايير الوصف المناسبة لتطوير وصف الإدارة، وتزويد المستخدمين المحتملين بمعلومات حول الشركة ووصف لبرنامج إدارة مخاطر الأمن السيبراني للشركة.
٢- تأكيد الإدارة بشأن فعالية ضوابط الأمن السيبراني، وأنها تتوافق مع معايير AICPA وأن الضوابط التي تنفذها الإدارة يمكن أن تحقق أهداف الأمن السيبراني للشركة بشكل فعال، وتستند هذه الأهداف إلى مجموعة من معايير الرقابة المناسبة مثل معايير خدمات الثقة (الأمان، التوافر، السرية)
٣- رأي المراجع في إفصاحات الإدارة وفعالية ضوابط الشركة ومنها (تقرير ضوابط النظام والتنظيم للأمن السيبراني).

وأشارت دراسة Han, S. ,et al (2016:26-27) إلى أن عملية مراجعة الشركات التي تتبنا تكنولوجيا المعلومات في عملياتها بدرجة عالية، تواجه مخاطر مراجعة عالية، وخاصة في حالة مراجعة العميل لأول مرة حيث يحتاج المراجع إلى وقت وجهد للتعرف على العميل الجديد وطبيعة أنشطة تكنولوجيا المعلومات لديه، كما يحتاج المراجعين الخارجيين إلى تطوير قدراتهم في مراجعة نظم المعلومات المتطورة والرقابة الداخلية القائمة على تكنولوجيا المعلومات، وتحسين المهارات المهنية لتقليل المخاطر وكشفها عند مراجعة منظمات الأعمال كثيفة تكنولوجيا المعلومات. Rosati, P., et al (2019A)

وترى الباحثة أنه يمكن صياغة خطوات المنهج الإجرائي لمراجعة الإفصاح عن مخاطر الأمن السيبراني فيما يلي:

١/٣/١ الخطوة الأولى: التأكد من مواءمة الأمن السيبراني ضمن الأولويات التنظيمية:

يجب أن تأخذ المنظمات في الاعتبار ديناميكيات مشهد الأعمال المتغير بسرعة ليس فقط للتكيف بفعالية ولكن أيضاً لتطبيق منهج متكامل لعملية ضمان الأمن السيبراني بكفاءة بناءً على أفضل الممارسات، فمن المهم ضمان الوعي بعملية تأكيد الأمن السيبراني عبر وحدات الأعمال وهو أمر حيوي لتحقيق الأولويات التنظيمية، فهناك حاجة لتنسيق ومواءمة ضمان الأمن السيبراني مع السياسات التنظيمية لدعم وتسهيل التعاون الاستراتيجي وتبادل المعلومات بين وحدات الأعمال والموظفين ذوي الصلة في بيئة العمل اليومية، وبالتالي فإن مواءمة الأمن السيبراني والوظائف والفئات الفرعية ومعايير الصناعة وأفضل الممارسات مع متطلبات العمل وتحمل المخاطر وموارد المنظمة هي مفتاح النجاح، حيث يجب تحديد الفجوات بين الوضع الحالي والموضع المستهدف لنقاط ضعف تنفيذ الأمن السيبراني. Kahyaoglu, S. B., & Caliyurt, K. (2018)

وفى هذا أكدت دراسة Kahyaoglu, S. B., & Caliyurt, K. (2018) ضرورة إنشاء إطار عمل لمراقبة الأمن السيبراني فعادة ما يكون لدى المؤسسات إطار عمل قديم أو غير مكتمل للاستجابة للمخاطر وهي تركز بشكل كبير على تكنولوجيا المعلومات، لذا من الضروري وجود منهج متكامل للتعامل مع مخاطر الأمن السيبراني، فقد يكون هناك وعي محدود بمخاطر الأمن السيبراني على المستوى التنظيمي ولم يتم وضع منهج على مستوى المنظمة لإدارة مخاطر الأمن السيبراني بدقة، فقد تقوم المؤسسات في الغالب بتنفيذ إدارة مخاطر الأمن السيبراني على أساس غير منتظم، ويظهر دور المراجع الخارجي في التأكد من تعاون المنظمة مع منظمات تكنولوجيا المعلومات أو الهيئات المعنية لصياغة وتطوير وتنسيق المعايير أو الإرشادات أو الممارسات لتلبية احتياجاتهم بدقة.

ولحصول المراجع على فهم بيئة تكنولوجيا المعلومات ذات العلاقة بتدفقات المعاملات ومعالجة المعلومات في نظم المعلومات، يقوم المراجع بجمع معلومات حول طبيعة وخصائص تطبيقات تكنولوجيا المعلومات المستخدمة، بالإضافة إلى البنية التحتية الداعمة لتكنولوجيا المعلومات وتكنولوجيا المعلومات. ويتطلب ذلك دمج فهم المراجع للبيئة السيبرانية للمنشأة كجزء من تقييمه لمخاطر التكنولوجيا المستخدمة في المنشأة، فالبيئة السيبرانية للمنشأة هي منطقة يجب ان يفهمها المراجع فهماً كافياً (CAQ: 2016). وبالتالي توفير أساس لتصميم وتنفيذ الاستجابات للمخاطر المقدرة للتحريف الجوهري وفقاً لمعيار المراجعة الدولي رقم (٣٣٠).(ISA 330: 2019)

وبالتالي كجزء من فهم تكنولوجيا المعلومات، يحتاج المراجع إلى فهم كيفية تحديد المنشأة لمخاطر الأمن السيبراني وكيفية الرقابة عليها من خلال توسيع الفهم ليشمل البيئة السيبرانية للمنشأة، مع التركيز على الجوانب التقنية والتي منها (الأمن المطبق في أنظمة تكنولوجيا المعلومات)، إضافة إلى التركيز على العمليات (مثل الاستجابة لحادث الأمن السيبراني) والحوكمة (من يقوم بالتوجيه أو الإبلاغ عن مخاطر وتدابير الأمن السيبراني). بالإضافة إلى ذلك يجب الاهتمام بالجوانب القانونية والامتثال، حيث أن القوانين أو اللوائح ذات العلاقة باستخدام تكنولوجيا المعلومات مثل تشريعات حماية البيانات، قد يكون لها تأثير مباشر أو غير مباشر على البيانات المالية. ووفقاً لمعيار المراجعة الدولي (ISA: 250)تتمثل إجراءات المراجعة عند تحديد حدوث عدم الالتزام أو الاشتباه في حدوثة فيما يلي :

١- عندما يصبح المراجع مدركاً لمعلومات تتعلق بحالة عدم التزام، أو عدم التزام مشتبه فيه بالأنظمة واللوائح فيجب عليه أن يتوصل إلى فهم لطبيعة التصرف والظروف التي حدث فيها، وأن يحصل على المزيد من المعلومات لتقويم التأثير المحتمل على القوائم المالية.
٢- إذا اشتبه المراجع في وجود عدم التزام فيجب عليه ما لم يكون ذلك محظورا بموجب الأنظمة واللوائح مناقشة المستوى الإداري المناسب والمكلفين بالحوكمة حسب مقتضى الحال ، وإذا لم تقدم الإدارة أو المكلفون بالحوكمة معلومات كافية تؤيد التزام المنشأة بالأنظمة واللوائح ، ورأي المراجع بحسب حكمة أن عدم الالتزام المتشبه فيه قد يكون له تأثير جوهري على القوائم المالية ، فيجب أن ينظر المراجع في مدى الحاجة للحصول على مشورة قانونية، وعلى ذلك يتضمن فهم المراجع لعمليات تكنولوجيا المعلومات في المنشأة والضوابط العامة لتكنولوجيا المعلومات التي تنفذها المنشأة ضرورة فهم القوانين أو اللوائح ذات العلاقة (IFAC: ISA 250) .

وتشمل الأمثلة على المخاطر الناشئة عن استخدام تكنولوجيا المعلومات والمخاطر المتعلقة بالاعتماد على تطبيقات تكنولوجيا المعلومات غير مناسبة والتي تقوم بمعالجة البيانات بشكل غير دقيق أو معالجة البيانات غير الدقيقة أو كليهما، ما يلي: (IFAC: ISA: 315: 2019: 107)

١- الوصول غير المصرح به إلى البيانات الذي قد يؤدي إلى تدمير البيانات أو تغييرات غير مرغوبة في البيانات، بما في ذلك تسجيل معاملات غير مصرح بها أو غير حقيقية، أو التسجيل غير الدقيق للمعاملات، وتزيد هذه المخاطر نتيجة لإمكانية وصول العديد من المستخدمين إلى قاعدة البيانات المشتركة.
٢- إمكانية حصول موظفي تكنولوجيا المعلومات على امتيازات الوصول بحيث تتجاوز امتيازات الوصول اللازمة لأداء واجباتهم المعينة وبالتالي كسر الفصل بين الواجبات.
٣- تغييرات غير مصرح بها على البيانات الموجودة في الملفات الرئيسية، وتطبيقات تكنولوجيا المعلومات أو الجوانب الأخرى لبيئة تكنولوجيا المعلومات.
٤- الفشل في إجراء التغييرات اللازمة على تطبيقات تكنولوجيا المعلومات أو الجوانب الأخرى لبيئة تكنولوجيا المعلومات.
٥- تدخل يدوي غير مناسب، وفقدان محتمل للبيانات أو عدم القدرة على الوصول إلى البيانات كما هو مطلوب.

هذا ويمكن توضيح أنه بدون امتلاك المراجعين خلفية كافية في مجال الأمن السيبراني ، لا يمكن لهم المصادقة على الصحة العامة لأعمال العملاء وصحتهم المالية وهي مسئوليتهم الأساسية في عملية المراجعة، وعملياً يمكن للمراجعين اكتساب معرفة عميقة بمخاطر الأمن السيبراني عندما يقع عملاؤهم ضحية للهجمات الإلكترونية، فبعد وقوع مثل هذا الحادث يجب على المراجعين فحص البيئات الداخلية والخارجية للأمن السيبراني للشركة، وتقييم نقاط الوصول المحتملة لأنظمة المعلومات الخاصة بها، وتحديد ممارساتها الشائعة التي تمنع وتكشف الوصول غير المستهلك إلى أنظمتها وأصولها المعلوماتية. (PCAOB، 2019b)

٢/٣/١ الخطوة الثانية: التأكد من السياسات والإجراءات الخاصة في دعم عمليات الإفصاح عن إدارة مخاطر الأمن السيبراني.

تتضمن هذه الخطوة الاختبار الفعلي لتكنولوجيا المعلومات وإجراءات الرقابة الخاصة بالأمن السيبراني ضمن عناصر رقابة تكنولوجيا المعلومات الإلكترونية، ويمكن أيضاً تحديد عناصر ضوابط تكنولوجيا المعلومات السيبرانية التي سيتم اختبارها من خلال العناصر التالية:

١- اختبار رقابة تكنولوجيا المعلومات.

يمثل الأمن السيبراني من وجهة نظر الشركة مصدر قلق كبير، وعلى الصعيد الداخلي أصبحت خبرة تكنولوجيا المعلومات سمة ضرورية لأعضاء مجلس الإدارة من أجل أداء مسئولياتهم في مجال الإشراف على تكنولوجيا المعلومات والأمن السيبراني، حيث تبحث الشركات عن مديرين يتمتعون بخبرة في مجال تكنولوجيا المعلومات والأمن السيبراني من أجل إنشاء استراتيجيات دفاع إلكتروني تسمح للشركات بإدارة حوادث وانتهاكات الأمن السيبراني والتكيف مع الاضطرابات التكنولوجية. وخارجياً من المهم أن يتم إعلام المستثمرين بمخاطر وهجمات الأمن السيبراني الجوهرية التي تؤثر على الشركات التي يستثمرون فيها.(Badawy, H. A. E. S. (2021)

ووفقاً لمعيار المراجعة الدولي (ISA 315, 2019: 107) إذا استنتج المراجع أن عملية الرقابة مصممة ومنفذة بشكل فعال فقد تكون مناسبة من أجل أخذ فعاليتها التشغيلية في الاعتبار عند تصميم الإجراءات الموضوعية. ومع ذلك عندما لا يتم تصميم عنصر الرقابة أو تنفيذها بشكل فعال فلا فائدة من اختبارها، وعندما يخطط المراجع لاختبار عنصر الرقابة، فإن المعلومات التي يتم الحصول عليها حول مدى معالجة عنصر الرقابة لمخاطر التحريفات الجوهرية قد تكون بمثابة مدخلات لتقييم المخاطر الرقابية للمراجعة على مستوى التأكيد. وبالنسبة لعناصر الرقابة الآلية قد يخطط المراجع لاختبار فعالية تشغيل عناصر الرقابة التلقائية عن طريق تحديد واختبار عناصر الضوابط العامة لتكنولوجيا المعلومات التي توفر التشغيل المتسق لعنصر الرقابة الآلي بدلاً من إجراء اختبارات فعالية التشغيل على عناصر الرقابة الآلية بشكل مباشر، إن الحصول على أدلة مراجعة حول تنفيذ عنصر تحكم يدوي في وقت ما لا يوفر أدلة مراجعة حول الفعالية التشغيلية للرقابة في أوقات أخرى خلال الفترة قيد المراجعة.

ويتضمن ذلك تقييم السياسات المطبقة والإجراءات المتبعة في بيئة تكنولوجيا المعلومات بصورة شاملة في المنشأة، وذلك للتأكيد على وجود الضوابط والآليات المناسبة في الموضع الصحيح، ويحدد نطاق المراجعة مدى دقة الفحص ونظم المعلومات التي سيتم تغطيتها أو أ

ي وظائف منها، وعمليات تكنولوجيا المعلومات التي ستخضع للمراجعة، ومواقع نظم تكنولوجيا المعلومات INTOSAI (2019). واستناداً إلى ملف تعريف المخاطر السيبرانية يمكن تحديد واحد أو أكثر من عناصر رقابة تكنولوجيا المعلومات ليتم اختباره، ومن الموضوعات التي تتناولها رقابة تكنولوجيا المعلومات حوكمة الأمن السيبراني، تأمين النظام وعمليات الأمن، هذا وتغطي هذه الموضوعات الثلاثة إجراءات الحماية والاكتشاف والاستجابة، منها المراقبة الأمنية والاستجابة للحوادث والوعي الأمني والأمن السحابي، يتبع اختبار عناصر الرقابة هذه العملية نفسها تماماً مثل اختبار رقابة تكنولوجيا المعلومات السيبرانية ويمكن اعتباره امتداداً لمجموعة أدوات الضوابط العامة لتكنولوجيا المعلومات، وفي حالة عدم فعالية الرقابة على تكنولوجيا المعلومات حيث يمكن أن يكون هناك ثغرات أمنية في بيئة تكنولوجيا المعلومات يجب إجراء مزيد من الفهم والتقصي المتعمق للأمن السيبراني.(2016),.Van .M

٢. اختبار فعالية نظام الرقابة الداخلية للحد من مخاطر الأمن السيبراني

ربطت دراسة Lawrence, A., et al (2018)، بين حوادث الأمن السيبراني ونقاط الضعف المحتملة في الرقابة الداخلية حيث يمكن أن تتجسد مخاطر الأمن السيبراني في شكل ما يسمى بضعف الرقابة أكثر من التقرير، حيث تمثل الرقابة الداخلية على التقارير المالية (ICFR)عملية مصممة من قبل أو تحت إشراف المسؤولين التنفيذيين والمسؤولين الماليين الرئيسيين للشركة، أو الأشخاص الذين يؤدون وظائف مماثلة ويتم تنفيذها من قبل مجلس إدارة الشركة ، والإدارة ، والموظفين الآخرين لتقديم تأكيد معقول فيما يتعلق بموثوقية التقارير المالية وإعداد البيانات المالية للأغراض الخارجية وفقاً لمبادئ المحاسبة المقبولة عموماً، وتتضمن ICFR أيضاً الإجراءات والسياسات المتعلقة بمسك السجلات المحاسبية وتوثيق المعاملات وتفويض الإيصالات والنفقات وحماية الأصول، حيث تتطلب المادة ٤٠٤ من قانون (SOX) من الإدارة تقييم فعالية ICFR الخاصة بشركتهم وتقديم تقرير عنها، ويتطلب أيضاً من المراجعين الخارجيين المصادقة والإبلاغ عن التقييمات التي أجرتها إدارة العميل. ومن ثم فإن المراجعين الخارجيين مسؤولون قانونًا عن اكتشاف أوجه القصور في ICFR للشركات.

