مجلة الإسكندرية للبحوث المحاسبية
قسم المحاسبة والمراجعة

العدد الثاني– مايو 2023– المجلد السابع

أثر توكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين بالأسهم – دراسة تجريبية

د/ محمد أحمد عبدالعزيز عثمان

أستاذ المحاسبة المساعد بكلية التجارة
جامعة بني سويف
أستاذ المحاسبة المساعد بالكلية الجامعية برنية
جامعة الطائف

ملخص البحث

استهدف البحث دراسة واختبار أثر **توكيد مراقب الحسابات** على الإفصاح عن عمليات إدارة مخاطر **الأمن السيبراني** على رغبة و**قرارات** المستثمرين في الأسهم، وكذلك اختبار أثر مستوى **الخبرة والتأهيل العلمي** للمستثمر كمتغيرات **مُعدَّلة** على العلاقة محل الدراسة، وذلك من خلال دراسة **تجريبية** على عينة من المستثمرين في بيئة الأعمال المصرية.

وتوصلت الدراسة إلي وجود علاقة معنوية إيجابية بين التوكيد المهني لمراقب الحسابات 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 **السحابة** 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 الأخرين 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 معًا على العلاقة بين التوكيد المهني لمراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني ورغبة وقرارات المستثمرين بالأسهم،** وكذلك **وجود** تأثير معنوي **لخبرة** المستثمر على العلاقة بين التوكيد المهني لمراقب الحسابات 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.

الكلمات المفتاحية: إدارة مخاطر الأمن السيبراني، الفضاء السيبراني، التوكيد المهني لمراقب الحسابات، رغبة وقرارات المستثمرين بالأسهم.

E.mail: draziz20201980@gmail.com
maothman@tu.edu.sa

The effect of CPA assurance on the disclosure of cybersecurity risk management processes on Investors' Willingness and Decisions in stocks - An experimental study

Abstract

The research aimed to study and examined the effect of assurance on the disclosure of cybersecurity risk management processes on Investors' Willingness and Decisions in stocks, as well as testing the impact of the level of experience and scientific qualification of the investor as modified variables on the relationship under study, through an experimental study on a sample of investors in the Egyptian business environment.

The study concluded that there is a positive significant relationship between the CPA Assurance on disclosure of cybersecurity risk management processes and Investors' Willingness and Decisions in stocks, As disclosure of the cybersecurity risks faced by companies and the knowledge of how companies operate their business on networks and in the cloud and the security risks they face that may lead to huge financial losses, loss of reputation and damage to the competitiveness of the company is becoming increasingly important for investors, governments, consumers, vendors and other stakeholders to make sound decisions and judgments, and the effect on stock price, and long-term shareholder value, The necessity of assurance disclosures and managing cybersecurity risks in a way that enhances the validity and reliability of financial reports and the level of transparency and reduces the level of information asymmetry between managers and stakeholders in general and on the decisions and judgments of investors in particular, and increases confidence and Willingness to invest in companies' stosks. The study also concluded there is a significant effect of the variables of experience and scientific qualification of the investor together on the relationship between CPA Assurance on disclosure of cybersecurity risk management processes and Investors' Willingness and Decisions in stocks, as well as a significant effect of investor experience on the relationship between CPA Assurance on disclosure of cybersecurity risk management processes and Investors' Willingness and Decisions in stocks, As well as there is no a significant effect of the level of scientific qualification of the investor on that relationship under study.

Keywords: Cybersecurity risk management, Cyberspace, CPA Assurance, on Investors' Willingness and Decisions in stocks.

1- مقدمة

يُعدّ الفضاء السيبراني والتقنيات ذات الصلة من أهم **مصادر** الطاقة في الألفية الثالثة. فيتم تنفيذ معظم الأنشطة الاقتصادية والتجارية والثقافية والاجتماعية والحكومية وتفاعلات البلدان، على جميع المستويات، بما في ذلك الأفراد والمنظمات والمؤسسات الحكومية وغير الحكومية في الفضاء السيبراني. **والفضاء السيبراني** هو المكان الذي **يُنشئ** فيه الأشخاص والمنظمات وجودًا **إلكترونيًا** ويشاركون في أنشطة افتراضية، ويتبادلون المعلومات والمنتجات والخدمات عبر الإنترنت. وبينما يوفر العمل في الفضاء السيبراني العديد من المزايا، فإنه يجعل جميع المؤسسات أيضًا عرضة **للتهديدات والهجمات السيبرانية.** وتصل هذه التهديدات إلي الحكومات **وأمنها القومي،** والذي لم يعد من الممكن تعريفه من حيث القضايا العسكرية والحدود الداخلية والخارجية، ولكن اليوم، يُشكل خطر تدهور نوعية حياة المواطنين تهديدًا للأمن القومي، واختفاء البعد الجغرافي للتهديدات السيبرانية مقارنة بالبعد الجغرافي المحدد للتهديدات العسكرية، وارتفاع مستوى الضرر للتهديدات السيبرانية لأنها متفرقة ومتعددة الأبعاد ومرتبطة بشبكات وبنية تحتية حساسة. و**نظرًا** لأن الأمن في عصر المعلومات ليس حكوميًا فقط فإن التهديدات السيبرانية لا تقتصر على الحكومات، ولكن الأفراد والشركات لن يكونوا مُحصَّنين ضد أضرار هذه التهديدات، والحكومات وحدها ليست كافية لمواجهتها(Li & Liu,2021) .

ويُثيرالتأثير الكبير **للانتهاكات** الأمنية والقرصنة على الشركات والمنظمين تساؤلات بشأن اقتصاديات أمن المعلومات. **ففي** واقع الأمر، يمكن أن يكون التأثير المباشر لخرق البيانات مدمرًا **لسمعة** الشركة، مما يؤدي إلى معدل دوران غير طبيعي للعملاء **وفقدان** السمعة التجارية ، مما يؤثر بدوره على التدفقات النقدية والأرباح ويضر بأدائها المالي. علاوة على ذلك ، فإن حوادث الانتهاكات الأمنية التي تكشف عن معلومات حساسة وسرية لا يمكن أن تؤدي فقط إلى التقاضي والعقوبات الحكومية، ولكن أيضًا إلى فقدان الميزة **التنافسية** ضد المنافسين من نفس الصناعة (Tosun, 2021).

وعلى الرغم من صعوبة جمع البيانات التفصيلية، فإن تكلفة الخروقات الأمنية والقرصنة للشركات كانت مذهلة، **وفقًا** لتقرير دراسة تكلفة انتهاك وخرق البيانات الصادر عن معهد بونيمون IBM Security and the Ponemon Institute ، فقد وصلت التكلفة إلى 4.24 مليون دولار لكل حادثة في عام 2021، وهي الأعلى منذ 17 عامًا، وكان متوسط تكلفة اختراق البيانات في عام 2020 هو 3.86 مليون دولار، ويُظهر التقرير انخفاضًا بنسبة 1.5٪ في التكاليف عن عام 2019 والتي بلغت 3.92 مليون دولار (IBM Corporation ,2021)، وهو ما يمثل مصدر قلق كبير للهيئات التنظيمية بقدر ما هو مصدر قلق للشركات.

ونظرًا للآثار المالية والسمعة والقانونية الكبيرة للهجمات السيبرانية، فإن الإفصاح عن مخاطر الأمن السيبراني التي تواجهها الشركات وكيفية إدارة هذه المخاطر أصبح ذا أهمية **متزايدة للمستثمرين** والحكومات والمستهلكين والبائعين وأصحاب المصلحة الآخرين لإصدار قرارات وأحكام سليمة(Gao et al., 2020).

وفي هذا الصدد، تناولت عدة دراسات (e.g: Khari et al., 2017; Ettredge et al.,2018;Ghadge et al., 2019; Calliess & Baumgarten, 2020; Rea-Guaman et al., 2020; Wang et al.,2020; Armenia et al., 2021;Kaur & Ramkumar, 2021; Lallie et al., 2021; Li & Liu,2021) **التهديدات السيبرانية** وتصنيفاتها المختلفة وآثارها سواء أكانت ضد الأفراد أم المنظمات والممتلكات والمجتمع، **وأيضًا** تناولت **إرشادات مهنية ودراسات** عدة (e.g: AICPA,2017a; AICPA,2017b; COSO,2019; Eaton et al.,2019; Ghadge et al., 2019; Yang et al., 2020; Armenia et al., 2021)، المراحل الفعالة **لإدارة مخاطر الأمن السيبراني** باعتبار أن إدارة المخاطر السيبرانية عملية مرتبطة بإستراتيجية بقاء حاسمة لاستمرارية الأعمال، **وكذلك صدرت العديد من الإرشادات المهنية الخاصة بالإفصاح والتوكيد** على مخاطر الأمن السيبراني عن لجنة الأوراق المالية والبورصات (SEC)، ومجلس الرقابة على شركات المحاسبة العامة (PCAOB)، والمعهد الأمريكي للمحاسبين القانونيين المعتمدين (AICPA)، ومركز جودة المراجعة (CAQ) وتتضمن سياسات تتعلق بقضايا الأمن السيبراني، والتي من المحتمل أن تؤثر على الشركات والتقارير المالية والإفصاحات والتوكيد (SEC, 2018; PCAOB ,2018; AICPA ,2017; CAQ,2018).

ويتفق البحث الأكاديمي في أنه بالرغم من، اكتساب قضايا المحاسبة المتعلقة بحوكمة الأمن السيبراني وإدارته وإفصاحاته اهتمامًا من واضعي معايير المحاسبة وشركات المحاسبة الكبرى والجمعيات المهنية، إلا أن **عددًا محدودًا** من الدراسات الأكاديمية تناولت الإفصاح عن الأمن السيبراني ومحتواه المعلوماتي وخدمات التوكيد المرتبطة به(Héroux & Fortin, 2020)، **مع تعدد الجوانب المختلفة والزوايا** المتعلقة بالإفصاح والتوكيد على عمليات إدارة مخاطر الأمن السيبراني وتأثيراتها **وعلاقاتها** بقرارات وأحكام المستثمرين، ومعرفة كيف تدير الشركات أعمالها على الشبكات وفي السحابة وما تواجهه من مخاطر أمنية قد تؤدي إلى خسائر مالية ضخمة وفقد السمعة.

وتناول البحث المحاسبي (e.g.: Li, 2017; Yen et al., 2018; Eaton et al., 2019; Moreira, 2019; PCAOB,2019; Rosati et al., 2019; Velez, 2019; Aldorisio, 2020;Rosati et al.,2020; Badawy, 2021; Bao Ngo et al., 2021; Calderon & Gao 2021; Hampton et al., 2021; Knechel, 2021; Li et al.,2021) **دور مراقبي الحسابات** فيما يتعلق بالتوكيد على برنامج إدارة مخاطر الأمن السيبراني للشركات والآثار المترتبة على أحداث

الانتهاك السيبراني الفعلية، والمردود الإيجابي للتوكيد على الاستثمار، وجودة المعلومات والوعي بالأمن السيبراني على الاستعداد والنية للاستثمار.

2- مشكلة البحث

وفقًا للاتجاه البحثي السابق، واهتمام المنظمين وممتهني المهنة وواضعي معايير المحاسبة والمراجعة بشأن إرشادات الإفصاح والتقرير لأصحاب المصلحة عن إدارة مخاطر الأعمال بشكل عام ومخاطر الأمن السيبراني بشكل خاص وتطبيق أفضل الممارسات لتأثيرها على قرارات المساهمين والمستثمرين، **وعواقبها** المالية السلبية الكبيرة على المؤسسات، والتقرير عن النتائج المحتملة من مخاطر قانونية، وزيادة أقساط التأمين، والإضرار بالقدرة التنافسية للشركة، والتأثير على سعر السهم، وقيمة المساهمين في الأجل الطويل عند تقييم مخاطر الأمن السيبراني، وإن كانت هذه الإرشادات لا تزال قيد التطوير.

وكما لم تقدم الدراسات (e.g., Berkman et al., 2018; Ettredge et al. 2018; Li et al., 2018; Tan & Yu, 2018; Cheng & Walton, 2019; Frank et al., 2019; Héroux& Fortin, 2020; Kelton & Pennington, 2020; Calderon & Gao, 2021; Walton et al.,2021) **التي تناولت المحتوي المعلوماتي وآثار إفصاحات الأمن السيبراني** أدلة حاسمة حول فعالية الإفصاح عن مخاطر الأمن السيبراني في تقليل عدم تماثل المعلومات، وتخصيص السوق قيمًا أعلى في السوق للشركات ذات الجودة العالية والإفصاحات ذات الصلة بالأمن السيبراني.

وفي السياق نفسه، يُظهر البحث المحاسبي تباين نتائج الدراسات (e.g.: Li et al., 2018; Cheng & Walton, 2019; Frank et al., 2019; Perols, 2019; Velez, 2019; Yang et al., 2020; Badawy, 2021; Navarro & Sutton, 2021; Perols & Murthy, 2021) التي تناولت **دراسة إدراك وتصور وفهم المستثمرين وخاصة غير المحترفين منهم** تجاه إطار إعداد تقارير الأمن السيبراني الذي طوره المعهد الأمريكي للمحاسبين القانونيين المعتمدين (AICPA)، **وتوفيره** لغة مشتركة يمكن لأصحاب المصلحة استخدامها لتقييم موقف الأمن السيبراني للشركة وفعالية برنامج إدارة المخاطر الخاص بها. **وعلى الرغم من وجود هذا الإطار، فإنه لا يُعرف الكثير** عن تصورات وإدراكات المستثمرين وفهمهم وخاصة غير المحترفين منهم ومدى تأثيرها على قراراتهم وأحكامهم وفق جودة المعلومات المتوافرة والوعي بالأمن السيبراني والثقة في عملية صنع القرار، وبما يعمل على تعزيز مستوى الشفافية وتقليل مستوى عدم تماثل المعلومات ، وزيادة الثقة والرغبة في الاستثمار في أسهم تلك الشركات.

وبناءً على ذلك، تتمثل مشكلة البحث في الإجابة عن الأسئلة التالية؛ هل يؤثر الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني وقيام مراقبي الحسابات بالتوكيد عليه على رغبة المستثمرين وقراراتهم بالاستثمار بالأسهم ؟ وهل يختلف هذا التأثير باختلاف مستوى خبرة المستثمر وتأهيله العلمي المستمر؟

3- هدف البحث

يهدف البحث إلي دراسة واختبار **أثر التوكيد على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين بالأسهم** في بيئة الأعمال والممارسة المهنية المصرية، وكذلك اختبار أثر كل من مستوى **الخبرة والتأهيل العلمي** للمستثمر كمتغيرين معدلين للعلاقة.

4 – أهمية البحث ودوافعه

تنبع **أهمية البحث أكاديميًّا** من مسايرته لتوجهات واهتمامات الأكاديميين ووسائل الإعلام وواضعي معايير المحاسبة وشركات المحاسبة الكبرى والجمعيات المهنية **بقضايا** المحاسبة المتعلقة بحوكمة الأمن السيبراني وإدارته وإفصاحاته ومحتواها المعلوماتي. **علاوة** على خدمات **التوكيد** على تقارير إدارة مخاطر الأمن السيبراني وكيف ينظر إليها المستثمرون عند اتخاذ قرارات الاستثمار، ومعرفة كيف تدير الشركات أعمالها على الشبكات وفي السحابة وما تواجهه من مخاطر أمنية قد تؤدي إلى خسائر مالية ضخمة وفقد السمعة.

ويستمد البحث أهميته **العلمية من كونه يتناول قضية مهنية لم تلق البحث الكافي في مصر، ويعمل على توجيه الممارسة المهنية نحو الاهتمام** بقضايا الأمن السيبراني والتي يمكن أن تؤثر في النهاية على سلامة **وموثوقية** التقارير المالية وجودة عملية المراجعة، وكذلك قيمة التوكيد على إفصاحات وإدارة 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 الاستثمار في أسهم الشركات.

ويكتسب البحث أهميته **مهنيًّا** من خلال تقديمه **دليلًّا** على أهمية وقيمة خدمة التوكيد على إفصاحات وإدارة مخاطر الأمن السيبراني، والذي يتطلب تدخلاً تنظيميًّا لتلك الخدمة المهنية الجديدة، ويتطلب من المهنيين توافر الكفاءات اللازمة لتوفير هذه الخدمة المهنية الجديدة.

5 – حدود البحث

يتحدد نطاق البحث بدراسة واختبار التوكيد المهني على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين بالأسهم، وبالتالي يخرج عن نطاق البحث دراسة واختبار التوكيد

المهني على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على متغيرات أخري بخلاف رغبة وقرارات المستثمرين بالأسهم (مثل قرار منح الائتمان)، كما يقتصر البحث على اختبار **أثر بعض المتغيرات المعدلة للعلاقة (خبرة المستثمر وتأهيله)** بخلاف المتغيرات الأخري **(مثل نوع المستثمر، العمر، الجنس، وتوقيت نشر تقرير التوكيد)**، كما إنه لن **يتطرق** البحث إلي **بدائل الرأي** في تقرير مراقب الحسابات وبدائل التقرير المعدل على رغبة وقرارات المستثمرين بالأسهم. **وأخيرًا** فإن قابلية نتائج البحث للتعميم ستكون مشروطة بضوابط اختيار عينة البحث.

