أثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارات المستثمرين

(دراسة تجريبية)

بحث مُستَل من رسالة دكتوراه في المحاسبة

إعداد

أ.يارا محمود يونس محمود
باحثة دكتوراه في المحاسبة
كلية التجارة، جامعة المنصورة
yarayounis2024@gmail.com

د. سماح طارق حافظ
أستاذ المحاسبة
كلية التجارة، جامعة المنصورة
sthafez2011@mans.edu.eg

د. إبراهيم السيد الجوهري
استاذ مساعد المحاسبة
كلية التجارة، جامعة المنصورة
ibrahim_elgohary@mans.edu.eg

المجلة العلمية للدراسات والبحوث المالية والتجارية

كلية التجارة – جامعة دمياط

المجلد السادس - العدد الأول – الجزء الثاني - يناير ٢٠٢٥

التوثيق المقترح وفقاً لنظام APA:

محمود، يارا محمود يونس، **حافظ**، سماح طارق؛ **الجوهري**، إبراهيم السيد (٢٠٢٥). أثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارات المستثمرين: دراسة تجريبية، **المجلة العلمية للدراسات والبحوث المالية والتجارية**، كلية التجارة، جامعة دمياط، ٦(١) ج٢، ٨٢٧-٨٦٠.

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

أثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارات المستثمرين

(دراسة تجريبية)

أ.يارا محمود يونس محمود؛ د. سماح طارق حافظ؛ د. إبراهيم السيد الجوهري

الملخص:

هدف البحث: دراسة أثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارات المستثمرين.

التصميم والمنهجية : تحقيقاً لأهداف الدراسة، ومن أجل اختبار الفروض اعتمدت الدراسة على الدراسة التجريبية، وتمثل مجتمع الدراسة في المستثمرين وشكلت عينة الدراسة (٧٥) مفردة صحيحة.

نتائج البحث : توصل إلى أهمية توكيد المراجع الخارجي عن مخاطر الأمن السيبراني . كما توصل الى أهمية الإفصاح عن مخاطر الأمن السيبراني في الشركة وأهمية قيام الإدارة بالتقييم الذاتي لنظام إدارة مخاطر الأمن السيبراني لتحديد ما إذا كان هناك أوجه ضعف جوهرية في هذا النظام واتخاذ ما يلزم من إجراءات للتغلب على أوجه الضعف في برنامج إدارة مخاطر الأمن السيبراني. وتوصلت نتائج الدراسة التجريبية الى وجود تأثير لتوكيد المراجع الخارجي عن مخاطر الأمن السيبراني معنوياً على قرارات المستثمرين.

توصيات البحث : ضرورة اهتمام الهيئة العامة للرقابة المالية بتوجيه وزيادة وعي الشركات بأهمية الإفصاح عن مخاطر الأمن السيبراني في التقارير السنوية للشركات عن طريق إصدار المعايير الإرشادية التي تنظم عملية إعداد وعرض تقرير مخاطر الأمن السيبراني والاستفادة من تجارب الدول الأخرى في هذا الشأن. كما يجب على الهيئة العامة للرقابة المالية وصانعي السياسات النظر فيما إذا كان ينبغي حث الشركات على المزيد من الإفصاحات المتعلقة بالأمن السيبراني وفرض عقوبات علنية وصارمة على الشركات لعدم التزامها بالإفصاح عن تعرضها لإختراقات الأمن السيبراني ، واتخاذ إجراءات تنظيمية لتعزيز الإفصاح في الوقت المناسب عن الاختراقات السيبرانية.

الكلمات المفتاحية

الأمن السيبراني ، مخاطر الأمن السيبراني، خدمات توكيد المراجع الخارجي، قرارات المستثمرين.

١- المقدمة:

يعتمد العالم بأسره تقريبا الآن على الإنترنت وأنظمة الكمبيوتر في إدارة جميع جوانب الحياة اليومية، وحوالى ٦٠% من سكان العالم هم من مستخدمي الإنترنت. ويتزايد التبني العالمي للتكنولوجيا الرقمية بسرعة كبيرة. وفي الوقت الحاضر، معظم الأنشطة الاقتصادية، التجارية الثقافية والأنشطة الحكومية، كذلك التفاعلات بين البلدان على جميع المستويات، بما في ذلك الأفراد المؤسسات الحكومية والمؤسسات غير الحكومية، والمنشآت تتم في الفضاء السيبراني. الأنظمة والبنية التحتية الحيوية والحساسة إما جزء من الفضاء السيبراني أو يتم إدارتها، التحكم فيها، واستغلالها من خلال الفضاء السيبراني، معظم المعلومات السرية والحساسة يتم نقلها أو تشكيلها بشكل أساسي في الفضاء السيبراني، كذلك معظم عمليات التبادل المالي تتم في هذا الفضاء (Li & Liu, 2021).

ومع تزايد الإعتماد على المعاملات الإلكترونية وقواعد البيانات الرقمية والإتصالات الإلكترونية، وأيضاً التبني الواسع للتقنيات الرقمية الحديثة (مثل تطبيقات إنترنت الأشياء الحوسبة السحابية)، أصبحت تواجه شركات الأعمال مجموعة من المخاطر الحديثة بما في ذلك "جرائم الأمن السيبراني والتي ربما تعتبر أهم تحدي يواجه بيئة الأعمال في الوقت الحالي. ويتم تعريف جرائم الأمن السيبراني بعدة طرق ولكن بشكل أساسي، تعتبر أي جريمة يمكن إرتكابها أو تمكينها من خلال إستخدام التقنيات الرقمية. وتتضمن هذه التقنيات أجهزة الكمبيوتر الشخصية، أجهزة الكمبيوتر المحمولة، الهواتف والأجهزة الذكية (مثل الكاميرات المتصلة بالإنترنت والمساعدات الصوتية)، ويتسع هذا النطاق ليشمل الأنظمة والبنية التحتية الذكية مثل المنازل المكاتب والمباني التي يقودها إنترنت الأشياء. وتؤثر اختراقات الأمن السيبراني على الشركات بطرق عديدة، على سبيل المثال، قد تؤثر على أداء الشركات بما في ذلك انخفاض المبيعات والأرباح، أو والحاق الضرر بسمعة الشركة ويعتبر هذا من أخطر النتائج لإختراقات الأمن السيبراني؛ لأن فقدان الصورة الجيدة للمنشأة والإضرار بسمعتها، قد يؤدي إلى فقدان ثقة العملاء، وبالتالي، خسارة الأرباح مما قد يفقد الشركة قدرتها على الاستمرار (Roskot et al., 2021). وعلى الرغم من هذا، لا تولي الشركات إهتماماً كافياً فيما يتعلق بمخاطر الأمن السيبراني، وتعتقد أنها لن تتعرض إلى هجوم سيبراني أو في حالة حدوث ذلك ستتمكن من المواجهة. لذا، يعتبر نقص المعرفة لدى الشركات فيما يتعلق بمخاطر الأمن السيبراني، من الأسباب الرئيسية التي تجعل الشركات أكثر تعرضاً لجرائم الأمن السيبراني مثل الهندسة الاجتماعية أو القرصنة (Smith et al., 2019; Singh,2024).

ولذلك تعتبر مخاطر الأمن السيبراني مشكلة معقدة؛ وذلك لأنها قد تتداخل مع مخاطر أعمال الشركة الأخرى مثل مخاطر السمعة ، والمخاطر التشغيلية، وأيضاً مع قضايا التكنولوجيا. وقد تم التعامل مع مخاطر الأمن السيبراني لفترات طويلة جداً على أنها مشكلة تقنية وأن إدارة تكنولوجيا المعلومات في المنشأة هي الإدارة الوحيدة المسئولة عنه ولكن، في ظل بيئة العمل الحالية ومعدل التغير السريع لإختراقات الأمن السيبراني، أصبحت مخاطر الأمن السيبراني تمثل تهديد رئيسي لإستمرار شركات الأعمال، وتتسبب في تحمل الشركات لتكاليف عالية وذلك عند تعرضها للإختراق(Elnagar et al.,2024). على سبيل المثال، تعرضت بعض البنوك في سلطنة عمان وفي الإمارات العربية المتحدة، لخسائر تجاوزت ٤٥ مليون دولار أمريكي، وذلك بسبب سرقة بعض أجهزة الصراف الآلي الإلكتروني، وأيضاً تعتبر المملكة العربية السعودية من أكثر الدول التي عانت من الهجمات السيبرانية ، حيث يعتبر الهجوم على شركة

أرامكو السعودية النفطية في عام ٢٠١٢ ، واحد من أسوأ الأزمات التي حدثت في المملكة العربية السعودية؛ حيث تسبب هذا الهجوم في تدمير ٣٠ ألف جهاز كمبيوتر. لذلك، من المتوقع أن يصل سوق الأمن السيبراني في المملكة العربية السعودية إلى ٥.٧ مليار دولار أمريكي فى عام ٢٠٢٣ وذلك بدلاً من ٢٠٩ مليار دولار أمريكي في عام ٢٠١٩ (سالم، ٢٠٢٣؛ عيسى، محمد، ٢٠٢٢؛Alharbi et al., 2021)

و يعتبر الهدف الرئيسي لمراجعة القوائم المالية هو إعطاء المراجع الخارجي القدرة على إبداء رأيه فيما يتعلق بالقوائم المالية، ولتحقيق هذا ، يجب على المراجع أن يقوم بتخطيط وأداء عملية المراجعة وذلك من أجل الوصول إلى درجة التأكد المناسبة حول ما إذا كانت القوائم المالية ككل خالية من التحريفات الهامة والمؤثرة (الجوهرية) سواء كان ذلك بسبب غش أو خطأ. وللوصول إلى درجة التأكد المناسبة، يجب أن يحصل المراجع على ما يكفي من أدلة المراجعة الملائمة وذلك لتخفيض مخاطر المراجعة إلى مستوى منخفض نسبياً والحصول على درجة توكيد معقولة. ومع تعرض الشركات إلى اختراقات الأمن السيبراني التي تمثل تهديداً حقيقياً لمعظمهم، فقد أظهرت العديد من الدراسات أن هذا يضع المزيد من الضغط على المراجعيين الخارجيين وذلك بسبب زيادة مخاطر التوكيد (Smith et al.,2018; Rosati et al., 2019; Li et al., 2020; Sapiri,2024).

٢ـ مشكلة البحث :

أصبح الآن الأمن السيبراني قضية حيوية لكل مؤسسة، وذلك نظراً لانتشار استخدام المؤسسات التكنولوجيا المعلومات. إذ تعتمد العديد من الصناعات على الانترنت بما في ذلك الاتصالات السلكية واللاسلكية والخدمات المصرفية والمالية والطاقة والنقل وغيرها من الخدمات الحكومية الاساسية. كما أن القطاعين العام والخاص أصبحوا اكثر اعتماداً على التقنيات والشبكات القائمة على الويب في انظمة الإدارة المالية الخاصة بها (Haris et al., 2023) ونتيجة لذلك قد تتعرض الشركات للمخاطر والاختراقات السيبرانية أثناء المسار الطبيعي لأعمال الشركة (Sheneman , 2017; Harris et al., 2023) إذ في السنوات الأخيرة ارتفعت كمية وشدة اختراقات الأمن السيراني مثل (١) اختراق ٢ Equifax في يوليو ٢٠١٧ للمعلومات الشخصية ١٤٥ مليون فرد (٢) هجوم برنامج الفدية wannacry في مايو ٢٠١٧ عبر ١٥٠ دولة والذي أدى إلى إغلاق أكثر من ٣٠٠ الف جهاز (٣) اختراق capital one في يوليو ٢٠١٩ والذي أثر على بيانات ١٠٦ مليون عميل (٤) هجوم برامج الفدية في عام ٢٠٢١ والذي أثر على حزمة برمجيات طورتها شركة kasya وهي شركة أمريكية لتكنولوجيا المعلومات موزعة على ٨٠٠ إلى ١٥٠٠ شركة على مستوى العالم (مطر، علي، ٢٠٢٤؛Harris et al., 2023).