وفى هذا السياق أشار معيار المراجعة الدولي (٢٦٥) بعنوان " إبلاغ أوجه القصور في الرقابة الداخلية للمكلفين بالحوكمة والإدارة "، إلى ضرورة أن يتوصل المراجع إلى فهم للرقابة الداخلية ذات الصلة بالمراجعة عند تحديده لمخاطر التحريف الجوهري وتقييمها، وعند إجراء تلك التقييمات للمخاطر يأخذ المراجع في الحسبان الرقابة الداخلية من أجل تصميم إجراءات المراجعة المناسبة في ظل الظروف القائمة، وقد يتعرف المراجع على أوجه قصور في الرقابة الداخلية، ليس فقط أثناء آلية تقييم المخاطر، ولكن أيضاً في أية مرحلة أخرى من مراحل المراجعة، وعلى ذلك فإن المراجعين مسؤولون عن الحصول على فهم كاف للرقابة الداخلية على التقارير المالية من أجل تحديد وتقييم مخاطر التحريف الجوهري وتصميم وتنفيذ إجراءات مراجعة إضافية (PCAOB ،AS No. 12 2010) ، وفي حالة وقوع حادث إلكتروني فمن المتوقع أن يأخذ المراجعون الخارجيون في الاعتبار آثاره على ICFR، فإذا كان الهجوم مباشراً على أنظمة محاسبة الشركة، فقد يشمل الحادث أو قد يشير إلى مخاطر التلاعب بدفاتر وسجلات الشركة مما قد يؤثر على البيانات المالية، ولهذا فإن مدى استجابة السوق السلبية بعد الإعلان عن حادث إلكتروني يرجع إلى أن مثل هذا الحدث يشير إلى وجود نقاط ضعف جوهرية في الرقابة الداخلية.

فيما أشارت دراسة Lawrence, A., et al (2018) أنه حتى إذا لم يكن للهجمات الإلكترونية تأثير مباشر على أنظمة المحاسبة في الشركة، فقد يحتاج المراجعون الخارجيون إلى بذل جهد إضافي لأن الهجمات الإلكترونية على طبقات الشبكة الداخلية أو المحيطة قد تشير إلى نقاط ضعف في الضوابط العامة لتكنولوجيا المعلومات مما قد يشير إلى مخاطر في ICFR، وأوضحت الدراسة وجود ارتباط إيجابي بين نقاط الضعف في الرقابة التشغيلية والضعف المادي في ICFR ، مما يشير إلى أن نقاط الضعف في أي من الأنظمة والإجراءات يمكن أن تؤثر على أنشطة التقارير التشغيلية والمالية. حيث يوضح تقرير صادر عن شركة (Verizon Wireless (2016 أن الثغرات الأمنية الأقدم مُستهدفة بشكل كبير، وأن العديد من الانتهاكات مسموح بها من خلال الأخطاء أو الثغرات الأمنية المعروفة.

ونظراً إلى أن أنظمة المعلومات المحاسبية للشركات تلعب دوراً مركزيا في الأعمال ومن المحتمل أن تكون ثروة البيانات المخزنة على هذه الأنظمة ذات أهمية كبيرة لمجرمي الإنترنت، يجب على المراجعين الخارجيين النظر في المخاطر المحتملة التي تأتي من تهديدات الأمن السيبراني، وبالنظر إلى أن المراجعين الخارجيين يستجيبون للمستويات الأعلى من مخاطر الرقابة من خلال توسيع إجراءات المراجعة الخاصة بهم ، وعلى ذلك وفى ضوء معيار المراجعة الدولي رقم (٢٦٥) على المراجع اتخاذ الخطوات التالية عند اكتشاف فشل في الرقابة الداخلية ذات صلة بهجمات الأمن السيبراني:

أ- استناد إلى أعمال المراجعة التي تم تنفيذها يجب على المراجع أن يحدد ما إذا كان قد تعرف على واحد أو أكثر من أوجه القصور في الرقابة الداخلية الناتجة عن اختراقات الأمن السيبراني، والتي قد تؤدى إلى تحريفات جوهرية في القوائم المالية في المستقبل، التحديد غير الموضوعي والمعقد للمبالغ المقدرة أو قابلية تعرض الأصل أو الالتزام للفقدان أو الغش.

ب- إذا تعرف المراجع على أوجه القصور في الرقابة الداخلية، يجب أن يحدد استناد إلى أعمال المراجعة التي تم تنفيذها ما إذا كانت تشكل منفردة أو في مجملها أوجه قصور مهمة.

ج- على المراجع أن يبلغ المكلفين بالحوكمة كتابة في الوقت المناسب بأوجه القصور المهمة في الرقابة الداخلية التي تعرف عليها أثناء عملية المراجعة، كما يجب أن يبلغ المستوى الإداري المناسب المسئول في الوقت المناسب.

٣. التحقق من سياسات الإدارة بشأن مخاطر الأمن السيبراني

وفقا لدراسة (فرج ،٢٠٢٢) يشمل نموذج توكيد المراجع الخارجي على مزاعم الإدارة عن إدارة مخاطر الأمن السيبراني على ثلاثة عناصر أساسية تتمثل في :

أ- طبيعة توقيت التقرير: حيث أن تهديدات الأمن الإلكتروني مرتبطة بفترة زمنية وتستند على متغيرات متعددة منها الخصائص التنظيمية، طبيعة العمليات المعرضة للخطر خلال فترة معينة، فلا يجب أن يكون استنتاج المراجع الخارجي معبراً عن نقطة زمنية معينة وإنما يكون تقريره عن فترة زمنية ممتدة على حسب التغطية .

ب- طبيعة استنتاج المراجع: تقدم تقارير المراجعة التقليدية الرأي حول مدى عدالة تعبير التقارير المالية عن المركز المالي ونتائج الأعمال (عادلة/ غير عادلة) وهو ما لا ينطبق على حالة التوكيد على إدارة مخاطر الأمن الإلكتروني، فهي عملية مستمرة متغيرة لا تأخذ حكما واحد على طول الوقت، وإنما من الأنسب وجود مراجعة فورية مستمرة لحالة درجة الأمن الإلكتروني والتعبير عن الحالة في أوقات متتالية مستمرة.

ج- الأهمية النسبية: تنص معايير المراجعة المقبولة على مفهوم الأهمية النسبية للعناصر/ والذى يفسر عادة كنسبة من الدخل أو من إجمالي الأصول، الأمر الذى لا يصلح مع التوكيد على إدارة مخاطر الأمن السيبراني، فهناك عناصر لا يمكن قياسها نقدا مثل الاستدامة ، سلاسل التوريد، العلامات التجارية ، إدراك المخاطر، وبالتالي لا يصلح مفهوم الأهمية النسبية في هذه الحالة .

٤. مدى اعتماد المراجع الخارجي على أعمال المراجع الداخلي بشأن مخاطر الأمن السيبراني

تلعب المراجعة الداخلية دوراً أساسياً في تقييم المخاطر السيبرانية كجزء من عملية تقييم المخاطر الاستراتيجية التي تتعرض لها الشركات وتحديد فجوة الرقابة التشغيلية على مستوى الأعمال ، فوفقاً لما ذكرته دراسة (محروس& صالح ، ٢٠٢٢) أن الأمن السيبراني يأتي في المرتبة الأولى ضمن أولويات المراجعة الداخلية الرئيسية، هذا وتستطيع المراجعة الداخلية من خلال خدمات التأكيد وتقديم المشورة تحقيق التوزان والمساعدة في تحديد المساءلة بشكل واضح، كما يمكن أن تقدم المراجعة رؤيتها بشأن احتمالات زيادة مخاطر انتهاك البيانات والاختراقات الأمنية الناتجة عن تخفيف أو زيادة الضوابط الرقابية ، وعلى ذلك فإن يمكن الربط بين مراحل التعامل مع مخاطر هجمات الأمن السيبراني ودور المراجعة الداخلية وفقا لما ذكرته الدراسات السابقة (محروس ، صالح ،٢٠٢٢) & Alina, C. M., et al. (2017) على النحو التالي :

أ- مرحلة الحماية: تساعد المراجعة الداخلية من خلال العمل مع خطى الدفاع الأول والثاني في تطوير برنامج حوكمة تكنولوجيا المعلومات ويشمل استراتيجيات وسياسات الأمن السيبراني، كما أنها تشارك في تقييم واختبار مخاطر الأمن السيبراني، وعلى المراجع الخارجي التأكد من فعالية المراجعة الداخلية في تقييم خطط الأمن السيبراني وكذلك تقييم مدى فعاليتها في الحد من هذه المخاطر ، وعلى المراجع.

ب- مرحلة الكشف عن المخاطر: تقوم المراجعة الداخلية بتقييم ضوابط الرقابة على الأمن السيبراني، وتقدم تقاريرها إلى الإدارة التنفيذية ولجنة المراجعة حوال فعالية هذه الضوابط والتهديدات المحتملة ، وعلى المراجع الخارجي التحقق من فعالية الإجراءات المطبقة ومدى فعالية نظام الرقابة الداخلية.

ج- مرحلة استمرار النشاط: تعد برامج الاستجابة للمخاطر السيبرانية وبرامج استمرار النشاط من أهم أولويات منظمات الأعمال للصمود ضد الهجمات السيبرانية ، لذلك على المراجع الخارجي التأكد من فعالية دور المراجعة الداخلية في التحقق من توافر إجراءات وخطط بديلة فعالة لاستمرار النشاط في حالة وقوع هجوم سيبراني.

د- مرحلة رد الفعل: تحتاج منظمات الأعمال لإعداد برنامج إدارة الأزمة كأحد أجزاء إدارة استمرار النشاط ، ويعد تقييم المخالفات وإيجاد طرق الاستجابة المناسبة لها الخطوة الأولى في التعامل مع الهجمات السيبرانية ، حيث يجب على المراجع الخارجي تقييم مدى فعالية المراجعة الداخلية في مراقبة وتقييم مدى ملاءمة طرق الاستجابة التي اتبعتها الإدارة .

ه- مرحلة التطوير: تضيف وظيفة المراجعة الداخلية قيمة في هذه المرحلة من خلال إبداء الرأي في كل من النشاط بشكل كامل ، وإجراءات الأمن ، وبروتوكولات التعامل مع المخاطر، والاستراتيجيات ، بالإضافة إلى اقتراح التحسينات الضرورية لضمان الاستعداد الدائم للتصدي للهجمات السيبرانية .

٣/٣/١ الخطوة الثالثة: تحديد أثر اختراقات الأمن السيبراني على البيانات المالية

عندما يدرك المراجع أن الاختراقات السيبرانية تمثل مصدر قلق كبير للأطراف ذات المصلحة وسيتم التحقيق فيها من قبل المنظمين وأصحاب المصلحة، سيحتاج المراجع إلى تحديد مدى انتشار الإختراق وما إذا كان له تأثير على البيانات المالية. يجب على المراجع أيضاً تقييم مخاطر الشركة الكلية، والتي قد تتضمن تحديد ما إذا كان التعرض لمستويات أعلى من مخاطر الاختراق قد تؤثر على العمليات التجارية أي (خسارة العملاء، الدعاية السلبية التي تؤدي إلى تخفيضات في المبيعات المستقبلية، وانخفاض قيمة الأصول)، وعليه فعندما يلاحظ المراجع وجود اختراق أو يتوقع خطراً لاختراق مستقبلي، فإنه سيرفع مستوى المخاطر المدركة لأعمال العميل ويحدد مخاطر الأعمال التجارية للعملاء بمستوى عالي. Smith, T. J., et al (2019)

ويتم استخدام المعلومات التي تم جمعها من خلال تنفيذ إجراءات تقييم المخاطر كأدلة مراجعة لتوفير الأساس المناسب لتحديد وتقييم مخاطر التحريفات الجوهرية، حيث يتم استخدام أدلة المراجعة التي تم الحصول عليها عند تقييم تصميم عناصر الرقابة المحددة وتحديد ما إذا كانت تلك الضوابط قد تم تنفيذها في مكون أنشطة المراقبة ، كأدلة مراجعة لدعم تقييم المخاطر، حيث توفر هذه الأدلة أيضاً أساساً للمراجع لتصميم الاستجابات الإجمالية لمعالجة المخاطر التي تم تقييمها من التحريفات الجوهرية على مستوى البيانات المالية ، وكذلك تصميم وتنفيذ المزيد من إجراءات المراجعة التي تستجيب طبيعتها وتوقيتها ومداها للمخاطر المقدرة كتحريفات جوهرية على مستوى التأكيد وفقًا لمعيار (ISA:330) . وعليه في حالة وقوع حادثة سيبرانية، يجب على المراجع الخارجي تقييم مخاطر التحريفات الجوهرية الناتجة عن تقييم الشركة للخسائر المعروفة المتعلقة بالأمن السيبراني والتي تشمل الالتزامات والمطالبات المحتملة والمحاسبة عنها (CAQ,2014) . وبناءاً على ما سبق فقد تتكبد الشركات التي تقع ضحية لهجمات سيبرانية ناجحة تكاليف كبيرة وتعاني من أضرار كبيرة، وبالتالي يجب على المراجع:.(2016),.Van M

أ- فهم طبيعة وسبب حادثة الهجوم السيبراني، والنظر بعناية في التكاليف وأية عواقب ضارة ناجمة عن الحادثة، وتقييم الأثر الذي قد يترتب عن الحادثة على التقارير المالية.

ب- تقييم تأثير الهجوم على إيرادات المنشأة، وتدفقاتها النقدية المستقبلية والقيمة المستقبلية للمنشأة، ومصروفات التقاضي المحتملة، وتكاليف حماية الأمن السيبراني .

ج- تقييم سلامة الإفصاح والعرض في التقارير المالية.