6- منهجية البحث

لتحقيق هدف البحث والإجابة على تساؤلاته فإن الباحث يعتمد على **دراسة نظرية وأخرى تجريبية،** حيث تعتمد الدراسة **النظرية** على **تحليل** الدراسات السابقة والإرشادات المهنية والخاصة بقضايا **الأمن السيبراني** وإداراتها وإفصاحاتها **وخدمات التوكيد** عليها وأثرها على قرارات وأحكام المستثمرين والثقة والرغبة في الإستثمار في أسهم الشركات، إضافة لاشتقاق فروض البحث. ثم ينتقل البحث إلي شقه **التطبيقي** لاختبار فروض الدراسة من خلال عينة من أمناء ومديري الاستثمار بمصر. **ويمر** المشاركون بالحالة التجريبية بمرحلتين المرحلة الأولي تقديم القوائم المالية **وتقرير** إدارة مخاطر الأمن السيبراني **دون** تقرير خدمة توكيد من قبل مراقب الحسابات ويطلب منهم الإجابة عن بعض الأسئلة وتقديم أحكامهم المهنية بشأن الاستثمار في أسهم الشركة **وتوقعاتهم** بشأن سعر سهم الشركة. ثم في المرحلة التالية يتم تقديم القوائم المالية وتقرير إدارة مخاطر الأمن السيبراني **وتقرير** خدمة توكيد على إفصاحات وإدارة مخاطر الأمن السيبراني من قبل مراقب الحسابات ويطلب منهم الإجابة عن بعض الأسئلة **وتقديم** أحكامهم المهنية بشأن الاستثمار في أسهم الشركة **وتوقعاتهم** بشأن سعر سهم الشركة في ضوء **المعلومات الجديدة.**

7- خطة البحث

تحقيقاً لهدف البحث يقترح الباحث تقسيم باقي أجزاء البحث كما يلي:

7-1 الإطار النظري للبحث

7-1-1 الأمن السيبراني وعمليات إدارة المخاطر.

7-1-2 الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني.

7-1-3 التوكيد المهني على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني.

7-1-4 تحليل العلاقة بين التوكيد المهني على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني ورغبة وقرارات المستثمرين في الأسهم واشتقاق فروض البحث.

7-2 نموذج ومنهجية الدراسة التجريبية.

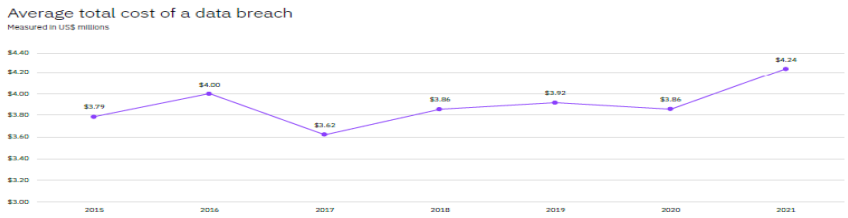
7-3 نتائج البحث والتوصيات ومجالات البحث المقترحة.

7-1 الإطار النظري للبحث

7-1-1 الأمن السيبراني وعمليات إدارة المخاطر

يُعرِّف الاتحاد الدولي للاتصالات The International Telecommunications Union (ITU) **الأمـن** السيبراني بأنه " مجموعة من الأدوات والسياسات والمفاهيم الأمنية وضمانات الأمن والمبادئ التوجيهية وأساليب إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمان والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمة والمستخدمين" (Walton et al., 2021; ITU, 2008). **ويُعرِّف** Dunn-Cavelty (2010) **الأمن** السيبراني بأنه يتعلق بانعدام الأمن الناتج عن الفضاء السيبراني وحول الممارسات التقنية / غير التقنية لجعلها (أكثر) أمنا. **وتشير** هذه التعريفات إلى أن الأمن السيبراني يتضمن عمومًا بعدين: الحماية والتهديدات. تؤكد الحماية الآليات التي تحمي من الاستخدام أو التعديل أو الاستغلال غير المصرح به، بينما تركز التهديدات على محددات الانتهاك (على سبيل المثال، الأصول ذات القيمة، وثغرات البنى التحتية، والرقابة الداخلية الضعيفة) وعواقب الانتهاك (على سبيل المثال، خسائر المنظمة والمستخدمين) (Walton et al.,2021). **ووفق** ISO/IEC 27032:2012 **يُعرف** الأمن السيبراني بأنه الحفاظ على سرية وسلامة وتوافر المعلومات في البيئات المعقدة الناتجة عن تفاعل الأشخاص والبرامج والخدمات على الإنترنت باستخدام أجهزة التكنولوجيا والشبكات المتصلة (Lee, 2021).

ووفقًا لتقرير دراسة تكلفة انتهاك وخرق البيانات الصادرة عن معهد بونيمون IBM Security and the Ponemon Institute، فقد وصلت التكلفة إلى 4.24 مليون دولار لكل حادثة في عام 2021 ، وهي الأعلى منذ 17 عامًا، وكان متوسط تكلفة اختراق البيانات في عام 2020 هو 3.86 مليون دولار، ويُظهر التقرير انخفاضًا بنسبة 1.5٪ في التكاليف عن عام 2019 والتي **بلغت** 3.92 مليون دولار، بزيادة 1.6 بالمائة عن عام 2018[1] (IBM Corporation ,2021).



1 المصدر : available at: https://www.ibm.com/security/data-breach

ووفقًا لتقرير معهد بونيمون Ponemon Institute، فإن **الأسباب** الخمسة الأولى لارتفاع تكلفة انتهاكات وخروقات البيانات في الولايات المتحدة هي مشاركة طرف ثالث، والترحيل الشامل للبيانات إلى السحابة، وعدم الامتثال لخصوصية البيانات، والاستخدام المكثف لمنصات الهاتف المحمول، والأجهزة المفقودة أو المسروقة، كما حدثت العديد من خروقات البيانات البارزة في السنوات الأخيرة، بما في ذلك الانتهاكات التي تم الإعلان عنها كثيرًا مثل (e.g.:Equifax Inc., Facebook, Inc., Exactis LLC, and Under Armour, Inc) (Walton et al., 2021).

وفي هذا **الصدد** تناولت عدة دراسات (e.g.: Khari et al.,2017; Ettredge et al., 2018; Ghadge et al., 2019; Calliess & Baumgarten, 2020; Rea-Guaman et al., 2020; Wang et al., 2020; Armenia et al., 2021;Kaur & Ramkumar, 2021; Lallie et al., 2021; Li & Liu,2021) **التهديدات** السيبرانية وتصنيفاتها المختلفة وآثارها سواء أكانت ضد الأفراد أم المنظمات والممتلكات والمجتمع، وسواء تأتي التهديدات من الخارج (حيث يستخدم مجرمو الإنترنت الإنترنت لإطلاق حملات البرامج الضارة والهندسة الاجتماعية) أو تأتي التهديدات أيضًا من البيئة الداخلية(وتشمل الاحتيال والتخريب وسرقة الملكية الفكرية وانتهاك حقوق الطبع والنشر)، إلا أنها تتوافق مع تقسيمات المسح الوطني لأمن الكمبيوتر (NCSS) The National Computer Security Survey ، الذي شارك في رعايته مكتب إحصاءات العدل والشعبة الوطنية للأمن السيبراني the Bureau of Justice Statistics and the National Cyber Security Division (NCSD) بوزارة الأمن الداخلي الأمريكية، بثلاثة أنواع عامة من التهديدات السيبرانية:

•**الهجمات السيبرانية** Cyber attacks: هي الجرائم التي يكون نظام الكمبيوتر هو الهدف. تتكون الهجمات الإلكترونية من فيروسات الكمبيوتر (بما في ذلك الفيروسات المتنقلة وأحصنة طروادة) وهجمات رفض الخدمة والتخريب الإلكتروني المتعمد (Trojan horse, Worms, Denial of service, logical bomb, Abuse tools, Sniffer, Send spam, and Botnet)

• **الجريمة السيبرانية** Cyber Crime: تشمل الجرائم التي يتم فيها استخدام الكمبيوتر لسرقة المال أو الأشياء الأخرى ذات القيمة. وتشمل الغش والاحتيال والتزوير وسرقة الملكية الفكرية وسرقة بطاقات الائتمان وفقد السجلات الطبية وسرقة البيانات الشخصية أو المالية وكسر كلمات المرور وانتحال البريد الإلكتروني (online fraud, and online forgery, theft of intellectual property, stolen credit cards, lost medical records, unauthorized access and theft of business information, Password sniffing, e-mail spoofing, computer sabotage)

• **حوادث أمان الكمبيوتر** الأخرىOther computer security incidents : تشمل الإرهاب والتخريب السيبراني والحروب السيبرانية وبرامج التجسس وبرامج الإعلانات المتسللة والقرصنة والتصيد الاحتيالي والانتحال وفحص المنافذ، بغض النظر عما إذا كان الاختراق ناجحًا أم لا. (Cyber Terrorism and Cyber Vandalism Cyber War, Cyber Espionage ,spyware, adware, hacking, phishing, spoofing, pinging, port scanning)

ومما سبق **يتضح** أن مخاطر الأمن السيبراني هي ظاهرة جديدة ناشئة عن تبني التكنولوجيا على نطاق واسع وتزايد الانتهاكات بوتيرة أعلى مع اعتماد التكنولوجيا. ليس للتكنولوجيا في حد ذاتها دور في خرق الأمن السيبراني، ولكن لدى الإنسان دافع متأصل للغش باستخدام التكنولوجيا عندما تكون هناك فرصة لجني عوائد، كما تحدث مخاطر الأمن السيبراني لأن المؤسسات غالبًا ما تكون غير قادرة على ضمان مجموعة مناسبة من الأدوات والتقنيات والتدريب وأفضل الممارسات لحماية الشبكات والأجهزة والبرامج والبيانات من الوصول غير المصرح به. ولقد نمت الهجمات والتهديدات السيبرانية بسرعة من حيث الحجم والنطاق والتطور. كما إنها تتعلق بالنظام البيئي بأكمله، سواء أكانت دولًا أم أفرادًا أو شركات، وسواء أكانت داخلية / خارجية، وعامة / خاصة، ومدنية / عسكرية، وعلنية / سرية لتحقيق أهداف محددة.

وفيما يتعلق بنهج إدارة المخاطر السيبرانية، تعتبرإدارة المخاطر السيبرانية عملية مرتبطة بإستراتيجية بقاء حاسمة حاليًا لاستمرارية الأعمال(Armenia et al., 2021). يجب أن يعتبر المالكون والمديرون مخاطر الأمن السيبراني على أنها مخاطر أعمال مهمة على نفس مستوى المخاطر التشغيلية والمالية ومخاطر السمعة مع وجود معايير القياس المناسبة والنتائج التي تتم إدارتها ومتابعتها (Jr& Arnold, 2019).

وبشكل عام، من المعروف جيدًا أن إدارة مخاطر الأمن السيبراني لها أهمية حاسمة، ولكن لا يزال التركيز الأساسي **موجهًا** إلى الحلول التكنولوجية بسبب النمو السريع للحوادث السيبرانية في جميع أنحاء العالم، ومع ذلك ، يؤكد الباحثون والممارسون الآن على النهج **غير التقني** كإجراء إضافي للتغلب على الآثار المنتشرة لحوادث الأمن السيبراني. يُعد الحل التقني لخرق الأمن السيبراني أحد طرق تقليل عدد أحداث المخاطر. ومع ذلك، لا توجد تقنية مثالية لأن اكتشاف التهديدات أمر صعب للغاية حيث لا يمكن لمستخدمي النظام أو المشغلين التنبؤ مسبقًا بالثغرات التي سيتم اختراق نظام الأمان من خلالها. ومع ذلك ، تؤكد بعض المؤسسات بشكل أساسي على الحماية التقنية مثل **التحكم في البوابة وتشفير البيانات وحماية مواقع الويب وإدارة السحابة والذكاء الاصطناعي وتتبع البرامج الضارة واكتشاف برامج التجسس والحماية من التصيد الاحتيالي.** عادةً ما تشترك المؤسسات مع موردي الجهات الخارجية للأمان التقني (e.g., Securelink Norton, Kaspersky, Backbase, Apex banking software,

(Uddin et al., 2020) Innovatrics). **لذلك**، تحتاج المؤسسات إلى النظر في كل من الحلول التقنية والأساليب الإدارية للتحكم في وإدارة مخاطر الأمن السيبراني(Lee, 2021).

وخلال مراحل إدارة مخاطر الأمن السيبراني تحتاج المنظمات لإطار عمل لإدارة تلك المخاطر. **يوجد حاليًا** عدد كبير من أُطر[2] الأمن السيبراني (e.g., NIST Cybersecurity Framework;ISO/IEC 27001; Control Objectives for Information and Related Technology (COBIT); ANSI/ISA-62443-3-3 (99.03.03)-2013); the Cyber Kill Chain® framework) (Lee, 2021).

وفي **تحليله لتلك الأُطر أشار** Lee (2021) إلى أنه في حين أن هذه الأُطر المعروفة توفر إرشادات نوعية عالية المستوى للمديرين، إلا أن أيًا من هذه الأطر لا يقدم رؤية متوازنة لإدارة المخاطر السيبرانية، فهي لا تتناول صراحة نظام الأمن السيبراني وتأثيراته على إدارة المخاطر، كما أنها لم **تعكس** بشكل كامل الجوانب البشرية للمخاطر السيبرانية مثل الأخطاء البشرية والتهديدات الداخلية علاوة على ذلك، لا تقدم أطر العمل أي إرشادات حول كيفية قياس المخاطر من الناحية الكمية وكيف يمكن تبرير الاستثمار في الأمن السيبراني. لذلك ، يُترك المديرون لتطوير مشاريع الأمن السيبراني دون فهم قضايا الأمن السيبراني على المستوى الكلي التي تحدث في النظام البيئي السيبراني وبدون أساليب تقييم المخاطر الكمية لتحليل الاستثمار المالي الكافي.

---

[2] **في هذا الإطار**، تم تصميم عدد من الأُطر المحددة خصيصًا للتعامل مع بيئات رقابية وصناعات معينة، والتي يمكن أن تكون قابلة للتطبيق على المنظمات المختلفة منها (Jamison et al.,2018, COSO,2019):

- **NIST CSF و NIST SP 800-53**: وتم نشر النسخة الأولى من إطار عمل تحسين الأمن السيبراني للبنية التحتية NIST CSF في عام 2014.
- **ISO / IEC 27001**: نشرت ISO و IEC معيار الأمان 2005:27001 كتحديث لمعيار 2005:27001.
- **CIS Top 20**: والتي نشرها مركز أمن الإنترنت (CIS)The Center for Internet Security.
- **HIPAA و HITECH**: قانوني التأمين الصحي وتكنولوجيا المعلومات الصحية The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical .Health Act (HITECH)
- **COBIT.5** : طورت ISACA النسخة الأصلية الصادرة Control Objectives for Information and Related Technologies (COBIT) in 1996.
- **FFIEC CAT** و **FDIC InTREx** : والصادر عن FFIEC في عام 2014.
- **PCI DSS. PCI DSS** عبارة عن مجموعة محدثة باستمرار من معايير أمان المعلومات التي يفرضها مجلس the Payment Card Industry Security Standards Council.
- **AICPA**: تم تقديم إطار إعداد تقارير إدارة مخاطر الأمن السيبراني من قبلAICPA.

وفي **ضوء** التقييم السابق لأُطر عمل إدارة المخاطر السيبرانية **اقترح** Lee (2021) إطار عمل لإدارة المخاطر السيبرانية مع التركيز على النظام البيئي السيبراني الكلي وتقدير المخاطر السيبرانية. يُصنّف الإطار المقترح العوامل التي تؤثر على المخاطر السيبرانية إلى أربعة مستويات، كل منها مخصص لوظائف ومسؤوليات محددة تتعلق بإدارة المخاطر السيبرانية. ويتكون ذلك الإطار من مستوى النظام السيبراني، ومستوى البنية التحتية السيبرانية، ومستوى تقييم المخاطر السيبرانية، ومستوى الأداء السيبراني(Lee,2021).

- **The cyberecosystem:** يركز النظام السيبراني على فهم أصحاب المصلحة في البيئة التنظيمية والذين قد تختلف أهدافهم ومصالحهم (مثل: شركاء سلسلة التوريد والعملاء والمتسللين / المخترقين والوكالات التنظيمية ومطوري التكنولوجيا والاستشاريين في المجال السيبراني).
- **The cyber infrastructure:** يركز على فهم العناصر داخل المنظمة مثل المنظمة والموظفين / المستخدمين الداخليين والتقنيات السيبرانية التي تتفاعل مع عناصر كل من النظام السيبراني وتقييم المخاطر السيبرانية.
- **The cyber risk assessment:** يتم تحديد المخاطر السيبرانية وتقديرها وقياسها واتخاذ قرارات الاستثمار/ الإنفاق للتخفيف من المخاطر السيبرانية.
- **The cyber performance:** يتم تنفيذ خطط الاستثمار ومراقبة التهديدات السيبرانية ذات الأولوية وإجراء تحسينات مستمرة.

وفيما يتعلق بمراحل الإدارة الفعالة لمخاطر الأمن السيبراني فقد تناولت إرشادات مهنية ودراسات عدة تلك المراحل (e.g: AICPA,2017a; AICPA,2017b; COSO,2019; Eaton et al.,2019; Ghadge et al., 2019;Yang et al.,2020; Armenia et al., 2021)، فقد حددت دراسة Eaton et al.(2019) المراحل الفعالة لإدارة مخاطر الأمن السيبراني وفق الإرشادات الصادرة عن المجمع الأمريكي AICPA والخاصة بالتقرير والتوكيد على الأمن السيبراني، حيث تشمل (Eaton et al.,2019):

- تحديد مخاطر التعرض للأمن السيبراني وتحديد الأولويات.
- تصميم نظام ضوابط رقابة الأمن السيبراني.
- اختبار الفعالية التشغيلية لضوابط الأمن السيبراني
- إعداد تقارير الأمن السيبراني الخارجية.

- التوكيد على تقارير الأمن السيبراني الخارجية.