وتنشأ اختراقات الأمن السيبراني نتيجة فشل الشركات في حماية معلومات الملكية الخاصة بالعملاء والموظفين والموردين والمستثمرين الآخرين. إذ تعتبر تلك المعلومات أصولاً غير ملموسة تسجل خارج الميزانية العمومية (مثل علاقات العملاء)، كما تعد تلك المعلومات ضرورية لأداء الشركة في المستقبل (Sheneman ,2017;Sheneman, 2022 ; Kaplan and Demek,2023) وتكون الشركات أكثر عرضة للهجمات السيبرانية عندما تكون كبيرة الحجم، واقل عرضه للقيود المالية، وأكثر قيمة، وعاملة في صناعات اقل قدرة على المنافسة ولديها المزيد من الأصول غير الملموسة (Kamiya et al., 2021; Harris et al., 2023).

كما تؤدي اختراقات الأمن السيبراني إلى العديد من الآثار السلبية مثل خسائر في سمعة الشركة، وخسائر في ثروة المساهمين، وانخفاض فرص النمو المستقبلية للشركة، وانخفاض اسعار أسهم الشركات النظيرة في الصناعة (Havakhor et al., 2020; Kamiya et al., 2021; Sheneman, 2022; Harris et al,2023)، وإلحاق الضرر بالعملاء (إذ يؤدي إلى تعريض العملاء لخسائر في الخصوصية والتي يمكن أن تتراوح من الازعاج مثل تغيير كلمة المرور إلى الاحتيال مثل استخدام بيانات العملاء لارتكاب عمليات الاحتيال) (Demek and Kaplan, 2023)، وارتفاع تكلفة التمويل (Sheneman, 2017; Sheneman, 2022 ، وارتفاع تكليف التقاضي والغرامات، والتأثير السلبي على بقاء واستمرارية الشركات، وفقدان الملكية الفكرية، وانخفاض قيمة العلامة التجارية، وفقدان العلاقات مع العملاء(Sheneman,2022; Demek and Kaplan, 2023; Sheneman,2017) . لذا، يعتبر الأمن السيبراني من الوسائل الحديثة التي تستخدم في حماية المعلومات المربوطة بشبكة الإنترنت وتكنولوجيا المعلومات، حيث يحافظ على المعلومات من أي سرقة أو دخول غير مصرح على الأنظمة التي تخص منظمات الأعمال (السرحان ،٢٠٢٠; Singh,2024).

وعلى الرغم من صعوبة جمع البيانات التفصيلية، فإن تكلفة الخروقات الأمنية والقرصنة للشركات كانت مذهلة، وفقا لتقرير دراسة تكلفة انتهاك وخرق البيانات الصادر عن معهد بونيمون IBM Security and the Ponemon Institute، فقد وصلت التكلفة إلى ٤,٢٤ مليون دولار لكل حادثة في عام ٢٠٢١، وهي الأعلى منذ ١٧ عاما، وكان متوسط تكلفة اختراق البيانات في عام ٢٠٢٠ هو ٣,٨٦ مليون دولار، ويظهر التقرير انخفاضا بنسبة ١٥٪ في التكاليف عن عام ٢٠١٩ والتي بلغت ٣,٩٢ مليون دولار (IBM Corporation ,2021) وهو ما يمثل مصدر قلق كبير للهيئات التنظيمية بقدر ما هو مصدر قلق للشركات.

كما تؤكد "Ginni Rommetty" (المدير والرئيس التنفيذي الحالي لشركة أي بي إم) على أن اختراقات الأمن السيبراني، تمثل التهديد الأعظم حالياً لأي منشأة في العالم لذلك، يتعين على جميع المنشأت الاستعداد وتجهيز بيئاتها الداخلية لذلك، ومحاولة منع الهجمات الإلكترونية التي قد تؤدي إلى إختراق بياناتها، خاصة السرية منها. وعادة ما تكون اختراقات الأمن السيبراني إشارة على ضعف هيكل الرقابة الداخلية المطبق والموجود في الشركة (Benaroch & Chernobai, 2017)، وذلك يتطلب من المراجع المزيد من الدقة عند التخطيط لعملية المراجعة نتيجة لإحتمالية زيادة المخاطر وبالتالي، بذل المراجع المزيد من الجهد وكذلك الاختبارات للتأكد من أن هيكل الرقابة الداخلية على التقارير المالية لم يتم المساس به (Calderon & Gao, 2020).

وفي نفس السياق أوضحت Kathleen Hamm، وهي خبيرة في التكنولوجيا المالية والأمن السيبراني وعضو سابق في مجلس المراقبة على حسابات الشركات العامة ((PCAOP) أنه إذا قام المراجع بتحديد مخاطر مرتبطة بالأمن السيبراني للعميل والتي من الممكن أن يكون لها تأثير جوهري على القوائم المالية الخاصة بالشركة، يجب عليه تصميم وتنفيذ الإجراءات لتحديد تلك المخاطر، ثم أوضحت بعد ذلك أنه سواء قد وقع حادث أم لا أثناء التخطيط لعملية المراجعة، يجب على المراجع إجراء تقييم للمخاطر ويجب أن يأخذ هذا التقييم في عين الاعتبار أي مخاطر للأمن السيبراني، والتي من الممكن أن يكون لها تأثير جوهري على القوائم المالية الخاصة بالشركة (Hamm, 2019) .

ومع تزايد عدد مخاطر الأمن السيبراني كل عام، قد يأتي هنا السؤال فيما يتعلق بالدور الذي سوف يقوم به المراجع الخارجي عند مراجعة الشركات التي تعرضت بالفعل لمخاطر الأمن السيبراني، حيث قد تعتبر مخاطر الأمن السيبراني مؤشر على وجود ضعف في هيكل الرقابة الداخلية للشركة، لذا أصبح على المراجع الخارجي عند تعرض شركة عميل المراجعة لمخاطر الأمن السيبراني أن يلتزم بمزيد من الدقة عند التخطيط لعملية المراجعة وكذلك بذل المزيد من الجهد والاختبارات لتخفيض مخاطر المراجعة والحصول على درجة توكيد معقولة.

وفي ضـــوء ماســـبق تظهر المشـــكلة البحثية : وماهو دور المراجع فى التوكيد عن مخاطر الأمن السيبراني ؟ وما هو أثر هذا التوكيد على قرارات المستثمرين ؟.

٣- هدف البحث:

في ضوء مشكلة الدراسة يمكن للباحث صياغة هدف الدراسة كتالي:

دراسة تأثير توكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارات المستثمرين.

٤- أهمية البحث:

أ.الأهمية العلمية: تتمثل الأهمية العلمية في اتجاه مصر للاهتمام بالأمن السيبراني، حيث تم وضع الإستراتيجية الوطنية للأمن السيبراني في مصر (٢٠٢٣- ٢٠٢٧)، والذي يستهدف تطوير وصياغة رؤية مصر لتعظيم الاستفادة من إمكانيات مصر ومميزاتها التنافسية، ولذلك تظهر الحاجة إلى إلقاء الضوء على إفصاح الشركات، وكيفية توكيد المراجع عن مخاطر الأمن السيبراني ممكن ينعكس إيجابياً على قرار المستثمر ، بالإضافة إلي ندرة البحوث - في حدود علمنا - التي تناولت أثر أثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارات المستثمرين.

أ. **ب. الأهمية العملية:** تكمن أهمية الدراسة في تناولها موضوعا حيوياً، حديث المفهوم ومتكامل وذلك بقصد باستخدام أثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارات المستثمرين ، والبحث عن دليل تجريبي في بيئة الأعمال والممارسة المهنية المصرية، كما قد تساهم الدراسة في زيادة إدراك القائمين على البورصة المصرية، والجهات الرقابية، لمدى احتياج المستثمرين بشكل عام لخدمة التوكيد عن مخاطر الأمن السيبراني، وبالتالي جعلها إحدى متطلبات الشركات المقيدة بالبورصة المصرية كخطوة أولى، ومن ثم جعلها إلزامية على الشركات المقيدة بالبورصة المصرية.

٥- منهج البحث:

تستند الدراسة في طبيعتها، وأهميتها، وأهدافها، واختبار فروضها إلى استخدام مناهج متعددة للوفاء بأغراضها، **ولذلك سوف تعتمد الدراسة على المنهج الاستقرائي** للمساعدة على توضيح مشكلة وأهمية الدراسة من خلال الاستناد إلى الدراسات السابقة العربية والأجنبية المتنوعة، والتي تناولت موضوع الدراسة، فضلاً عن معرفة الإطار النظري للموضوع، والنقاط الرئيسية له، وبالتالي صياغة فروض الدراسة القابلة للاختبار العلمي، و**المنهج الاستنباطي** لربط الإطار النظري للبحث بالواقع العملي، وذلك من خلال اختبار فروض الدراسة، وتحليل وتفسير النتائج للوصول إلى تحقيق أهداف الدراسة، و**المنهج التجريبي** من أجل التحليل والاستنتاج استنادا إلى البيانات التي يقوم الباحثين بالحصول عليها من خلال

إجراء تجربة على فئات مختلفة من المشاركين. وتقوم الدراسة التجريبية على مجموعة من الحالات الافتراضية، مع تدعيم تلك الحالات بمجموعة من الأسئلة الاستقصائية لتجميع البيانات اللازمة، والتي سيتم تحليلها إحصائيا لاختبار فروض الدراسة.

٦- حدود ومجال البحث:

وفقا لأهداف الدراسة ومشكلتها، فإن حدود ومجال الدراسة هي:

- تقتصر الدراسة على توكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارات المستثمرين.
- يقتصر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارات المستثمرين بإجراء دراسة تجريبية على عينة من المحللين الماليين والمستثمرين بالأسهم.
- يخرج عن نطاقه التوكيد الداخلي بمعرفة المراجع الداخلي عن مخاطر الأمن السيبراني على قرارات المستثمرين.

٧- خطة البحث

٧-١ الدراسات السابقة واشتقاق الفروض.
٧-٢ مفهوم الأمن السيبراني وأنواعه و مخاطر اختراقات الأمن السيبراني.
٧-٣ مفهوم توكيد المراجع الخرجي عن مخاطر الأمن السيبراني وأطرافه وأهم الإصدارات المهنية.
٧-٤ مفهوم قرارات المستثمرين وأنواع القرارات.
٧-٥ الدراسة التجريبية.

٧-١ الدراسات السابقة واشتقاق الفروض:

تشتمل الدراسات السابقة في هذا البحث على دراسات متعلقة بتوكيد المراجع الخارجي عن مخاطر الأمن السيبراني و قرارات المستثمرين.:

استهدفت دراسة (Navarro and Sutton, 2019) تأثير التوكيد الاختياري لإدارة مخاطر الأمن السيبراني على قرارات المستثمرين غير المحترفين. كما تناولت الدراسة أيضًا كيفية تغيير أهمية التوكيد الاختياري لإدارة مخاطر الأمن السيبراني عندما يكون الحصول على هذا التوكيد متوقعًا أو غير متوقع. و تناولت هذه الدراسة ما إذا كان هناك طلب على التوكيد الذي تقدمه شركات المراجعة، لا سيما في ضوء المخاوف المستمرة في البحث والممارسة فيما يتعلق بجدوى خدمات التوكيد المتعلقة بتكنولوجيا المعلومات. ولتحقيق هدف الدراسة تم إستخدام تجربة ٣ × ٢ بإستخدام عينة من المشاركين الذين يمثلون المستثمرين غير المحترفين وبلغ عدد العينة ٢٤٣ فردًا من (Amazon Mechanical Turk (MTurk لإكمال الحالة التجريبية من أجل مراقبة سلوك القرار.