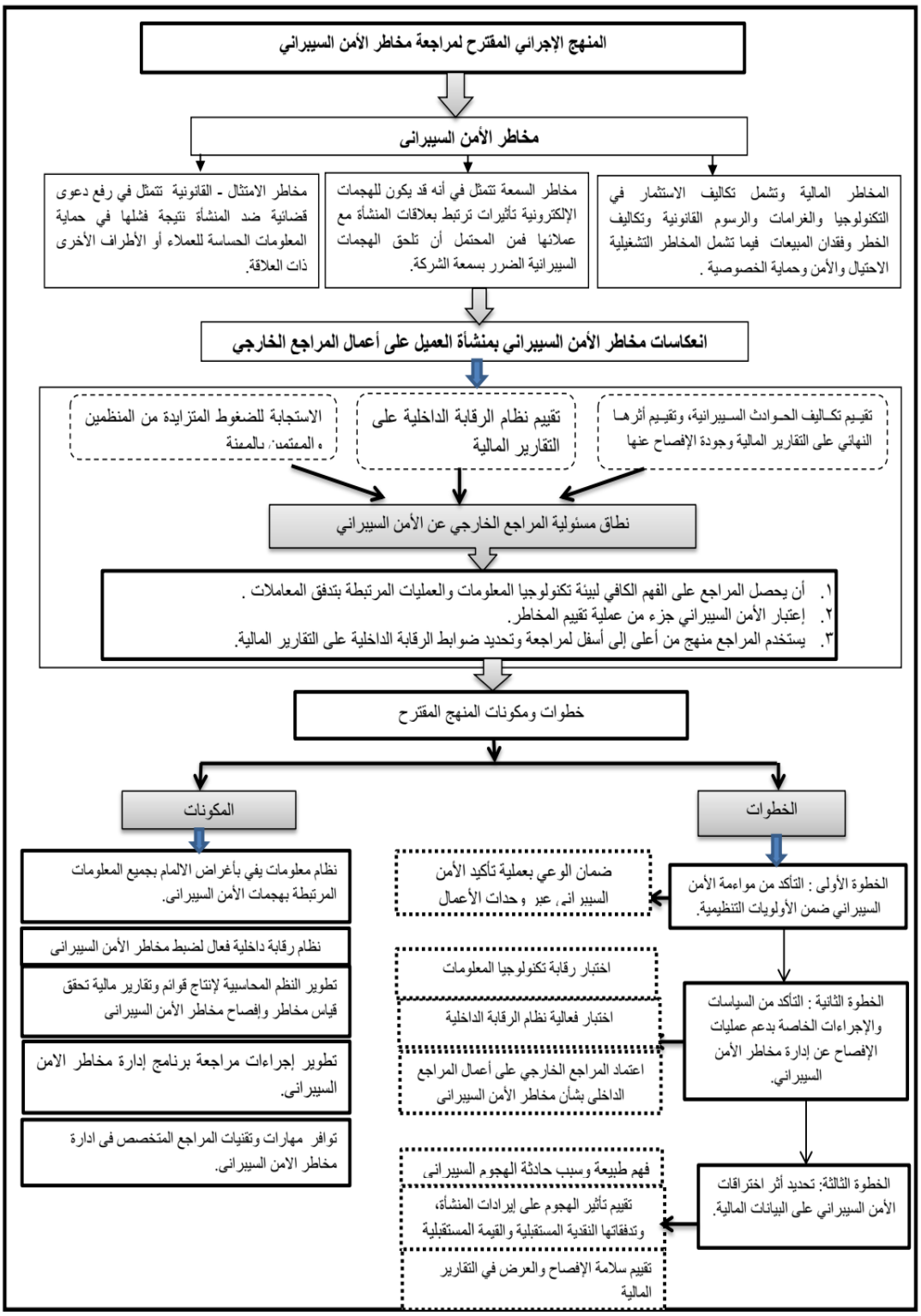
د- النظر في أي متطلبات أخرى لإخطار السلطات المختصة في حالة عدم قيام الإدارة بالإفصاح المناسب أو عدم اخذها لتوصيات المراجع بالاعتبار.

ه- تقييم القوانين واللوائح التي قد يكون لها تأثير مباشر أو غير مباشر على البيانات المالية للمنشأة، مثل التشريعات والقوانين المتعلقة بحماية البيانات. وبالتالي يجب النظر إلى اي مدى امتثلت المنشاة بتلك القوانين أو اللوائح وفقًا للمعيار(ISA 250).

هذا وتشير إرشادات (PCAOB) إلى أن موظفي التفتيش يقومون بمراجعة كيفية تقييم الفرق المشاركة في عملية المراجعة لمخاطر التحريفات الجوهرية المرتبطة بالأمن السيبراني والضوابط ذات العلاقة في المراجعة المتكاملة، وتحذير المراجعين الخارجيين بضرورة النظر في الآثار المترتبة لحوادث الأمن السيبراني على الرقابة الداخلية والتي قد تحدث خلال فترة المراجعة (PCAOB: 2016). كما تتابع هيئة الأوراق المالية والبورصات أيضاً الشركات بناءً على أوجه القصور الملحوظة في الرقابة الداخلية بعد الحوادث السيبرانية وإلى أي حد يمكن للأشخاص غير المصرح لهم الوصول إلى الأصول المادية أو سرقتها أو تعطيل أنظمة المعلومات (SEC: 2016).

وبالتالي عندما تتسبب مخاطر الأمن السيبراني في مخاطر وجود تحريفات جوهرية على مستوى التقارير المالية، يجب على المراجع اتخاذ الخطوات المناسبة لمعالجة هذه المخاطر، وقد يشمل ذلك تعيين مساعدين ذوي خبرة وكفاءة أكبر أو ذوي مهارات خاصة مثل متخصصي تكنولوجيا المعلومات للمشاركة، مع تضمين عناصر إضافية من عدم القدرة على التنبؤ في اختيار إجراءات المراجعة الأخرى التي يتعين القيام بها وتعديل طبيعة إجراءات المراجعة للحصول على أدلة مراجعة أكثر إقناعاً وتوثيقها جيدا .Van .M.,(2016)

فيما يتعلق بدور المراجع في تقييم الإفصاحات عن أنشطة الأمن السيبراني أشار Hamm, K. (2019) إلى أن المراجع يلعب دورا مميزا بالنسبة للحوادث المتعلقة بالأمن السيبراني المفصح عنها في التقارير المالية، حيث يقوم المراجع بتقييم ما إذا كانت تلك التقارير كوحدة واحدة مقدمة بشكل عادل وفقاً لمبادئ المحاسبة المقبولة عاماً ومن جميع النواحي الجوهرية، فإذا حددت الشركة مسئولية طارئة جوهرية عن حادثة إلكترونية فعلية، فإنه يجب على المراجع أن يقيم مدى ملاءمة الإفصاح عن تلك المسؤولية في الايضاحات المتممة للتقارير المالية. وعندما لا يتم تضمين المعلومات المتعلقة بتكنولوجيا المعلومات في التقارير المالية ولكن في مكان آخر من التقرير السنوي للشركة فلا يحتاج المراجع تأكيد المعلومات الواردة في التقرير. ولكن يحتاج المراجع فقط إلى قراءة والنظر في ما إذا كانت المعلومات المتعلقة بتكنولوجيا المعلومات في هذا التقرير أو في الايضاحات المتممة جوهرية ومظللة، أم أنها عبارة عن خطأ جوهري في الحقائق أو تتعارض جوهرياً مع المعلومات الواردة في البيانات المالية (AS 2710). ويمكن تلخيص المنهج الإجرائي المقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل من خلال الشكل رقم (١) التالي.


المنهج الإجرائي المقترح لمراجعة مخاطر الأمن السيبراني
مخاطر الأمن السيبرانى
المخاطر المالية وتشمل تكاليف الاستثمار في التكنولوجيا والغرامات والرسوم القانونية وتكاليف الخطر وفقدان المبيعات فيما تشمل المخاطر التشغيلية الاحتيال والأمن وحماية الخصوصية .
مخاطر السمعة تتمثل في أنه قد يكون للهجمات الإلكترونية تأثيرات ترتبط بعلاقات المنشأة مع عملائها فمن المحتمل أن تلحق الهجمات السيبرانية الضرر بسمعة الشركة.
مخاطر الامتثال - القانونية تتمثل في رفع دعوى قضائية ضد المنشأة نتيجة فشلها في حماية المعلومات الحساسة للعملاء أو الأطراف الأخرى ذات العلاقة.
انعكاسات مخاطر الأمن السيبراني بمنشأة العميل على أعمال المراجع الخارجي
تقييم تكاليف الحوادث السيبرانية، وتقييم أثرها النهائي على التقارير المالية وجودة الإفصاح عنها
تقييم نظام الرقابة الداخلية على التقارير المالية
الاستجابة للضغوط المتزايدة من المنظمين والمعتمدين بالمهنة
نطاق مسئولية المراجع الخارجي عن الأمن السيبراني
١. أن يحصل المراجع على الفهم الكافي لبيئة تكنولوجيا المعلومات والعمليات المرتبطة بتدفق المعاملات .
٢. إعتبار الأمن السيبراني جزء من عملية تقييم المخاطر.
٣. يستخدم المراجع منهج من أعلى إلى أسفل لمراجعة وتحديد ضوابط الرقابة الداخلية على التقارير المالية.
خطوات ومكونات المنهج المقترح
الخطوات
المكونات
الخطوة الأولى : التأكد من مواءمة الأمن السيبراني ضمن الأولويات التنظيمية.
ضمان الوعي بعملية تأكيد الأمن السيبراني عبر وحدات الأعمال
الخطوة الثانية : التأكد من السياسات والإجراءات الخاصة بدعم عمليات الإفصاح عن إدارة مخاطر الأمن السيبراني.
اختبار رقابة تكنولوجيا المعلومات
اختبار فعالية نظام الرقابة الداخلية
اعتماد المراجع الخارجي على أعمال المراجع الداخلى بشأن مخاطر الأمن السيبرانى
الخطوة الثالثة: تحديد أثر اختراقات الأمن السيبراني على البيانات المالية.
فهم طبيعة وسبب حادثة الهجوم السيبرانى
تقييم تأثير الهجوم على إيرادات المنشأة، وتدفقاتها النقدية المستقبلية والقيمة المستقبلية
تقييم سلامة الإفصاح والعرض في التقارير المالية
نظام معلومات يفي بأغراض الالمام بجميع المعلومات المرتبطة بهجمات الأمن السيبرانى.
نظام رقابة داخلية فعال لضبط مخاطر الأمن السيبرانى
تطوير النظم المحاسبية لإنتاج قوائم وتقارير مالية تحقق قياس مخاطر وإفصاح مخاطر الأمن السيبرانى
تطوير إجراءات مراجعة برنامج إدارة مخاطر الامن السيبرانى.
توافر مهارات وتقنيات المراجع المتخصص فى ادارة مخاطر الامن السيبرانى.

المحور الثاني: الدراسة التطبيقية

تأتي الدراسة التطبيقية لتدعيم المحور النظري للبحث، وحتى تحقق الدراسة التطبيقية الهدف منها فلابد من تناول منهجية هذه الدراسة ونتائج التحليل الإحصائي وذلك لاختبار مدى صحة فروض الدراسة وذلك كما يلي:

١/٢ منهجية الدراسة التطبيقية

تتمثل منهجية الدراسة التطبيقية في تناول هدف ومجتمع الدراسة وكيفية تحديد العينة والأساليب الإحصائية المستخدمة في تحليل البيانات وذلك كما يلي:

١/١/٢ هدف الدراسة التطبيقية

تهدف الباحثة من خلال الدراسة التطبيقية إلى تحليل أثر مخاطر هجمات الأمن السيبراني بمنشأة العميل على أعمال المراجع الخارجي، بالإضافة إلى استقصاء وجهات النظر حول المنهج الإجرائي المقترح لأعمال المراجع الخارجي، وعلاقته بإدارة الإفصاح عن مخاطر الأمن السيبراني، وذلك بالتطبيق على عينة من شركات المساهمة المقيدة في البورصة المصرية والعاملة في القطاعات والأنشطة المرتبطة بالتقنيات الحديثة في نظم المعلومات والتكنولوجيا الرقمية مثل انترنت الأشياء وسلاسل الكتل وخدمات الحوسبة السحابية بالإضافة إلى مكاتب المراجعة التي تقوم بمراجعة التقارير المالية لهذه الشركات.

٢/١/٢ مجتمع وعينة الدراسة التطبيقية

يمكن تحديد مجتمع الدراسة وعينة الدراسة كما يلي:

حددت الباحثة مجتمع الدراسة التطبيقية في شركات المساهمة المقيدة في البورصة المصرية والعاملة في القطاعات والأنشطة المرتبطة بالتقنيات الحديثة في نظم المعلومات والتكنولوجيا الرقمية مثل انترنت الأشياء وسلاسل الكتل وخدمات الحوسبة السحابية بالإضافة إلى مكاتب المراجعة التي تقوم بمراجعة التقارير المالية لهذه الشركات، و بعد قيام هيئة سوق المال بإعادة هيكلة قطاعات البورصة المصرية، أصبحت القطاعات الأقرب إلى هدف البحث هي قطاع المؤسسات المالية المصرفية (البنوك) والتي بلغ عددها (١٤) شركة، بالإضافة إلى قطاع الاتصالات والاعلام وتكنولوجيا المعلومات لقطاع العقارات والتي بلغ عددها (٦) شركات، ليصبح عدد الشركات الممثلة لمجتمع الدراسة (٢٠) شركة. (البورصة المصرية: https://www.egx.com.eg)

وقامت الباحثة باختيار شركات المساهمة المسجلة في البورصة المصرية كمجتمع للدراسة واستبعد التطبيق على الشركات غير المدرجة في البورصة وذلك للأسباب التالية:

١- إختيار الشركات المقيدة في البورصة يضمن وجود وحدات تكنولوجيا المعلومات والتقنيات الحديثة بها واستخداماها التكنولوجيا الرقمية مثل انترنت الأشياء وسلاسل الكتل وخدمات الحوسبة السحابية ومن ثم احتماليه تعرضها لمخاطر الأمن السيبراني.

٢- إختيار الشركات المقيدة في البورصة يضمن كفاءة مسئولي تكنولوجيا المعلومات في هذه الشركات، بالإضافة إلى خبرة أعضاء مجلس الإدارة في هذه الشركات حول مدى استجابة المراجع الخارجي لمخاطر الأمن السيبراني.

٣- إختيار الشركات المقيدة في البورصة يضمن الوصول لمكاتب المراجعة الكبرى حيث تراجع هذه الشركات بواسطة مكاتب مراجعة ترتبط بمكاتب المراجعة الكبرى (BIG4)، مما يتيح

الفرصــة للاسـتفادة من خبرات العاملين بهذه المكاتب في إسـتخلاص أي ملاحظات منهم حول خطوات المنهج الإجرائي المقترح لعملية مراجعة الإفصاح عن مخاطر الأمن السيبراني.

كما قامت الباحثة باختيار عينة من شركات مجتمع الدراسة بعد استبعاد الشركات التي عملة نشاطها الرئيسي بالدولار لتصبح عدد شركات العينة (١٥) شركة بواقع (١٠) بنوك و (٥) شركات عاملة في نشاط الاتصالات وتكنولوجيا المعلومات (ملحق رقم ١).

وتتمثل فئات عينة الدراسة المستقصى أرائهم في مسئولي وحدات تكنولوجيا المعلومات، وأعضاء مجلس الإدارة في شركات العينة بالإضافة إلى المراجعين بمكاتب المراجعة المرتبطة بهذه الشركات والتي بلغ عددهم (٨) مكاتب مراجعة، وحيث أن مفردات هذه الفئات يصعب حصر عددها الفعلي بشكل دقيق، فقد قامت الباحثة بتحديد عينة الدراسة من كل فئة عشوائيا (الطريقة الحكمية في إختيار العينات) حيث تم توزيع قائمة الإستقصاء على شركات العينة بواقع (٥) قوائم لكل شركة، و(٥) قوائم لكل مكتب مراجعة لتصبح إجمالي العينة (١١٥) مفردة مع مراعاة إختيار الخبرات والكفاءات والذين لديهم الفهم والقدرة على إستيعاب استفسارات قائمة الإستقصاء من خلال إختيار ذوى الخبرة والحاصلين على الشهادات المهنية، بالإضافة إلى توافر الخلفية المحاسبية لأعضاء مجلس الإدارة.

وبعد تحديد العينة المبدئية لكل فئات الدراسة قامت الباحثة بتوزيع قوائم الإستقصاء (١١٥ قائمة) من خلال المقابلة الشخصية والتسليم باليد أو إرسالها وإستلامها عن طريق البريد الإلكتروني، بالإضافة إلى اللجوء إلى إعداد نموذج لقائمة الإستقصاء من خلال نماذج جوجل من خلال الرابط التالي: (https://www.google.com/intl/ar_eg/forms/about)

وقامت الباحثة بفرز الاستمارات المستردة لتحديد نسبة الاستجابة من قبل فئات الدراسة، ومدى صلاحية هذه الاستمارات لإخضاعها للتحليل الاحصائي واستخلاص النتائج الاحصائية منها، ويمكن للباحثة توضيح مجتمع الدراسة وطريقة تحديد عينة الدراسة من خلال الجدول التالي:

جدول (١) عدد قوائم الاستقصاء المستردة والصالحة للتحليل الإحصائي

مجتمع الدراسة	العدد*	طريقة توزيع قوائم الإستقصاء وإختيار العينة	عينة الدراسة	عدد قوائم الاستقصاء الموزعة	عدد قوائم الاستقصاء المستردة والصالحة للتحليل الإحصائي		
					العدد	النسبة**	النسبة***
البنوك المصرية المسجلة في البورصة	١٠	قامت الباحثة بتحديد عينة الدراسة من كل فئة عشوائيا حيث تم توزيع قائمة الإستقصاء على شركات العينة بواقع (٥) قوائم لكل شركة، و(٥) قوائم لكل مكتب مراجعة والتي بلغ عدد المكاتب (٨) مكاتب	مراجع بمكاتب المحاسبة والمراجعة لشركات العينة	٤٠	٣٥	٨٧,٥٠٪	٣٤,٦٥٪
			مسئولي تكنولوجيا المعلومات	٤٥	٤١	٩١,١١٪	٤٠,٥٩٪
شركات قطاع الاتصالات وتكنولوجيا المعلومات	٥		أعضاء مجلس الإدارة	٣٠	٢٥	٨٣,٣٣٪	٢٤,٧٥٪
الإجمالى	١٥		الإجمالي	١١٥	١٠١	٨٧,٨٣٪	١٠٠,٠٠٪

* العدد بعد إستبعاد الشركات التي تتعامل بالدولار

** النسبة على أساس عدد قوائم الاستقصاء الموزعة من كل فئة

*** النسبة على أساس حجم العينة الإجمالى.

ويتضح من الجدول السابق أن نسبة قوائم الاستقصاء المستردة (نسبة الاستجابة) من عينة الدراسة على قوائم الاستقصاء ٨٧,٨%، وهي نسبة جيدة تدل على إستجابة وإهتمام عينة الدراسة بموضوع البحث.