و**تعتبر** المراحل الثلاث الأولى أساسية لأي برنامج فعال لإدارة المخاطر، وتمثل المرحلتان الأخيرتان إرشادات من قبل AICPA بشأن إعداد تقارير الأمن السيبراني وتوكيدها، والتي تم تصميمها لمعالجة مخاوف أصحاب المصلحة الخارجيين بشأن إدارة مخاطر الأمن السيبراني للمنظمة التي قامت بالتقرير .**ويجب أن** يوفر إطار العمل(**أيًا** ما كان الإطار المستخدم والطريقة المستخدمة في إدارة مخاطر الأمن السيبراني) لغة مشتركة يمكن لأصحاب المصلحة استخدامها لتقييم موقف الأمن السيبراني للمنظمة وفعالية برنامج إدارة المخاطر الخاص بها، وتلبية توقعات المستثمرين وتوفير الثقة في صنع قرارات الاستثمار.

7-1-2 الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني

أثارت قضايا الأمن السيبراني **اهتمامًا** كبيرًا بين الأكاديميين ووسائل الإعلام والممارسين والمنظمين، والتي يمكن أن تؤثر في النهاية على سلامة وموثوقية التقارير المالية وجودة عملية المراجعة (Ettredge et al. 2018; Calderon & Gao, 2021). و**تُنتج** انتهاكات (أو حوادث) الأمن السيبراني آثارًا اقتصادية سلبية ليس فقط على الشركات، ولكن أيضًا على أصحاب المصلحة (CPA Canada, 2017). ويُطالب أصحاب المصلحة الرئيسيون مثل المستثمرين بمزيد من المعلومات حول مخاطر وانتهاكات الأمن السيبراني للشركات، فضلاً عن كيفية معالجة هذه المخاطر والانتهاكات وعلاجها، ومع ذلك، لا يتوفر سوى قدر محدود من المعلومات حول مسائل الأمن السيبراني الخاصة بالشركات في المواقف التي يحتاج فيها أصحاب المصلحة إلى معرفة وتقييم مخاطر الأمن السيبراني التي تواجهها الشركات، فليس لديهم خيار سوى الاعتماد على إفصاحات الشركات العامة عن مخاطر الأمن السيبراني، بسبب عدم تماثل المعلومات بين الشركات وأصحاب المصلحة (Cheong et al.,2021). **وبدون** الإفصاح الكافي عن المخاطر، لا تستطيع المؤسسات ضمان أفضل شفافية في عملية صنع القرار، ومن الضروري إعلام جميع أصحاب المصلحة بمخاطر التكنولوجيا السيبرانية، والتدابير المتخذة للتخفيف من آثارها، والتقليل من عدم تماثل المعلومات (Uddin et al., 2020).

ففيما يتعلق بالإرشادات المهنية الخاصة بالإفصاح عن مخاطر الأمن السيبراني، **ونظرًا** للآثار المالية والسمعة والآثار القانونية الكبيرة للهجمات السيبرانية، فإن الإفصاح عن مخاطر الأمن السيبراني التي تواجهها الشركات وكيفية إدارة هذه المخاطر أصبح ذا أهمية متزايدة للمستثمرين والحكومات والمستهلكين والبائعين وأصحاب المصلحة الآخرين لإصدار أحكام سليمة (Gao et al., 2020). **أصدرت** لجنة الأوراق المالية والبورصات (SEC)، ومجلس الرقابة على شركات المحاسبة العامة (PCAOB)، والمعهد الأمريكي للمحاسبين القانونيين المعتمدين (AICPA) ، ومركز جودة المراجعة (CAQ) سياسات تتعلق

بقضايا الأمن السيبراني[3]، والتي من المحتمل أن تؤثر على الشركات والتقارير المالية والإفصاحات والتوكيد (Walton et al.,2021) (SEC, 2018; PCAOB ,2018; AICPA ,2017; CAQ,2018).

وفي عام 2011، أصدر قسم تمويل الشركات التابع للجنة الأوراق المالية والبورصات إرشادات الإفصاح (the CF Disclosure Guidance: Topic No. 2). ووفقًا للإرشاد، يجب على الشركات العامة الإفصاح في ملفات SEC الخاصة بها عن مخاطر الهجمات الإلكترونية والانتهاكات إذا كانت مثل هذه الحوادث من بين أهم العوامل التي تجعل الاستثمار في الشركة مخاطرة(SEC, 2011).

وفي فبراير 2018، وبعد خرق وانتهاكات Equifax وقاعدة بيانات EDGAR الخاصة بـ SEC عام 2017، أصدرت هيئة الأوراق المالية والبورصات إرشادات محدثة للشركات العامة لإعداد عمليات الإفصاح عن مخاطر الأمن السيبراني (SEC,2018). وضرورة التزام الشركات بالإفصاح عن مخاطر الأمن السيبراني والانتهاكات المادية والتأثير المحتمل لها، والتأكيد على تطوير سياسات وإجراءات شاملة للأمن السيبراني لتقييم مخاطر الأمن السيبراني بشكل صحيح ومراجعة ضوابط الإفصاح الخاصة بها بشكل دوري، ويجب أن يكون لدى الشركات إجراءات وسياسات قائمة لمنع التداول والمتاجرة الداخلية بناءً على مخاطر وحوادث الأمن السيبراني(Calderon & Gao,2021). كما **يتعيّن** على الشركات مراجعة والتقرير عن المجالات التالية عند تقييم عوامل الخطر المرتبطة بالاستثمارات وحوادث الأمن السيبراني: 1) خطورة وتكرار الحوادث السيبرانية السابقة. 2) احتمال وحجم وقوع حوادث سيبرانية. 3) الإجراءات الوقائية للحد من مخاطر الأمن السيبراني وتكاليفها المقدّرة. 4) مخاطر الأمن السيبراني **المتلازمة** لطبيعة أعمال الشركات وعملياتها. 5) تكاليف الحماية والتغطية التأمينية في حالة وقوع حادث محتمل. 6) الإضرار المحتمل بالسمعة. 7) التكاليف المتعلقة بالإجراءات التنظيمية الجديدة الحالية أو المحتملة والدعاوي القضائية. 8) مخاطر التقاضي وتكاليف المعالجة المتعلقة بحوادث الأمن السيبراني (SEC,2018; Moreira, 2019). **ويجب** على الشركات **تجنب** الإفصاح العام المتعلق بالأمن السيبراني، وتقديم معلومات محددة مفيدة للمستثمرين(Gao et al.,2020).

وهنا، يمكن توضيح الاختلاف بين **إصدار** 2011 **وإصدار** 2018 والخاص بالإفصاح عن مخاطر الأمن السيبراني، حيث شمل الإصدار بعض التعديلات(SEC,2018; Moreira, 2019):

- يجب الإفصاح عن الأهمية النسبية لمخاطر الأمن السيبراني وتأثيراتها اللاحقة.

[3] في المقابل توجد إرشادات خاصة بمخاطر الأمن السيبراني صادرة عن منظمات دولية ، مثل صندوق النقد الدولي (IMF) ، وبنك التسويات الدولية (BIS) ، والبنك الدولي، ومنظمة التعاون الاقتصادي والتنمية (OECD) تتعلق بقضايا الأمن السيبراني وإدارة المخاطر في المؤسسات المالية، ومفوضية الإتصالات الفيدرالية (FCC) the Federal Communications Commission للشركات التي تخضع لولايتها(Uddin et al., 2020 ; Cheong et al.,2021).

- حظر التداول والمتاجرة بناءً على معلومات داخلية.
- الالتزامات التي تفرضها متطلبات الإدراج في البورصة. على سبيل المثال(يتعين على الشركات المدرجة الإفصاح الفوري للجمهور عن أي معلومات جوهرية من المتوقع أن تؤثر على قيمة الأوراق المالية أو تؤثر على قرارات المستثمرين.

وفي ضوء ما سبق، تحتاج الشركات إلى الإفصاح عن مخاطر الأمن السيبراني الجوهرية بما في ذلك آثارها المالية أو المتعلقة بالسمعة أو القانونية، والإفصاح للمستثمرين عن حوادث الأمن السيبراني السابقة ، والإفصاح عن حالات حدوث انتهاك وخرق للبيانات وأسباب وقوعها وآثارها على العمليات. علاوة على ذلك ، يجب على الشركة تقديم معلومات عن حالة **ارتباط** المخاطر الجوهرية للأمن السيبراني بالمنتجات أو الخدمات أو المنافسة أو العلاقة مع العملاء أو الموردين.

وفي عام 2017، طور المعهد الأمريكي للمحاسبين القانونيين المعتمدين (AICPA) في الولايات المتحدة إطار عمل لإعداد التقارير لممارسي CPA يساعد المنظمات على توصيل المعلومات ذات الصلة والمفيدة حول فعالية برامج إدارة مخاطر الأمن السيبراني System and Organization Controls (SOC) for Cybersecurity (SOC for Cybersecurity): **يتضمن** تقرير فحص إدارة مخاطر الأمن السيبراني المكونات الرئيسية الثلاثة التالية: 1) وصف سردي معد من قبل الإدارة لبرنامج إدارة مخاطر الأمن السيبراني، وسياسات الأمان الرئيسية والعمليات التي تم تنفيذها وتشغيلها لحماية أصول المعلومات الخاصة بالمنشأة من تلك المخاطر. 2) تأكيد من الإدارة حول ما إذا كان الوصف مقدمًا وفقًا للمعايير التي طورها AICPA ، وما إذا كانت الضوابط الرقابية داخل البرنامج فعالة لتحقيق أهداف الأمن السيبراني بناءً على المقاييس الرقابية الخاصة بـ AICPA. 3) رأي ممارس CPA حول وصف وتأكيد الإدارة على فعالية الضوابط الرقابية داخل برنامج إدارة المخاطر السيبرانية. أصدر AICPA مثالاً توضيحيًا لتقرير إدارة مخاطر الأمن السيبراني، بما في ذلك معايير تقييم وصف الإدارة وفعالية الضوابط الموضوعة لتحقيق أهداف الأمن السيبراني، مما يوفر نقطة مرجعية مفيدة للإدارة في تصميم و تنفيذ برنامج إدارة مخاطر الأمن السيبراني(CPA Canada, 2018).

وفي عام 2016، أصدر مركز جودة المراجعة (CAQ) التابع لـ (AICPA) منشورًا يشرح دور المراجعين الخارجيين فيما يتعلق بمخاطر الأمن السيبراني للشركات، ويشتمل: مراجعة القوائم المالية ونظم الرقابة الداخلية على التقارير المالية، والإفصاحات (Calderon&Gao,2021). أما مجلس (PCAOB)، فأشار إلي أنه يجب على المراجعين ألا يقوموا فقط بتقييم تأثير الحادث على القوائم المالية للشركة ، ولكن

أيضًا تقييم مخاطر أحداث الأمن السيبراني حتى لو لم تحدث مثل هذه الأحداث بعد (Calderon & Gao, 2021).

ومما سبق يتضح، اهتمام المنظمين وممتهني المهنة وواضعي معايير المحاسبة والمراجعة بشأن إرشادات الإفصاح والتقرير لأصحاب المصلحة عن إدارة مخاطر الأعمال بشكل عام ومخاطر الأمن السيبراني بشكل خاص وتطبيق أفضل الممارسات لتأثيرها على قرارات المساهمين والمستثمرين، وعواقبها المالية السلبية الكبيرة على المؤسسات الإلكترونية. ويعتمد مستوى ونوع الإفصاح على حقائق الشركة وظروفها، بما في ذلك احتمالية الهجمات السيبرانية وحجم تأثيرها على الشركة. والتقرير عن النتائج المحتملة من مخاطر قانونية، وزيادة أقساط التأمين، والإضرار بالقدرة التنافسية للشركة، والتأثير على سعر السهم، وقيمة المساهمين في الأجل الطويل عند تقييم مخاطر الأمن السيبراني. وإن كانت هذه الإرشادات لا تزال قيد التطوير.

وفيما يتعلق بمحددات الإفصاح[4]، فإن عددا محدودا من الدراسات (e.g, Gordon et al.,2006; Brown et al., 2018; SEC, 2018; Walton et al.,2021) التي تناولت محددات الإفصاح عن مخاطر الأمن السيبراني، فمن جانبها أشارت دراسة Walton et al.(2021) إلي أنه على غرار المخاطر الأخرى التي يتم الإفصاح عنها، **يهدف** الإفصاح عن مخاطر الأمن السيبراني إلى تقليل عدم تماثل المعلومات، وخفض التكاليف القانونية وتكاليف السمعة اللاحقة. ومع ذلك ، فإنه في حين أن الشركات مطالبة بتقديم توصيفات نوعية للمخاطر في قسم مناقشات وتحليلات الإدارة (MD & A) في التقارير السنوية، لا يوجد شرط واضح لتقديم تقدير كمي للمخاطر. وبالإضافة إلى ذلك، يحتفظ المديرون بالسلطة التقديرية في تحديد ماذا وكيف يتم الإفصاح عن مخاطر الأمن السيبراني. أما دراسة Gordon et al.(2006) فقد أشارت إلى التأثير الكبير للمنظمين على عملية الإفصاح ، حيث قانون Sarbanes–Oxley act of 2002 (SOX) له تأثير إيجابي على الإفصاح عن أمن المعلومات. **أوضح** (Brown et al. 2018) أن الشركات تُعدل إفصاحاتها اللاحقة لتشمل المزيد من العناصر المتعلقة بالأمن السيبراني إذا تلقى أحد رواد الصناعة أو المنافسين المقربين أو النظراء في الصناعة خطاب تعلق من هيئة الأوراق

[4] في المسح الذي أجرته دراسة Cheong et al.(2021) لإفصاحات عدد من الشركات، قامت بتصنيف إفصاحات مخاطر الأمن السيبراني إلي مجموعات من عوامل الخطر على النحو التالي: التحكم في الحوادث وتخفيف المخاطر، والمخاطر التشغيلية، والمتعلقة بالعميل، والمتعلقة بالتعاقدات، واستمرارية الأعمال، ونظم الدفع، وأمان الشبكات، وموفري البرامج من الجهات الخارجية third–party software providers (TPSPS)) والتوكيد. نقوم بتصنيف كل موضوع خطر داخل كل عامل إلى مكونات الضعف والثغرات الأمنية والرقابة. يمثل مكون الضعف والثغرات الأمنية مخاطر الأمن السيبراني التي تواجهها الشركة (على سبيل المثال ، القرصنة وخصوصية البيانات) ، بينما يشير عنصر الرقابة إلى الضمانات أو الإجراءات المضادة التي تكتشف المخاطر أو تتصدى لها أو تقللها (على سبيل المثال ، السياسات الأمنية والضوابط الداخلية والتنظيم) (Cheong et al., 2021).

المالية والبورصات (SEC) يتعلق بالإفصاح عن مخاطر الأمن السيبراني. وتشير هذه النتائج إلى أن اهتمام المنظمين بالأمن السيبراني يمكن أن يكون آلية رقابية فعالة للغاية في مجالات الإفصاح عن مخاطر الأمن السيبراني.

وفيما يتعلق بالمحتوى المعلوماتي وآثار إفصاحات الأمن السيبراني فقد تناولت العديد من الدراسات (e.g., Berkman et al., 2018; Ettredge et al. 2018; Li et al., 2018; Tan & Yu, 2018;Cheng & Walton, 2019; Frank et al.,2019; Héroux& Fortin,2020; Kelton & Pennington, 2020; Calderon & Gao, 2021; Walton et al.,2021) آثار إفصاحات الأمن السيبراني، على الرغم من وجود آثار عملية كبيرة، تقدم الدراسات أدلة غير حاسمة حول فعالية الإفصاح عن مخاطر الأمن السيبراني. من ناحية أخرى ، قد تؤدي زيادة الإفصاح عن مخاطر الأمن السيبراني إلى تقليل عدم تماثل المعلومات، ويخصص السوق قيمًا أعلى للشركات ذات الجودة العالية والإفصاحات ذات الصلة بالأمن السيبراني.علاوة على ذلك ، توثق الدراسات الارتباط الإيجابي بين الإفصاح عن الأمن السيبراني وجاذبية الاستثمار. في المقابل عندما تفصح الشركة علنًا عن المخاطر المتعلقة بالأمن السيبراني، فإن المخاطر التي تم الكشف عنها قد تجذب المتسللين عن غير قصد إلى أنظمة معلومات الشركة. تجد أن محتوى الإفصاح عن مخاطر الأمن السيبراني مفيد في التنبؤ بحوادث الأمن السيبراني في المستقبل.

وبشكل عام، يُعد الإفصاح عن مخاطر الأمن السيبراني سيفًا ذا حدين لأنه يُمكن أن يقلل من عدم تماثل المعلومات ولكنه يزيد أيضًا من احتمال وقوع حوادث الأمن السيبراني في المستقبل. وبالتالي ، فإن استكشاف تأثير الإفصاح عن مخاطر الأمن السيبراني يمكن أن يزود المنظمين عمليًا برؤى جديدة حول الفعالية والعواقب المحتملة غير المقصودة للإفصاح عن مخاطر الأمن السيبراني، وحول ما إذا كانت القواعد التشريعية الإضافية ضرورية لتشجيع الشركات على الإفصاح أكثر عن مخاطر الأمن السيبراني الخاصة بهم.

7-1-3 التوكيد المهني على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني

تُشير القيمة الاقتصادية **للمراجعة** من جعل المعلومات أكثر موثوقية للمستخدمين (أي الحد من مخاطر المعلومات الخاطئة أو المُحرّفة التي تؤثر على أحكام المشاركين في أسواق رأس المال لجعلها أكثر كفاءة وشفافية) إلى حتمية تطوير وتوسيع **خدمات التوكيد. عرّف** Lessambo, (2018) و Arens et al.,(2016) **خدمات التوكيد** بأنها خدمات مهنية مستقلة تعمل على تحسين جودة المعلومات، أو سياقها، لصانعي القرار. وتشمل **خدمات التوكيد** العديد من مجالات المعلومات، بما في ذلك المجالات غير

المالية والتي من بينها **توكيدات** تكنولوجيا المعلومات، كما تتطلب معايير المراجعة من مراقبي الحسابات فهما لكيفية استخدام الشركة لتكنولوجيا المعلومات **وتأثيرها** على موثوقية القوائم المالية. **ويمكن** لمراقبي الحسابات أيضًا تقديم خدمات استشارية أو **توكيد** على معلومات الأمن السيبراني التي تُعدها الشركة، من خلال تقديم خدمات لمساعدة الشركات على تحديد المجالات الرئيسية لمخاطر الأمن السيبراني، **واكتشاف** الثغرات في العمليات والضوابط الرقابية، وتطوير ضوابط رقابية فعالة، **وأيضًا** يمكن إجراء عملية فحص وفقًا لمعايير التصديق الخاصة بـ AICPA لتقديم تقرير مستقل حول ما إذا كان وصف الإدارة لبرنامج **إدارة** مخاطر الأمن السيبراني يفي بمواصفات إطار عمل تقارير الشركة أم لا ؟ (Tysiac, 2020) .