وتوصلت الدراسة أنه بعد حدوث اختراق للأمن السيبراني، تحصل الشركات التي قدمت سابقًا توكيد اختياري لإدارة مخاطر الأمن السيبراني على تقييمات أكثر إيجابية من المستثمرين لمصداقية الإدارة، وبالتالي، تقييمات أعلى للأسهم. وتوصلت الدراسة أيضاً أن الإدارة ومجالس الإدارة بحاجة إلى إدراك أن مخاطر الأمن السيبراني ستختلف باختلاف الصناعة وأن المستثمرين سيهتمون بإنتهاكات معايير الصناعة لإدارة مخاطر الأمن السيبراني. وتوضح النتائج أيضًا أهمية الحصول على توكيد مسبق لإدارة مخاطر الأمن السيبراني لتحديد مصداقية الإدارة بعد حدوث اختراق أمن سيبراني؛ و تعد السمعة والسيطرة على الضرر من الاختراق أمرًا مهمًا لكل من الإدارة والشركة.

استهدفت دراسة (Badawy,2021) تحليل تأثير جودة التوكيد (مقاسا بحجم شركة مراجعة الحسابات التي تقوم بهذا التوكيد. مراجعين Big4 مقابل (non Big4) ومستوى التوكيد (توكيد معقول مقابل توكيد محدود) على برنامج إدارة مخاطر الأمن السيبراني على استعداد المستثمرين غير المحترفين للاستثمار وتقييم أسهمهم، ولتحقيق هدف الدراسة تم تصميم تجربة ٢×٢ بإستخدام عينة من ٦٤ طالب ماجستير في إدارة الأعمال وطلاب دراسات عليا في كلية التجارة وجامعة الإسكندرية وجامعة ESLSCA لاختبار فرضيات الدراسة.

وتوصلت الدراسة إلى وجود دليلا على أن جودة التوكيد العالية (Big4 auditor) ومستوى التوكيد المعقول في تقرير التوكيد على برنامج إدارة مخاطر الأمن السيبراني لهما تأثير كبير وإيجابي على رغبة المستثمرين في الاستثمار وتقييم أسهمهم ومع ذلك لم تجد الدراسة فرقا كبيرا في رغبة المستثمرين في الاستثمار أو تقييم أسهمهم في حالة تقديم تقرير توكيد محدود من قبل شركة مراجعة Big4 مقارنة بحالة تقرير التوكيد المعقول الذي تقدمه شركة مراجعة غير Big4، وتضيف هذه الدراسة دليلا تجريبيا إلى الدراسات الخاصة بالخدمات غير المراجعة والأمن السيبراني وستساعد في تقليل فجوة البحوث المحاسبية المتعلقة ببرنامج إدارة مخاطر الأمن السيبراني ، وهو ما يتوافق مع جهود الحكومة المصرية واهتمامها بالأمن السيبراني والمخاطر المرتبطة به.

استهدفت دراسة (فرج، ٢٠٢٢) اختبار العلاقة بين توكيد المراجع الخارجي على مزاعم الإدارة عن إدارة مخاطر الأمن السيبراني cyber security 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 المراجع الخارجي على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكتروني إيجابا ومعنويا على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية. وتم استخدام متغيرات معدلة هي؛ مستوى التأهيل العلمي للمستثمر، ومستوى خبرة المستثمر . وكما توصلت الدراسة إلى عدم وجود تأثير معنوي لمتغيري التأهيل والخبرة، كل على حده، على قرار الاستثمار بالأسهم، وكذلك عدم وجود تأثير معنوي لمتغيري التأهيل والخبرة معا على قرار الاستثمار بالأسهم.

استهدفت دراسة (Saleh , 2023) اختبار درجة ثقة المستثمرين غير المحترفين في تأكيدات الإدارة المتعلقة بإجراءات الرقابة الداخلية عن إدارة مخاطر الأمن السيبراني و يمكن أن تتوسط العلاقة بين التوكيد المهني عن إدارة مخاطر الأمن السيبراني وأحكام وقرارات المستثمرين غير المحترفين. ولتحقيق ذلك، تم إجراء دراسة تجريبية بتصميم 2x2x2 بين وداخل المتغيرات باستخدام عينة من ١٤٣ من طلاب ماجستير إدارة الأعمال والدراسات العليا للقيام بدور المستثمرين المصريين غير المحترفين.

وتوصلت الدراسة الى أدلة تدعم أهمية التوكيد المهني المستقل للمراجع الخارجي عن إدارة مخاطر الأمن السيبراني في تعزيز أحكامهم وقراراتهم الاستثمارية. وعلى وجه التحديد، تبين أن تقرير التوكيد المهني المستقل عن إدارة مخاطر الأمن السيبراني يؤثر بشكل إيجابي على أحكام المستثمرين المصريين غير المحترفين بشأن مدى جاذبية الاستثمار في الشركة محل الدراسة والتي تستخدم خدمات الحوسبة السحابية، وكذلك القرار بشأن المبلغ المراد استثماره، ويتوسط هذا التأثير بشكل كامل درجة الموثوقية المدركة لتأكيدات الإدارة المنشورة بالإضافة إلى ذلك، فإن التأثير المباشر للتوكيد المهني المستقل للمراجع الخارجي عن إدارة مخاطر الأمن السيبراني على قرار مبلغ الاستثمار أقوى بالنسبة للمستثمرين الذكور، في حين تلعب المؤهلات التعليمية للمشاركين دورا مهما في التفاعل مع التوكيد المهني المستقل للمراجع الخارجي عن إدارة مخاطر الأمن السيبراني في التأثير على كل من جاذبية الاستثمار وحجمه، ومع ذلك، لا يؤثر متغير الجنس بشكل كبير على العلاقة بين تقرير التوكيد ومدى جاذبية الاستثمار. بشكل عام، تؤكد النتائج، والتي تم تدعيمها بإجراء اختبارات إضافية أخرى، على أهمية التوكيد المهني المستقل الاختياري عن إدارة مخاطر الأمن السيبراني والتي لها تأثيرات عديدة على مختلف أصحاب المصالح والإدارة والمراجعين الخارجيين وصانعي السياسات.

استهدفت دراسة (عثمان،٢٠٢٣) اختبار أثر توكيد المراجع الخارجي على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين في الأسهم، وكذلك اختبار أثر مستوى الخبرة والتأهيل العلمي للمستثمر كمتغيرات وسيطة على العلاقة محل الدراسة، وتم إجراء دراسة تجريبية بإستخدام عينة من ١٠٠ من المستثمرين في بيئة الأعمال المصرية عن عامين ٢٠١٩، ٢٠٢٠، وتم توزيع الحالات التجريبية إلكترونياً على مجتمع الدراسة .

وتوصلت الدراسة إلى وجود علاقة معنوية إيجابية بين التوكيد المهني للمراجع الخارجي على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني ورغبة وقرارات المستثمرين بالأسهم، حيث أصبح الإفصاح عن مخاطر الأمن السيبراني التي تواجهها الشركات ومعرفة كيف تدير الشركات أعمالها على الشبكات وفي الصحابة وما تواجهه من مخاطر أمنية قد تؤدي إلى خسائر مالية ضخمة وفقد السمعة والإضرار بالقدرة التنافسية للشركة ذا أهمية متزايدة للمستثمرين والحكومات والمستهلكين والبائعين وأصحاب المصلحة الآخرين لإصدار قرارات وأحكام سليمة والتأثير على سعر السهم، وقيمة المساهمين في الأجل الطويل، وضرورة التوكيد على إفصاحات وإدارة مخاطر الأمن السيبراني بما يعمل على تعزيز سلامة وموثوقية التقارير المالية ومستوى الشفافية وتقليل مستوى عدم تماثل المعلومات بين المديرين وأصحاب المصلحة بشكل عام وعلى قرارات وأحكام المستثمرين بشكل خاص، وزيادة الثقة والرغبة في الاستثمار في أسهم الشركات. كما توصلت الدراسة لوجود تأثير معنوي لمتغيري الخبرة والتأهيل العلمي

للمستثمر معا على العلاقة بين التوكيد المهني للمراجع الخارجي على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني ورغبة وقرارات المستثمرين بالأسهم، وكذلك وجود تأثير معنوي لخبرة المستثمر على العلاقة بين التوكيد المهني للمراجع الخارجي على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني ورغبة وقرارات المستثمرين بالأسهم، وكذلك عدم وجود تأثير معنوي لمستوى التأهيل العلمي للمستثمر على تلك العلاقة محل الدراسة.

التعليق على الدراسات السابقة واشتقاق فروض الدراسة

ويتضح من تحليل الدراسات السابقة إلى اتفاق بعض الدراسات السابقة **(فرج، ٢٠٢٣ ؛ عثمان،٢٠٢٣؛ Navarro and Sutton, 2019; Badawy,2021; Saleh , 2023)** على وجود علاقة معنوية إيجابية بين توكيد المراجع الخارجي عن مخاطر الأمن السيبراني وقرارات المستثمرين بالأسهم، حيث أن تحصل الشركات التي قدمت سابقًا توكيد اختياري لإدارة مخاطر الأمن السيبراني على تقييمات أكثر إيجابية من المستثمرين لمصداقية الإدارة، وبالتالي، تقييمات أعلى للأسهم، وأن جودة التوكيد العالية (Big4 auditor) ومستوى التوكيد المعقول في تقرير التوكيد على برنامج إدارة مخاطر الأمن السيبراني لهما تأثير كبير وإيجابي على رغبة المستثمرين في الاستثمار وتقييم أسهمهم، وأن تقرير التوكيد المهني المستقل عن إدارة مخاطر الأمن السيبراني يؤثر بشكل إيجابي على أحكام المستثمرين غير المحترفين بشأن مدى جاذبية الاستثمار.

ويخلص البحث؛ في ضوء ما سبق أن توكيد المراجع الخارجي عن مخاطر الأمن السيبراني وقرارات المستثمرين بالأسهم يضفي الثقة والمصداقية وزيادة إمكانية الاعتماد عليها، ويحد من عدم تماثل المعلومات، ويزيد قدرة المستثمرين على تقييم الأداء الحالي والمستقبلي للشركة، وتقدير أسعار الأسهم والأرباح المتوقعة، ومن ثم اتخاذ قرارات استثمارية سليمة، وبالتالي من المتوقع أن يؤثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارات المستثمرين، وعليه يمكن اشتقاق فرض الدراسة الأول كتالي:

الفرض الأول H1: يؤثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني معنوياً على قرارات المستثمرين.

٧-٢- مفهوم الأمن السيبراني وأنواعه و مخاطر اختراقات الأمن السيبراني:

لقد تعددت تعريفات الامن السيبراني كما يلي تعددت مفاهيم الأمن السيبراني

يعرف الأمن السيبراني Cyber Security" بأنه مجموعة من الوسائل التقنية والإدارية التكنولوجية والعمليات والممارسات المصممة التي يتم استخدامها لحماية الشبكات والأجهزة والبرامج والبيانات من الهجمات أو الأضرار أو الوصول غير المصرح به(Li et al ,2018). كما عرفه المعهد القومي للمعايير والتكنولوجيا بأنه عملية(National Institute of Standards and Technology NIST,2018) حماية المعلومات عن طريق منع الهجمات واكتشافها والتصدي لها، وكذلك منع سوء الاستغلال، واستعادة المعلومات الإلكترونية، ونظم الاتصالات والمعلومات التي تحتويها، لضمان توافرها وسلامتها ومصداقيتها وسريتها، وتأمين خصوصية البيانات. وعرفته جمعية المراجعة ومراقبة نظم المعلومات (ISACA,2017) بأنه حماية الأصول المعلوماتية من خلال معالجة التهديدات التي تتعرض لها المعلومات التي تتم معالجتها وتخزينها ونقلها بواسطة أنظمة المعلومات المتداخلة بين الشبكات.

وفي نفس السياق أشارت دراسة (Al-Zyoud, 2020; Badawy ,2021) أن الأمن السيبراني هو مفهوم شامل يشمل أمن المعلومات وضمان المعلومات، فهو يشمل كل التقنيات والعمليات والضوابط المصممة لحماية الأنظمة والشبكات والمعلومات من الهجمات السيبرانية وتقليل أو منع الآثار المالية المرتبطة بها، كما يقلل برنامج الأمن السيبراني الفعال من مخاطر الهجمات والحوادث الإلكترونية ويحمي الجميع من سوء الاستخدام أو الاستخدام غير المصرح به للأنظمة والشبكات والتقنيات ذات الصلة.