٣/١/٢ أداة الدراسة والأساليب الإحصائية المستخدمة

قامت الباحثة بالاعتماد على قائمة الاستقصاء كأداة للدراسة التطبيقية ولتحقيق الهدف منها تم تقسيمها إلى ثلاثة أقسام:

١- القسم الأول بيانات شخصية عن المستقصي منه وذلك لإيضاح خبرة ومؤهل المستقصي منه وتحديد درجة الاعتماد على إجابته.

٢- القسم الثاني: بيانات وصفية مرتبطة بالمخاطر السيبرانية في منشأة العميل ومدى استجابة المراجع الخارجي، وهذا القسم عبارة عن مجموعة من الاستفسارات تم توجيهها إلى شركات المساهمة والتي تختلف عن مجموعة أخرى من الاستفسارات وجهت أيضا للمسئولين في مكاتب المراجعة التي تقوم بمراجعة هذه الشركات كل فيما يخصه.

٣- القسم الثالث: أسئلة قائمة الاستقصاء: وهي مجموعة من الإستفسارات المتدرجة يختار المستقصي منه للإجابة عليها إجابة من خمس إجابات وذلك كأساس لاستخدام مقياس ليكرت المتدرج الخماسي المكون من خمس إجابات، والتي يعبر كل منها على درجة من درجات الموافقة أو الأهمية النسبية، ويأخذ معيار ليكرت للحكم على درجة الموافقة أساس أن لكل عبارة وزن (Weights)، ويتم بعد ذلك حساب المتوسط المرجح.

ويتضمن القسم الثالث لقائمة الاستقصاء محورين كما يلي:

أ- المحور الأول: مخاطر الأمن السيبراني بمنشأة العميل وانعكاساتها على أعمال المراجع الخارجي، ويتكون في قائمة الاستقصاء من (١٢) عبارة، ويختص باختبار مدى صحة الفرض الأول، وهو: "لا يوجد تأثير معنوي لمخاطر هجمات الأمن السيبراني بمنشأة العميل على أعمال المراجع الخارجي"،

ب- المحور الثاني: طبيعة العلاقة بين إدارة الإفصاح عن مخاطر الأمن السيبراني والمنهج الإجرائي المقترح لعملية مراجعة الإفصاح عن مخاطر الأمن السيبراني، ويتكون في قائمة الاستقصاء من (٢٠) عبارة، ويختص باختبار مدى صحة الفرض الثاني، وهو: "لا توجد علاقة ذات دلالة معنوية بين إدارة الإفصاح عن مخاطر الأمن السيبراني والمنهج الإجرائي المقترح لأعمال المراجع الخارجي"،

وقامت الباحثة بتفريغ بيانات قوائم الاستقصاء الصالحة للتحليل وتحليلها واستخلاص النتائج من خلال تطبيق بعض الأساليب الإحصائية الواردة بمجموعة البرامج الإحصائية للعلوم الاجتماعية [Statistical Package for Social Science (SPSS)] (الإصدار (٢٥) في تحليل البيانات إحصائيا) وقد تطلبت طبيعة البيانات تحديد الأساليب الإحصائية اللازمة والملائمة، والتي تتمثل فيما يلي: سليمان (٢٠٠٧)، Abu-Bader,(2021)

١- تحديد مدى صلاحية البيانات للتحليل الإحصائي من خلال معامل الثبات والصدق لأداة الدراسة (ألفا كرونباخ Alpha Cronbach's)، بالإضافة إلى اختبار مدى إتباع البيانات للتوزيع

الطبيعي من خلال إختبار اختبار (Kolmogorov - Smirnov) واختبار (Shapiro –Wilk) وذلك لتحديد نوع الاختبارات المستخدمة بعد ذلك.

٢- توصيف وجهات النظر من خلال أساليب الإحصاء الوصفي وأهمها الوسط الحسابي، الانحراف المعياري، الأهمية النسبية.

٣- تحديد مدى الاتفاق أو الاختلاف بين مجموعات العينة (الفئات) حول بيانات الدراسة وذلك من خلال اختبارات الفروق وأهمها اختبار (Kruskal -Wallis Test).

٤- إختبار فروض الدراسة من خلال أساليب الإحصاء الاستدلالي وأهمها تحليل الارتباط (Correlation analysis)، وتحليل الإنحدار (Simple Regression Model) مع التركيز على معامل التحديد (R Square).

٢/٢ مدى صلاحية البيانات للتحليل الإحصائي

لتحديد صلاحية البيانات للتحليل الإحصائي ومن ثم الإعتماد عليها في إستخلاص النتائج قامت الباحثة بما يلي:

١- تنوع وكفاية الممارسات المهنية والمؤهلات العلمية للمستقصي منهم

تتناول الباحثة من خلال الجدول التالي نسب فئات عينة الدراسة من حيث المؤهل العلمي وسنوات الخبرة، وذلك كما يلي:

جدول (٢) التوزيع التكراري والنسبي للبيانات الأساسية للمستقصي منهم

حسب المؤهل العلمي			حسب سنوات الخبرة		
المؤهل العلمي	التكرار	النسبة	سنوات الخبرة	التكرار	النسبة
دكتوراه	٢٣	٢٢,٨٪	أقل من خمس سنوات	١٣	١٢,٩٪
ماجستير	١٩	١٨,٨٪	من خمس سنوات إلى أقل من عشر سنوات	٢٦	٢٥,٧٪
دبلومات وشهادات مهنية	٣١	٣٠,٧٪	من عشر سنوات إلى أقل من خمسة عشر سنة	٢٧	٢٦,٧٪
بكالوريوس	٢٨	٢٧,٧٪	خمسة عشر سنة فأكثر	٣٥	٣٤,٧٪
الإجمالي	١٠١	١٠٠,٠٪	الإجمالي	١٠١	١٠٠,٠٪

يتضح من الجدول السابق أن عينة الدراسة تتسم بتنوع وكفاية الممارسات المهنية والمؤهلات العلمية للمستقصي منهم مع توافر عامل الخبرة بشكل كافٍ في العينة حيث بلغت نسبة المستقصي منهم لمن تجاوزت سنوات الخبرة لديه عشر سنوات ٦٠٪ وهي نسبة جيدة، مما يساهم في الاطمئنان لنتائج الدراسة وإمكانية تعميمها.

٢- اختبار صلاحية واعتمادية أداة الدراسة (إختبار ألفا كرونباخ - معامل الاتساق الداخلي)

لتحديد درجة صلاحية وثبات العناصر المستخدمة في قياس نتائج فروض الدراسة، قامت الباحثة باستخدام معامل ألفا كرونباخ، ومعامل الاتساق الداخلي وذلك على النحو الذي يوضحه الجدول التالي:

جدول (٣) مدى الثبات والصدق لقائمة الاستقصاء (اختبار ألفا كرونباخ)

الفرض	صيغة الفرض	متغيرات الفرض	عدد العبارات	معامل الثبات (الفا كرونباخ)	معامل الصدق	معامل الإرتباط الذاتي
الفرض الأول	لا يوجد تأثير معنوي لمخاطر هجمات الأمن السيبراني بمنشأة العميل على أعمال المراجع الخارجي	▪ مخاطر هجمات الأمن السيبراني بمنشأة العميل	٦	٠,٧٦٢	٠,٨٧٣	قيم معاملات الارتباط (الإتساق الداخلي) لجميع عبارات الفرض الأول والثاني زادت عن ٠,٥ وقد جاءت جميعها معنوية عند مستوي ٠,٠١
		▪ أعمال المراجع الخارجي	٦	٠,٧٢٤	٠,٨٥١	
	▪ ألفا كرونباخ للفرض الأول ككل		١٢	٠,٨٤٠	٠,٩١٧	
الفرض الثاني	لا توجد علاقة ذات دلالة معنوية بين إدارة الإفصاح عن مخاطر الأمن السيبراني والمنهج الإجرائي المقترح لأعمال المراجع الخارجي	▪ إدارة الإفصاح عن مخاطر الأمن السيبراني	٧	٠,٧٩٣	٠,٨٩١	
		▪ المنهج الإجرائي المقترح لأعمال المراجع الخارجي	١٣	٠,٨٣٩	٠,٩١٦	
	▪ ألفا كرونباخ للفرض الثاني ككل		٢٠	٠,٨٩٤	٠,٩٤٦	
ألفا كرونباخ للقائمة ككل			٣٢	٠,٩٢٧	٠,٩٦٣	

يتضح من الجدول السابق أن معاملات الثبات والصدق عالية جدا مما يشير إلى وجود درجة عالية من التجانس والتناسق بين متغيرات الدراسة، بالإضافة إلى وجود تناسق داخلي لعناصر وعبارات القائمة بدرجة كبيرة. كما أكدت نتائج الجدول أيضا على صلاحية جميع العناصر التي تحدد متغيرات وفروض الدراسة حيث أكدت على ذلك قيم معاملات الارتباط (الاتساق الداخلي) والتي زادت عن ٠,٥ وقد جاءت جميعها معنوية عند مستوي ٠,٠١.

٣- اختبار مدى إتباع البيانات للتوزيع الطبيعي (Normal Distribution Test)

للتحقق من مدى اقتراب البيانات من التوزيع الطبيعي تم استخدام اختبار (Kolmogorov - Smirnov) واختبار (Shapiro –Wilk) للتأكد من أن نمط التوزيع الذي تسلكه بيانات الدراسة هو توزيع طبيعي، وذلك لتحديد نوع الاختبارات التي ستستخدمها الباحثة في التحليل الإحصائي للبيانات ما بين اختبارات الإحصاء المعلمى واختبارات الإحصاء اللامعلمى، والجدول التالي يوضح قيم الاختبارين ومستوى المعنوية لكل متغير أمام كل اختبار:

جدول (٤): نتائج اختبار مدى إتباع البيانات للتوزيع الطبيعي.

الرمز	متغيرات الدراسة (Variables)	Shapiro-Wilk Statistic		Kolmogorov-Smirnov Statistic	
		value	Sig.	value	Sig.
G1X	▪ مخاطر هجمات الأمن السيبراني بمنشأة العميل	٠,١١٤	٠,٠٠٢	٠,٩١٦	٠,٠٠٠
G1Y	▪ أعمال المراجع الخارجي	٠,١٤٢	٠,٠٠٠	٠,٩٤٦	٠,٠٠٠
G2X	▪ إدارة الإفصاح عن مخاطر الأمن السيبراني	٠,١٤٠	٠,٠٠٠	٠,٩٣٩	٠,٠٠٠
G2Y	▪ المنهج الإجرائي المقترح لأعمال المراجع الخارجي	٠,٠٩٧	٠,٠٢٠	٠,٩٧٢	٠,٠٣١

ويتضح من الجدول السابق أن قيمة مستوى المعنوية (.Sig) لاختبار (Shapiro-Wilk) واختبار (Kolmogorov-Smirnov) أقل من (٠,٠٥) لجميع المتغيرات، وبناءا على ذلك فإن البيانات الخاصة بمتغيرات الدراسة لا تتبع التوزيع الطبيعي، وفى ضوء ما سبق قامت الباحثة بمراعاة ذلك أثناء التحليل الإحصائي، حيث قام بإتباع الاختبارات اللامعلمية أثناء التحليل الإحصائي للبيانات ومنها إختبار كروسكال ويلز للفروق بين المجموعات، وترى الباحثة، أن عدم إتباع البيانات للتوزيع الطبيعي لا يؤثر على نتائج التحليل ويبرر ذلك بكبر حجم المشاهدات والتي تمثلت في

(١٠١) مشاهدة، حيث وفقا لنظرية النهاية المركزية الإحصائية تعتبر البيانات تتبع التوزيع الطبيعي إذا كان حجم المجتمع كبير. الزغبي، الطلاحفة (٢٠١٢)

٣/٢ التحليل الإحصائي للبيانات واختبار فروض الدراسة

تقوم الباحثة بإختبار مدى صحة فروض الدراسة من خلال الإحصاء الوصفي للبيانات وتحديد الأهمية النسبية لكل عبارة وإختبار الفروق بين فئات العينة حول أبعاد كل فرض، بالإضافة إلى تحليل الإرتباط والانحدار وذلك كما يلي:

٣/٢ /١ التحليل الإحصائي للبيانات المرتبطة بالفرض الأول واختباره

نص الفرض الأول:" لا يوجد تأثير معنوي لمخاطر هجمات الأمن السيبراني بمنشأة العميل على أعمال المراجع الخارجي"، ويتم إختبار صحة هذا الفرض كما يلي:

١- التحليل الوصفي للبيانات المرتبطة بالفرض الأول

تتناول الباحثة نتائج توصيف الآراء من قبل عينة الدراسة حول العبارات المرتبطة بمتغيرات الفرض الأول من خلال المقاييس الإحصائية (الوسط الحسابي والانحراف المعياري والوزن النسبي وترتيب العناصر) وذلك كما يلي:

جدول (٥) توصيف الآراء حول العبارات التي تحدد متغيرات الفرض الأول

العناصر (العبارات) التي تحدد متغيرات الفرض الأول	مقاييس الإحصاء الوصفي			
	الوسط الحسابي	الانحراف المعياري	الأهمية النسبية	ترتيب الموافقة
أولا: مخاطر الأمن السيبراني بمنشأة العميل				
١- ترتبط المخاطر السيبرانية بتعدد أهداف الهجمات الإلكترونية ومنها السرقة والابتزاز، أو تدمير الأصول المالية أو سرقة الملكية الفكرية أو سرقة المعلومات الحساسة الأخرى التي تخص الشركات أو عملائها أو شركائها التجاريين	٤,٤١	١,٠٥١	٨٨,٢٠ %	١
٢- المخاطر التشغيلية للتهديدات السيبرانية تشمل الاحتيال والأمن وحماية الخصوصية والمخاطر القانونية والمخاطر المادية، والمخاطر البيئية، وتؤثر المخاطر التشغيلية على رضاء العملاء وسمعة الشركة وحقوق المساهمين مع زيادة المخاطر الشاملة للمنشأة	٤,٣٤	٠,٨١٦	٨٦,٨٠ %	٣
٣- يكون للهجمات الإلكترونية تداعيات وتأثيرات ترتبط بعلاقات المنشأة مع عملائها أو مورديها فمن المحتمل أن تلحق الهجمات السيبرانية الضرر بسمعة الشركة	٤,٠٩	٠,٨٩٦	٨١,٨٠ %	٦
٤- أن فقدان الأعمال هي أكبر عامل يساهم في ارتفاع تكاليف اختراق البيانات إذ أن فقدان ثقة العملاء ينتج عنه مخاطر مالية كبيرة وخسارة الأعمال هي أكبر فئات التكاليف الرئيسية الخارجية التي تساهم في إجمالي تكلفة اختراق البيانات	٤,٢١	٠,٩٢	٨٤,٢٠ %	٤