وبالتالي، يحتاج دور مراقبي الحسابات إلى التكيف أو التوسع في المستقبل نظرًا لسرعة إنشاء المعلومات ونشرها. **هناك** ثلاثة مجالات يمكن أن يساعد فيها المراجعون في تحسين جودة المعلومات: (1) الأرباح غير المتوافقة مع مبادئ المحاسبة المقبولة عموماً Non-GAAP Earnings، (2) تقارير الاستدامة ESG ، و(3) **الإفصاح** عن مخاطر الأمن السيبراني. لتوفير توكيد بشأن هذه الأنواع من المعلومات، تحتاج شركات المحاسبة إلى تحديد الموضوع المناسب للتوكيد، والحصول على الخبرة لتقديم التوكيد، وتطوير عملية التحقق لتوفير التوكيد(Knechel, 2021).

ووفقًا لمركز جودة المراجعة The Center for Audit Quality (CAQ) يشتمل دور **مراقبي الحسابات** على جانبين مهمين: مراجعة القوائم المالية ونظم الرقابة الداخلية على التقارير المالية Internal Control Over Financial Reporting (ICFR)، والإفصاحات. **ويحتاج** مراقبو الحسابات إلى تقييم مخاطر التحريف الجوهري الناتج عن القضايا المتعلقة بالأمن وتأثيره على القوائم المالية وعلى نظم الرقابة الداخلية على التقارير المالية (ICFR) ، كما يحتاج مراقبو الحسابات أيضًا إلى تنفيذ الإجراءات المتعلقة بمعلومات الأمن السيبراني التي تم الإفصاح عنها في القوائم المالية وفي أي مكان آخر. وتعتمد مسؤوليات المراجع على ما إذا كان الإفصاح مدرجًا في القوائم المالية المراجعة أو في أي مكان آخر. فإذا كان الإفصاح في القوائم المالية المراجعة، **يحتاج** مراقب الحسابات إلى إجراءات مراجعة محددة لتقييم ما إذا كانت القوائم المالية ككل معروضة بشكل عادل من جميع الجوانب الجوهرية. أما إذا تم الإفصاح عن معلومات الأمن السيبراني في مكان آخر، يحتاج المراجع إلى قراءة الإفصاح والنظر فيما إذا كانت المعلومات التي تم الإفصاح عنها أو طريقة عرضها غير متوافقة جوهريًا مع الإفصاح الظاهر في القوائم المالية(Calderon & Gao, 2021; CAQ,2016). أما مجلس (PCAOB)، **فأشار** إلي أنه يجب على المراجعين ألا يقوموا فقط بتقييم تأثير الحادث والتحريفات الجوهرية على القوائم المالية للشركة، ولكن أيضًا تقييم مخاطر أحداث الأمن السيبراني حتى لو لم تحدث مثل هذه الأحداث بعد (Calderon & Gao, 2021; PCAOB, 2014).

وفي نفس السياق، أصدر مجلس AICPA إطارًا لإعداد تقارير الأمن السيبراني على مستوى الشركة، لتشجيع الشركات على إيصال جهود إدارة مخاطر الأمن السيبراني إلى أصحاب المصلحة ومن خلالها يقوم الممارس المعتمد CPA بإجراء فحص على برنامج إدارة مخاطر الأمن السيبراني للشركة. يتكون الإطار من **ثلاثة** مكونات: وصف الإدارة لبرنامج إدارة مخاطر الأمن السيبراني للكيان ، وتأكيد الإدارة ، وتقرير الممارس. **المكون الأول** هو وصف سردي لبرنامج إدارة مخاطر الأمن السيبراني للشركة والذي يوفر أساسًا لفهم الطريقة التي تدير بها الشركة مخاطر الأمن السيبراني وضوابطها الرقابية استجابة لتلك المخاطر. **المكون الثاني** هو تأكيد من الإدارة حول ما إذا كان وصف الإدارة مقدمًا بما يتماشى مع معايير الوصف المحددة من قبل AICPA وما إذا كانت الضوابط المنفذة كجزء من البرنامج فعالة في تحقيق أهداف. **المكون الأخير** هو رأي الممارس حول العرض العادل لوصف الإدارة ومدى ملاءمة تصميم ضوابط الرقابة وفعاليتها في تحقيق أهداف الأمن السيبراني (AICPA, 2017a ;Yang et al. 2020; Li et al.(2021)

وفيما يتعلق بالدراسات التي تبحث في دور **مراقبي** الحسابات فيما يتعلق بالتوكيد على برنامج إدارة مخاطر الأمن السيبراني للشركات والآثار المترتبة على أحداث الانتهاك السيبراني الفعلية، **فقد تعددت الزوايا التي تناولت الدراسات هذا الدور** (e.g.: Li, 2017; Yen et al., 2018; Eaton et al., 2019; Moreira, 2019; PCAOB,2019; Rosati et al., 2019; Velez, 2019; Aldorisio, 2020;Rosati et al.,2020; Badawy, 2021; Bao Ngo et al., 2021; Calderon & Gao 2021; Hampton et al., 2021; Knechel, 2021; Li et al.,2021)، **فقد أشارت** دراسة Li, (2017) إلى أنه من المتوقع أن يأخذ مراقبو الحسابات في الاعتبار آثار وقوع حادث سيبراني على نظم الرقابة الداخلية على التقارير المالية ICFR ، مما قد يؤثر على القوائم المالية. يقوم مراقبو الحسابات بفرض رسوم أعلى بعد وقوع حادث سيبراني وتوسيع إجراءات مراجعة ICFR المتعلقة بالأمن وقد ترتبط الحوادث السيبرانية أيضًا بمخاطر التحريف الجوهري. يمكن أن يؤدي وقوع الحوادث السيبرانية إلى زيادة مخاطر الأعمال التجارية للعميل، والتي تشير إلى "خطر تدهور الوضع الاقتصادي للعميل على المدى القصير أو الطويل ".

ومن جهة أخرى تشير نتائج دراسة Rosati et al. (2019) إلى أن الزيادة في **أتعاب** المراجعة في سنة خرق وانتهاك الأمن السيبراني مؤقتة فقط ، وأن المراجعين يدرجون مخاطر الأمن السيبراني في تقييمهم لمخاطر المراجعة حتى قبل وقوع أي حادث، وهو ما يتوافق مع نتائج دراسة Moreira, (2019) بقيام مراقبي الحسابات بزيادة أتعاب المراجعة لتقليل مخاطر المراجعة المرتبطة بحوادث الأمن السيبراني ، وذلك للجهود الإضافية لتقييم الشركة المخترقة، وكذلك نتائج دراسة Yen et al. (2018) من أن أتعاب

المراجعة تكون أعلى بعد حدوث خرق لأمن المعلومات، علاوة على دراسة Bao Ngo et al. (2021) والتي وجدت الدراسة علاقة إيجابية بين أتعاب المراجعة والشركات التي تتعرض للهجوم من خلال الأمن السيبراني بأحجامها المختلفة.

علاوة على ذلك ، توسعت دراسة PCAOB,(2019) في دور مراقبي الحسابات حتى إذا لم يتم تحديد حادثة معينة للأمن السيبراني، فمن المهم أن يظل المراجع متشككًا مهنيًا خلال عملية المراجعة وعليه أن يُناقش مع الإدارة ولجنة المراجعة طبيعة ونوع الإفصاحات التي في القوائم المالية للشركة أو في إيضاحاتها المتممة.

ومن زاوية أخري، Eaton et al. (2019) يمكن لشركات المحاسبة تقديم مهمة توكيد رسمية فيما يتعلق بفعالية برنامج إدارة مخاطر الأمن السيبراني للشركة، ومشاركة تقارير التوكيد علنًا بشرط ألا تكون شركة المحاسبة قد قدمت أي خدمات استشارية لأغراض الاستقلالية.

وجادلت دراسة Velez (2019) بوجوب أن تكون خدمات توكيد إدارة مخاطر الأمن السيبراني أكثر قيمة في الظروف التي تكون فيها الإدارة غير قادرة على تقديم إفصاحات في الوقت المناسب.

ومن زاويتها أشارت دراسة Rosati et al. (2020) إلي أن المراجعين قادرون على معالجة مخاطر الأمن السيبراني والاستجابة لها بشكل كافٍ حتى في حالة عدم وجود متطلبات إفصاح محددة من المنظمين، وتوافق ذلك مع نتائج دراسة Aldorisio (2020) بأن عمليات مراجعة الأمن السيبراني تعمل كمرجعية يمكن للمؤسسات استخدامها للتحقق من سياساتها وإجراءاتها الأمنية، وتقييم ما إذا كانت لديها آليات الأمان المناسبة أم لا مع التأكد أيضًا من امتثالها للوائح ذات الصلة. يساعد ذلك الشركات على اتخاذ نهج استباقي عند تصميم سياسات الأمن السيبراني ، مما يؤدي إلى إدارة تهديدات أكثر ديناميكية.

وفي السياق نفسه، ركزت دراسة على توكيد مراقبي الحسابات على إدارة مخاطر الأمن السيبراني لسلسلة التوريد والقيمة المضافة للمراجعين الذين يقدمون مثل هذا التوكيد،(2021) Hampton et al. ، **وأيدت ذلك دراسة**(2021) Knechel **من** دور المراجعين في تحسين جودة معلومات **الإفصاح** عن مخاطر الأمن السيبراني، بتوفير توكيد بشأن هذا النوع من المعلومات والحاجة لتحديد الموضوع المناسب للتوكيد، والحصول على الخبرة لتقديم التوكيد، وتطوير عملية التحقق لتوفير التوكيد.

ومن **جانبها** وجدت دراسة Calderon & Gao (2021) أن شركات المراجعة تُقيّم مخاطر المراجعة ليس فقط من خلال تقييم حوادث الاختراق السيبراني الفعلية، ولكن من خلال طبيعة ومحتوى الإفصاح عن مخاطر الأمن السيبراني. وأوضحت دراسة Knechel, (2021) أن هناك مزيدا من التطور في العلاقة بين المراجع والعميل حيث يقوم المراجعون بتوسيع توكيداتهم في مجالات أخرى من المنظمة – البيئية

والاجتماعية والأمنية والحوكمة– وأن مراقبي الحسابات يقومون بالفعل بتقييم مخاطر الأمن السيبراني كجزء من المراجعة الأساسية، وقد يمثل الأمن السيبراني توسعًا طبيعيًا لتلك التوكيدات.

كما جادلت دراسة Li et al.(2021) بأن تحليلات البيانات يجب أن تكون جزءًا لا يتجزأ من توكيد الأمن السيبراني وفي اختبار ضوابط الأمن السيبراني. تم تقديم تحليلات البيانات كنهج مناسب تمامًا لتوفير توكيد بشأن الأمن السيبراني.

وفي البيئة المصرية أشارت دراسة Badawy (2021) نظرًا لأن توكيد برنامج إدارة مخاطر الأمن السيبراني له أهمية كبيرة لأصحاب المصلحة في الشركة بشكل عام ، وأن إطار مجلس (AICPA) لإعداد تقارير مخاطر الأمن السيبراني صدر لزيادة ثقة أصحاب المصلحة في قدرة الشركة على إدارة أعمالها.

ومما سبق يتضح اهتمام المنظمات المهنية والدراسات الأكاديمية وأصحاب المصلحة بأهمية ودور مراقبي الحسابات في التوكيد على عمليات إدارة مخاطر الأمن السيبراني وعلى معلومات الأمن السيبراني التي تُعدها الشركة، من خلال تقديم خدمات لمساعدة الشركات على تحديد المجالات الرئيسية لمخاطر الأمن السيبراني، واكتشاف الثغرات في العمليات والضوابط الرقابية، وتطوير ضوابط رقابية فعالة، وأيضًا إجراء عملية فحص لتقديم تقرير مستقل حول ما إذا كان وصف الإدارة لبرنامج إدارة مخاطر الأمن السيبراني يفي بمواصفات إطار عمل تقارير الشركة أم لا.

كما تناولت الدراسات عملية التوكيد على إفصاحات وعمليات إدارة مخاطر الأمن السيبراني **من أكثر من زاوية، منها:** تقييم مخاطر التحريف الجوهري الناتج عن القضايا المتعلقة بالأمن وتأثيره على القوائم المالية وعلى نظم الرقابة الداخلية على التقارير المالية (ICFR)؛ وتنفيذ الإجراءات المتعلقة بمعلومات الأمن السيبراني التي تم الإفصاح عنها في القوائم المالية وفي الإيضاحات المتممة؛ وتقييم مخاطر أحداث الأمن السيبراني حتى لو لم تحدث مثل هذه الأحداث بعد؛ ويجب أن تكون تحليلات البيانات جزءًا لا يتجزأ من توكيد الأمن السيبراني وفي اختبار ضوابط الأمن السيبراني؛ كما يتعلق بفعالية برنامج إدارة مخاطر الأمن السيبراني للشركة ومشاركة تقارير التوكيد علنًا ألا تكون شركة المحاسبة قد قدمت أي خدمات استشارية لأغراض الاستقلالية؛ ويقوم مراقبو الحسابات بزيادة أتعاب المراجعة لتقليل مخاطر المراجعة المرتبطة بحوادث الأمن السيبراني، وللجهود الإضافية لتقييم الشركة المخترقة.

وأيضا أقرت الدراسات بأهمية إطار مجلس AICPA لإعداد تقارير الأمن السيبراني على مستوى الشركة، لتشجيع الشركات على إيصال جهود إدارة مخاطر الأمن السيبراني إلى أصحاب المصلحة ولزيادة ثقتهم في قدرة الشركة على إدارة أعمالها ومخاطرها، وتوفير طريقة موحدة لتقديم معلومات حول مخاطر الأمن السيبراني وتقييم الاستثمارات في التكنولوجيا، ومساعدة الشركات على اتخاذ 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.

7-1-4 تحليل العلاقة بين التوكيد المهني على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني ورغبة وقرارت المستثمرين في الأسهم واشتقاق فروض البحث

اكتسبت قضايا المحاسبة المتعلقة بحوكمة الأمن السيبراني وإدارته وإفصاحاته اهتمامًا من واضعي معايير المحاسبة وشركات المحاسبة الكبرى والجمعيات المهنية، ولكن عددًا محدودًا من الدراسات الأكاديمية التي تناولت الإفصاح عن الأمن السيبراني ومحتواه المعلوماتي وخدمات التوكيد المرتبطة به (Héroux & Fortin, 2020). وتوجد حاجة مُلحة لتحديد قيمة التوكيد على تقارير إدارة مخاطر الأمن السيبراني وكيف ينظر إليها المستثمرون عند اتخاذ قرارات الاستثمار، ومعرفة كيف تدير الشركات أعمالها على الشبكات وفي السحابة وما تواجهه من مخاطر أمنية قد تؤدي إلى خسائر مالية ضخمة وفقد السمعة.

وفي هذا السياق، تعددت الجوانب المختلفة والزوايا التي تناولتها الدراسات الأكاديمية المتعلقة بالإفصاح والتوكيد على عمليات إدارة مخاطر الأمن السيبراني وتأثيراتها وعلاقاتها بقررات وأحكام المستثمرين، فبعض تلك الدراسات تناولت ردود الفعل السوقية والقيم السوقية لإفصاحات وتوكيدات مخاطر وانتهاكات الأمن السيبراني، وأخرى تناولت القيمة الملاءمة لتوكيدات الأمن السيبراني وتوكيدات الرقابة الداخلية على التقارير المالية وتحريفاتها الجوهرية بما فيها مخاطر وأحداث الأمن السيبراني، وأخرى تناولت جهد وأتعاب المراجعة المرتبطة بتوكيدات انتهاكات وحوادث الأمن السيبراني. تُشير الجوانب السابقة لأثر توكيدات وإفصاحات عمليات إدارة مخاطر الأمن السيبراني على قرارات وأحكام المستثمرين.

فمن زاوية ردود الفعل السوقية والقيم السوقية لإفصاحات وتوكيدات مخاطر وانتهاكات الأمن السيبراني، **بعض الدراسات وجدت ردود فعل سلبية** في السوق لانتهاكات وحوادث الأمن السيبراني :.e. g) Gordon et al., 2011; Morse et al., 2011; Pirounias et al., 2014;Hinz et al., 2015; Modi et al.,2015; Amir et al., 2018) **وبعض الدراسات وجدت ردود فعل إيجابية** (e. g.: Brown-Liburd & Zamora ,2014; Cheng et al.,2015;Gordon et al., 2015; Berkman et al.2018;)

فقد أوضحت دراسة Brown-Liburd & Zamora (2014) أيضًا أن وجود تقارير توكيد خارجية له تأثير إيجابي على تقييمات أسعار الأسهم والاستعداد للاستثمار بالتوافق مع نتائج دراسة Cheng et al.(2015).

كما وجدت دراسة Berkman et al.(2018) علاقة إيجابية بين أهمية وملاءمة الإفصاحات السيبرانية والقيم السوقية والوعي بالأمن السيبراني. تظهر الدراسة أيضًا أن الأحداث الأكثر سلبية في عمليات الإفصاح السيبراني مرتبطة بقيم السوق المنخفضة. تتوافق نتائج هذه الدراسة مع نتائج دراسة Gordon et al.(2015) من أن الإفصاح للمستثمرين عن معلومات حول وعي الشركات بالأمن السيبراني يحظى بتقدير إيجابي من قبل السوق.