وتنشأ مخاطر الأمن السيبراني نتيجة هجمات متعدة أو أحداث غير متعمدة، وتأخذ هذه الهجمات العديد من الأنواع، كما في حالة الوصول غير المصرح به إلى الأنظمة الرقمية لأغراض سرقة الأصول المالية، والفكرية، والشخصية، وغيرها من المعلومات الحساسة الخاصة بالشركات أو عملائها، أو شركاء الأعمال الآخرين، أو إفساد البيانات، أو تعطل أو التوقف عن ممارسة الأعمال، ويمكن أيضاً تنفيذ تلك الهجمات بالاعتماد علي هجمات الحرمان، التي تؤدي إلى رفض الخدمة علي مواقع الويب للشركة، وأيضا قد يتم تنفيذ هذه الهجمات من أفراد من خارج الشركة أو من داخلها، لذا تتعرض الشركات إلى خسائر فادحة عند حدوث مثل هذه الهجمات(Singh,2024 ; Elnagar et al.,2024)

كما أشارت دراسة (Florakis et al., 2020; Elnagar et al.,2024 ; Singh,2024 ; Kamiya et al., 2021) إلى الآثار السلبية لمخاطر الأمن السيبراني علي الشركات حيث تؤدي إلي تلف أو فقد بعض المعلومات المالية للشركات مما تؤثر علي صافي أرباح الشركات، وتؤدي إلى زيادة التكاليف وتخفيض الإيرادات، وبالتالي قد يكون لها تأثير سلبي علي ثروة الملاك وسمعة الشركة واحتمال تعرضها للدعاوى القضائية وقرارات المستثمرين نتيجة التأثير السلبي علي أسعار أسهم الشركات وعلى تقييم أصحاب المصالح على قدرة الشركة على الحفاظ علي أمن المعلومات، كما أنها قد تضر بقدرة الشركة على الابتكار واكتساب العملاء والحفاظ عليهم ، وعلي وضعها التنافسي في السوق. وهو الأمر الذي يشير الي ضرورة قيام الشركات بإدارة مخاطر الأمن السيبراني حتي يمكن تجنب آثارها السلبية.

وفي ضوء ما سبق فإن مخاطر الأمن السيبراني تمثل أحد المخاطر المستحدثة في البيئة العالمية والمحلية وأن الشركات بحاجة إلى الإفصاح عن مخاطر الأمن السيبراني التي تواجهها أو التي يتوقع أن تواجهها لتعزيز الإفصاح والشفافية في تقاريرها السنوية وبما يساهم في ترشيد القرارات الاستثمارية.

وبالنسبة لأنواع الأمن السيبراني أكدت عدة دراسات (Mendhurwa& Mishra , 2021 ; Peslak & Hunsinger, 2019 ; Parker & Brown , 2019) أنه يتكون من ستة أنواع وهي :

- تأمين الشبكات : هي تأمين شبكة الحاسب الآلي من المتطفلين، سواء كانوا مهاجمين مستهدفين أو برامج ضارة انتهازية.
- تأمين التطبيقات : من الممكن أن يوفر التطبيق المخترق الوصول الى البيانات المصممة لحمايتها، ويبدأ الأمان الناجح في مرحلة التصميم، قبل نشر البرنامج أو الجهاز بوقت طويل .
- أمن المعلومات : هي خصوصية البيانات وسلامتها سواء في عملية التخزين أو أثناء النقل.

- الأمن التشغيلي : هي القرارات والعمليات الخاصة بمعالجة أصول البيانات وحمايتها والأذونات التي يمتلكها المستخدمون عند الوصول الى الشبكة والإجراءات التي تحدد كيف وأين يمكن تخزين البيانات أو مشاركتها كلها تندرج تحت هذه المظلة.
- تعزيز تعافي الشركات من الهجمات الالكترونية بأشكالها المختلفة: وهي تحديد التعافي من الكوارث وكيفية استجابة المنظمة لحوادث مخاطر هجمات الأمن السيبراني أو أي حدث آخر يتسبب في فقدان العمليات أو البيانات، وكيفية استعادة الشركة لعملياتها ومعلوماتها للعودة الى نفس القدرة التشغيلية كما كانت قبل الحدث، وبالتالي استمرارية العمل هي الخطة التي عليها الشركة أثناء محاولتها العمل بدون موارد معينة.
- تدريب المستخدم النهائي (الأشخاص) : وهم أكثر عوامل مخاطر هجمات الأمن السيبراني التي لايمكن التنبؤ بها، حيث يمكن لأي شخص إدخال فيروس بطريق الخطأ الى نظام آمن من خلال عدم اتباع ممارسات الأمان الجيدة، وتدريب المستخدمين على حذف المرفقات البريد الالكتروني المشبوهة.

في ضوء تطبيق استراتيجيات التحول الرقمي بالمؤسسات الحكومية وفيما يلي نستعرض أهم مخاطر اختراقات الأمن السيبراني (Conteh & Schmick, 2021 ; Van Wyk, &Fonseca, 2021 ; Alic ,2021).

مخاطر انتهاك الخصوصية: حيث الحفاظ على الخصوصية الشخصية في العالم الرقمي أصبح أكثر صعوبة، مع تزايد مخاطر سرقة البيانات الشخصية أو المساومة عليها .

مخاطر تأمين البيانات والمعلومات: ساعدت التكنولوجيا الرقمية في جمع كميات هائلة من البيانات وتخزينها، والتي من الممكن أن تكون معلومات خاصة تتعلق بالأفراد أو الشركات، ويمكن أن يكون من الصعب جداً الحفاظ على أمان هذه البيانات، ومع خرق واحد يمكن وصول كميات هائلة من المعلومات الخاصة الى أيدي الخصوم أو المنافسين التجاريين، أو الكيانات الأخرى.

مخاطر انتهاك حقوق الملكية الفكرية: أصبح من السهل في ظل عصر الرقمنة نسخ الوسائط الرقمية واعادة انتاجها، كما أنه من الصعوبة تطبيق قوانين حقوق النشر بأي مكان، ونلاحظ أن هناك تأخر على مستوى التشريعات القانونية في هذا الصدد، وبما أن هذه النقلة الرقمية حديثة بعض الشئ فلا يوجد أطر قانونية تحكم مسار عمل هذا العالم الرقمي وتحمي خصوصية الأفراد والشركات وحقوق ملكيتهم الفكرية والأدبية لمنتجاتهم ومؤلفاتهم المختلفة.

مخاطر عدم الكشف عن الهوية : حيث توفر التكنولوجيا الرقمية مجالاً واسعاً للمستخدمين لإخفاء هوياتهم، وتشير الكثير من الدراسات الى أنه يجب أن تكون هناك عواقب صارمة لذلك.

وفي ضوء ما سبق، يتضح لنا أن هناك العديد من مخاطر الأمن السيبراني التي ترتبط بتطبيق استراتيجيات التحول الرقمي وتقف حائل أمام قدرته على تحقيق الأهداف المنشودة، والتي يجب أن تؤخذ في الاعتبار عند تطبيق المؤسسات الحكومية لاستراتيجيات التحول الرقمي، ومن ثم يمكننا التأكيد على ضرورة استخدام الأدوات والأساليب التقنية الحديثة واستغلالها الاستغلال الأمثل ومحاولة تقليل مخاطرها.

٧-٣- مفهوم توكيد المراجع الخارجي عن مخاطر الأمن السيبراني وأطرافه وأهم الإصدارات المهنية:

ولقد عرف المعيار الدولي ISAE ٣٠٠٠ خدمات التوكيد المهني بأنها خدمة مهنية يهدف فيها المراجع الخارجي الى الحصول على ما يكفي من الأدلة المناسبة لإبداء استنتاج يهدف إلى رفع درجة الثقة لدى المستخدمين المستهدفين، بخلاف الطرف المسؤول، حيال معلومات الموضوع (أي مخرجات تقويم أو قياس موضوع ما محل ارتباط مقارنة بالضوابط). وهو نفس التعريف الذي اتفقت عليه معايير التوكيد في العديد من الدول مثل نظيره الاسترالي (ASAE No.3000)، ونظيره الكندي (CSAE . 3000 No) ، ونظيره النيوزيلاندي (ISAE) (NE) No.3000). في حين أن المعايير الأمريكية الخاصة بخدمات التوكيد لم تختلف كثيرا عن التعريف السابق، حيث عرفت خدمة التوكيد المهني بأنه ذلك التكليف الذي يتطلب من المراجع الخارجي إبداء استنتاج بشأن إمكانية الاعتماد على توكيدات (إفصاحات) الإدارة الخاصة بمجال التكليف، وذلك طبقاً لمعايير القياس المناسبة، وأن يكون هذا الاستنتاج في شكل تقرير مكتوب يوجه إلى المستخدمين المستهدفين (Cho et al.,2014 ; Velte and Stawinoga,2020 ; Channuntapipat et al.,2020).

ومن حيث أطراف توكيد الأمن السيبراني يتضمن ثلاثة أطراف كالتالي (IAASB,2013) :

الممارس : وهو مصطلح أوسع من المراجع لأنه قد يطلب منه أداء عمليات تأكيد تتطلب منه مهارات ومعرفة متخصصة تفوق ما هو متعارف عليه فى مراجعة الحسابات كما يمكن للممارس الاستعانة بخبير.

الطرف المسئول : وهو الشخص الذى يكون مسئولا عن موضوع المهمة مباشرة أو عن المعلومات الخاصة به ويقدم الطرف المسئول اقرارا مكتوبا بتقييم او قياس موضوع المهمة بالرجوع الى مقاييس محددة.

المستخدمون : شخص أو مجموعة أشخاص يقوم الممارس بإعداد التقرير لهم(لطفى، ٢٠١٠) ويتمثل الهدف من الخدمة في إبداء مقدم الخدمة إستنتاجا إيجابيا محايدا أو توكيدا معقولا بشأن إفصاح الشركات عن إدارة المخاطر في شكل تقرير مكتوب, حيث يحرص مقدم خدمة التوكيد على توفير توكيد معقول بشأن تخفيض خطر القيام بتلك الخدمة إلى حد مقبول أو محدود في ظل الظروف المحيطة بأداء الخدمة، وكذلك تقييم مدى إكتمال وملاءمة ودرجة الإعتماد على تقارير إدارة الخطر بالنسبة لأصحاب المصالح.

الخدمات بخلاف التوكيد هي الخدمات التي يمكن أن يتم تقديمها عن طريق المراجع الخارجي ولكنها لا تستوفي تعريف خدمات التوكيد (IESBA , 2018 p. 4) ولعل السمة المشتركة للخدمات بخلاف التوكيد هي أن هذه الخدمات مصممة لتوفير المهارات التقنية والتعليم والملاحظات والخبرات والمعرفة وذلك فيما يتعلق بموضوع معين للاستخدام المباشر وتحقيق منفعة للعميل، ونتائج العمل ليست مصممة لتقديم أي مستوى من التوكيد لأطراف خارجية أو للطرف المسئول .(Lessamb ,2018 , p. 83).

ومع تزايد عدد التهديدات الأمنية أصبح من الضرورى تضمين خطة المراجعة للشركة التهديدات الأمنية، وبالتالي على المراجع الخارجي مراجعة عمليات وأدوات وسياسات الأمن السيبراني لتوفير استنتاج حول درجة مصداقية تقارير الإدارة عن مخاطر الأمن السيبراني. ومن الطرق المستخدمة لمراجعة الأمن السيبراني في الشركات :

- مراجعة سياسات أمن البيانات قبل بداية المراجعة من حيث السرية والسلامة والإتاحة.

- تصنيف البيانات وتحديد مستويات الأمان اللازم لحمايتها وتفاصيل هيكل الشبكة.