العناصر (العبارات) التي تحدد متغيرات الفرض الأول	مقاييس الإحصاء الوصفي			
	الوسط الحسابي	الانحراف المعياري	الأهمية النسبية	ترتيب الموافقة
٥- ظهور التهديدات السيبرانية حافزاً لمعظم الدول لوضع قوانين وقواعد صارمة للأمن السيبراني بهدف الحفاظ على سرية وسلامة نظم المعلومات.	٤,٣٩	٠,٧٦١	٨٧,٨٠ %	٢
٦- يؤدي عدم الامتثال الشركات لإجراءات للحماية ضد مخاطر التهديدات السيبرانية إلى تعرض المنشآت للدعاوى القضائية والإجراءات العقابية نتيجة فشلها في حماية المعلومات الحساسة للعملاء أو الأطراف الأخرى ذات العلاقة	٤,٠٩	١,٠٣١	٨١,٨٠ %	٥
درجة الموافقة الكلية على مخاطر الأمن السيبراني بمنشأة العميل	٤,٢٥	٠,٦٢	٨٥,٠٠ %	**موافقة**
ثانيا: انعكاسات مخاطر الأمن السيبراني بمنشأة العميل على أعمال المراجع الخارجي				
١- ضرورة تقييم تكاليف الحوادث السيبرانية، وتقييم نظام الرقابة الداخلية وأثر ذلك النهائي على التقارير المالية وجودة الإفصاح عنها.	٤,١٢	٠,٩٠٩	٨٢,٤٠ %	٣
٢- الاستجابة للضغوط المتزايدة من المنظمين والمهتمين بالمهنة.	٤,٠٤	١,٠٢٩	٨٠,٨٠ %	٦
٣- يحصل المراجع على الفهم الكافي لبيئة تكنولوجيا المعلومات والعمليات المرتبطة بتدفق المعاملات ومعالجة المعلومات في نظام المعلومات	٤,٠٥	١,١٨٦	٨١,٠٠ %	٥
٤- فهم المراجع للضوابط الرقابية لتكنولوجيا المعلومات في شركة العميل وعلاقتها بالتقارير المالية وبما في ذلك الضوابط العامة لتكنولوجيا المعلومات ومدى التشغيل الفعال لتلك الضوابط.	٤,١٥	٠,٨١٧	٨٣,٠٠ %	١
٥- اعتبار الأمن السيبراني جزء من عملية تقييم المخاطر من خلال الاستفسار المراجعين عما إذا كان قد حدث هجوم سيبراني ومدى نجاحه وقدرة ذلك الاختراق في التأثير على التقارير المالية.	٤,٠٩	٠,٧٨٩	٨١,٨٠ %	٤
٦- يستخدم المراجع منهج من أعلى إلى أسفل لمراجعة وتحديد ضوابط الرقابة الداخلية على التقارير المالية فيبدأ المراجع وفق هذا المنهج بتقييم المخاطر على مستوى التقارير المالية.	٤,١٢	٠,٨٨٦	٨٢,٤٠ %	٢
درجة الموافقة الكلية على انعكاسات مخاطر الأمن السيبراني بمنشأة العميل على أعمال المراجع الخارجي	٤,٠٩	٠,٦١٣	٨١,٨٠ %	**موافقة**

**** الوسط الحسابي لكل العبارات دال إحصائيًا عند مستوى معنوية ٠,٠٥**

تخلص الباحثة من الجدول السابق إلى النتائج التالية:

تشير قيم الوسط الحسابي لجميع ردود المستقصي منهم حول جميع العناصر (أكبر من ٣) إلى أن الآراء تميل لصالح الموافقة حول وجود مخاطر للأمن السيبراني بمنشأة العميل وأن هذه المخاطر تنعكس على أعمال المراجع الخارجي؛ وهو ما تؤكد عليه نسب الوزن النسبي لجميع العناصر والتي تزيد عن ٦٠٪ الممثلة لإختيار"محايد"، وجاءت جميع الأوساط الحسابية لجميع العبارات دالة إحصائيا عند مستوى معنوية (٠,٠٥) ويدل ذلك على أنه يوجد إختلافات (فروق معنوية) في أراء المستقصي منهم بين القيم المشاهدة وقيمة (٣) والممثلة لإختيار محايد. ويشير ترتيب درجة الموافقة (الأهمية النسبية) إلى العبارات الأكثر أهمية وصاحبة الأعلى موافقة من المستقصي منهم كما يلي:

أ- ترتبط المخاطر السيبرانية بتعدد أهداف الهجمات الإلكترونية ومنها السرقة والابتزاز، أو تدمير الأصول المالية، أو سرقة الملكية الفكرية، أو سرقة المعلومات الحساسة الأخرى التي تخص الشركات أو عملائها أو شركائها التجاريين.

ب- ظهور التهديدات السيبرانية حافزاً لمعظم الدول لوضع قوانين وقواعد صارمة للأمن السيبراني بهدف الحفاظ على سرية وسلامة نظم المعلومات.

ج- فهم المراجع للضوابط الرقابية لتكنولوجيا المعلومات في شركة العميل وعلاقتها بالتقارير المالية وبما في ذلك الضوابط العامة لتكنولوجيا المعلومات ومدى التشغيل الفعال لتلك الضوابط.

د- يستخدم المراجع منهج من أعلى إلى أسفل لمراجعة وتحديد ضوابط الرقابة الداخلية على التقارير المالية فيبدأ المراجع وفق هذا المنهج بتقييم المخاطر على مستوى التقارير المالية.

وترى الباحثة في ضوء التحليل الوصفي للبيانات المرتبطة بالفرض الأول للدراسة إلى إتفاق عينة الدراسة على وجود مخاطر للأمن السيبراني بمنشأة العميل وأن هذه المخاطر تنعكس على أعمال المراجع الخارجي، وهو ما يدعم صحة الفرض الأول للدراسة.

٢- تحليل التباين (مدى الاتفاق والاختلاف) بين فئات العينة حول الفرض الأول

تتناول الباحثة التباين (مدى الاتفاق والاختلاف) في آراء فئات العينة حول العبارات المرتبطة بالفرض الأول وذلك من خلال إختبار كروسكال ويلز (Kruskal -Wallis Test) وهو من الاختبارات اللامعلمية التي تطبق مع المتغيرات التي لا تتبع بياناتها التوزيع الطبيعي لقياس التباين بين عدة عينات مستقلة وذلك كما يلي:

جدول (٦) تحليل التباين بين آراء فئات العينة حول بيانات الفرض الأول

العناصـــــر (الأبعاد) المرتبطة بالفرض الأول	فئات العينة	عدد المشاهدات	متوسط الرتب	الترتيب	معنوية إختبار Kruskal-Wallis
▪ مخاطر هجمات الأمن السيبراني بمنشأة العميل	مراجع بمكاتب المحاسبة والمراجعة لشركات العينة	٣٥	٥٦,٨٤	١	٠,٠١٢
	مسئولي تكنولوجيا المعلومات	٤١	٥٥,١٢	٢	
	أعضاء مجلس الإدارة	٢٥	٣٦,٠٦	٣	
	الإجمالـــــى	١٠١			
▪ إنعكاسات مخاطر الأمن السيبراني بمنشأة العميل على أعمال المراجع	مراجع بمكاتب المحاسبة والمراجعة لشركات العينة	٣٥	٥٣,٦٩	٢	٠,٠٣٥
	مسئولي تكنولوجيا المعلومات	٤١	٥٦,٥٧	١	
	أعضاء مجلس الإدارة	٢٥	٣٨,١٠	٣	
	الإجمالـــــى	١٠١			

*** دال إحصائيًا عند مستوى معنوية ٠,٠٥**

تخلص الباحثة من الجدول السابق إلى النتائج التالية:

أ- تشـــير قيم متوســـط الرتب والترتيب إلى أن أعلى الفئات موافقة على مخاطر هجمات الأمن الســـيبراني بمنشـــأة العميل هي فئة المراجعين الخارجيين في مكاتب المحاســـبة والمراجعة لشركات العينة بمتوسط رتب بلغ (٥٦,٨٤)، بينما جاءت فئة الدراسة من مسئولي تكنولوجيا المعلومات أعلى الفئات موافقة على انعكاســـات هذه المخاطر على أعمال المراجع الخارجي بمتوسـط رتب بلغ (٥٦,٥٧) ، وجاءت فئة الدراســة من أعضــاء مجلس الإدارة في شــركات العينة أقل الفئات موافقة على بيانات الفرض الأول .

ب- بلغت قيم مستوى المعنوية لاختبار (Kruskal-Wallis Test) للبيانات المرتبطة بمتغيري الفرض الأول (٠,٠١٢) (٠,٠٣٥) على الترتيب وهى أقل من ٥٪ ويدل ذلك على وجود فروق معنوية بين الفئات الممثلة للعينة محل البحث حول وجود مخاطر للأمن السيبراني بمنشأة العميل وأن هذه المخاطر تنعكس على أعمال المراجع الخارجي.

٣- تحليل نتائج إختبـار الفـرض الأول

يتم اختبار مدى صحة الفرض الأول للدراسة من إجراء التحليل ثنائي المتغير (تحليل الإرتباط) لمتغيرات الفرض وذلك لاختبار علاقة الإرتباط بين مخاطر هجمات الأمن السيبراني بمنشأة العميل وأعمال المراجع الخارجي، بالإضافة إلى قياس أثر هذه المخاطر على أعمال المراجع الخارجي (المتغير التابع) من خلال تحليل الإنحدار (Regression analysis) وذلك كما يلي:

جدول رقم (٧) نتائج تحليل الإرتباط والإنحدار لمتغيرات الفرض الأول

١- تحليل نتائج الإرتباط		**معامل الإرتباط بين مخاطر هجمات الأمن السيبراني بمنشأة العميل وأعمال المراجع الخارجي**				**٠,٦٥٥**
		مستوى المعنوية (عند ٠,٠١)				**٠,٠٠٠**
٢- تحليل نتائج الإنحدار		**المتغير التابع (أعمال المراجع الخارجي)**				
		معامل الانحدار(B)	**قيم Beta**	**قيمة T**	**مستوى المعنوية**	**الدلالة**
Constant	**ثابت**	**١,٣٤٢**		**٤,١٦٧**	**٠,٠٠٠**	**-**
مستقل	**مخاطر هجمات الأمن السيبراني بمنشأة العميل**	**٠,٦٤٧**	**٠,٦٥٥**	**٨,٦٣١**	**٠,٠٠٠**	**دال إحصائياً عند مستوى معنوية ٠,٠١**
القيمة التفسيرية لنموذج الإنحدار		**معامل التحديد R^2 = ٠,٤٢٩**				
قيمة F		**قيمة F = ٧٤,٤٩١**				
المعنوية الكلية لنموذج الإنحدار		**مستوى المعنوية لتحليل ANOVA= ٠,٠٠٠**				

يتضح للباحثة من الجدول السابق النتائج الأتية:

أ- وجود ارتباط طردي معنوي عند مستوى معنوية (٠,٠١) بين مخاطر هجمات الأمن السيبراني بمنشأة العميل وأعمال المراجع الخارجي، حيث أن معامل الارتباط موجب ويبلغ (٠,٦٥٥)، ومستوي المعنوية (sig) أقل من (٠,٠١).

ب- وجود تأثير طردي معنوي عند مستوى معنوية (٠,٠١) لمخاطر هجمات الأمن السيبراني بمنشأة العميل على أعمال المراجع الخارجي، حيث أن معامل الإنحدار موجب ومستوي المعنوية (sig) أقل من (٠,٠١).

ج- أن قيمة معامل التحديد (R^2) بالنسبة لنموذج الإنحدار تبلغ (٠,٤٢٩)، وهو ما يعكس القيمة التفسيرية للنموذج، حيث أن التغيرات التى تحدث للمتغير التابع (أعمال المراجع الخارجي) يمكن تفسيرها من خلال المتغير التابع (وجود مخاطر هجمات الأمن السيبراني بمنشأة العميل) بنسبة ٤٢,٩% وباقى التغيرات ترجع لأسباب ومتغيرات أخرى.

وفى ضوء ما سبق يمكن صياغة معادلة كمية لنموذج الانحدار تحكم علاقة تأثير مخاطر هجمات الأمن السيبراني بمنشأة العميل على أعمال المراجع الخارجي كما يلي:

معادلة رقم(١) : الفرض الأول

أعمال المراجع الخارجي = ١,٣٤٢ + ٠,٦٤٧ مخاطر هجمات الأمن السيبراني بمنشأة العميل

وتخلص الباحثة مما سبق أنه في ضوء ضوابط ومحددات العينة المختارة ووفقا للآراء المستقصي منهم فأنه كلما زادت مخاطر هجمات الأمن السيبراني بمنشأة العميل كلما إنعكس ذلك على نطاق ومسئوليات أعمال المراجع الخارجي، وبالتالي رفض الفرض العدم، وقبول الفرض الأول البديل للبحث (H_1) بأنه " يوجد تأثير معنوي لمخاطر هجمات الأمن السيبراني بمنشأة العميل على أعمال المراجع الخارجي".

٣/٢ /٢ التحليـل الإحصائي للبيانـات المرتبطـة بالفـرض الثاني واختبـاره

نص الفرض الثاني:" لا توجد علاقة ذات دلالة معنوية بين إدارة الإفصـــاح عن مخاطر الأمن السـيبراني والمنهج الإجرائي المقترح لأعمال المراجع الخارجي"، ويتم إختبار صـحة هذا الفرض كما يلي:

١- التحليل الوصفي للبيانات المرتبطة بالفرض الثاني

تتناول الباحثة نتائج توصـــيف الآراء من قبل عينة الدراســـة حول العبارات المرتبطة بمتغيرات الفرض الثاني وذلك كما يلي:

جدول (٨) توصيف الآراء حول العبارات التي تحدد متغيرات الفرض الثاني

العناصر (العبارات) التي تحدد متغيرات الفرض الثاني	مقاييس الإحصاء الوصفي			
	الوسط الحسابي	الانحراف المعياري	الأهمية النسبية	ترتيب الموافقة
أولا: إدارة الإفصاح عن مخاطر الأمن السيبراني				
١- هناك مخاوف من أن أصحاب المصلحة ليس لديهم معلومات كافية في الوقت المناسب بشأن مخاطر الأمن السيبراني للشركات وجهود إدارة المخاطر وبالتالي يجب تعزيز إفصاحات الأمن السيبراني للشركات	٤,١٤	٠,٨٢٥	٨٢,٨٠٪	٢
٢- يجب على الشركات الالتزام بالإرشادات بشأن الإفصاح عن مخاطر الأمن السيبراني، والتي توضح العوامل والإفصاحات الموصي به بشأن المسائل الجوهرية، مثل وقوع حوادث الأمن السيبراني السابقة، واحتمال وحجم الأحداث المستقبلية للأمن السيبراني، وأي تكاليف تقاضي ومعالجة مرتبطة بحوادث الأمن السيبراني السابقة.	٤,١٤	٠,٩٣٨	٨٢,٨٠٪	٣
٣- إعداد تقارير إدارة مخاطر الأمن السيبراني تساعد الشركات في تعزيز عمليات الإفصاح المتعلقة بالأمن السيبراني، ويمكن استخدامها للإفصاح عن المعلومات المفيدة لأصحاب المصلحة حول برنامج إدارة مخاطر الأمن السيبراني وفعاليته.	٤	٠,٨٩٤	٨٠,٠٠٪	٦
٤- يجب على الإدارة تقديم وصف لبرنامج إدارة مخاطر الأمن السيبراني للشركة، حيث تستخدم الإدارة معايير الوصف المناسبة لتطوير وصف الإدارة، وتزويد المستخدمين المحتملين بمعلومات حول الشركة ووصف لبرنامج إدارة مخاطر الأمن السيبراني.	٤,١٨	٠,٩٦٣	٨٣,٦٠٪	١
٥- يجب على الإدارة توفير معلومات بشأن فعالية ضوابط الأمن السيبراني، وأن الضوابط التي تنفذها الإدارة يمكن ان تحقق أهداف الأمن السيبراني للشركة.	٣,٨٨	١,١٩٤	٧٧,٦٠٪	٧
٦- يجب على الإدارة الإفصاح عن رأي المراجع في إفصاحات الإدارة وفعالية ضوابط الشركة ومنها على سبيل المثال تقرير ضوابط النظام والتنظيم للأمن السيبراني.	٤,٠٦	١,٠٩٤	٨١,٢٠٪	٥
٧- لا يستطيع المراجع الخارجي وحده التعامل مع تلك المشاكل والتحديات، لذلك فهو بحاجة إلى مشاركة خبراء تكنولوجيا المعلومات لإبداء رأي حول بيئة الرقابة في أنظمة تكنولوجيا المعلومات للتصدي بشكل مناسب للمخاطر الناشئة عن الاستخدام وتشغيل الحلول التكنولوجية التي لها تأثير واسع على اكتمال ودقة البيانات المالية	٤,١	٠,٩٦٤	٨٢,٠٠٪	٤
درجة الموافقة الكلية على بعد إدارة الإفصاح عن مخاطر الأمن السيبراني	٤,٠٧	٠,٦٥٩	٨١,٤٠٪	**موافقة**
ثانيا: خطوات المنهج الإجرائي المقترح لعملية مراجعة الإفصاح عن مخاطر الأمن السيبراني.				
▪ **الخطوة الأولى: التأكد من مواءمة الأمن السيبراني ضمن الأولويات التنظيمية**				
١- التأكد من إنشاء المنظمة لإطار عمل لمراقبة الأمن السيبراني.	٤,١	٠,٨٣١	٨٢,٠٠٪	٤