أما دراسة Amir et al.(2018) فوجدت أن المديرين لديهم دوافع لحجب المعلومات السلبية المتعلقة بالهجمات السيبرانية ، ولا يستطيع المستثمرون اكتشاف معظم الهجمات السيبرانية بشكل مستقل دون التقرير عنها. وجدت الدراسة أيضًا أن الهجمات السيبرانية المحجوبة مرتبطة بانخفاض في قيم الأسهم في الوقت الذي تم فيه اكتشاف الهجوم، وأن المديرين يفصحون عن معلومات حول الهجمات السيبرانية الأكثر خطورة عندما يَشك المستثمرون بالفعل في احتمال حدوث الهجوم بشكل كبير.

وفي البيئة المصرية, هدفت دراسة الرشيدي& السيد (2019) إلى التعرف على طبيعة الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية وعن برنامج إدارة مخاطر الأمن السيبراني في الشركات المصرية المسجلة في قطاع تكنولوجيا المعلومات حيث إنه أكثر القطاعات المعرضة للتهديدات والحوادث السيبرانية وأثره على أسعار السهم وأحجام التداول. أظهرت الدراسة ضعف الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية وعن برنامج إدارة مخاطر الأمن السيبراني في الشركات المصرية المسجلة في قطاع تكنولوجيا المعلومات مقارنة بالشركات الأمريكية وما يحمله ذلك من آثار سلبية على أسعار السهم وأحجام التداول.

ومن زاوية القيمة الملاءمة لتوكيدات الأمن السيبراني، وتوكيدات الرقابة الداخلية على التقارير المالية وتحريفاتها الجوهرية بما فيها مخاطر وأحداث الأمن السيبراني، هدفت دراسة Li et al. (2018) إلى تحديد فائدة الإفصاح عن مخاطر الأمن السيبراني على أنها القدرة على مساعدة أصحاب المصلحة في تقييم إمكانية حدوث أحداث خرق الأمن السيبراني في المستقبل. يُعد فهم المعلومات التي تنقلها عمليات الإفصاح عن مخاطر الأمن السيبراني أمرًا مهمًا لأنه يمكن أن يساعد المستثمرين في تقييم مخاطر الأمن السيبراني للشركة وتزويد صانعي السياسات والمنظمين بمعلومات حول ما إذا كانت القواعد التشريعية الإضافية ضرورية لتشجيع الشركات على الإفصاح أكثر عن مخاطر الأمن السيبراني الخاصة بهم.

ومن جانبها، أوضحت دراسة Yang et al. (2020) أن الإطار الذي طوره المعهد الأمريكي للمحاسبين القانونيين المعتمدين(AICPA) لإعداد تقارير الأمن السيبراني، يمكن للشركات استخدامه للإفصاح عن معلومات مفيدة لأصحاب المصلحة حول برنامج إدارة مخاطر الأمن السيبراني وفعاليته،

وتوفير لغة مشتركة يمكن لأصحاب المصلحة استخدامها لتقييم موقف الأمن السيبراني للشركة وفعالية برنامج إدارة المخاطر الخاص بها. على الرغم من وجود هذا الإطار، لا يُعرف الكثير عن تصورات وإدراكات المستثمرين ومدى تأثيرها على قرارات الاستثمار.

وفي المقابل، أكدت دراسة Rosati et al. (2019) على مسؤولية مراقبي الحسابات على تقديم توكيدات موضوعية ومستقلة فيما يتعلق بجودة التقارير المالية للشركة وهم مسؤولون عن مراجعة القوائم المالية ونظم الرقابة الداخلية على التقارير المالية (ICFR) وعلى هذا النحو ، فهم يقدمون توكيدات لأصحاب المصلحة الخارجيين بشأن جودة وموثوقية المعلومات الواردة في البيانات المالية لعملائها. يجب أن يقوم مراقبو الحسابات بتقييم وفهم نقاط القوة والضعف في تكنولوجيا المعلومات الخاصة بالشركات بعناية وإدراجها في تقييم المخاطر الخاص بهم، كما إن الإفصاح عن حادثة الأمن السيبراني يزيد من المخاطر التي يتعرض لها المراجع الخارجي، ويشير الحادث إلى ضعف في ضوابط تكنولوجيا المعلومات، مما قد يزيد من مخاطر الفشل في نظام التقارير المالية وبالتالي مخاطر المراجعة.

وفي نفس السياق، أوضحت دراسة Rosati et al.(2020) أن حوادث الأمن السيبراني يمكن أن تمثل عوامل خطر كبيرة لجودة التقارير المالية كإشارات على نقاط ضعف الرقابة الداخلية. تدعم أدلة ونتائج الدراسة وجهة النظر القائلة بأن مراقبي الحسابات قد زادوا من وعيهم بمخاطر المراجعة من خلال اختبارات التحقق الجوهرية وجهود المراجعة ووضعوا إجراءات مناسبة للتعامل مع عواقب حوادث الأمن السيبراني.

ومن الزاوية الأخرى، فقد تناولت الدراسات جهد وأتعاب المراجعة المرتبطة بتوكيدات انتهاكات وحوادث الأمن السيبراني، فمن جانبها قامت دراسة Yen et al., (2018) باستخدام حوادث خرق أمن المعلومات التي تم التقرير عنها من 2004 إلى 2013 ، ووجدت أنه تكون أتعاب المراجعة أعلى بعد حدوث خرق لأمن المعلومات. ومع ذلك ، فإن مثل هذا الأتعاب تنخفض في المستقبل عندما يكون لدى منشأة المحاسبة خبرة خاصة بالصناعة، وتجربة أطول مع العميل، ومعرفة أفضل بصناعة وعمليات العميل، وسياسات وإجراءات أمن المعلومات ونقاط الضعف فيها، فإن هؤلاء المراجعين أكثر قدرة على تقييم أمن المعلومات المحتمل تغييره المخاطر التي ينطوي عليها وقوع حوادث خرق أمن المعلومات.

أما دراسة Moreira, G. P. (2019) فأشارت لوجود علاقة إيجابية ومهمة بين التغيير في أتعاب المراجعة في سنة خرق البيانات. يزيد مراقبو الحسابات من أتعاب المراجعة لتقليل مخاطر المراجعة المرتبطة بحوادث الأمن السيبراني ، وكذلك للجهود الإضافية لتقييم الشركة المخترقة.

وبشكل عام، تُشير نتائج Rosati et al. (2020) إلى أن الزيادة في أتعاب المراجعة في سنة الخرق مؤقتة فقط، وأن المدققين يدرجون مخاطر الأمن السيبراني في تقييمهم لمخاطر المراجعة حتى قبل وقوع الحادث. تنعكس مخاطر الأمن السيبراني المرتفعة في نهاية المطاف في ارتفاع أتعاب المراجعة.

ومن جانبها، هدفت دراسة Bao Ngo & Tick (2021) إلى البحث عما إذا كان مراقبو الحسابات يركزون بشكل أكبر على الشركات والأعمال التي تتعرض لهجمات الأمن السيبراني من خلال فرض أتعاب مراجعة أعلى. وجدت الدراسة علاقة إيجابية بين أتعاب المراجعة والانتهاكات باستخدام عينة من 100 شركة عالمية صغيرة ومتوسطة الحجم وكبيرة الحجم. يشير هذا إلى أن مراقبي الحسابات يجدون المزيد من المخاطر ويبذلون المزيد من الجهد أثناء مراجعة الأعمال التي تتعرض لهجمات الأمن السيبراني نتيجة بذل الشركات المتضررة من الأمن السيبراني لإخفاء صعوباتها وتحدياتها عن المستثمرين وأصحاب المصلحة.

وأخيرًا، ربطت دراستا Perols (2019); Perols & Murthy (2021) بين تأثير فحص الإدارة لمخاطر الأمن السيبراني وتوفير خدمة توكيد الأمن السيبراني وفق إطار المعهد الأمريكي للمحاسبين القانونيين المعتمدين (AICPA) الذي اعتُمد مؤخرًا لفحص إدارة مخاطر الأمن السيبراني على إدراك المستثمرين وقراراتهم. **ففي البداية** تم دراسة تأثير عمليات الإفصاح الطوعي وتوفير خدمة توكيد بشكل مشترك أو منفصل مع مراجعة القوائم المالية لفحص إدارة مخاطر الأمن السيبراني على إدراك المستثمرين وقراراتهم ، وما إذا كانت هذه الآثار تختلف عند وقوع حادث أمن سيبراني لاحق. وجدت الدراستان أن الإشارة السلبية لحادث أمن سيبراني لاحق يعكس إدراكات المستثمرين الإيجابية لكفاءة المراجع ويزيد من حساسية المستثمرين تجاه صعوبات الاستقلال المحتملة عندما يتم توفير فحص إدارة مخاطر الأمن السيبراني بشكل مشترك مع مراجعة القوائم المالية ، مما يؤدي إلى إدراك أقل لجودة المراجعة، وإنخفاض رغبة المستثمرين رغبة في الاستثمار مقارنة بفحص إدارة مخاطر الأمن السيبراني بشكل منفصل. **وبعد ذلك** تم دراسة تأثير نوع خدمة توكيد الأمن السيبراني على إدراكات المستثمرين وقراراتهم وما إذا كانت هذه التأثيرات تختلف عند التقرير عن حادث سابق للأمن السيبراني. وجدت الدراستان أن المستثمرين أكثر استعدادًا للاستثمار ولديهم إدراكات أعلى لمصداقية الإدارة عندما تتضمن عمليات الإفصاح الطوعية فحص إدارة مخاطر الأمن السيبراني مقارنةً بخدمة توكيد الأمن السيبراني الأقل شمولاً، وأن اختيار الإدارة للحصول على خدمة توكيد أمن سيبراني أكثر شمولاً له تأثير إيجابي على المستثمرين ، والتي بدورها لها تأثير إيجابي على رغبة المستثمرين في الاستثمار. هذه النتائج مهمة لأن مجالس إدارة الشركات العامة تتطلع بشكل متزايد إلى شركات المحاسبة لتقديم خدمات توكيد الأمن السيبراني. وجدتا أيضًا أن المستثمرين يرون أن فحص إدارة مخاطر الأمن السيبراني توفر جودة توكيد أعلى فيما يتعلق بقدرة المؤسسة ليس فقط

على منع حوادث الأمن السيبراني في المستقبل، ولكن أيضًا للتعافي من حوادث الأمن السيبراني المستقبلية التي لم يتم منعها.

ومما سبق يتضح للباحث من الدراسات السابقة الأتي:

- **بحثت الدراسات السابقة في تأثير** توكيدات وإفصاحات عمليات إدارة مخاطر الأمن السيبراني على قرارات وأحكام المستثمرين **فيما يتعلق بجوانب الاستثمار المختلفة (** ردود الفعل السوقية والقيم السوقية لإفصاحات وتوكيدات مخاطر وانتهاكات الأمن السيبراني، القيمة الملاءمة لتوكيدات الأمن السيبراني وتوكيدات الرقابة الداخلية على التقارير المالية وتحريفاتها الجوهرية بما فيها مخاطر وأحداث الأمن السيبراني، جهد وأتعاب المراجعة المرتبطة بتوكيدات انتهاكات وحوادث الأمن السيبراني**)**.
- يُعد **فحص إدارة مخاطر الأمن السيبراني** تقريرًا تطوعيًّا للاستخدام العام يهدف إلى إفادة مجموعة واسعة من المستخدمين المحتملين بما في ذلك المستثمرين والمديرين والمحللين والمنظمين.
- تُعتبر **خدمة توكيد إفصاحات وإدارة مخاطر** الأمن السيبراني خدمة فريدة وناشئة لها تأثير إيجابي على تصورات وقررات المستثمرين، والتي بدورها تعكس رغبتهم المستثمرين في الاستثمار من عدمه.
- **ضرورة توافر الكفاءات والخبرات** لشركات المحاسبة المطلوبة في مجال توكيد وتقييم فعالية إدارة مخاطر الأمن السيبراني، وتطوير المعارف في نظم الرقابة الداخلية وأمن المعلومات والتقارير.
- **أثارت الدراسات بعض المخاوف** بشأن أهمية معالجة مخاطر الأمن السيبراني في نظم الرقابة الداخلية على التقارير المالية ومراجعة القوائم المالية واحتمال ضعف الاستقلالية مقارنة بقيام مراقبي الحسابات بأداء خدمات توكيد الأمن السيبراني **بشكل مستقل.**
- وجود **عدد قليل من الدراسات** التي قامت باختبار كيفية تأثير خدمة التوكيد في الإطار الصادر عن AICPA على تصورات وقرارات المستثمرين وأحكام التقييم، وثقة المستثمرين تجاه هذا الإطار ونياتهم للاستثمار.
- أنه لكي **يقدم مراقب الحسابات** تقرير توكيد معقولا ويعبر عن رأيه، سيبذل المزيد من الجهود وسيجمع المزيد من الأدلة ويطبق إجراءات اختبار مختلفة، أكثر مما هو مطلوب في حالة عمليات التوكيد المحدودة، بما يقلل من مستوى عدم تماثل المعلومات وتكاليف الوكالة، وسيؤدي ذلك إلى تأثير إيجابي على قرارات المستثمرين ورغبتهم في الاستثمار وتقييم أسهمهم.

بناءً على وجهات النظر السابقة، وتباين النتائج فيما يتعلق بالاتجاه المتزايد من قبل الشركات نحو الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني، وقيام المراجعين بتوفير خدمة توكيد إفصاحات وإدارة

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 الاستثمار في أسهم تلك الشركات، يمكن صياغة **الفرض التالي :**

الفرض الأول H1: يؤثر توكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني معنويًا على رغبة وقرارات المستثمرين في الأسهم في مصر.

ووفقًا للاتجاه البحثي السابق، والاعتقاد بأن قيام مراقبي الحسابات بتوفير خدمة توكيد إفصاحات وإدارة مخاطر الأمن السيبراني بما يعمل على تعزيز مستوى الشفافية وتقليل مستوى عدم تماثل المعلومات بين المديرين وأصحاب المصلحة بشكل عام وعلى قرارات وأحكام المستثمرين المستثمرين بشكل خاص، وزيادة الثقة والرغبة في الاستثمار في أسهم الشركات. فمن جانبها أوضحت دراسة Yang et al. (2020) أن الإطار الذي طوره المعهد الأمريكي للمحاسبين القانونيين المعتمدين(AICPA) لإعداد تقارير الأمن السيبراني، يمكن للشركات استخدامه للإفصاح عن معلومات مفيدة لأصحاب المصلحة حول برنامج إدارة مخاطر الأمن السيبراني وفعاليته، كما يوفر إطار العمل لغة مشتركة يمكن لأصحاب المصلحة استخدامها لتقييم موقف الأمن السيبراني للشركة وفعالية برنامج إدارة المخاطر الخاص بها. على الرغم من وجود هذا الإطار، لا يُعرف الكثير عن تصورات وإدراكات المستثمرين غير المحترفين ومدى تأثيرها على قراراتهم وفق جودة المعلومات المتوافرة والوعي بالأمن السيبراني والثقة في عملية صنع القرار.

وفي هذا **الإطار** فقد تعددت الدراسات (e.g.: Li et al. ,2018; Cheng & Walton ,2019; Frank et al. ,2019;Perols ,2019; Velez,2019; Yang et al., 2020; Badawy ,2021; Navarro & Sutton, 2021; Perols & Murthy, 2021) التي تناولت **دراسة إدراك وتصور المستثمرين غير المحترفين** تجاه إطار إعداد تقارير الأمن السيبراني الذي طوره المعهد الأمريكي للمحاسبين القانونيين المعتمدين (AICPA)، والمردود الإيجابي لهذا الإطار على عملية الاستثمار، والتأثير الإيجابي لجودة المعلومات والوعي بالأمن السيبراني على الاستعداد والنية الاستثمار.

ففي البداية، قدمت دراسة Li et al. (2018) دليلًا على أن الإفصاح عن مخاطر الأمن السيبراني تحتوي على معلومات إضافية ذات قيمة ذات صلة بالمستثمرين في تقييم إمكانية حدوث أحداث خرق الأمن السيبراني في المستقبل، وتزويد صانعي السياسات والمنظمين بمعلومات حول ما إذا كانت القواعد التشريعية الإضافية ضرورية لتشجيع الشركات على الإفصاح أكثر عن مخاطر الأمن السيبراني الخاصة بهم.

أما دراسة (2019) Cheng & Walton فقد حققت في تأثير وتوقيت الإفصاح عن خرق البيانات على تقييمات المستثمرين. استنادًا إلى عينة من 107 مستثمرين غير محترفين من 32 ولاية في الولايات المتحدة، وجدت الدراسة أن تقييم المستثمرين كان سالبًا في حال كانت الشركة هي أول من أفصح عن خرق البيانات وعندما يكون هناك تأخير كبير بين وقت خرق البيانات ووقت الإفصاح العلني.

وفي السياق نفسه، حققت دراسة (2019) .Frank et al في تأثير توكيد الطرف الثالث الطوعي على برنامج إعداد تقارير إدارة مخاطر الأمن السيبراني على جاذبية الاستثمار. افترضت الدراسة أن تضمين توكيد الإدارة فقط سيكون أكثر فعالية في حالة عدم تعرض الشركة لهجوم سيبراني لأن المستثمرين غير المحترفين لن يشككوا في مصداقية الإدارة. أيضًا ، افترضت الدراسة أنه في حالة تعرض الشركة لهجوم سيبراني، فإن توكيد الطرف الثالث سيعزز جاذبية استثمارات الشركة. بشكل عام، فإن تقديم توكيد طرف ثالث بشأن تقارير إدارة مخاطر الأمن السيبراني سيكون له تأثير إيجابي على جاذبية الاستثمار للشركة، لأنه يزيد من موثوقية الإدارة من وجهة نظر المستثمرين. استنادًا إلى عينة من 547 مستثمرًا غير محترف.