- تجميع سياسات الأمن السيبراني ومتطلباتها في وثيقة واحدة للحصول على فهم شامل الممارسات أمن تكنولوجيا المعلومات لتحديد نقاط الضعف الموجودة بها.

- مراجعة معايير مخاطر الأمن السيبراني للشركة (معايير الوصف).

- إنشاء قائمة بأفراد الأمن السيبراني ومسئولياتهم.

وبشأن أهم الإصدارات والإرشادات المهنية لأداء خدمات التوكيد الأخرى :

المعيار الدولي ISAE ٣٠٠٠ عمليات التوكيد الأخرى بخلاف عمليات مراجعة أو فحص المعلومات المالية التاريخية :

نظراً للاهتمام العالمي الكبير حالياً بالمستوى العالي من الجودة وما يرتبط به من توكيد بشأن المعلومات بخلاف مراجعة أو فحص البيانات المالية، أصدر المجلس الدولي لمعايير المراجعة والتوكيد معياراً دولياً محدثاً بشأن عمليات التوكيد يطلق عليه (ISAE ٣٠٠٠ معدل) بعنوان: عمليات التوكيد الأخرى بخلاف عمليات مراجعة أو فحص المعلومات المالية التاريخية، والذي يغطي مجموعة واسعة من خدمات التوكيد.

وتشمل خدمات التوكيد وفقاً للمعيار ISAE ٣٠٠٠ كل من (IAASB, 2013): خدمات التوكيد وهي تلك التي يقوم فيها طرف آخر بخلاف المراجع الخارجي بقياس أو تقييم الموضوع محل عملية التوكيد وفقاً لمعايير القياس، وخدمات تقرير مباشر وهي تلك التي يقوم فيها المراجع الخارجي بقياس أو تقييم الموضوع محل عملية التوكيد وفقاً لمعايير القياس، ويحتوي المعيار على متطلبات ومواد تطبيقية وتفسيرية تتعلق بعمليات تصديق لتقديم توكيد معقول أو محدود. ويمكن أن يطبق المعيار أيضاً على عمليات التقرير المباشر لتقديم توكيد معقول أو محدود، بعد تكييفه والإضافة إليه حسب الحاجة في ظل ظروف عملية التوكيد.

كما أشارت الدراسات (No & Vasarhelyi, 2017; Haapamaki& Sihvonen, 2019 ; Rosati 2019; Aldorisio,2020;) أن نموذج التوكيد عن إدارة مخاطر الأمن السيبراني لابد أن يراعى ثلاثة عناصر أساسية هي:

- طبيعة توقيت التقرير: حيث أن تهديدات الأمن السيبراني مرتبطة بفترة زمنية وتستند على متغيرات متعددة مثل : الخصائص التنظيمية، وطبيعة 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.
- طبيعة الاستنتاج: تقدم تقارير المراجعة التقليدية الرأى حول مدى عدالة تعبير التقارير المالية عن المركز المالي ونتائج الأعمال (عادلة غير عادلة) وهو ما لا ينطبق على حالة التوكيد عن

إدارة مخاطر الأمن السيبراني، فهي عملية مستمرة مغيرة لا تأخذ حكماً واحداً على طول الوقت، وإنما من الأنسب وجود مراجعة فورية مستمرة لحالة درجة الأمن السيبراني والتعبير عن الحالة في أوقات متتالية مستمرة.

- الأهمية النسبية: عادة تنص معايير المراجعة المقبولة على مفهوم الأهمية النسبية للعناصر، والذي يفسر عادة كنسبة من الدخل أو من إجمالي الأصول، وهو ما لايصلح مع التوكيد عن إدارة مخاطر الأمن السيبراني، فهناك عناصر لا يمكن قياسها نقداً مثل؛ الإستدامة، وسلاسل التوريد والعلامات التجارية وإدراة المخاطر، وبالتالي لا يصلح مفهوم الأهمية النسبية في هذه الحالة. إلا أنه يثير التساؤل حول مبررات الطلب على المراجع الخارجي للقيام بمهمة التوكيد على الافصاح عن إدارة مخاطر الأمن السيبراني للشركة، حيث تذكر الدراسات :(AICPA 2021 , Eaton et al 2017) أن خبرة المراجع الخارجي تمثل أحد أسباب اللجوء له للقيام بخدمة التوكيد عن إدارة مخاطر الأمن السيبراني، ومعرفته بالرقابة الداخلية والتقارير المالية وتقييم المخاطر وتحديد حجم التهديدات، كما لديه من المؤهلات العلمية والتدريب والمعرفة بأنظمة تكنولوجيا المعلومات وأنظمة التشغيل وتقييم الأنظمة الرقابية وتقديم الخدمات الإستشارية وتصميم البرامج ما يبرر زيادة الطلب على خدماته.

٧-٤ مفهوم قرارات المستثمرين وأنواعها:

يعد القرار الاستثماري من أهم القرارات الجوهرية التي تتخذها المنشأت أو الأفراد، وذلك حيث أن القرار الاستثماري هو استثمار للأموال في مشاريع استثمارية متاحة بهدف الحصول على عائد متوقع مع إحتمالية وجود نسبة مخاطرة تتمثل في عدم الحصول على هذا العائد أو حدوث نوع من الخسارة، ولذلك ينبغي على متخذ القرار الاستثماري القيام بدراسة وتحليل الجدوى الاقتصادية للمشاريع الاستثمارية المتاحة، وموازنة العوائد المتوقعة بالمخاطر المحتملة لها.

وفي هذا الإطار عرفت دراسة (داود ، ٢٠٢٣) قرارات الاستثمار بأنها اختيار بين البدائل الاستثمارية المتاحة والممكنة والمتعددة على أسس ومعايير اقتصادية بالإضافة إلى معايير بيئية من أجل العمل على تحقيق دافع الاستثمار من خلال تسلم المستثمرين لرسائل الإفصاح عن الأداء الاقتصادي والبيئي للمنشآت ، كما عرفت دراسة (علي، ٢٠١٦) قرارات الإستثمار بأنها التضحية بمبلغ أو أصل مالي يمتلكه المستثمر في لحظة زمنية معينة ولفترة زمنية بهدف الحصول على عائد مستقبلي ، وقيامه بالاختيار من بين البدائل الاستثمارية المتعددة والتي قد تكون مبنية على أسس معايير اقتصادية وبيئية واجتماعية ، مع الأخذ في الاعتبار العائد المتوقع ودرجة المخاطرة مع أخذ عنصر الزمن في الإعتبار.

وبالنسبة لأنواع قرارات المستثمرين يقوم المستثمر باتخاذ القرارات الاستثمارية المختلفة التي تشمل ثلاثة أنواع رئيسية هي (أحمد عثمان ، ٢٠٢١):

- **قرار الشراء :** ذلك عندما يرغب المستثمر في حيازة أصل مالي عندما يرى بأن القيمة الحالية للتدفقات النقدية المتوقعة تفوق القيمة السوقية الحالية للأصل المالي مع الاهتمام بالمخاطرة المصاحبة لهذه التدفقات النقدية.

- **قرار عدم التداول :** في هذه الحالة يتساوى السعر السوقي مع القيمة ويصبح السوق في حالة توزان وبالتالي لا يتوقع المستثمر تحقيق أي عوائد إلا اذا تغيرت الظروف السائدة، مما لا يدفع المستثمر إلى القيام بأي قرار سواء متعلق بالشراء أو البيع.
- **قرار البيع :** عندما يرى المستثمر بأن القيمة السوقية للأصل الذي بحوزته أكبر من القيمة الحالية للتدفقات النقدية المتوقعة (مع الأخذ بعين الاعتبار المخاطر المصاحبة لهذه التدفقات النقدية) ، فإنه قد يتخذ قرار البيع نتيجة لوجود فرصة لتحقيق الأرباح.

٧-٥ الدراسة التجريبية :

٧-٥-١ مجتمع وعينة الدراسة :

يتمثل مجتمع الدراسة في المستثمرين في الأسهم، حيث تم سحب عينة منهم تضم ١٠٠ مفردة من المستثمرين. قياساً على (على&علي، ٢٠١٩؛ Reimsbach et al, 2018; Hoang & Phang, 2021 ويوضح الجدول التالي عدد الحالات التجريبية الموزعة على عينة الدراسة بالإضافة إلى عند ونسبة الردود، وكذلك عدد ونسبة الردود السليمة التي خضعت للتحليل الاحصائي.

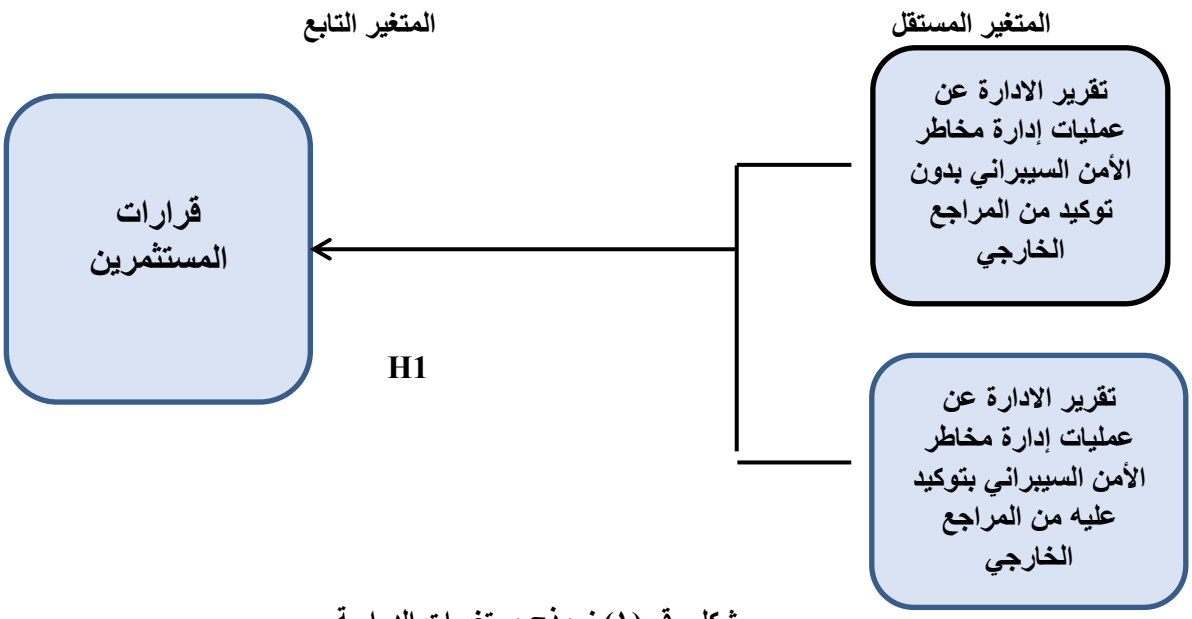
جدول ١ بيان بالردود على الحالات التجريبية

بيان	عدد الحالات التجريبية الموزعة	عدد الحالات التجريبية المستلمة	نسبة الردود على الحالات المستلمة إلى الحالات الموزعة	عدد الردود الصادقة
عينة المستثمرين في الأسهم	١٠٠	٨٢	٨٢٪	٧٥

فرض الدراسة:

الفرض الأول H1: يؤثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني معنوياً على قرارات المستثمرين..

يعرض الباحثين فيما يلي نموذج الدراسة وتوصيف وقياس متغيرات الدراسة:



شكل رقم (١) نموذج ومتغيرات الدراسة

٧-٥-٢ توصيف وقياس متغيرات الدراسة

المتغير المستقل: توكيد المراجع الخارجي عن مخاطر الأمن السيبراني ، وتم ذلك من خلال مقارنة قرارات المستثمرين بشأن أسعار الأسهم والاستثمار فيها في ظل عدم وجود خدمة توكيد عن مخاطر الأمن السيبراني ثم وجود خدمة توكيد عليها بعض النظر عن نوع الرأي أو الاستنتاج في تقرير المراجع الخارجي.