العناصر (العبارات) التي تحدد متغيرات الفرض الثاني	مقاييس الإحصاء الوصفي			
	الوسط الحسابي	الانحراف المعياري	الأهمية النسبية	ترتيب الموافقة
٢- التأكد من تعاون المنظمة مع منظمات تكنولوجيا المعلومات أو الهيئات المعنية لصياغة وتطوير وتنسيق المعايير أو الإرشادات لتلبية احتياجاتهم بدقة.	٤,١٤	٠,٨٧٢	٨٢,٨٠٪	١
٣- فهم بيئة تكنولوجيا المعلومات ذات العلاقة بتدفقات المعاملات ومعالجة المعلومات في نظم المعلومات حيث يقوم المراجع بجمع معلومات حول طبيعة وخصائص تطبيقات تكنولوجيا المعلومات المستخدمة	٤,١٣	٠,٨٧٩	٨٢,٦٠٪	٣
٤- يحتاج المراجع إلى فهم كيفية تحديد المنشأة لمخاطر الأمن السيبراني وكيفية الرقابة عليها من خلال توسيع الفهم ليشمل البيئة السيبرانية للمنشأة، مع التركيز على الجوانب التقنية والتي منه	٤,١٤	٠,٩٤٩	٨٢,٨٠٪	٢
درجة الموافقة الكلية على الخطوة الأولى من المنهج الإجرائي المقترح لعملية مراجعة الإفصاح عن مخاطر الأمن السيبراني	٤,١٢	٠,٦٤٦	٨٢,٤٠٪	**موافقة**
▪ **الخطوة الثانية: التأكد من السياسات والإجراءات الخاصة في دعم عمليات الإفصاح عن إدارة مخاطر الأمن السيبراني**				
١- اختبار رقابة تكنولوجيا المعلومات من خلال اختبار الفعالية التشغيلية لضوابط الأمن الإلكتروني.	٤,١٨	٠,٧٩٢	٨٣,٦٠٪	٢
٢- اختبار فعالية نظام الرقابة الداخلية للحد من مخاطر الأمن السيبراني.	٣,٨٥	١,١٢٦	٧٧,٠٠٪	٤
٣- التحقق من سياسات الإدارة بشأن مخاطر الأمن السيبراني.	٣,٩٦	١,٠٥٨	٧٩,٢٠٪	٣
٤- اعتماد المراجع الخارجي على أعمال المراجع الداخلية بشأن مخاطر الأمن السيبراني.	٤,٢٢	٠,٨٢	٨٤,٤٠٪	١
درجة الموافقة الكلية على الخطوة الثانية من المنهج الإجرائي المقترح لعملية مراجعة الإفصاح عن مخاطر الأمن السيبراني	٤,٠٥	٠,٦١١	٨١,٠٠٪	**موافقة**
▪ **الخطوة الثالثة: تحديد أثر اختراقات الأمن السيبراني على البيانات المالية**				
١- فهم طبيعة وسبب حادثة الهجوم السيبراني، والنظر بعناية في التكاليف وأية عواقب ضارة ناجمة عن الحادثة، وتقييم الأثر الذي قد يترتب عن الحادثة على التقارير المالية.	٣,٩٩	٠,٩٨٥	٧٩,٨٠٪	٢
٢- تقييم تأثير الهجوم على الإيرادات، والتدفقات النقدية المستقبلية والقيمة المستقبلية للمنشأة، ومصروفات التقاضي المحتملة، وتكاليف حماية الأمن السيبراني.	٤,٠٣	١,٠١٤	٨٠,٦٠٪	١
٣- تقييم سلامة الإفصاحات والعرض في التقارير المالية.	٣,٩٤	٠,٩٠٤	٧٨,٨٠٪	٥
٤- النظر في أي متطلبات أخرى لإخطار السلطات المختصة في حالة عدم قيام الإدارة بالإفصاح المناسب أو عدم اخذها لتوصيات المراجع بالاعتبار.	٣,٩٦	٠,٨٢٤	٧٩,٢٠٪	٣
٥- تقييم القوانين واللوائح التي قد يكون لها تأثير مباشر أو غير مباشر على البيانات المالية للمنشأة، مثل التشريعات والقوانين المتعلقة بحماية البيانات. وبالتالي يجب النظر إلى اي مدى امتثلت المنشاة بتلك القوانين أو اللوائح.	٣,٩٥	٠,٩٧٣	٧٩,٠٠٪	٤
درجة الموافقة الكلية على الخطوة الثالثة من المنهج الإجرائي المقترح لعملية مراجعة الإفصاح عن مخاطر الأمن السيبراني	٣,٩٧	٠,٦٤٨	٧٩,٤٠٪	**موافقة**
درجة الموافقة الكلية على المنهج الإجرائي المقترح لعملية مراجعة الإفصاح عن مخاطر الأمن السيبراني	٤,٠٤	٠,٥٤٣	٨٠,٨٠٪	**موافقة**

** الوسط الحسابي لكل العبارات دال إحصائيًا عند مستوى معنوية ٠,٠٥

تخلص الباحثة من الجدول السابق إلى النتائج التالية:

تشـــير قيم الوســـط الحســـابي لجميع ردود المســـتقصـــي منهم حول جميع العناصـــر (أكبر من ٣) إلى أن الآراء تميل لصـالح الموافقة حول بنود إدارة الإفصـاح عن مخاطر الأمن السـيبراني، وخطوات المنهج الإجرائي المقترح لعملية مراجعة الإفصـاح عن مخاطر الأمن السـيبراني؛ وهو ما تؤكد عليه نســب الوزن النســبي لجميع العناصــر والتي تزيد عن ٦٠٪ الممثلة لإختيار"محايد"، وجاءت جميع الأوسـاط الحسـابية لجميع العبارات دالة إحصـائيا عند مسـتوى معنوية (٠,٠٥) ويدل ذلك على أنه يوجد إختلافات (فروق معنوية) في أراء المستقصي منهم بين القيم المشاهدة وقيمة (٣) والممثلة لإختيار محايد.

بالنســبة لإدارة الإفصـــاح عن مخاطر الأمن الســيبراني: يشــير ترتيب درجة الموافقة (الأهمية النسبية) إلى العبارات الأكثر أهمية وصاحبة الأعلى موافقة من المستقصي منهم " هناك مخاوف من أن أصـحاب المصـلحة ليس لديهم معلومات كافية في الوقت المناسـب بشـأن مخاطر الأمن السـيبراني للشــركات وجهود إدارة المخاطر وبالتالي يجب تعزيز إفصــاحات الأمن الســيبراني للشــركات، ثم عبارة " يجب على الإدارة تقديم وصـــف لبرنامج إدارة مخاطر الأمن الســـيبراني للشـــركة، حيث تسـتخدم الإدارة معايير الوصـف المناسـبة لتطوير وصـف الإدارة، وتزويد المسـتخدمين المحتملين بمعلومات حول الشركة ووصف لبرنامج إدارة مخاطر الأمن السيبراني" .

وبالنسبة للمنهج المنهج الإجرائي المقترح لعملية مراجعة الإفصـاح عن مخاطر الأمن السيبراني جاء تقييمه من قبل عينة الدراسة كما يلي:

أ- أهم جوانب الإطار المقترح من وجهة نظر عينة الدراسة تتمثل فى العبارات التالية على التوالى ، التأكد من تعاون المنظمة مع منظمات تكنولوجيا المعلومات أو الهيئات المعنية لصـــياغة وتطوير وتنســـيق المعايير أو الإرشـــادات لتلبية احتياجاتهم بدقة وذلك عند التأكد من مواءمة الأمن الســيبراني ضـــمن الأولويات التنظيمية، اعتماد المراجع الخارجي على أعمال المراجع الداخلية بشأن مخاطر الأمن السيبراني وذلك عند التأكد من السياسات والإجراءات الخاصة في دعم عمليات الإفصـاح عن إدارة مخاطر الأمن السـيبراني، تقييم تأثير الهجوم على الإيرادات، والتدفقات النقدية المســتقبلية والقيمة المســتقبلية للمنشــأة، ومصــروفات التقاضـــي المحتملة، وتكاليف حماية الأمن السـيبراني وذلك عند تحديد أثر اختراقات الأمن السـيبراني على البيانات المالية.

ب- أقل جوانب الإطار المقترح من وجهة نظر عينة الدراســة إهتماما هي على التوالى ، التأكد من إنشــاء المنظمة لإطار عمل لمراقبة الأمن الســيبراني، اختبار فعالية نظام الرقابة الداخلية للحد من مخاطر الأمن السيبراني، تقييم سلامة الإفصاحات والعرض في التقارير المالية.

٢- تحليل التباين (مدى الاتفاق والاختلاف) بين فئات العينة حول الفرض الثاني

تتنـاول البـاحثـة التبـاين (مـدى الاتفـاق والاختلاف) في آراء فئـات العينـة حول العبـارات المرتبطة بالفرض الثاني وذلك كما يلي:

جدول (٩) تحليل التباين بين آراء فئات العينة حول بيانات الفرض الثاني

العناصر المرتبطة بالفرض الثاني	فئات العينة	عدد المشاهدات	متوسط الرتب	الترتيب	معنوية إختبار Kruskal-Wallis
▪ إدارة الإفصاح عن مخاطر الأمن السيبراني	المراجعين بمكاتب المحاسبة والمراجعة لشركات العينة	٣٥	٥٥,٧٤	٢	٠,٠٠٥
	مسئولي تكنولوجيا المعلومات	٤١	٥٦,٩٩	١	
	أعضاء مجلس الإدارة	٢٥	٣٤,٥٤	٣	
	الإجمالـــــى	١٠١			
▪ المنهج الإجرائي المقترح لعملية مراجعة الإفصاح عن مخاطر الأمن السيبراني	المراجعين بمكاتب المحاسبة والمراجعة لشركات العينة	٣٥	٥٧,٠٦	١	٠,٠٠٣
	مسئولي تكنولوجيا المعلومات	٤١	٥٦,٥١	٢	
	أعضاء مجلس الإدارة	٢٥	٣٣,٤٨	٣	
	الإجمالـــــى	١٠١			

*** دال إحصائيًا عند مستوى معنوية ٠,٠٥**

تخلص الباحثة من الجدول السابق إلى النتائج التالية:

أ- تشـير قيم متوسـط الرتب والترتيب إلى أن أعلى الفئات موافقة على بنود إدارة الإفصـاح عن مخاطر الأمن السيبراني، هي فئة مسئولي تكنولوجيا المعلومات بمتوسط رتب بلغ (٥٦,٩٩)، بينما جاءت فئة الدراسـة من المراجعين الخارجيين في مكاتب المحاسـبة والمراجعة لشـركات العينة أعلى الفئات موافقة على خطوات المنهج الإجرائي المقترح لعملية مراجعة الإفصاح عن مخاطر الأمن السيبراني بمتوسط رتب بلغ (٥٧,٠٦)، وجاءت فئة الدراسة من أعضاء مجلس الإدارة في شركات العينة أقل الفئات موافقة على بيانات الفرض الثاني .

ب- بلغت قيم مستوى المعنوية لاختبار (Kruskal-Wallis Test) للبيانات المرتبطة بمتغيري الفرض الأول (٠,٠٠٥) (٠,٠٠٣) على الترتيب وهى أقل من ٥٪ ويدل ذلك على وجود فروق معنوية بين الفئات الممثلة للعينة محل البحث حول بنود إدارة الإفصاح عن مخاطر الأمن السيبراني، وخطوات المنهج الإجرائي المقترح .

٣- تحليل نتائج إختبـار الفـرض الثاني

يتم اختبار مدى صحة الفرض الثاني للدراسة من إجراء التحليل ثنائي المتغير (تحليل الإرتباط) لمتغيرات الفرض وذلك لاختبار علاقة الإرتباط بين إدارة الإفصاح عن مخاطر الأمن السيبراني والمنهج الإجرائي المقترح لأعمال المراجع الخارجي، وذلك كما يلي:

جدول رقم (١٠) نتائج تحليل الإرتباط لمتغيرات الفرض الثاني

تحليل نتائج الإرتباط	معامل الارتباط بين إدارة الإفصاح عن مخاطر الأمن السيبراني والمنهج الإجرائي المقترح لأعمال المراجع الخارجي	٠,٧٤٥
	مستوى المعنوية (عند ٠,٠١)	٠,٠٠٠

يتضح للباحثة من الجدول السابق وجود ارتباط طردي معنوي عند مستوى معنوية (٠,٠١) بين إدارة الإفصاح عن مخاطر الأمن السيبراني والمنهج الإجرائي المقترح لأعمال المراجع الخارجي، حيث أن معامل الارتباط موجب، ومستوي المعنوية أقل من (٠,٠١).

وتخلص الباحثة مما سبق أنه في ضوء ضوابط ومحددات العينة المختارة ووفقا للآراء المستقصي منهم فإن إدارة الإفصاح عن مخاطر الأمن السيبراني تتعلق بالمنهج الإجرائي المقترح لأعمال المراجع الخارجي، وبالتالي رفض الفرض العدم، وقبول الفرض الثاني البديل للبحث (H_2) بأنه " توجد علاقة ذات دلالة معنوية بين إدارة الإفصاح عن مخاطر الأمن السيبراني والمنهج الإجرائي المقترح لأعمال المراجع الخارجي".

وبعد إختبار صحة فروض البحث والتوصل إلى وجود إنعكاسات لمخاطر هجمات الأمن السيبراني على أعمال المراجع الخارجي، وأن هناك أهمية للمنهج المقترح من الباحثة لأعمال المراجع الخارجي عند تقييم هذه المخاطر، تتناول الباحثة تحليل وصفى لإجابات المختصين في شركات عينة الدراسة والمراجعين بمكاتب المراجعة حول بعض التساؤلات المرتبطة بمخاطر هجمات الامن السيبراني ومدى إستجابة المراجع الخارجي لها وذلك من خلال النقطة التالية.