وفي الإطار نفسه، قامت دراسة (2019) Perols ووفقًا لإطار مصداقية الإفصاح الإداري management disclosure credibility framework لـ (2004) Mercer بالتأكيد على أن تصورات وإدراكات المستثمرين للتوكيد الخارجي ومصداقية الإدارة تؤثر معًا على أحكام تقييمات المستثمرين، لأن التوكيد الخارجي الذي يدعم الإفصاح الإداري يكون أكثر مصداقية من إفصاحات الإدارة بدون تقارير توكيد خارجية ويقلل من عدم تماثل المعلومات، وله تأثير إيجابي على تقييمات أسعار الأسهم. هناك اختلاف آخر بين سياقات توكيد الويب وتوكيد الأمن السيبراني the web assurance and cybersecurity assurance ، وهو أن المستثمرين غير المحترفين لديهم وعي متزايد بمخاطر الأمن السيبراني لأن حوادث الأمن السيبراني التي تنطوي على سرقة معلومات العملاء الحساسة غالبًا ما يتم الإعلان عنها بشكل كبير وتكون المعلومات الشخصية للمستثمرين غير المحترفين والأجهزة متصلة رقميًا بشكل متزايد وعرضة لذلك، وبالتالي، ستزيد خدمات التوكيد الخارجي من أحكام تقييم المستثمرين ومن الرغبة والاستعداد للاستثمار.

وفي هذا الجانب، قامت دراسة Velez,2019 بالتحقيق في كيفية تأثير خدمة توكيد إدارة مخاطر الأمن السيبراني والقيمة الملاءمة لها على أحكام وقرارات المستثمرين غير المحترفين، عندما يختلف هذا التوكيد مع توقعات المستخدمين أو يتوافق معها، وأيضًا دراسة تأثير توقيت الإفصاح عن خرق الأمن السيبراني في سياق حكم المستثمرين واتخاذهم للقرار، وما إذا كان توكيد إدارة مخاطر الأمن السيبراني يمكن أن يساعد في تخفيف الأثر السلبي للإفصاحات المتأخرة. بشكل عام ، تشير النتائج إلى أن الإفصاح في الوقت

المناسب عن خرق للأمن السيبراني يقلل من المسؤولية ويحسن تقييمات مصداقية الإدارة ويؤدي إلى أحكام تقييم أعلى من جانب المستثمرين، كما أن السوق يتفاعل سلبًا مع تأخر الإفصاح.

بالإضافة إلى ذلك، قدمت دراسة Yang et al. (2020) نموذجًا بحثيًا لتصور وإدراك المستثمرين لإطار إعداد تقارير إدارة مخاطر الأمن السيبراني. افترضوا أن جودة المعلومات والوعي بالأمن السيبراني سيكون لهما تأثير إيجابي على الفوائد المدركة لبرنامج إدارة المخاطر وأن الثقة تتوسط هذه العلاقة وأن الفوائد المدركة للمستثمرين سيكون لها تأثير إيجابي على نيتهم في الاستثمار. بناءً على عينة من 226 مستثمر غير محترف في الولايات المتحدة ، وجدت الدراسة أدلة تؤكد توقعاتها.

علاوة على ذلك، دراسة Navarro & Sutton, 2021 بحثت في كيفية تأثير توكيد إدارة مخاطر الأمن السيبراني الطوعي على أحكام وقرارات المستثمرين غير المحترفين. باستخدام نهج تجريبي، وجدت الدراسة أنه بعد حدوث خرق إلكتروني ، تتلقى الشركات المشاركة سابقًا في توكيد إدارة مخاطر الأمن السيبراني تقييمات أفضل للمستثمرين لمصداقية الإدارة ، وبالتالي تقييمات أعلى للأسهم.

وفي نفس الإطار، قام Perols & Murthy (2021) بالتحقيق في تأثير تقديم خدمة توكيد منفصلة مقابل خدمة توكيد مشتركة على إدارة مخاطر الأمن السيبراني على إدراك المستثمرين وقراراتهم وما إذا كان هذا التأثير سيختلف في حالة وجود جريمة سيبرانية لاحقة. استنادًا إلى عينة من 106 طلاب ماجستير إدارة أعمال في إحدى الجامعات الحكومية الكبرى في الولايات المتحدة، وجدت الدراسة أنه في حالة غياب حادثة الأمن السيبراني اللاحقة، سيزداد توفير خدمات توكيد الأمن السيبراني والمراجعة لنفس الشركة (توكيد مشترك للأمن السيبراني) كفاءة مراقب الحسابات من وجهة نظر المستثمرين ، إلا أنها تقلل من مستوى استقلالية مراقب الحسابات. من ناحية أخرى ، وجدت الدراسة أنه في حالة وقوع حادث أمن سيبراني لاحق، فإن التأثير السلبي على استقلالية المراجع يفوق التأثير الإيجابي على كفاءة مراقب الحسابات من وجهة نظر المستثمرين.

وفي البيئة المصرية، تناولت دراسة Badawy (2021) اختبار وتحليل أثر جودة التوكيد(المقاسة من خلال حجم مكتب المراجعة الذي يوفر هذا التوكيد، مكتب مراجعة ينتمي إلى إحدى مكاتب المراجعة الأربعة الكبار في مقابل مكتب مراجعة آخر بخلاف هذه المكاتب) ومستوى التوكيد (توكيد معقول في مقابل توكيد محدود) على برنامج إدارة مخاطر الأمن السيبراني على رغبة المستثمرين غير المحترفين في الاستثمار وتقييمهم لأسهمهم. ووجدت الدراسة دليلاً على أن لجودة التوكيد المرتفعة ومستوى التوكيد المعقول تأثيرا جوهريا وإيجابيا على رغبة المستثمرين في الاستثمار وتقييمهم لأسهمهم.

بناءً على المناقشة أعلاه، من الواضح أن توكيد الأمن السيبراني له قيمة من وجهة نظر المستثمرين، وسيؤدي ذلك إلى تأثير إيجابي على قراراتهم ورغبتهم في الاستثمار وتقييم أسهمهم. من المتوقع أيضًا أنه لكي يقدم المراجع تقرير توكيد معقولا ويعبر عن رأيه، سيبذل المزيد من الجهود وسيجمع المزيد من الأدلة ويطبق إجراءات اختبار مختلفة **وفق** الإطار الذي طوره المعهد الأمريكي للمحاسبين القانونيين المعتمدين (AICPA) لإعداد تقارير الأمن السيبراني. على الرغم من وجود هذا الإطار، لا يُعرف الكثير عن تصورات وإدراكات المستثمرين غير المحترفين ومدى تأثيرها على قراراتهم وفق جودة المعلومات المتوافرة والوعي بالأمن السيبراني والثقة في عملية صنع القرار، **يمكن صياغة الفرض التالى وفروضه الفرعية كما يلي:**

الفرض الثاني H2: يختلف التأثير المعنوي لتوكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين في الأسهم في مصر باختلاف مستوى خبرتهم العملية وتأهيلهم المستمر.

ومن جانبها أشارت دراسات (شرف، 2015؛ كعموش،2018؛ موسى، 2018؛ محمد، 2020؛ Reimsbach et al.,2018; Hoang & Phang, 2021) إلى أهمية **التأهيل العلمي** لمتخذ القرار بصفة عامة والمستثمر بصفة خاصة في تكوين المعرفة والمهارة لتحسين فهمهم وتقييمهم للمعلومات التي تفصح عنها الشركات وتوكيد مراقب الحسابات عليها وتحسين جودة قرارات الاستثمار، وبالتالي يمكن القول بالتأثير **الإيجابي** للتأهيل العلمي للمستثمر على العلاقة بين التوكيد على عمليات إدارة مخاطر الأمن السيبراني وقرار الاستثمار مقارنة بالمستثمرين غير المؤهلين. كما **خلصت** الدراسات أيضًا إلى اختلاف تأثير **خبرة المستثمر** على قراراته نتيجة للتفاوت في إدراك المستثمرين للمحتوى المعلوماتي لتقرير التوكيد، حيث يختلف رد فعل المستثمر المحترف عن غير المحترف تجاه تقرير توكيد عمليات إدارة مخاطر الأمن السيبراني، وبالتالي يمكن القول بالتأثير الإيجابي لخبرة المستثمر على العلاقة بين التوكيد على عمليات إدارة مخاطر الأمن السيبراني، **وبناءً عليه يمكن اشتقاق الفرضين الفرعيين التاليين:**

فرعي 1(H2a): يختلف التأثير المعنوي لتوكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين في الأسهم في مصر باختلاف مستوى خبرتهم العملية.

فرعي 2(H2b): يختلف التأثير المعنوي لتوكيد على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين في الأسهم في مصر باختلاف تأهيلهم المستمر.

7-2 نموذج ومنهجية الدراسة التجريبية

يستهدف هذا الجزء من الدراسة تناول أهداف الدراسة التجريبية، ومجتمع وعينة الدراسة، ونموذج ومتغيرات الدراسة، بالإضافة إلي التصميم التجريبي والاختبارات الإحصائية اللازمة لإختبار فروض الدراسة.

7-2-1 أهداف الدراسة التجريبية

تهدف الدراسة التجريبية **لاختبار** أثر **التوكيد** المهني على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين في الأسهم، وكذلك اختبار أثر مستوى **التأهيل** العلمي **وخبرة** المستثمرين **كمتغيرين** معدلين للعلاقة محل الدراسة، وذلك قياساً على دراسات (شرف، 2015؛ كعموش،2018؛ موسى، 2018؛ الصيرفي، 2019؛ عبدالرحيم،2020؛ محمد، 2020؛ Li,2017;Perols ,2019; Vekez,2019; Badawy,2021 ;Navarro & Sutton,2021; Perols & Murthy, 2021)

7-2-2 مجتمع وعينة الدراسة ومصادر الحصول على البيانات

يتمثل مجتمع الدراسة من **المستثمرين في الأسهم** ويمثلهم أمناء الاستثمار ببعض البنوك التجارية ومعاونوهم ومديرو الاستثمار بصناديق الاستثمار بالأسهم، والمحللون الماليون في شركات السمسرة وتداول الأوراق المالية، وقد تم توزيع الحالات التجريبية إلكترونيًا على مجتمع الدراسة من خلال إعداد Google Forms للحالة التجريبية وتوزيعها إلكترونيًا من خلال موقع LinkedIn على عينة الدراسة، ويوضح الجدول التالي عدد الحالات التجريبية الموزعة على عينة الدراسة بالإضافة إلي عدد ونسبة الردود، وكذلك عدد ونسبة الردود السليمة والخاضعة للتحليل الإحصائي:

جدول 1: عدد الحالات التجريبية ونسبة الردود عليها

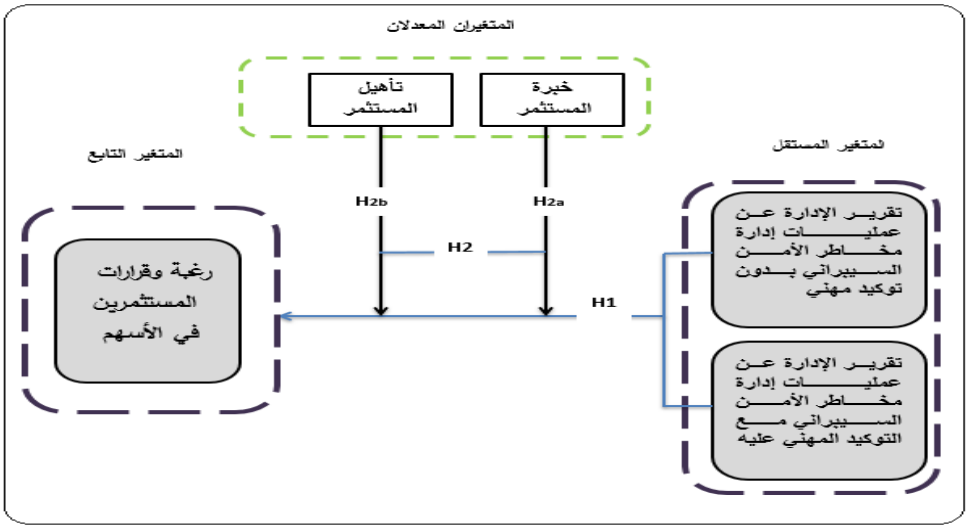
البيان	عدد الحالات التجريبية الموزعة	عدد الحالات التجريبية المستلمة	نسبة الردود على الحالات المستلمة إلي الموزعة	عدد الردود الصادقة	نسبة الردود الصادقة إلي الردود السليمة
عينة المستثمرين	100	58	58%	51	87.93%

7-2-3 نموذج الدراسة وتوصيف وقياس متغيرات الدراسة

يعرض الباحث فيما يلي نموذج الدراسة وتوصيف وقياس متغيرات الدراسة:

7-2-3-1 نموذج الدراسة

يظهر نموذج ومتغيرات الدراسة كما يلي:



شكل 1: نموذج ومتغيرات الدراسة

المصدر: من إعداد الباحث

7-2-3-2 توصيف وقياس متغيرات الدراسة

أ- **المتغير المستقل: توكيد مراقب الحسابات على إفصاحات عمليات إدارة مخاطر الأمن السيبراني**، وتم ذلك من خلال مقارنة رغبة وقرارات المستثمرين بشأن أسعار الأسهم والاستثمار فيها في ظل عدم وجود خدمة توكيد على إفصاحات عمليات إدارة مخاطر الأمن السيبراني ثم وجود خدمة توكيد عليها بغض النظر عن نوع الرأي أو الاستنتاج في تقرير مراقب الحسابات قياسًا على دراسات (Li,2017;Perols ,2019; Vekez,2019; Badawy,2021 ;Navarro & Sutton,2021; Perols & Murthy, 2021)

ب- **المتغير التابع : رغبة وقرارات المستثمرين في الأسهم**، ويتم قياسه من خلال مقارنة بين حالتي الثبات وعدم الثبات بالنسبة لسعر السهم وتوقع سعر السهم في نهاية الفترة التالية واتخاذ قرار الاستثمار قياسًا على دراسات(موسي، 2018؛ رميلي، 2020؛ عبدالرحيم،2020؛ محمد، 2020).

ج- **المتغيرات المعدلة:**

1- **مستوى خبرة المستثمر:** ويتم قياسه من خلال متغير ثنائي يأخذ القيمة (1) للمشاركين الخبراء إذا كانت المدة التي قضاها المستثمر في ممارسة عمله عشر سنوات فأكثر، والقيمة (صفر) للمشاركين الأقل خبرة إذا كانت أقل من عشرة سنوات. وقد توافق ذلك مع منهجية دراسة (موسي، 2018؛ رميلي،2020؛ محمد، 2020).

2- **مستوى التأهيل العلمي للمستثمر:** وتم قياسه من خلال متغير يأخذ القيمة (1) إذا كان لدي المشارك شهادات مهنية أو دراسات عليا و(صفر) بخلاف ذلك قياسًا على دراسات (شرف، 2015؛ كعموش،2018؛ موسي، 2018؛ رميلي،2020؛ محمد، 2020)، وإن كان تصنيف المستوى العلمي لمقياس ترتيبي يكتنفه بعض القصور والمتمثل في عدم وجود معيار موضوعي لإعطاء درجات محددة لكل مستوى من الشهادات المهنية أو العلمية وفق دراسة كعموش(2018).

7-2-4 التصميم التجريبي

اعتمد الباحث على التصميم التجريبي (2×2×2) قياسًا على دراسات (شرف، 2015؛ كعموش،2018؛ موسي، 2018؛ الصيرفي، 2019؛ عبدالرحيم،2020؛ محمد، 2020؛ Li,2017;Perols ,2019; Vekez,2019; Badawy,2021 ;Navarro & Sutton,2021; Perols & Murthy, 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، وتم تحديد المتغيرات **المعدلة** والتي يُفترض أن تؤثر على العلاقتين محل الدراسة وهما خبرة المستثمر ومستوى تأهيله العلمي.

وقد تم **تصميم** الحالات التجريبية وفق الأقسام التالية:

القسم الأول : البيانات الديموغرافية وخبرة وتاهيل المستثمر.

القسم الثاني: المصطلحات الفنية المستخدمة في الدراسة.

القسم الثالث: الحالات التجريبية، وتتضمن:

- **الحالة التجريبية الأولي** : وتشمل تقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني لشركة مساهمة مقيدة في البورصة المصرية عن سنتي(2019،2020) مرفقا به ملخص للقوائم المالية للشركة وإيضاحاتها المتممة ورأي مراقب الحسابات عليها، ويرافق الحالة التجريبية مجموعة من الأسئلة

للحصول على استجابات المشاركين في التجربة لمتغيرات الدراسة، ومطالبتهم بتوضيح مدي استعدادهم للاستثمار في أسهم الشركة بالإجابة على بعض التساؤلات.

- **الحالة التجريبية الثانية** : وتشمل تقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني لشركة مساهمة مقيدة في البورصة المصرية عن سنتي(2019،2020) مرفقا به تقرير توكيد مقترح على تقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني مع ملخص للقوائم المالية للشركة وإيضاحاتها المتممة ورأي مراقب الحسابات عليها، ويرافق الحالة التجريبية مجموعة من الأسئلة للحصول على استجابات المشاركين في التجربة لمتغيرات الدراسة، ومطالبتهم بتوضيح مدى استعدادهم للاستثمار في أسهم الشركة بالإجابة على بعض التساؤلات.