المتغير التابع: قرارات المستثمرين ، ويتم قياسه من خلال مقارنة بين حالتي الثبات وعدم الثبات بالنسبة لسعر السهم وتوقع سعر السهم في نهاية الفترة التالية واتخاذ قرار الاستثمار.

٧-٥-٣ التصميم التجريبي

اعتمدت الباحثة على التصميم التجريبي (٢×١) قياسا على دراسات (شرف ، ٢٠١٥ ؛ Badawy, 2021؛ Navarro & Sutton.2021)، بهدف اختبار العلاقة محل الدراسة، حيث تم صياغة شكل مقترح لتقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني وفق الإصدارات والإرشادات المهنية ذات الصلة، واقتراح نموذج للتوكيد المهني على تلك الإفصاحات في ضوء المعايير المهنية ذات الصلة.

ولاختبار فرض الدراسة تم استخدام تصميم تجريبي (٢×١)، وذلك كما يلي:

الحالات	المستثمرين
تقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني بدون توكيد من المراجع الخارجي.	المعالجة (١) استعداد المستثمر للاستثمار بالاسهم
تقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني بتوكيد عليه من المراجع الخارجي.	المعالجة (٢) استعداد المستثمر للاستثمار بالاسهم

وفق هذا التصميم التجريبي يوجد (٢) معالجة تجريبية كما يلي:

المعالجة ١: يقدم تقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني بدون توكيد من مراجع خارجي/ ويطلب من المستثمر تحديد مدى استعداده للإستثمار بالأسهم .

المعالجة ٢: يقدم تقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني بتوكيد عليه من المراجع الخارجي / . ويطلب من المستثمر تحديد مدى استعداده للإستثمار بالأسهم.

ولإختبار الفرض الأول تم إجراء المقارنة التالية:

واستخدم الباحثون اختبار معامل ألفا كرونباخ Cronbach's Alpha لتحديد مدي إمكانية الاعتماد على العناصر المكونة لأسئلة الحالات التجريبية، من خلال اختبار مدى ثبات ومصداقية إجابات أفراد عينة الدراسة، وتاخذ قيمة معامل الاختبار قيما تتراوح بين الصفر والواحد الصحيح ، فإذا كانت الإجابات بها ثبات فإن قيمة المعامل تساوي الواحد الصحيح مقارنة بعدم ثبات الإجابات في حالة قيمة المعامل تكون مساوية للصفر. ويشير الثبات إلى استقرار المقياس وعدم تناقضه مع نفسه بمعنى أن المقياس يعطي نفس النتائج إذا أعيد تطبيقه على نفس العينة، ويشير ارتفاع قيمة معامل الاختبار إلى صدق أداة الدراسة وصحة العلاقة السببية بين المتغير التابع والمستقل أي الصدق الداخلي ، وبالتالي إمكانية تعميم النتائج أي الصدق الخارجي ، وأشارت النتائج لمصداقية كل عنصر من العناصر المكونة لأسئلة الحالات التجريبية لعينة المستثمرين على حدة حيث كان معامل ألفا كرونباخ أكبر من ٦٠٪ وهي أصغر قيمة مقبولة لمعامل ألفا كرونباخ Cronbach's Alpha ، كذلك أشار المعامل إلى مصداقية وامكانية الاعتماد على عناصر الأسئلة ككل حيث كان المعامل لعينة الدراسة ٩٤,٣٪ وهو أكبر من ٦٠٪ وتقع بين ٩٠% و ٩٥٪ وهو المدى الذي يمثل لأفضل قيمة لمعامل ألفا كرونباخ Cronbach's Alpha ، ويتضح ذلك من الجدول التالي:

جدول ١ : معامل الفا كرونباخ لعينة الدراسة

Sample	Cronbach's Alpha	N of Items	الصدق الذاتى
المستثمرون	.943	10	0.971

المصدر: نتائج التحليل الإحصائي لبرنامج SPSS.

كما قام الباحثين باستخدام اختبار كا تربيع (x2) Ka -squar لتحديد مدي معنوية الأسئلة قياسًا على دراسة (موسى ٢٠١٨ ؛ محمد، ٢٠٢٠) ، وأظهرت النتائج أن قيمة P - Value أقل من مستوى ٥٪ لمعظم الأسئلة المرافقة للحالات التجريبية، مما يعني رفض الفرض العدم (القائل بأنه لا توجد اختلافات بين فئات الإجابة) وقبول الفرض البديل (القائل بأنه توجد اختلافات بين فئات الإجابة).

وقامت الباحثة باجراء اختبار Kolmogorov - Smirnov واختبار Shapiro-Wilk لتحديد مدى تبعية بيانات العينة للتوزيع الطبيعي المعتدل. حيث تكون الاختبارات الإحصائية مناسبة في حالة تبعية توزيع بيانات العينة للتوزيع الطبيعي المعتدل، بينما تكون الاختبارات اللامعلمية هي المناسبة في حالة عدم تبعية بيانات العينة للتوزيع الطبيعي المعتدل (شرف ٢٠١٥ بدوي ، ٢٠١٨ ؛ موسي ٢٠١٨؛ محمد ،٢٠٢٠)

ويتمثل الفرض العدم والبديل لهذه الاختبارات فيما يلي:

فرض العدم HO: توزيع بيانات العينة يساوي التوزيع الطبيعي المعتدل.

فرض البديل H1 توزيع بيانات العينة لا يساوي التوزيع الطبيعي المعتدل.

وفيما يلي جدول يوضح نتائج هذا الاختبار كما يلي:

جدول ٢ نتائج اختبارات توزيع بيانات العينة

كود العبارة	العبارات	Kolmogorov-Smirnov[b]		Shapiro-Wilk	
		Statistic	Sig.	Statistic	Sig.
Q_1	هل توافق على أن تقرير الإدارة عن برنامج إدارة مخاطر الأمن السيبراني يوفر لك معلومات مفيدة يمكن الاعتماد عليها في اتخاذ قرار الاستثمار.	.271	.000	.838	.000
		.361	.000	.635	.000
Q_2	هل توافق على أن هذه الشركة سيكون لها أولوية أكبر عند دراسة قرار الاستثمار في الأسهم مقارنة بالشركات التي لم تقدم إفصاحًا عن برنامج إدارة مخاطر الأمن السيبراني:	.261	.000	.856	.000
		.361	.000	.635	.000
Q_3	ما هو احتمال استثمارك في أسهم هذه الشركة	.232	.000	.833	.000
		.342	.000	.715	.000
Q_4	من وجهة نظركم هل توافق على أن إخضاع تقرير الإدارة عن برنامج إدارة مخاطر الأمن السيبراني للتوكيد من قبل المراجع الخارجي سيكون له أثر أكبر على اعتمادكم على هذا التقرير عند اتخاذ قرار الاستثمار.	.454	.000	.487	.000
		.531	.000	.328	.000
Q_5	إذا كان سعر الإقفال الفعلى لسهم الشركة في يوم العمل التالي لتاريخ تقرير المراجع الخارجي كان 15 جنيه فإن سعر الإقفال المتوقع لسهم الشركة بعد تقرير المراجع الخارجي في 2023 في ضوء المعلومات السابقة من وجهة نظركم سيكون جنيه.	.412	.000	.607	.000
		.290	.000	.763	.000

Q_6	هل توافق على أن تقرير الإدارة عن برنامج إدارة مخاطر الأمن السيبراني وتقرير المراجع الخارجي يوفر لك معلومات مفيدة يمكن الاعتماد عليها في اتخاذ قرار الاستثمار	.321	.000	.703	.000
		.408	.000	.610	.000
Q_7	هل توافق على أن هذه الشركة سيكون لها أولوية أكبر عند دراسة قرار الاستثمار في الأسهم مقارنة بالشركات التي لم تقدم إفصاحا وتوكيدًا عن برنامج إدارة مخاطر الأمن السيبراني:	.290	.000	.782	.000
		.454	.000	.558	.000
Q_8	ما هو احتمال استثمارك في أسهم هذه الشركة	.442	.000	.449	.000
		.454	.000	.558	.000
Q_9	من وجهة نظركم هل توافق على أن تقرير توكيد المراجع الخارجي على تقرير الإدارة عن برنامج إدارة مخاطر الأمن السيبراني سيكون له أثر أكبر على اعتمادكم على هذا التقرير عند اتخاذ قرار الاستثمار:	.348	.000	.559	.000
		.497	.000	.471	.000
Q_{10}	إذا كان سعر إقفال سهم الشركة الندى في 31/12/ 2022 يبلغ 15 جنيها ، وسعر إقفال السهم في 31/ 12/2023كان 16 جنيها، فإن سعر الإقفال المتوقع من وجهة نظركم31/12/2024	.470	.000	.531	.000
		.497	.000	.471	.000

المصدر: نتائج التحليل الإحصائي لبرنامج SPSS.

يتضح من جدول رقم (٢) أنه وفقا لاختبار الاعتدال السابق تم رفض العدم (القائل بأن المجتمع الذي سحبت منه عينة الدراسة يتبع التوزيع الطبيعي وقبول الفرض البديل القائل بأن المجتمع الذي سحبت منه عينة الدراسة لا يتبع التوزيع الطبيعي) حيث أظهرت نتائج هذا الاختبار أن قيمة P-Value تساوى (٠,٠٠٠) لجميع المتغيرات محل الدراسة، وهي أقل من مستوى المعنوية (٠,٠٥)، وبذلك فإن بيانات

عينتي الدراسة لا تتبع التوزيع الطبيعي المعتدل، وبالتالي يتم الاعتماد على الاختبارات اللامعلمية لاختبار فرض الدراسة وفق دراسات (شرف ٢٠١٥ بدوي ٢٠١٨؛ موسى ٢٠١٨ محمد ٢٠٢٠).

٧-٥-٤ نتائج اختبار فروض الدراسة

الفرض: يؤثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني معنوياً على قرارات المستثمرين.

استهدف الفرض اختبار ما إذا كان **توكيد المراجع الخارجي عن مخاطر الأمن السيبراني يؤثر معنويا على قرارات المستثمرين** ، وقد استخدم الباحثون اختبار Wilcoxon Signed Ranks Test لتحديد مدي الاختلاف بين متوسطي عينتين غير مستقلتين، وقد تم صياغة فرض العدم كما يلي:

فرض العدم HO : لا يؤثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني معنوياً على قرارت المستثمرين.

وبالتالي يكون الفرض الإحصائي لهذا الاختبار كما يلي:

$$H_o: M1 = M2$$

$$H_1: M1 \neq M2$$

ويشير فرض العدم بأنه لا يوجد اختلافات معنوية في ردود المجموعتين في ظل عدم وجود اختلاف في تقرير التوكيد عن مخاطر الأمن السيبراني، في حين يشير الفرض البديل لوجود اختلافات معنوية في ردود المجموعتين في ظل اختلاف تقرير التوكيد عن مخاطر الأمن السيبراني، ويتم رفض الفرض العدم وقبول الفرض البديل إذا كانت قيمة P-value أقل من أو تساوي ٥٪ والعكس إذا كانت قيمتها أكبر من ٥٪، وذلك وفقا لنتائج الاختبار الموضحة في الجدول رقم (٥) التالي:

جدول رقم ٣: اختبار الفرض الأول H_1

Test Statistics					
	Q6 - Q1	Q7 - Q2	Q8 - Q3	Q9 - Q4	Q10 - Q5
Z	-7.453[b]	-6.351[b]	-6.765[c]	-6.036[b]	-3.699[b]
Asymp. Sig. (2-tailed)	.000	.000	.000	.000	.000
a. Wilcoxon Signed Ranks Test					
b. Based on negative ranks.					
c. Based on positive ranks.					