٤/٢ دليل تطبيقي لواقع المخاطر السيبرانية في شركات المساهمة ومدى استجابة المراجع الخارجي لها:

قامت الباحثة بتوجيه بعض الأسئلة لعينة الدراسة المنتمين إلى شركات المساهمة ومكاتب المراجعة المرتبطة بها، ويوضح الجدول التالي التحليل الوصفي لبعض المعلومات عن موقف الشركات ومكاتب المراجعة من المخاطر السيبرانية وانعكاساتها على أعمال المراجع، وذلك وفقا للأسئلة التي تم توجيهها لهم وإجاباتهم عليها، وذلك كما يلي:

جدول (١١): التحليل الوصفي لبعض البيانات عن موقف الشركات ومكاتب المراجعة من المخاطر السيبرانية

بيـــان	الاختيارات المتاحة	العدد	النسبة
هل تعرضت شركتكم من قبل إلى تهديدات أو هجمات مخاطر الأمن السيبراني؟	نعم	١٠	٦٦,٧٪
	لا	٥	٣٣,٣٪
هل ترى أن فريق عمل تكنولوجيا المعلومات والأنظمة الإلكترونية لدى شركتكم لدية المعرفة والدراية بمخاطر الأمن السيبراني - خاصة في ظل الأزمة المالية الحالية وأزمة جائحة كورنا – وأنه على دراية بأثر هذه المخاطر على سمعة الشركة واستثماراتها في السوق؟	نعم	٥	٣٣,٣٪
	لا	٢	١٣,٣٪
	يحتاج إلى زيادة المعرفة والتدريب على مواجهة هذه المخاطر ومعرفة أثارها	٨	٥٣,٣٪
في حالة وإن تعرضت شركتكم للحوادث والتهديدات السيبرانية هل تم اكتشافها وإدارة المخاطر الناتجة عنها من قبل المختصين لديكم أم كان للمراجع الخارجي النصيب الأهم في التعامل معها والانتظار لتقريره لتقييم المخاطر واتخاذ القرارات بشأنها؟	التعامل تم من خلال الشركة	٤	٢٦,٧٪
	المراجع الخارجي هو المنوط بها ورأيه هو الأساس في تقييم هذه المخاطر.	٣	٢٠,٠٪
	يتم مواجهتها وتقيمها من خلال الشركة بالتنسيق مع المراجع الخارجي.	٨	٥٣,٣٪
هل ترى أن هناك ضرورة لاتخاذ الشركة جميع الإجراءات اللازمة والمطلوبة لإبلاغ المستثمرين والإفصاح بشأن مخاطر وحوادث الأمن السيبراني في الوقت المناسب؟	نعم	٢	١٣,٣٪
	لا	٢	١٣,٣٪
	وفقا لتقرير ورأى المراجع الخارجي	١١	٧٣,٣٪
	زادت	١٢	٨٠,٠٪

هل تأثرت أتعاب المراجعة التي يحصل عليها مكتب المراجع قبل وبعد تعرض الشركة للمخاطر السيبرانية؟	انخفضت	٠	٠,٠٪
	لم تتأثر	٣	٢٠,٠٪
ماهي علاقة مكتب المراجعة مع مكاتب المراجعة الكبرى (BIG4)؟	فرع / شراكة / ممثل	٤	٥٠,٠٪
	خلاف ذلك	٤	٥٠,٠٪
ما مدى خبرة مكتبكم في مجال مراجعة الشركات العاملة في القطاعات والأنشطة المرتبطة بالتقنيات الحديثة في نظم المعلومات والتكنولوجيا الرقمية مثل انترنت الأشياء وسلاسل الكتل وخدمات الحوسبة السحابية والتي يزداد فيها احتمالية التعرض لتهديدات ومخاطر الأمن السيبراني؟	غير موجودة	٠	٠,٠٪
	خبرة كافيه	٨	١٠٠,٠٪
هل التعديلات في معايير المراجعة وما يرتبط بها من إصدارات وإرشادات وتوصيات مهنية تصدرها الجهات المنظمة لمهنة المراجعة كافيه للمراجع لتحقيق استجابة فعالة وتكوين رأى فنى حول التقارير المالية للشركات التي تتعرض لمخاطر الأمن السيبراني؟	نعم كافية	١	١٢,٥٪
	غير كافية	٣	٣٧,٥٪
	تحتاج لمزيد من التكيف مع البيئة المصرية	٤	٥٠,٠٪
هل هناك حاجة ضرورية لوجود منهج إجرائي لمراجعة وتقييم عملية إدارة مخاطر الأمن السيبراني يأخذ في الاعتبار مزايا الإصدارات المهنية في هذا الشأن ويتلافى عيوبها؟	نعم	٦	٧٥,٠٪
	لا	٢	٢٥,٠٪
هل تختلف أتعاب المراجعة التي يحصل عليها المكتب في حالة مراجعة الشركات التي تتعرض لمخاطر الأمن السيبراني عنها في حالة مراجعة الشركات الأخرى؟	نعم	٤	٥٠,٠٪
	لا	١	١٢,٥٪
	حسب عقد الإرتباط	٣	٣٧,٥٪

وتظهر الردود وفقا للجدول السابق النتائج التالية:

١- تعرض (١٠) شركات من شركات العينة إلى تهديدات أو هجمات مخاطر الأمن السيبراني بنسبة (٦٦,٧٪)، ووجدت (٥٣٪) من شركات العينة أن فريق عمل تكنولوجيا المعلومات والأنظمة الإلكترونية لدى الشركة يحتاج لمزيد من المعرفة والدراية بمخاطر الأمن السيبراني - خاصة في ظل الأزمة المالية الحالية وأزمة جائحة كورنا – وأنه يحتاج للتدريب على خطط مواجهة هذه المخاطر نظرا للآثار المباشرة لهذه المخاطر على سمعة الشركة واستثماراتها في السوق.

٢- بالنسبة للقائمين على تقييم المخاطر المرتبطة بهجمات الأمن السيبراني يري المختصين في (٨) شركات تمثل (٥٣٪) من عينة الدارسة أن مخاطر الأمن السيبراني يتم مواجهتها وتقيمها من خلال الشركة بالتنسيق مع المراجع الخارجي، وأن (١١) شركة تمثل (٨٠٪) من شركات العينة يرو من وجهة نظر المختصين لديهم أي أن هناك ضرورة لاتخاذ الشركة جميع الإجراءات اللازمة والمطلوبة لإبلاغ المستثمرين والإفصاح بشأن مخاطر وحوادث الأمن السيبراني في الوقت المناسب وفقا لتقرير ورأى المراجع الخارجي.

٣- جميع مكاتب المحاسبة والمراجعة التي تقوم بمراجعة شركات العينة والبالغ عددها (٨) مكاتب يرتبط (٥٠٪) منهم بشراكة مع مكاتب المراجعة الكبرى (BIG4) لديهم خبرة كافية في مجال مراجعة الشركات العاملة في القطاعات والأنشطة المرتبطة بالتقنيات الحديثة في نظم المعلومات والتكنولوجيا الرقمية مثل انترنت الأشياء وسلاسل الكتل وخدمات الحوسبة السحابية والتي يزداد فيها احتمالية التعرض لتهديدات ومخاطر الأمن السيبراني.

٤- (٥٠٪) من مكاتب المحاسبة والمراجعة التي تقوم بمراجعة شركات العينة يرون أن التعديلات في معايير المراجعة وما يرتبط بها من إصدارات وإرشادات وتوصيات مهنية تصدرها الجهات المنظمة لمهنة المراجعة غير كافيه للمراجع لتحقيق استجابة فعالة وتكوين رأى فنى حول

التقارير المالية للشركات التي تتعرض لمخاطر الأمن السيبراني وأنه يجب تتماشى مع متطلبات البيئة المصرية والظروف الراهنة.

٥- نسبة كبيرة من مكاتب المحاسبة والمراجعة التي تقوم بمراجعة شركات العينة بلغت (٧٥٪) يرون أن هناك حاجة ضرورية لوجود منهج إجرائي لمراجعة وتقييم عملية إدارة مخاطر الأمن السيبراني يأخذ في الاعتبار مزايا الإصدارات المهنية في هذا الشأن ويتلافى عيوبها.

٦- بالنسبة لأتعاب مراجعة شركات المساهمة التي يحصل عليها مكتب المراجع في ظل تعرض الشركة للمخاطر السيبرانية اتفقت شركات المساهمة ومكاتب المراجعة المستقصي منهم البيانات على أن هذه الأتعاب زادت في حالة تعرض الشركة للهجمات الإلكترونية والمخاطر السيبرانية.

هذا وبناء على الدراسة النظرية والتحليل الإحصائي واتفاقا ما ذكرته دراسة Lindsay, et. al. (2019) فإن اختبار المراجع لرقابة المخاطر السيبرانية يعد امتداد للاختبارات المعتاده للضوابط العامة لتكنولوجيا المعلومات ويستخدم نفس المنهج عندما يتعلق الأمر باختبار الرقابة، ويكمن الاختلاف بشكل أساسي في الموضوعات التي يجب تناولها واستخدام الفهم المتعمق لتقنيات الأمن السيبراني للحصول على مزيد من الحقائق، حيث يجب على المراجع الحفاظ على شكوك مهنية كافية عند مراجعة وتقييم إدارة المخاطر السيبرانية، وفهم كيف يمكن أن تؤثر مخاطر الأمن السيبراني على تدفق المعاملات، وتقييم مدى اكتمال أنظمة الرقابة الداخلية على القوائم المالية، وتصميم المراجع للخطط المناسبة والاستجابة الكافية والمناسبة لتلك المخاطر. تقييم مدى ملاءمة عمليات الإدارة لتحديد وتطوير وتشغيل وصيانة الضوابط المتعلقة بالأمن السيبراني وإدارة مخاطره.

وفي ضوء ما أشارت إليه الدراسة النظرية وما توصلت إليه الدراسة التطبيقية في مجال البحث، توصلت الباحثة إلى العديد من النتائج يمكن عرضها على النحو التالي:

١. اتفقت النتائج النظرية مع الدراسات السابقة في أن تقييم مخاطر الأمن السيبراني يعتمد على عمليات المراجعة التي تدرس وتقيم مجموعة من الضوابط المحددة مسبقاً في مجموعة متنوعة من الموضوعات المتعلقة بالأمن السيبراني .
٢. تتفق النتائج النظرية مع الدراسات السابقة في أن حوادث الأمن السيبراني تؤثر بشكل مباشر على الضوابط الداخلية وعلى التقارير المالية للشركات المتضررة.
٣. عند حدوث هجمات الأمن السيبراني يكون المراجع الخارجي مسئول عن تقييم أسلوب العميل في المحاسبة عن الخسائر والمطالبات والالتزامات المتعلقة بالحادثة وتقييم أثرها النهائي على التقارير المالية.
٤. يكون لتهديدات الأمن السيبراني آثار كبيرة على فعالية الرقابة الداخلية حالياً أو في المستقبل وبالتالي قد يكون المراجع ملزماً بالتحقيق فيما إذا كانت الإدارة قد نفذت الضوابط المناسبة.
٥. اتفقت النتائج النظرية مع التطبيقية في أن المخاطر السيبرانية ترتبط بتعدد أهداف الهجمات الإلكترونية ومنها السرقة والابتزاز، أو تدمير الأصول المالية، أو سرقة الملكية الفكرية، أو سرقة المعلومات الحساسة الأخرى التي تخص الشركات أو عملائها أو شركائها التجاريين.
٦. أوضح التحليل الإحصائي أهمية الخطوة الأولى من المنهج الإجرائي المقترح "التأكد من مواءمة الأمن السيبراني ضمن الأولويات التنظيمية عند مستوى أهمية نسبية ٨٢,٤٠٪.
٧. كما برزت أهمية الخطوة الثانية" التأكد من السياسات والإجراءات الخاصة في دعم عمليات الإفصاح عن إدارة مخاطر الأمن السيبراني" عند مستوى أهمية نسبية ٨١٪.

٨. فيما أوضحت النتائج أهمية على الخطوة الثالثة من المنهج الإجرائي المقترح لعملية مراجعة الإفصاح عن مخاطر الأمن السيبراني عند مستوى أهمية نسبية ٧٩,٤٠٪.
٩. أوضح التحليل الإحصائي وجود تأثير طردي معنوي عند مستوى معنوية (٠,٠١) لمخاطر هجمات الأمن السيبراني بمنشأة العميل على أعمال المراجع الخارجي.
١٠. يوجد ارتباط طردي معنوي بين إدارة الإفصاح عن مخاطر الأمن السيبراني والمنهج الإجرائي المقترح لأعمال المراجع الخارجي.

بينما تتمثل أهم التوصيات والأبحاث المستقبلية في مجال البحث فيما يلي:

١. تضمين مخاطر الأمن السيبراني كجزء من تقييم المراجع لمخاطر تكنولوجيا المعلومات في منشأة العميل.
٢. التأكد من تعاون إدارة الشركات مع منظمات تكنولوجيا المعلومات أو الهيئات المعنية لصياغة وتطوير وتنسيق المعايير أو الإرشادات لتلبية احتياجاتهم بدقة في ضوء متطلبات الأمن السيبراني.
٣. على الإدارة تقديم وصف لبرنامج إدارة مخاطر الأمن السيبراني للشركة، حيث تستخدم الإدارة معايير الوصف المناسبة لتطوير وصف الإدارة، وتزويد المستخدمين المحتملين بمعلومات حول الشركة ووصف لبرنامج إدارة مخاطر الأمن السيبراني.
٤. تطبيق المدخل الإجرائي المتبع عند إجراء عملية مراجعة مخاطر الأمن السيبراني .
٥. إجراء المزيد من الدراسات المستقبلية حول مخاطر الأمن السيبراني وإعادة إصدار القوائم المالية.
٦. إجراء المزيد من الدراسات المستقبلية حول تأثير العلاقة بين مجلس الإدارة ولجان المراجعة على إدارة مخاطر الأمن السيبراني.
٧. إجراء المزيد من الدراسات المستقبلية حول تطوير قواعد القيد والشطب في مصر بشأن إدارة مخاطر وحوكمة والإفصاح عن حوادث الأمن السيبراني على قرار الاستثمار في الأسهم- دراسة تجريبية.
٨. إجراء المزيد من الدراسات المستقبلية حول التكاليف التقديرية لإعداد برنامج مخاطر الأمن السيبراني للمؤسسات وأثره على سعر السهم للشركات المقيدة في البورصة المصرية.

قائمة المراجع

المراجع العربية:

١. المنظمة الدولية للأجهزة العليا للرقابة المالية والمحاسبة (٢٠١٨) . دليل تدقيق تكنولوجيا المعلومات لأجهزة الرقابة العليا- مجموعة عمل الإنتوساي لتدقيق تكنولوجيا المعلومات- ومبادرة الإنتوساي للتنمية INTOSAI. ص٨٦.

٢. محروس ، رمضان عارف & صالح ، أبو الحمد مصطفى .(٢٠٢٢) استخدام المنهجية الرشيقة في تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبرانى ، ***مجلة البحوث المالية والتجارية*** ، كلية التجارة ، جامعة بورسعيد، العدد٣، المجلد ٢٣، ص ص:٤٣٢-٤٩١.

٣. فرج، هاني خليل فرج . (٢٠٢٢). أثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكتروني على قرار الاستثمار بالأسهم - دراسة تجريبية، ***مجلة المحاسبة والمراجعة لاتحاد الجامعات العربية***. العدد٢، المجلد ١١، ص ص: ١٢٩-٢٠٩ .

٤. سليمان، أسامة ربيع أمين.(٢٠٠٧) ، ***التحليل الإحصائي باستخدام برنامج SPSS الجزء الأول مهارات أساسية اختبارات الفروض الإحصائية (المعلمية – اللامعلمية)*** ، مكتبة الأنجلو المصرية، القاهرة، ص ص ١١٥- ١٩٧.

٥. الزغبى، محمد بلال ، الطلاحفة.(٢٠١٢). عباس ،***النظام الإحصائى spss فهم وتحليل البيانات الإحصائية*** ،الجامعة الأردنية، الأردن ، الطبعة الثالثة، ص ٣١٤.