ولاختبار فرض الدراسة الأول والثاني وفرعياته، تم استخدام التصميم التجريبي التالي **(2×2×2)** للدراسة:

جدول 2: التصميم التجريبي للدراسة

خصائص المستثمر / بدائل الإفصاح والتقرير	مستوى خبرة المستثمر (x1)		مستوى تأهيل المستثمر (x2)	
	مرتفع	منخفض	مرتفع	منخفض
تقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني بدون توكيد مهني	المعالجة (١) الاستعداد للاستثمار والتنبؤ بسعر السهم	المعالجة (٢) الاستعداد للاستثمار والتنبؤ بسعر السهم	المعالجة (٣) الاستعداد للاستثمار والتنبؤ بسعر السهم	المعالجة (٤) الاستعداد للاستثمار والتنبؤ بسعر السهم
تقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني مع تقرير توكيد مهني عليه	المعالجة (٥) الاستعداد للاستثمار والتنبؤ بسعر السهم	المعالجة (٦) الاستعداد للاستثمار والتنبؤ بسعر السهم	المعالجة (٧) الاستعداد للاستثمار والتنبؤ بسعر السهم	المعالجة (٨) الاستعداد للاستثمار والتنبؤ بسعر السهم

ووفق هذا التصميم التجريبي، يوجد 8 معالجات تجريبية كما يلي:

المعالجة (1): مستثمرون ذوو خبرة مرتفعة / يقدم لهم تقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني بدون توكيد مهني لشركة مقيدة في البورصة/ ويطلب منهم تحديد مدى استعدادهم للاستثمار بأسهم الشركة والتنبؤ بسعر السهم.

المعالجة (2): مستثمرون ذوو خبرة منخفضة / يقدم لهم تقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني بدون توكيد مهني لشركة مقيدة في البورصة/ ويطلب منهم تحديد مدى استعدادهم للاستثمار بأسهم الشركة والتنبؤ بسعر السهم.

المعالجة (3): مستثمرون ذوو مستوى تأهيل علمي مرتفع / يقدم لهم تقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني بدون توكيد مهني لشركة مقيدة في البورصة/ ويطلب منهم تحديد مدى استعدادهم للاستثمار بأسهم الشركة والتنبؤ بسعر السهم.

المعالجة (4): مستثمرون ذوو مستوى تأهيل علمي منخفض / يقدم لهم تقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني بدون توكيد مهني لشركة مقيدة في البورصة/ ويطلب منهم تحديد مدى استعدادهم للاستثمار بأسهم الشركة والتنبؤ بسعر السهم.

المعالجة (5): مستثمرون ذوو خبرة مرتفعة / يقدم لهم تقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني مرفق به تقرير توكيد مهني لشركة مقيدة في البورصة/ ويطلب منهم تحديد مدى استعدادهم للاستثمار بأسهم الشركة والتنبؤ بسعر السهم.

المعالجة (6): مستثمرون ذوو خبرة منخفضة / يقدم لهم تقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني مرفق به تقرير توكيد مهني لشركة مقيدة في البورصة/ ويطلب منهم تحديد مدى استعدادهم للاستثمار بأسهم الشركة والتنبؤ بسعر السهم.

المعالجة (7): مستثمرون ذوو مستوى تأهيل علمي مرتفع / يقدم لهم تقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني مرفق به تقرير توكيد مهني لشركة مقيدة في البورصة/ ويطلب منهم تحديد مدى استعدادهم للاستثمار بأسهم الشركة والتنبؤ بسعر السهم.

المعالجة (8): مستثمرون ذوو مستوى تأهيل علمي منخفض/ يقدم لهم تقرير الإدارة عن عمليات إدارة مخاطر الأمن السيبراني مرفق به تقرير توكيد مهني لشركة مقيدة في البورصة/ ويطلب منهم تحديد مدى استعدادهم للاستثمار بأسهم الشركة والتنبؤ بسعر السهم.

ولاختبار الفرض الأول والثاني وفرعياته تم اجراء المقارنات التالية:

المقارنة الأولي: بين المعالجات(1+2+3+4) والمعالجات (5+6+7+8) وذلك لقياس الأثر الإيجابي للتوكيد المهني على تقرير الإدارة على عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارت المستثمرين بالأسهم، وبالتالي اختبار الفرض الأول **H1**.

المقارنة الثانية: بين المعالجات[(1+3) × (5+7) ×(2+4) × (6+8)] وذلك لقياس أثر اختلاف التأثير الإيجابي للتوكيد المهني على تقرير الإدارة على عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارت المستثمرين بالأسهم، باختلاف خبرة المستثمر ومستوى تأهيله معًا وبالتالي اختبار الفرض الرئيسي الثاني **H2**.

المقارنة الثالثة: بين المعالجات[(1×5)] ×[(2×6) وذلك لقياس أثر اختلاف التأثير الإيجابي للتوكيد المهني على تقرير الإدارة على عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارت المستثمرين بالأسهم ، باختلاف مستوى خبرة المستثمر، وبالتالي اختبار الفرض الثاني الفرعي **H2a.**

المقارنة الرابعة: بين المعالجات[(3×7)] ×[(4×8) وذلك لقياس أثر اختلاف التأثير الإيجابي للتوكيد المهني على تقرير الإدارة على عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارت المستثمرين بالأسهم ، باختلاف مستوى تأهيل المستثمر، وبالتالي اختبار الفرض الثاني الفرعي **H2b.**

7-2-5 نتائج الدراسة التجريبية

7-2-5-1 الأساليب الإحصائية المستخدمة لتحليل نتائج الدراسة التجريبية

استخدم الباحث العديد من الاختبارات الإحصائية التي تتفق مع طبيعة بيانات الدراسة التجريبية وفروض البحث، كالأتي:

7-2-5-1-1 اختبارات الاعتمادية والاتساق والاعتدالية Reliability, Validity and Normality Tests

قام الباحث بإجراء مجموعة من الاختبارات للتحقق من مدى إمكانية الاعتماد على البيانات الواردة من المشاركين في الدراسة، وللتحقق من ملاءمة عينة الدراسة والاتساق الداخلي للحالات التجريبية، وتحديد الاختبارات الإحصائية الملائمة لاختبار فروض الدراسة.

واستخدم الباحث 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 قيمًا 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 إلي استقرار المقياس وعدم تناقضه مع نفسه بمعنى أن المقياس يعطي نفس النتائج إذا أُعيد تطبيقه على نفس العينة. ويشير ارتفاع قيمة معامل الاختبار إلى صدق أداة الدراسة وصحة العلاقة السببية بين المتغير التابع والمستقل أي **الصدق** الداخلي internal validity ، وبالتالي إمكانية تعميم النتائج أي **الصدق** الخارجي External validity، وأشارت النتائج لمصداقية كل عنصر من العناصر المكونة لأسئلة الحالات التجريبية لعينة المستثمرين على حدة حيث كان معامل ألفا كرونباخ أكبر من 60% وهي أصغر قيمة مقبولة لمعامل ألفا كرونباخ Cronbach`s Alpha ، كذلك أشار المعامل إلي مصداقية وإمكانية الاعتماد على عناصر الأسئلة ككل حيث كان المعامل لعينة الدراسة78.8% وهو

أكبر من 60% وتقع بين 70% و80% وهو المدى الذي يمثل لأفضل قيمة لمعامل ألفا كرونباخ Cronbach`s Alpha ، ويتضح ذلك من الجدول التالي:

جدول 3: معامل ألفا كرونباخ لعينة الدراسة

N of Items	Cronbach`s Alpha	Sample
10	.788	المستثمرون

كما قام الباحث باستخدام اختبار كا2 (χ2)chi-squar لتحديد مدي معنوية الأسئلة قياسًا على دراسة(موسى، 2018؛ محمد، 2020)، وأظهرت النتائج أن قيمة P – Value أقل من مستوى 5% لمعظم الأسئلة المرافقة للحالات التجريبية، مما يعني **رفض العدم** (القائل بأنه لا توجد اختلافات بين فئات الإجابة) **وقبول الفرض البديل** (القائل بأنه توجد اختلافات بين فئات الإجابة).

7-2-5-1-2 تحديد نوعية الاختبارات التي تناسب بيانات عينة الدراسة

قام الباحث 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، 2015؛ بدوي،2018؛ موسي، 2018؛ محمد، 2020) ويتمثل الفرض العدم والبديل لهذه الاختبارات فيما يلي:

فرض العدم **H0:** 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 4: نتائج اختبارات توزيع بيانات العينة

Tests of Normality

	EXPIN Value	Kolmogorov-Smirnov(a)		Shapiro-Wilk	
		Statistic	Sig.	Statistic	Sig.
Q1	0	.330	.000	.774	.000
	1	.286	.000	.798	.000
Q2	0	.300	.000	.760	.000
	1	.392	.000	.622	.000
Q3	0	.347	.000	.639	.000
	1	.374	.000	.631	.000
Q4	0	.239	.001	.815	.001
	1	.498	.000	.468	.000
Q5	0	.447	.000	.566	.000
	1	.348	.000	.668	.000
Q6	0	.239	.001	.815	.001
	1	.482	.000	.508	.000

Q7	0	.264	.000	.810	.001
	1	.482	.000	.508	.000
Q8	0	.347	.000	.639	.000
	1	.392	.000	.622	.000
Q9	0	.239	.001	.815	.001
	1	.392	.000	.622	.000
Q10	0	.322	.000	.712	.000
	1	.322	.000	.716	.000

a Lilliefors Significance Correction

يتضح من جدول (4) 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 تتراوح بين (0.000) وبين (0.001) **لجميع** المتغيرات محل الدراسة، وهي أقل من مستوى المعنوية (0.05)، وبذلك فإن بيانات عينتي الدراسة لا تتبع التوزيع الطبيعي المعتدل، وبالتالي يتم الاعتماد على **الاختبارات اللامعلمية** لاختبار فروض الدراسة وفق دراسات (شرف، 2015؛ بدوي، 2018؛ موسى، 2018؛ محمد، 2020).

7-2-5-2 نتائج اختبار فروض الدراسة

يعرض الباحث نتائج اختبار فروض البحث، كما يلي:

7-2-5-2-1 نتائج اختبار فرض الدراسة الأول (H1) (التحليل الأساسي)

استهدف الفرض الأول (H1) اختبار **ما إذا كان توكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني يؤثر معنويًا على رغبة وقرارات المستثمرين في الأسهم** في مصر، وقد استخدم الباحث اختبار Wilcoxon Signed Ranks Test لتحديد مدي الاختلاف بين متوسطي عينتين غير مستقلتين، وقد تم صياغة فرض العدم كما يلي:

فرض العدم H0: لا يؤثر توكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارت المستثمرين بالأسهم في مصر.

وبالتالي يكون الفرض الإحصائي لهذا الاختبار كما يلي:

$$H0: M1 = M2$$

$$H1: M1 \neq M2$$

ويشير فرض **العدم** لعدم وجود اختلافات معنوية في ردود المجموعتين في ظل اختلاف تقرير التوكيد الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني، في حين يشير الفرض **البديل** لوجود اختلافات معنوية في ردود المجموعتين في ظل اختلاف تقرير التوكيد على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني، ويتم رفض فرض العدم وقبول الفرض البديل إذا كانت قيمة P–value أقل من أو تساوي 5%، والعكس إذا كانت قيمتها أكبر من 5%، وذلك وفقا لنتائج الاختبار الموضحة في الجدول التالي:

جدول 5: اختبار الفرض الأول H1

Test Statistics

W	Q6 - Q1	Q7 - Q2	Q8 - Q3	Q9 - Q4	Q10 - Q5
Z	-3.636(a)	-4.796(a)	-3.528(b)	-3.668(a)	-3.668(a)
Asymp. Sig. (2-tailed)	.000	.000	.000	.000	.000
a Based on negative ranks.					
b Based on positive ranks.					
c Wilcoxon Signed Ranks Test					

ويتضح من الجدول السابق أن قيمة P–value هي (0.000) أقل من مستوى المعنوية 5% لكل مقارنة سؤال من الأسئلة، مما يعني **رفض** فرض العدم **وقبول** الفرض البديل، **وبالتالي** وجود تأثير **معنوي** لتقرير التوكيد المهني لمراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارت المستثمرين بالأسهم بما **يتوافق** مع نتائج دراسات (Li,2017;Perols ,2019; Vekez,2019 ; Navarro & Sutton,2021; Perols & Murthy, 2021) **بالاتجاه** المتزايد من قبل الشركات نحو الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني، **وقيام** مراقبي الحسابات بتوفير خدمة **توكيد** إفصاحات وإدارة 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 مراقبي الحسابات في التوكيد على عمليات إدارة مخاطر الأمن السيبراني وعلى معلومات الأمن السيبراني التي تُعدها 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)، وأيضًا تقييم مخاطر أحداث 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 **إيجابًا على ثقة ورغبة المستثمرين في الاستثمار في أسهم تلك الشركات.**

ويُظهر الجدول التالي رقم (6) أن الرتب Ranks كانت لصالح الحالة الثانية وهي وجود تقرير توكيد مهني على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني، والذي يعني أن اتجاه الاستجابات هو ضرورة وجود توكيد مهني مع إفصاحات الإدارة عن عمليات إدارة مخاطر الأمن السيبراني للمساعدة على اتخاذ قرارات الاستثمار في الأسهم.

جدول 6: Wilcoxon Signed Ranks Test

		N	Mean Rank	Sum of Ranks
Q6 - Q1	Negative Ranks	5(a)	7.00	35.00
	Positive Ranks	21(b)	15.05	316.00
	Ties	25(c)		
	Total	51		
Q7 - Q2	Negative Ranks	0(d)	.00	.00
	Positive Ranks	23(e)	12.00	276.00
	Ties	28(f)		
	Total	51		
Q8 - Q3	Negative Ranks	22(g)	13.20	290.50
	Positive Ranks	3(h)	11.50	34.50
	Ties	26(i)		
	Total	51		
Q9 - Q4	Negative Ranks	0(j)	.00	.00
	Positive Ranks	17(k)	9.00	153.00
	Ties	34(l)		
	Total	51		
Q10 - Q5	Negative Ranks	0(m)	.00	.00
	Positive Ranks	17(n)	9.00	153.00
	Ties	34(o)		
	Total	51		

ويتضح من تلك الاستجابات أن هناك اهتمامًا من جانب المستثمرين بتوكيد المعلومات المتعلقة بمخاطر الأمن السيبراني لأهميتها في اتخاذ قرار الاستثمار. حيث يعمل التوكيد على تعزيز مستوى الشفافية وتقليل مستوى عدم تماثل المعلومات وقدرة المستثمرين على تقييم أداء الشركة وأدائها المستقبلي والتعامل مع التهديدات والمخاطر السيبرانية واتخاذ قرار الاستثمار المناسب.

7-2-5-2 نتائج اختبار فرض الدراسة الثاني (H2) وفرعياته (التحليل الأساسي)

استهدف الفرض الرئيسي الثاني H2 اختبار ما إذا كان كل من **خبرة ومستوى التأهيل العلمي** للمستثمر كمتغيرين معدلين يؤثران على العلاقة المعنوية الإيجابية بين التوكيد المهني على الإفصاح عن عمليات مخاطر الأمن السيبراني على رغبة وقرارت المستثمرين بالأسهم ، واستخدم الباحث اختبار Wilcoxon للعينات غير المستقلة من خلال التصميم داخل المتغيرات Within groups لاختبار أثر كل من خبرة ومستوى التأهيل العلمي للمستثمر على العلاقة الإيجابية بين التوكيد المهني على الإفصاح عن عمليات مخاطر الأمن السيبراني على رغبة وقرارت المستثمرين بالأسهم ، **ويساعد** هذا الاختبار في تحديد أثر الفروق الطبيعية بين الأقل خبرةً وتاهيلًا والأكثر خبرةً وتأهيلًا، والتي قد تؤدي إلي اختلاف أحكامهم نتيجة تلك العوامل الأخري بخلاف تقرير التوكيد، حيث أن الاختبار القبلي والبعدي هنا يأخذ الفرق على مستوى كل فئة من خلال مقارنة أحكام تلك الفئة بدون تقرير توكيد مقارنة بوجود تقرير توكيد. وتتضح نتائج الاختبار من خلال الجدول التالي:

جدول 7: نتائج اختبار Wilcoxon للعينات غير المستقلة لاختبار الفرض الرئيسي الثاني H2

الفرض		الاختبار الاحصائي	الاختبار المستخدم	N	Z	p-value
H2	يختلف التأثير المعنوي لتوكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارت المستثمرين بالأسهم في مصر باختلاف مستوى خبرتهم العملية وتأهيلهم المستمر	أثر تقرير التوكيد المهني على رغبة وقرارت المستثمرين بالأسهم للمشاركين الأقل خبرة وتأهيلًا	Wilcoxon Signed Ranks Test Q5- Q10	29	1.465	.143
		أثر تقرير التوكيد المهني على رغبة وقرارت المستثمرين بالأسهم للمشاركين الأكثر خبرة وتأهيلًا		22	2.889	.004

وتشير نتائج الاختبار إلي أن المشاركين الأكثر **خبرة وتأهيلًا** يستجيبون بصورة معنوية بمستوى P-value (0.004) وهو أقل من 5% مقارنة بمستوى المعنوية للمشاركين الأقل خبرة وتأهيلًا P-value (0.143) وهو أكبر من 5%، مما يعني أن تقرير التوكيد المهني على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني له مردود إيجابي على المشاركين الأكثر خبرة وتأهيلًا مقارنة بالمشاركين الأقل خبرة وتأهيلًا.

وحاول الباحث التحقق من صدق ومتانة النتائج من خلال إعادة الاختبارات من خلال تقسيم العينة إلي عينتين مستقلتين، واستخدام اختبار **Mann–Whitney Test** لعينتين مستقلتين، وقد تم صياغة فرض العدم كما يلي:

فرض العدم H0: لا يختلف التأثير المعنوي لتوكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارت المستثمرين بالأسهم في مصر باختلاف مستوى خبرتهم العملية وتأهيلهم المستمر.