ويتضح من الجدول رقم (٣) أن قيمة P- value هي (٠,٠٠٠) وهي أقل من مستوى المعنوية ٥٪ لكل مقارنة سؤال من الأسئلة، مما يعني رفض الفرض العدم وقبول الفرض البديل، وبالتالي يوجد تأثير معنوي لتوكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارت المستثمرين بما يتوافق مع نتائج دراسات Vekez,2019: Navarro & Sutton, 2021; Perols Li,2017; Perols 2019 &؛ Murthy, 2021) بان هناك اتجاه متزايد من قبل الشركات نحو الإفصاح عن مخاطر الأمن السيبراني، وقيام المراجع الخارجي بتوفير خدمة توكيد عن مخاطر الأمن السيبراني بما يعمل على تعزيز مستوى الشفافية وتقليل مستوى عدم تماثل المعلومات بين المديرين وأصحاب المصلحة بشكل عام وعلى قرارات وأحكام المستثمرين بشكل خاص، وزيادة الثقة والرغبة في الإستثمار في أسهم تلك الشركات.

وهذا الانعكاس المعنوي الإيجابي يرجع لاهتمام المنظمات المهنية والدراسات الأكاديمية وأصحاب المصلحة بأهمية ودور المراجع الخارجي في التوكيد عن مخاطر الأمن السيبراني وعلى معلومات الأمن السيبراني التي تعدها الشركة، من خلال تقديم خدمات لمساعدة الشركات على تحديد المجالات الرئيسية لمخاطر الأمن السيبراني، واكتشاف الثغرات في العمليات والضوابط الرقابية، وتطوير ضوابط رقابية فعالة، وتقييم مخاطر التحريف الجوهري الناتج عن القضايا المتعلقة بالأمن وتأثيره على القوائم المالية وعلى نظم الرقابة الداخلية على التقارير المالية (ICFR)، وأيضا تقييم مخاطر الأمن السيبراني حتى لو لم تحدث مثل هذه الأحداث بعد، بالإضافة لتشجيع الشركات على إيصال جهود إدارة مخاطر الأمن السيبراني إلى أصحاب المصلحة ولزيادة ثقتهم في قدرة الشركة على إدارة أعمالها ومخاطرها، واتخاذ نهج استباقي عند تصميم سياسات الأمن السيبراني، وتمكينها من تقييم ما إذا كانت لديها آليات الأمان المناسبة أم لا مما يؤدي إلى إدارة تهديدات أكثر ديناميكية، بما ينعكس إيجابا على قرارات المستثمرين في الاستثمار في أسهم تلك الشركات.

ويُظهر الجدول رقم (٣) أن الرتب Ranks كانت لصالح الحالة الثانية وهي وجود تقرير توكيد مهني عن مخاطر الأمن السيبراني، والذي يعني أن اتجاه ضرورة وجود توكيد مهني عن الإفصاح عن مخاطر الأمن السيبراني للمساعدة علي اتخاذ قرارات الاستثمار في الأسهم.

جدول ٤: Wilcoxon Signed Ranks Test

Ranks				
		N	Mean Rank	Sum of Ranks
Q6 - Q1	Negative Ranks	3[a]	5.00	15.00
	Positive Ranks	69[b]	37.87	2613.00
	Ties	3[c]		
	Total	75		
Q7 - Q2	Negative Ranks	3[d]	15.50	46.50
	Positive Ranks	54[e]	29.75	1606.50
	Ties	18[f]		
	Total	75		
Q8 - Q3	Negative Ranks	69[g]	36.24	2500.50
	Positive Ranks	3[h]	42.50	127.50
	Ties	3[i]		
	Total	75		
Q9 - Q4	Negative Ranks	3[j]	53.00	159.00
	Positive Ranks	57[k]	29.32	1671.00
	Ties	15[l]		
	Total	75		
Q10 - Q5	Negative Ranks	6[m]	15.50	93.00
	Positive Ranks	27[n]	17.33	468.00
	Ties	42[o]		

	Total	75		
a. Q6 < Q1				
b. Q6 > Q1				
c. Q6 = Q1				
d. Q7 < Q2				
e. Q7 > Q2				
f. Q7 = Q2				
g. Q8 < Q3				
h. Q8 > Q3				
i. Q8 = Q3				
j. Q9 < Q4				
k. Q9 > Q4				
l. Q9 = Q4				
m. Q10 < Q5				
n. Q10 > Q5				
o. Q10 = Q5				

ويتضح من تلك الاستجابات ثبوت صحة الفرض الأول يؤثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني معنوياً على قرارات المستثمرين.

٦-٧ نتائج البحث

أولاً : النتائج النظرية:

- أهمية توكيد المراجع الخارجي عن مخاطر الأمن السيبراني .
- أهمية الإفصاح عن مخاطر الأمن السيبراني في الشركة وأهمية قيام الإدارة بالتقييم الذاتي لنظام إدارة مخاطر الأمن السيبراني لتحديد ما إذا كان هناك أوجه ضعف جوهرية في هذا النظام واتخاذ ما يلزم من إجراءات للتغلب على أوجه الضعف في برنامج إدارة مخاطر الأمن السيبراني.
- لا يوجد إلزام على الشركات المقيدة بالبورصة المصرية بإعداد تقرير عن الإفصاح عن مخاطر الأمن السيبراني وتقرير توكيد المراجع الخارجي على ذلك الإفصاح، و يجب أن تصدر الهيئة العامة للرقابة المالية قراراً بأن يكون الإفصاح إلزامياً وليس إختيارياً ومن ثم يتم التوكيد عليه من المراجع الخارجي لزيادة ثقة المستثمرين.

ثانياً : النتائج العملية :

توصلت الدراسة إلى وجود تأثير معنوي لتوكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارات المستثمرين ، ويتفق ذلك مع ما توصلت إليها الدراسة في شقها النظري. وقد ترجع هذه النتيجة أن التوكيد عن مخاطر الأمن السيبراني يوفر معلومات حول مخاطر الأمن السيبراني التي تواجهها الشركة وكيفية إدارتها، مما يزيد من وعي المستثمرين.

٧-٧ التوصيات والبحوث المستقبلية

وفقاً لما انتهت إليه الدراسة من نتائج بشقيه النظري والتجريبي، وفي ضوء حدوده، يوصي الباحثون بما يلي:

- ضرورة اهتمام الهيئة العامة للرقابة المالية بتوجيه وزيادة وعي الشركات بأهمية الإفصاح عن مخاطر الأمن السيبراني في التقارير السنوية للشركات عن طريق إصدار المعايير الإرشادية التي تنظم عملية إعداد وعرض تقرير مخاطر الأمن السيبراني والاستفادة من تجارب الدول الأخرى في هذا الشأن.
- يجب على الهيئة العامة للرقابة المالية وصانعي السياسات النظر فيما إذا كان ينبغي حث الشركات على المزيد من الإفصاحات المتعلقة بالأمن السيبراني وفرض عقوبات علنية وصارمة على الشركات لعدم التزامها بالإفصاح عن تعرضها لإختراقات الأمن السيبراني ، واتخاذ إجراءات تنظيمية لتعزيز الإفصاح في الوقت المناسب عن الاختراقات السيبرانية.
- ضرورة قيام الجهات المصرية المعنية بإصدار معايير المحاسبة والمراجعة بتوفير إرشادات كافية عن محتوى تقرير مخاطر الأمن السيبراني، وأيضاً توفير إرشادات كافية عن مسئولية المراجع الخارجي عند التوكيد عن إفصاح الشركات عن تقرير مخاطر الأمن السيبراني.
- من المهم أن تنشأ كل شركة لديها إدارة أو قسم خاص بإدارة مخاطر الأمن السيبراني، وتقوم بتحديثها باستمرار، والتدريب المستمر لفريق العمل المعني بالأمن السيبراني، لثقل وتطوير مهاراتهم وتوعيتهم بخطورة الأحداث السيبرانية وعواقبها.

مجالات البحث المقترحة:

يقترح الباحثين عدداً من مجالات البحوث المستقبلية، علي النحو التالي:

- أثر التوكيد المهني عن تقرير مخاطر الأمن السيبراني علي قرارات مانحي الائتمان.
- أثر خصائص مجلس الإدارة على اتجاه الشركات للاستثمار في الأمن السيبراني.
- نحو تفعيل دور المراجعة الداخلية في تعزيز الإفصاح عن مخاطر الأمن السيبراني.
- أثر توقيت المحتوي المعلوماتي لإفصاح الشركات عن حوادث الأمن السيبراني علي سلوك المستثمرين.

المراجع:

أولًا: المراجع العربية

أحمد ، عثمان بن سيد ، (٢٠٢١) ، مساهمة جودة المعلومات المالية في ترشيد قرارات المستثمرين على مستوى سوق الأوراق المالية - دراسة ميدانية لآراء عينة من المهنيين والأكاديميين في الجزائر ، مجلة الإصلاحات الإقتصادية والإندماج في الاقتصاد العالمي ، الجزائر.

البنك الدولي ٢٠٢٢ https://www.albankaldawli.org/ar/country/egypt.

الرشيدي، طارق عبد العزيز، عباس، داليا عادل. (٢٠١٩)، أثر الإفصاح عن مخاطر الأمن السيبرانى في التقارير المالية على أسعار الأسهم وأحجام التداو ل : دراسة مقارنة في قطاع تكنولوجيا المعلومات. مجلة المحاسبة والمراجعة، كلية التجارة، جامعة بني سويف، المجلد ٨ ، العدد الثاني، ص ٤٣٩ – ٤٨٧.

السرحان، سالم . (٢٠٢٠). أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الاردنية رسالة ماجستير ، جامعة آل البيت ، كلية الاقتصاد والعلوم الإدارية، الأردن.

داود ، عادل محمد امين محمد ، (٢٠٢٣) ، إطار مقترح لقياس أثر التقرير عن أمور المراجعة الجوهرية على فعالية المراجعة وانعكاسه على قرارات الاستثمار : دراسة ميدانية ، رسالة دكتوراه ، كلية التجارة - جامعة عين شمس.

شرف، إبراهيم أحمد إبراهيم (٢٠٢٣) أثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات المستثمرين المصريين غير المحترفين - دراسة تجريبية"، مجلة الإسكندرية للبحوث المحاسبية، كلية التجارة جامعة الإسكندرية، المجلد ٧ ، العدد ١ ص ص ٢٨٢-٢١١.

عثمان, محمد أحمد عبد العزيز. (٢٠٢٣). أثر توكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين بالأسهم–دراسة تجريبية. مجلة الاسكندرية للبحوث المحاسبية, ٧(٢), ١٦٧-٢٣٨.

على محمود أحمد أحمد، وعلي صالح علي صالح، (٢٠٢٢) ، أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستشار بأسهم الشركات المقيدة بالبورصة المصرية: دراسة تجريبية، مجلة الإسكندرية للبحوث المحاسبية، كلية التجارة، جامعة الإسكندرية، المجلد ٦ العدد ٣، ص ص ١-٤٨ .

عيسى، عارف محمد سمير، (٢٠٢٢). قياس أثر الثالوث المظلم كسمات شخصية على اتجاهات المحاسبين نحو الإفصاح عن مخاطر الأمن السيبراني دراسة شبه تجريبية. مجلة الاسكندرية للبحوث المحاسبية، قسم المحاسبة والمراجعة، كلية التجارة جامعة الإسكندرية، ٦(٣) ١٢٩-١٩٦.

فرج، هانى خليل فرج. (٢٠٢٢). أثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بالأسهم-دراسة تجربية. مجلة المحاسبة والمراجعه لاتحاد الجامعات العربيه, ١١(٢), ١٢٩-٢٠٩.

لطفي، أمين السيد أحمد، (٢٠١٠) ،المحاسبة والمراجعة الدولية، الدار الجامعية، الإسكندرية، مصر.

محمد، عمرو محمد خميس، ٢٠٢٠، أثر توكيد مراقب الحسابات على تقرير الأعمال المتكاملة على قرارات الاستثمار بالأسهم : دراسة تجريبية، مجلة الإسكندرية للبحوث المحاسبية، كلية التجارة، جامعة الإسكندرية، المجد ٤ العدد الثالث، ص ص ١٠٥١.