المراجع الاجنبية

1. Abu-Bader, Soleman H. Using statistical methods in social science research: With a complete SPSS guide. Oxford University Press, USA, 2021.
2. Alina, C. M., Cerasela, S. E., & Gabriela, G. (2017). Internal audit role in cybersecurity. Ovidius University Annals: ***Economic Sciences Series***, 17(2), 510-513.
3. Al-Matari, O. M., Helal, I. M., Mazen, S. A., & Elhennawy, S. (2021). Integrated framework for cybersecurity auditing. ***Information Security Journal: A Global Perspective***, 30(4), 189-204.
4. Althonayan, A., & Andronache, A. (2018, September). Shifting from information security towards a cybersecurity paradigm. In Proceedings of the 2018 10th International Conference on Information Management and Engineering (pp. 68-79).

5. American Institute of Certified Public Accountants (AICPA (2018b), "SOC for cyber security: a backgrounder.
6. American Institute of Certified Public Accountants (AICPA) (2018a), "Cyber security risk management reporting fact sheet".
7. American Institute of Certified Public Accountants AICPA (2017), Description Criteria for Management's Description of the
8. Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. ***Review of Accounting Studies***, 23(3), 1177-1206.
9. Antunes, M., Maximiano, M., & Gomes, R. (2022). A Client-Centered Information Security and Cybersecurity Auditing Framework. ***Applied Sciences***, 12(9), 4102.
10. Badawy, H. A. E. S. (2021). The Impact of Assurance Quality and Level on Cybersecurity Risk Management Program on Non-Professional Egyptian Investors' Decisions: An Experimental Study. ***Alexandria Journal of Accounting Research***, *5*(3).
11. Barta, G. (2018). The increasing role of IT auditors in financial audit: risks and intelligent answers. ***Business, Management and Economics Engineering***, 16, 81-93 .
12. Blakely, B., Kurtenbach, J., & Nowak, L. (2022). Exploring the information content of cyber breach reports and the relationship to internal controls. ***International Journal of Accounting Information Systems***, 46, 100568.
13. Calderon, T. G., & Gao, L. (2021). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. ***International Journal of Auditing***, *25*(1), 24-39.
14. Center for Audit Quality - CAQ. (2014). Cybersecurity and the External Audit. (March 2014).
15. Center for Audit Quality - CAQ. (2016). Understanding Cybersecurity and the External Audit. .

16. Center for Audit Quality - CAQ. (2017). The CPA's Role in Addressing Cybersecurity Risk. How the Auditing Profession Promotes Cybersecurity Resilience.
17. Center for Audit Quality (CAQ). 2016. A Model for Cyber security and Auditing. In Clinton, L. & Perera, D. (Eds), Social Contract 3.0: Implementing a Market-Based Model for Cyber security. Published by the Internet Security Alliance.
18. Center for Audit Quality. (2014).cyber security – its impact on the external audit and recent developments .
19. Cisco Annual Internet Report (2018–2023) White Paper (2020).
20. Cohen, J., Krishnamoorthy, G., & Wright, A. (2017). Enterprise risk management and the financial reporting process: The experiences of audit committee members, CFO s, and external auditors. ***Contemporary Accounting Research***, 34(2), 1178-1209.
21. Cojocaru, I., & Cojocaru, I. (2019). A Bibliometric analysis of Cyber security. Paper presented at Program CEE e|Dem and e|Gov Days 2019, Budapest, Hungary. doi: 10.24989/ocg.v335.12
22. Committee of Sponsoring Organizations of the Treadway. (2019). Managing Cyber Risk in a Digital Age – COSO.
23. Curtis, B. (2022). Creating the Next Generation Cyber security Auditor: Examining the Relationship between It Auditors' Competency, Audit Quality, & Data Breaches (Doctoral dissertation, Capitol Technology University),1.
24. Deelman, E., Stodden, V., Taufer, M., & Welch, V. (2019, June). Initial thoughts on cybersecurity and reproducibility. In Proceedings of the 2nd International Workshop on Practical Reproducible Evaluation of Computer Systems , 13:15.
25. DiStaso, M. W. (2018). Communication Challenges in Cybersecurity. Journal of Communication Technology, 1(1), 43-60.
26. Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and Cybersecurity Risk Management. ***Current Issues in Auditing***, 13(2), 1.

27. Florackis, C., Louca, C., Michaely, R., & Weber, M. (2020). Cybersecurity risk (No. w28196). National Bureau of Economic Research.
28. Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2019). How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. ***Journal of Information Systems***, 33(3), 183-200.
29. Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. ***Managerial Auditing Journal***, 34(7), 808-834.
30. Hamm, K. (2019). Keynote Address Cybersecurity: Where Are We, and What More Can Be Done?. ***The CPA Journal***, 89(8), 34-39.
31. Han, S., Rezaee, Z., Xue, L., & Zhang, J. H. (2016). The association between information technology investments and audit risk. ***Journal of Information Systems***, 30(1), 93-116 .
32. Hartmann, C. C., & Carmenate, J. (2021). Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches: Implications for Practice, Policy, and Research. ***Current Issues in Auditing***, *15*(2), A9-A23.
33. Hasanefendioglu., B., (2018). Cyber security management and control framework with 101 questions . https://technologydevelopmentgroup.net/. 96.
34. IBM Security and Ponemon Institute. (2019). Cost of a Data Breach Report 2019. Available at: https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf.
35. International Federation of Accountants (IFAC). Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment ISA 315 (Revised 2019). A140. P. 107.
36. Islam, M. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function: An international study. ***Managerial Auditing Journal***. 33(4), 377-409.

37. Kahyaoglu, S. B., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. ***Managerial Auditing Journal***.33(4).360-376.

38. Kajüter, P., Klassmann, F., & Nienhaus, M. (2016). Do Reviews by External Auditors Improve the Information Content of Interim Financial Statements?. ***The International Journal of Accounting***, 51(1), 23-50.

39. Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. ***Journal of Financial Economics***.

40. Kelton, A. S., & Pennington, R. R. (2020). Do voluntary disclosures mitigate the cybersecurity breach contagion effect?. ***Journal of Information Systems***, 34(3), 133-157.

41. Lawrence, A., Minutti-Meza, M., & Vyas, D. (2018). Is operational control risk informative of financial reporting deficiencies?. Auditing: ***A Journal of Practice & Theory***, 37(1), 139-165.

42. Lindsay, J., Doutt, A., & Ide, C. (2019). Emerging technologies, risk, and the auditor's focus .

43. Li, B., Li, Y., Pittman, J., & Wang, W. (2022). Auditors' Response to Cybersecurity Risk: Human Capital Investment and Cross-Client Influence. Available at SSRN 4192802.

44. Li, H. (2017). Three essays on cybersecurity-related issues (Doctoral dissertation, Rutgers University-Graduate School-Newark). 12.

45. Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. Auditing: A Journal of Practice, 39(1), 151-171.

46. Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. ***International Journal of Accounting Information Systems***, 30, 40-55.

47. Marotta, A., & Madnick, S. (2020). Analyzing the interplay between regulatory compliance and cybersecurity. Available at SSRN 3542563.
48. Masoud, N., & Al-Utaibi, G. (2022). The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical evidence. ***Research in Economics***, 76(2), 131-140.
49. Mazza, T., & Azzali, S. (2018). Information technology controls quality and audit fees: Evidence from Italy. ***Journal of accounting, auditing & finance***, 33(1), 123-146.
50. Möller D.P.., Haas R.E. (2019) Automotive Cybersecurity. In: Guide to Automotive Connectivity and Cybersecurity. Computer Communications and Networks. Springer, Cham. P.377.
51. Mordor Intelligence. (2020). Cyber security market growth ,trends, forcasts (2020 - 2025). www.mordorintelligence.com/industry-reports/cyber-security-market .
52. Moreira, G. P. (2019). Cyber security and external audit: the disclosure of risk factors in annual reports (Doctoral dissertation).
53. National Initiative for Cybersecurity Careers and Studies (NICCS). 2017. A glossary of common cybersecurity terminology.
54. Nick Eubanks, "The True Cost Of Cybercrime For Businesses," Forbes (Jul. 13, 2017), ww.forbes.com/sites/theyec/2017/07/13/the-true-cost-ofcybercrime- for-businesses/#6c0453c44947.
55. No, W. G., & Vasarhelyi, M. A. (2017). Cybersecurity and continuous assurance. Journal of Emerging Technologies in Accounting, 14(1), 1-12.
56. Pande, J. (2017). Introduction to Cyber Security. Technology, 7(1), 11-26.
57. Perols, R. R. (2019). Two essays on the impact of cybersecurity risk management examinations on investor perceptions and decisions .
58. Pricewaterhousecoopers.(PwC). (2020). Managing the impact ofCOVID-19 on cyber security.
59. Pricewaterhousecoopers.(PwC).. 2017. The US supplement to PwC's annual Global CEO Survey. 20th CEO Survey.

60. Public Company Accounting Oversight Board – PCAOB (2010) Auditing Standard No. 12, Identifying and Assessing Risks of Material Misstatement, Appendix B, Paragraph 4 for additional IT con- siderations.
61. Public Company Accounting Oversight Board – PCAOB (2013). Considerations for Audits of Internal Control over Financial Reporting: Public Company Accounting Oversight Board (PCAOB).
62. Public Company Accounting Oversight Board – PCAOB (2018). Standing Advisory Group Meeting – Panel Discussion – Cybersecurity: Public Company Accounting Oversight Board (PCAOB).
63. Public Company Accounting Oversight Board (PCAOB). (2007). An Audit of Internal Control Over Financial reporting That Is Integrated with An Audit of Financial Statements", Auditing Standard No. 5, Washington, DC, Government Printing Office,. http://pcaobus.orgl.
64. Public Company Accounting Oversight Board. (2014). Standing advisory group meeting: cybersecurity.
65. Public Company Accounting Oversight Board. (2015). Staff inspection brief.
66. Rosati, P., Gogolin, F., & Lynn, T. (2019). Audit Firm Assessments of Cyber-Security Risk: Evidence from Audit Fees and SEC Comment Letters. The International Journal of Accounting, 54(3).
67. Rosati, P., Gogolin, F., & Lynn, T. (2020). Cyber-Security Incidents and Audit Quality. ***European Accounting Review***, 1-28.
68. Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-security incidents and audit quality. ***European Accounting Review***, 31(3), 701-728.
69. Securities and Exchange Commission (SEC) (2018), “Commission statement and guidance on public company cybersecurity disclosures”.4.
70. Securities and Exchanges Commission – SEC (2011). CF Disclosure Guidance: Topic No. 2

71. Securities and Exchanges Commission – SEC (2014). SEC to Hold Cybersecurity Roundtable
72. Securities and Exchanges Commission – SEC (2015). OCIE's 2015 Cybersecurity Examination Initiative: Securities and Exchanges Commission (SEC).
73. Securities and Exchanges Commission – SEC (2018). Commission Statement and Guidance on Public Company Cybersecurity Disclosures.
74. Shaikh, F. A., & Siponen, M. (2022). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. ***Computers & Security***, 124, 102974.
75. Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44, 100548.
76. Smith, T. J., Higgs, J. L., & Pinsker, R. E. (2019). Do auditors price breach risk in their audit fees?. ***Journal of Information Systems***, *33*(2), 177-204.
77. Sonic Wall,(2022). SonicWall Cyber Threat Report, 2022, https://www.infopoint-security.de/media/2022-sonicwall-cyber-threat-report.pdf .
78. Staff of the Auditing and Assurance Standards Board (AUASB). AUASB Bulletin The Consideration of Cyber Security Risks in an Audit of a Financial Report.
79. Sylvia Tsen. (2019). Cybercrime Threatens Trust in Business – How Accountants Can Help. (IFAC).
80. Tarek, M., Mohamed, E. K., Hussain, M. M., & Basuony, M. A. (2017). The implication of information technology on the audit profession in developing country: Extent of use and perceived importance. ***International Journal of Accounting & Information Management.***25(2),237-255.

81. The Institute of Internal Auditors (IIA) (2015), "Common Body of Knowledge (CBOK) Resource Exchange", avaialble at: https://global.theiia.org/iiarf/pages/common-body-of-knowledge-cbok.aspx .
82. The Institute of Internal Auditors (IIA). (2022). Cybersecurity in 2022 Part 2: Critical Partners — Internal Audit and the CISO GLOBAL KNOWLEDGE BRIEF. The Institute of Internal Auditors ،Inc .
83. The Institute of Internal Auditors. (2022). Cybersecurity in 2022 Part 1: How the new SEC proposals could change the game GLOBAL KNOWLEDGE BRIEF. The Institute of Internal Auditors, Inc .
84. Tosun, O. K. (2021). Cyber-attacks and stock market activity. ***International Review of Financial Analysis***, *76*, 101795.
85. Ursillo, S., & Arnold, C. (2019). Cybersecurity Is Critical for All Organizations–Large and Small. ***International Federation of Accountants.***
86. Van .M.,(2016).CYBER SECURITY: A PARADIGM SHIFT IN IT AUDITING How to Deal with Cyber Security Risks in the Financial Statement Audit. https://www.compact.nl/en/compact_authors/m-van-veen-msc-re-cisa-cissp-crisc/
87. World Economic Forum(WEF). 2020. The Global Risks Report 2020. Available at: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf. (accessed 3 /2/ 2021).
88. Yang, L., Lau, L., & Gan, H. (2020). Investors' perceptions of the cybersecurity risk management reporting framework. ***International Journal of Accounting & Information Management***.

ملحق رقم (١)

شركات العينة ومكاتب المراجعة المرتبطة بها

م	اسم الشركة	مكتب المراجع
١)	البنك التجاري الدولي (مصر)	▪ Deloitte - صالح وبرسوم وعبد العزيز ▪ PwC
٢)	البنك المصري لتنمية الصادرات	▪ الجهاز المركزي للمحاسبات ▪ مزارز مصطفى شوقي وشركاءه
٣)	بنك البركة مصر	▪ خالد وشركاه ▪ PwC
٤)	بنك التعمير والاسكان	▪ المتضامنون للمحاسبة والمراجعة ▪ الجهاز المركزي للمحاسبات
٥)	بنك القاهرة	▪ خالد وشركاه
٦)	بنك فيصل الاسلامي المصرية بالجنية	▪ حازم حسن- KPMG ▪ خالد وشركاه
٧)	بنك قطر الوطني الاهلي	▪ حازم حسن - KPMG ▪ خالد وشركاه
٨)	بنك قناة السويس شركة مساهمة مصرية	▪ حازم حسن - KPMG ▪ خالد وشركاه
٩)	بنك كريدي اجريكول مصر	▪ المتضامنون للمحاسبة والمراجعة ▪ مزارز مصطفى شوقي وشركاءه
١٠)	مصرف أبو ظبي الإسلامي- مصر	▪ مزارز مصطفى شوقي وشركاءه ▪ PwC
١١)	راية لخدمات مراكز الاتصالات	▪ محمد أحمد أبو القاسم
١٢)	المصرية للاتصالات	▪ حازم حسن - KPMG
١٣)	اوراسكوم للاستثمار القابضة	▪ حازم حسن - KPMG
١٤)	اي فاينانس للاستثمارات المالية والرقمية	▪ حازم حسن - KPMG
١٥)	فوري لتكنولوجيا البنوك والمدفوعات الالكترونية	▪ Deloitte - صالح وبرسوم وعبد العزيز

A Proposed Procedural Approach to Measure the Extent of The External Auditor's Response to Cyber Risks in The Client's Company: An Applied Guide

Dr. Heba Gamal Hashim Ali

Abstract

The study aimed to reach a proposed procedural approach to measure the extent of the external auditor's response to cyber risks in the client's company in the Egyptian environment, and the theoretical study dealt with the implications of cyber security risks on the work of the external auditor and the steps of the proposed approach. Where the methodology of the applied study relied on joint stock companies listed on the Egyptian Stock Exchange and operating in sectors and activities related to modern technologies in information systems and technology. number of companies in the study community was (20) companies, and the study found that the assessment of cyber security risks depends on the audit processes that study and evaluate a set of pre-defined controls in a variety of topics related to cyber security, The results also showed that there is a significant direct effect of the risks of cyber security attacks in the client's company on the work of the external auditor, and the existence of a significant direct correlation between the management of the disclosure of cyber security risks and the proposed procedural approach.