محمد قاسم سالم, د., دنيا, & محمد إبراهيم منصور. (٢٠٢٣). تأثير جرائم الأمن السيبراني على مخاطر المراجعة وإنعكاسه على أتعاب المراجعة (دراسة تطبيقية). المجلة العلمية للدراسات التجارية والبيئية, ١٤(٣), ٩٧٤-١٠٠٩.

مطر, ن. ص. ع. ع., & نيفين صلاح على على. (٢٠٢٤). اثر افصاح شركات تكنولوجيا المعلومات عن تقرير إدارة مخاطر الأمن السيبراني على قرار منح الائتمان، الدور المعدل لنوع وخبرة مانح الائتمان: دراسة تجريبية. مجلة البحوث المحاسبية, ١١(٣), ١-٥٤.

موسى، سعاد زغلول عبده ٢٠١٨ ، أثر توكيد المراجع الخارجي على تقارير الأعمال المتكاملة على قراراي الاستثمار ومنح الائتمان: دراسة تجريبية رسالة دكتوراه غير منشورة، كلية التجارة، جامعة الإسكندرية.

ثانيًا: المراجع الأجنبية

Alidarous, M. (2024). Driving Venture Capital Interest: The Influence of the Big 4 Audit Firms on IPOs. Journal of Risk and Financial Management, 17(7), 292.

Al-Zyoud, A, M. (2020). " Managing Cybersecurity Risks in Jordanian Banks", Millennium Journal of Economic and Administrative Sciences, 1(1): 5-14, Available at: https://doi.org/10.47340/mjeas.v1i1.2.2020.

Alharbi, F., Alsulami, M., AL-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The Impact of Cybersecurity Practices on Cyberattack Damage: The Perspective of Small Enterprises in Saudi Arabia. Sensors, 21(20).

Alic, D. (2021). The role of data protection and cybersecurity regulations in artificial intelligence global governance: a comparative analysis of the European Union, the United States, and China Regulatory Framework. Search in.

American Institute of Certified Public Accountants (AICPA) (2017). Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program, AICPA Assurance Services Executive Committee, New York, NY.

Badawy,H. (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,3(5):1-56.

Bahmanziari, T., M. Odomb, and J. Ugrin.2009. An experimental evaluation of the effects of internal and external e-Assurance on initial trust formation in B2C e-commerce, International Journal of Accounting Information Systems, 10: 152–170.

BDO National Assurance practice , 2014 , CYBERSECURITY ITS IMPACT ON THE EXTERNAL AUDIT AND OTHER RECENT DEVELOPMENTS,pp 1- 3 . Available at :ww.bdo.com.

Benaroch, M., & Chernobai, A. (2017). Operational IT failures, IT value destruction, and board-level IT governance changes. MIS Quarterly: Management Information Systems, 41(3), 729-762.

Calderon, T., & Gao, L. (2020). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. International Journal of Auditing, 25(1), 24-39.

CESG .2012.Assurance of ICT systems and services. Good Practice Guide, No. 30, CESG Information Assurance Portal, available at: www.ncsc.gov.uk/content/files/guidance.

Channuntapipat, C., Samsonova-Taddei, A., & Turley, S. (2020). Variation in sustainability assurance practice: An analysis of accounting versus non-accounting providers. The British Accounting Review, 52(2), 100843.

Chernobai, A., Jorion, P., & Yu, F. (2011). The determinants of operational risk in US financial situations. Journal of Financial and Quantitative Analysis, 46(6), 1683-1725.

Cho, C. H., Michelon, G., Patten, D. M., & Roberts, R. W. (2014). CSR report assurance in the USA: an empirical investigation of determinants and effects. Sustainability Accounting, Management and Policy Journal, 5(2), 130-148.

Conteh, N. Y., & Schmick, P. J. (2021). Cybersecurity risks, vulnerabilities, and countermeasures to prevent social engineering attacks. In Ethical hacking techniques and countermeasures for cybercrime prevention (pp. 19-31). IGI Global.

Dakin, R. (2012). SEC cyber risk disclosure guidance. Available at: https://www.omegasecure.com/wp-content/uploads/2016/03/ Coalfire-Perspective-SEC-Cyber-Risk-Disclosure-Guidance.

Demek, K. C., & Kaplan, S. E. (2023). Cybersecurity breaches and investors' interest in the firm as an investment. International Journal of Accounting Information Systems. 49:1- 15.

Eaton, T., J. Grenier, and D. Layman.2019. Accounting and Cybersecurity Risk Management. American Accounting Association, Vol. 13, No. 2: C1–C9

Elnagar, S. M. A., Ahmed, A. S. A. A., & Basiouny, M. M. M. (2024). The Impact Of Cybersecurity Risk Disclosure On The Quality Of Financial Reporting And Market Value. Evidence From Egyptian Stock Market. Educational Administration: Theory and Practice, 30(5), 2504-2516.

Florakis, C., C. Louca, R. Michaely, & M. Weber. (2020). "Cybersecurity Risk" 1-73, Available at: http://ssrn.com.

Fonseca, R. S., & Van Wyk, J. A. (2021). Cybersecurity in South Africa: Status, governance, and prospects. In Routledge Companion to Global Cyber-Security Strategy (pp. 591-607). Routledge.

Goldstein, P. 2021. What Is a Cyber security Audit and Why Is It Important ? Cybersecurity audits help ensure agencies comply with IT security regulations and requirements. https://fedtechmagazine.com/.

Hancock, M. 2017.UK cyber security research report. Department for Digital, Culture, Media & Sport, available at: www.gov.uk/ government/publications/cyber-security-breaches-survey.

Hamm, K. (2019, September 19). Cybersecurity: A Holistic Approach. Public Company Accounting Oversight Board (PCAOB). https://pcaobus.org/news-events/speeches/speech-detail/cybersecurity-aholistic-approach_707.

Haapamäki, E. and J. Sihvonen.2019. Cybersecurity in accounting research. Managerial Auditing Journal, Vol. 34, No. 7: 808-834.

Harris, D., Kuzey, C. Naaman, C. & Sahyoun, N. (2023). Cybersecurity Risk Disclosure Quality: Does it Affect the Cost of Debt? Journal of Forensic and Investigative Accounting. 15(2):1-21.

Havakhor, T., Rahman, M. S. & Zhang, T. (2020). Cybersecurity investments and the cost of capital. SSRN Electronic Journal: 1-48.

Hoang. H. & Phang, S., 2021, How does Combined Assurance Afflect the Reliability of Integrated Reports and Investors' Judgments?, European Accounting Review, 30 (1): 175-195.

IAASB. (2013). International Standard on Assurance Engagements 3000 (Revised): Assurance Engagements Other than Audits or Reviews of Historical Financial Information.

IBM Security. 2023. Cost of a data breach report. https://www.ibm.com/reports/data-breach IMFBlog, International monetary fund. 2024. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-seriousconcerns-for-financial-stability.

ICAEW, 2016 , Audit insights: cyber security Taking control of the agenda. icaew.com/ auditinsights.

Information Systems Audit and Control Association (ISACA). (2017). Available at: https://csrc.nist.gov/glossary/term/cybersecurity.

International Ethics Standards Board for Accountants (IESBA) (2018). Roundtable Briefing Note- Non-assurance Services: Exploring Issues to Determine a Way Forward, New York, IFAC.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics , 139 (3), 719-749.

Lessambo, F. I. (2018). Auditing, Assurance Services, and Forensics. Palgrave Macmillan.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyberattacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176–8186.

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

Mendhurwar, S., & Mishra, R. (2021). Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. Enterprise Information Systems, 15(4), 565-584.

National institute of standards and technology (NIST) .(2018). a Glossary of key information security terms National institute of standards and technology interagency or internal report, Available athttp://csrc.nist.gov /publications.

Navarro, P. and S. Sutton. 2021. Investors' Judgment and Decisions after a Cyber security Breach: Understanding the Value Relevance of Cyber security Risk Management Assurance, (February, 1):1-52.

No, W. G., & Vasarhelyi, M. A. (2017). Cybersecurity and continuous assurance. Journal of Emerging Technologies in Accounting, 14(1), 1-12.

Parker, A. & Brown, I. (2019). Skills Requirements for Cyber Security Professionals: A Content Analysis of Job Descriptions in South Africa. In: Venter H., Loock M., Coetzee M., Eloff M., Eloff J. (eds) Information Security. ISSA 2018. Communications in Computer and Information Science.

Peslak, A., & Hunsinger, D. S. (2019). What Is Cybersecurity and What Cybersecurity Skills Are Employers Seeking?. Issues in Information Systems, 20(2).

Perols, R. and Murthy, U., 2021, The Impact of Cybersecurity Risk Management Examinations and Cybersecurity Incidents on Investor Perceptions and Decisions, Auditing: A Journal of Practice & Theory, 40 (1): 73-89.

Public Company Accounting Oversight Board(PCAOB). (2014). Standing advisory group meeting: cybersecurity. Available at http://pcaobus.org/News/Events/Documents/0624252014_SAG_Meeting/06252014_Cybersecurity.pdf.

Reimsbach, D., Hahn, R., and Gurturk, A., 2018, Integrated reporting and assurance of sustainability information: An experimental study on professional investors' information processing, European Accounting Review, 27 (3): 559-581.

Rosati, P.2019. Audit Firm Assessments of Cyber-Security Risk: Evidence from Audit Fees and SEC Comment Letters. The International Journal of Accounting, Vol. 54, No. 3:1-56.

Roškot, M., Wanasika, I., & Kroupova, Z. (2021). Cybercrime in Europe: surprising results of an expensive lapse. Journal of Business Strategy, 42(2), 91-98.

Sapiri, M. (2024). A Qualitative Analysis on the Role of Auditors in Preventing Financial Crises. Golden Ratio of Auditing Research, 4(2), 89-106.

Sheneman, A. (2017). Cybersecurity risk and the cost of debt. Available at SSRN 3406217.

Sheneman, A. (2022). Contagion or Competitive Effects? Lenders' Response to Peer Firm Cyberattacks. Working Paper. Available at https://weis2022.econinfosec.org/wpcontent/uploads/sites/10/2022/06/weis22-sheneman.pdf

Singh, H. (2024). Is corporate reputation associated with voluntary cybersecurity risk reporting?. Meditari Accountancy Research.

Smith, T., Higgs, J & Pinsker, R. (2018). Do Auditors Price Breach Risk in Their Audit Fees? Journal of Information Systems, Forthcoming.

Smith, T., Jones, A., Johnson, L., & Smith, L. (2019). Examination of cybercrime and its effects on corporate stock value. Journal of Information, Communication and Ethics in Society, 17(1), 42-60.

Vekez, N. 2019. Three Studies on Cybersecurity Disclosure and Assurance, A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy. University of Central Florida.

Abstract

The aim of the research: is to study the impact of the external auditor's assurance of cybersecurity risks on investors' decisions.

Design and methodology: To achieve the objectives of the study, and in order to test the hypotheses, the study relied on the experimental study, and the study community represented investors and financial analysts, and the study sample formed (75) correct items.

Research results: It was concluded that the importance of the external auditor's assurance of cybersecurity risks was important. It also concluded that the importance of disclosing cybersecurity risks in the company and the importance of the management conducting a self-assessment of the cybersecurity risk management system to determine whether there are fundamental weaknesses in this system and taking the necessary measures to overcome the weaknesses in the cybersecurity risk management program. The results of the experimental study concluded that there is a moral impact of the external auditor's assurance of cybersecurity risks on investors' decisions.

Research recommendations: The need for the General Authority for Financial Supervision to pay attention to directing and increasing companies' awareness of the importance of disclosing cybersecurity risks in the companies' annual reports by issuing guiding standards that regulate the process of preparing and presenting the cybersecurity risk report and benefiting from the experiences of other countries in this regard. The Financial Regulatory Authority and policymakers should also consider whether to encourage companies to make more cybersecurity disclosures, impose public and severe penalties on companies for failing to disclose their exposure to cybersecurity breaches, and take regulatory measures to promote timely disclosure of cyber breaches.

Key words:

Cybersecurity, Cybersecurity Risks, External Auditor Assurance Services, Investor Decisions.