وبالتالي يكون الفرض الإحصائي لهذا الاختبار كما يلي:

$$H0: M1 = M2$$

$$H1: M1 \neq M2$$

ويشير **فرض** العدم لعدم وجود تأثير معنوي لمستوى **الخبرة والتأهيل** (خبرة وتأهيل منخفض/ خبرة وتأهيل مرتفع) على العلاقة المعنوية الإيجابية بين التوكيد المهني على الإفصاح عن عمليات مخاطر الأمن السيبراني رغبة وقرارت المستثمرين بالأسهم مقارنة بالفرض البديل والذي يشير لوجود تأثير، ويتم رفض فرض العدم وقبول الفرض البديل إذا كانت قيمة P–value أقل من أو تساوي 5%، والعكس إذا كانت قيمتها أكبر من 5%، وذلك وفقا لنتائج الاختبار الموضحة في الجدول التالي:

جدول 8: نتائج اختبار الفرض الرئيسي الثاني H2

Mann-Whitney Test Ranks

	EXP.QUA	N	Mean Rank	Sum of Ranks
Q5	0	29	21.69	629.00
	1	22	31.68	697.00
	Total	51		
Q10	0	29	21.91	635.50
	1	22	31.39	690.50
	Total	51		

Test Statistics

	Q5	Q10
Mann-Whitney U	194.000	200.500
Wilcoxon W	629.000	635.500
Z	-2.445	-2.322
Asymp. Sig. (2-tailed)	.014	.020

a Grouping Variable: EXP.QUA

وقد جاءت نتيجة هذا **الاختبار** (المقارنة الثانية) بوجود تأثير **للخبرة والتأهيل** معًا على العلاقة المعنوية الإيجابية بين التوكيد المهني على الإفصاح عن عمليات مخاطر الأمن السيبراني على رغبة وقرارت المستثمرين بالأسهم، حيث بلغت قيمة P–value للسؤال Q5 والسؤال Q10 (0.014)، (0.020) على التوالي وهي أقل من 5%، مما يعني **رفض فرض العدم وقبول الفرض البديل** بوجود اختلافات معنوية في ردود المجموعتين في ظل اختلاف تقرير التوكيد على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني، تتوافق هذه النتائج مع نتائج دراسة Navarro & Sutton (2021) والتي قدمت أدلة نظرية وتجريبية عن أن قيام الإدارة بالإفصاح عن عمليات إدارة مخاطر الأمن السيبراني وتوكيد مراقب الحسابات عليها ينتج عنها تقييمات أكثر ملاءمة لمصداقية الإدارة ، وتقييمات أعلى لأسعار الأسهم. علاوة على ذلك، توصلت الدراسة إلى أدلة على أن المستثمرين يكافئون الشركات التي تشارك في توفير توكيد مهني لإفصاحات الأمن السيبراني عندما لا يكون من المتوقع وجود هذا التوكيد، كما يعاقب المستثمرون الشركات التي لا تشارك توفير توكيد مهني لإفصاحات الأمن السيبراني عندما يكون التوكيد متوقعًا.

7-2-5-2-1 نتائج اختبار فرض الدراسة الثاني الفرعي (H2a)

استهدف فرض الدراسة الثاني الفرعي H2a اختبار ما إذا كان مستوى **خبرة** المستثمر كمتغير معدل يؤثر على العلاقة المعنوية الإيجابية بين التوكيد المهني على الإفصاح عن عمليات مخاطر الأمن السيبراني ورغبة وقرارت المستثمرين بالأسهم ، واستخدم الباحث اختبار Wilcoxon للعينات غير المستقلة من خلال التصميم داخل المتغيرات Within groups لاختبار أثر خبرة المستثمر على العلاقة الإيجابية بين التوكيد المهني على الإفصاح عن عمليات مخاطر الأمن السيبراني على رغبة وقرارت المستثمرين بالأسهم ، **ويساعد** هذا الاختبار في تحديد أثر الفروق الطبيعية بين الأقل خبرةً والأكثر خبرةً ، والتي قد تؤدي إلي اختلاف أحكامهم نتيجة تلك العوامل الأخري بخلاف تقرير التوكيد، حيث أن الاختبار القبلي والبعدي هنا يأخذ الفرق على مستوى كل فئة من خلال مقارنة أحكام تلك الفئة بدون تقرير توكيد مقارنة بوجود تقرير توكيد. وتتضح نتائج الاختبار من خلال الجدول التالي:

جدول 9: نتائج اختبار Wilcoxon للعينات غير المستقلة

لاختبار الفرض الثاني الفرعي H2a

الفرض		الاختبار الاحصائي	الاختبار المستخدم	N	Z	p-value
H2a	يختلف التأثير المعنوي لتوكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارت المستثمرين بالأسهم في مصر باختلاف مستوى خبرتهم.	أثر تقرير التوكيد المهني على رغبة وقرارت المستثمرين بالأسهم للمشاركين الأقل خبرة .	Wilcoxon Signed Ranks Test Q5- Q10	28	2.236	.025
		أثر تقرير التوكيد المهني على رغبة وقرارت المستثمرين بالأسهم للمشاركين الأكثر خبرة.		23	3.145	.002

وتشير نتائج الاختبار إلي أن المشاركين الأقل والأكثر خبرة يستجيبون بصورة معنوية بمستوى P-value (0.025) و (0.002) على التوالي وهو أقل من 5%، مما يعني أن المستثمرين **الأقل والأكثر** خبرة يرغبون في وجود تقرير توكيد المهني على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني، بما يزيد من مصداقية الإدارة، وتقييم أفضل لأسعار الأسهم نتيجة تعزيز مستوى الشفافية وتقليل مستوى عدم تماثل المعلومات، وإضفاء المصداقية على محتوي تقرير الإدارة عن الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني.

وحاول الباحث التحقق من صدق ومتانة النتائج من خلال إعادة الاختبارات من خلال تقسيم العينة إلي عينتين مستقلتين، واستخدام اختبار **Mann-Whitney Test** لعينتين مستقلتين، وقد تم صياغة فرض العدم كما يلي:

فرض العدم H0: لا يختلف التأثير المعنوي لتوكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارت المستثمرين بالأسهم في مصر باختلاف باختلاف مستوى خبرتهم العملية.

وبالتالي يكون الفرض الإحصائي لهذا الاختبار كما يلي:

$$H0: M1 = M2$$

$$H1: M1 \neq M2$$

ويشير **فرض** العدم لعدم وجود تأثير معنوي لمستوى خبرة المستثمر (خبرة منخفضة/ خبرة مرتفعة) على العلاقة الإيجابية بين التوكيد المهني على الإفصاح عن عمليات مخاطر الأمن السيبراني ورغبة وقرارات المستثمرين في الأسهم مقارنة بالفرض البديل والذي يشير لوجود تأثير، ويتم رفض فرض العدم وقبول الفرض البديل إذا كانت قيمة P–value أقل من أو تساوي 5%، والعكس إذا كانت قيمتها أكبر من 5%، وذلك وفقا لنتائج الاختبار الموضحة في الجدول التالي:

جدول 10: نتائج اختبار الفرض الثاني الفرعي H2a

Mann-Whitney Test Ranks

	Exp.	N	Mean Rank	Sum of Ranks
Q5	0	28	19.21	538.00
	1	23	34.26	788.00
	Total	51		
Q10	0	28	19.46	545.00
	1	23	33.96	781.00
	Total	51		

Test Statistics

	Q5	Q10
Mann-Whitney U	132.000	139.000
Wilcoxon W	538.000	545.000
Z	-3.700	-3.563
Asymp. Sig. (2-tailed)	.000	.000

a Grouping Variable: Exp.

وقد جاءت نتيجة هذا الاختبار(المقارنة الثالثة) **بوجود** تأثير للخبرة على العلاقة المعنوية الإيجابية بين التوكيد المهني على الإفصاح عن عمليات مخاطر الأمن السيبراني على رغبة وقرارت الاستثمار بالأسهم، حيث بلغت قيمة P–value للسؤال Q5 والسؤال Q10 (0.000)، (0.000) على التوالي وهي أقل من 5%، مما يعني رفض فرض العدم وقبول الفرض البديل بوجود اختلافات معنوية في ردود المجموعتين في ظل اختلاف تقرير التوكيد على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني.

7-2-5-2-2 نتائج اختبار فرض الدراسة الثاني الفرعي (H2b)

استهدف الفرض الرئيسي الثاني الفرعي H2b اختبار ما إذا كان كل من **مستوى التأهيل العلمي** للمستثمر كمتغير معدل يؤثر على العلاقة المعنوية الإيجابية بين التوكيد المهني على الإفصاح عن عمليات مخاطر الأمن السيبراني على رغبة وقرارت الاستثمار بالأسهم في مصر، واستخدم الباحث اختبار Wilcoxon للعينات غير المستقلة من خلال التصميم داخل المتغيرات Within groups لاختبار أثر كل

من مستوى التأهيل العلمي للمستثمر على العلاقة الإيجابية بين التوكيد المهني على الإفصاح عن عمليات مخاطر الأمن السيبراني على قرارات وأحكام المستثمرين في الأسهم، **ويساعد** هذا الاختبار في تحديد أثر الفروق الطبيعية بين الأقل تأهيلًا والأكثر تأهيلًا، والتي قد تؤدي إلي اختلاف أحكامهم نتيجة تلك العوامل الأخري بخلاف تقرير التوكيد، حيث إن الاختبار القبلي والبعدي هنا يأخذ الفرق على مستوى كل فئة من خلال مقارنة أحكام تلك الفئة بدون تقرير توكيد مقارنة بوجود تقرير توكيد. وتتضح نتائج الاختبار من خلال الجدول التالي:

جدول 11: نتائج اختبار Wilcoxon للعينات غير المستقلة

لاختبار الفرض الثاني الفرعي H2b

الفرض		الاختبار الاحصائي	الاختبار المستخدم	N	Z	p-value
H2b	يختلف التأثير المعنوي لتوكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارت المستثمرين بالأسهم في مصر باختلاف تأهيلهم المستمر	أثر تقرير التوكيد المهني على رغبة وقرارات المستثمرين في الأسهم للمشاركين الأقل تأهيلًا.	Wilcoxon Signed Ranks Test Q5- Q10	21	2.469	.014
		أثر تقرير التوكيد المهني على رغبة وقرارات المستثمرين في الأسهم للمشاركين الأكثر تأهيلًا.		30	.805	.421

وتشير نتائج الاختبار إلي أن المشاركين الأقل تأهيلًا يستجيبون بصورة معنوية بمستوى P-value (0.014) وهو أقل من 5% مقارنة بمستوى المعنوية للمشاركين الأكثر تأهيلًا (0.421) P-value وهو أكبر من 5%، مما يعني أن تقرير التوكيد المهني على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني **ليس** له مردود إيجابي على المشاركين الأكثر تأهيلًا مقارنة بالمشاركين الأقل تأهيلًا، وتتفق هذه النتيجة مع نتائج دراسة (رميلي، 2020) والتي أشارت **لعدم** وجود تأثير لتأهيل المستثمر على قرار الاستثمار في الأسهم.

وحاول الباحث التحقق من صدق ومتانة النتائج من خلال إعادة الاختبارات من خلال تقسيم العينة إلي عينتين مستقلتين، واستخدام اختبار **Mann-Whitney Test** لعينتين مستقلتين، وقد تم صياغة فرض العدم كما يلي:

فرض العدم H0: لا يختلف التأثير المعنوي للتوكيد على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين في الأسهم في مصر باختلاف تأهيلهم المستمر.

وبالتالي يكون الفرض الإحصائي لهذا الاختبار كما يلي:

$$H0: M1 = M2$$

$$H1: M1 \neq M2$$

ويشير **فرض** العدم لعدم وجود تأثير معنوي لمستوى التأهيل(تأهيل منخفض/ تأهيل مرتفع) على العلاقة الإيجابية بين التوكيد المهني على الإفصاح عن عمليات مخاطر الأمن السيبراني ورغبة وقرارات المستثمرين في الأسهم مقارنة بالفرض البديل والذي يشير لوجود تأثير، ويتم رفض فرض العدم وقبول الفرض البديل إذا كانت قيمة P–value أقل من أو تساوي 5%، والعكس إذا كانت قيمتها أكبر من 5%، وذلك وفقا لنتائج الاختبار الموضحة في الجدول التالي:

جدول 12: نتائج اختبار الفرض الثاني الفرعي H2b

Mann–Whitney Test Ranks

	Qualif.	N	Mean Rank	Sum of Ranks
Q5	0	21	19.07	400.50
	1	30	30.85	925.50
	Total	51		
Q10	0	21	25.17	528.50
	1	30	26.58	797.50
	Total	51		

Test Statistics

	Q5	Q10
Mann-Whitney U	169.500	297.500
Wilcoxon W	400.500	528.500
Z	-2.939	-.345
Asymp. Sig. (2-tailed)	.003	.730

a Grouping Variable: Qualif.

وقد **جاءت** نتيجة هذا الاختبار(المقارنة الرابعة) **بعدم** وجود تأثير للتأهيل العلمي للمستثمر على العلاقة الإيجابية بين التوكيد المهني على الإفصاح عن عمليات مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين في الأسهم، حيث بلغت قيمة P–value للسؤال Q5 (0.003) وهي أقل من 5%، وبلغت قيمة P–value السؤال Q10 (0.003) على وهي أكبر من 5%، مما يعني **قبول** فرض العدم **ورفض** الفرض البديل بعدم وجود اختلافات معنوية في ردود المجموعتين في ظل اختلاف تقرير التوكيد على

الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني، وعدم وجود تأثير لتأهيل المستثمر على قرار الاستثمار في الأسهم.

ويمكن للباحث تلخيص نتائج اختبارات الفروض وفقًا للتحليل الأساسي كما يلي:

الفرض	فروض البحث	نتيجة الاختبار
H1	يؤثر توكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني معنويًا على رغبة وقرارات المستثمرين في الأسهم في مصر.	**قبول**
H2	يختلف التأثير المعنوي لتوكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين في الأسهم في مصر باختلاف مستوى خبرتهم العملية وتأهيلهم المستمر.	**قبول**
H2a	يختلف التأثير المعنوي لتوكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين في الأسهم في مصر باختلاف مستوى خبرتهم العملية.	**قبول**
H2b	يختلف التأثير المعنوي لتوكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين في الأسهم في مصر باختلاف تأهيلهم المستمر.	**رفض**

7-2-5-3 تحليل الحساسية

قياسًا على دراسة (على،2018؛ رميلي،2020) يعتبر تحليل الحساسية Sensitivity Analysis أحد المنهجيات المستخدمة لتقييم مدى قوة ومتانة Solidity النتائج التي تم التوصل إليها بالتحليل الأساسي من خلال تحديد تأثير اختلاف طرق قياس المتغيرات الرئيسية، وحجم العينة، والمدي الزمني المستند إليه بالتحليل، لذلك يهدف الباحث من هذا الجزء من البحث من إجراء تحليل الحساسية لاختبار مدى حساسية النموذج لتغيير طريقة قياس المتغير التابع.

- **تحليل الحساسية (تغيير طريقة قياس المتغير التابع):**

استخدم الباحث في التحليل الأساسي قيمة سعر السهم التي يتنبأ بها المستثمر في السنة المقبلة، بينما في تحليل الحساسية قام الباحث بإعطاء القيمة (صفر) في حالة ثبات سعر السهم في السنة المقبلة مقارنة بالسنة الحالية، واعطاء القيمة (واحد) في حالة توقع انخفاض أو زيادة سعر السهم في السنة المقبلة عن السنة الحالية.

أ- نتيجة اختبار فرض الدراسة الأول (H1) تحليل الحساسية:

وفقا لنتيجة اختبار Wilcoxon Signed Ranks Test يتم قبول فرض العدم ورفض الفرض البديل، حيث كانت قيمة p- value أكبر من مستوى المعنوية 5% لكل مقارنة سؤال من الأسئلة ، وبناء عليه يتم رفض الفرض (H1) ، كما يتضح في الجدول التالي:

جدول 13: اختبار الفرض الأول H1

Test Statistics

W	Q6 - Q1	Q7 - Q2	Q8 - Q3	Q9 - Q4	Q10 - Q5
Z	-1.827(a)	-1.914(a)	-1.853(a)	-1.687(a)	-1.732(a)
Asymp. Sig. (2-tailed)	.068	.056	.064	.092	.083
a Based on negative ranks.					
b Based on positive ranks.					
c Wilcoxon Signed Ranks Test					

ب- نتيجة اختبار فرض الدراسة الثاني (H2) تحليل الحساسية:

وفقا لنتيجة اختبار **Mann-Whitney Test يتم قبول فرض العدم ورفض الفرض البديل**، حيث بلغت قيمة P-value للسؤال Q5 والسؤال Q10 (0.105)، (0.082) على التوالي وهي أكبر من 5%، **وبناء عليه يتم رفض الفرض (H2)، كما يتضح من الجدول التالي:**

جدول 14: اختبار نتائج اختبار الفرض الثاني H2

Test Statistics

	Q5	Q10
Mann-Whitney U	248.500	241.000
Wilcoxon W	683.500	676.000
Z	-1.620	-1.740
Asymp. Sig. (2-tailed)	.105	.082

a Grouping Variable: EXP.QUA

ب-1 نتيجة اختبار فرض الدراسة الثاني الفرعي (H2a):

وفقا لنتيجة اختبار **Mann-Whitney Test يتم قبول فرض العدم ورفض الفرض البديل**، حيث بلغت قيمة P-value للسؤال Q5 والسؤال Q10 (0.093)، (0.272) على التوالي وهي أكبر من 5%، **وبناء عليه يتم رفض الفرض (H2a) ، كما يتضح من الجدول التالي:**

جدول 15: نتائج اختبار الفرض الثاني الفرعي H2a

Test Statistics

	Q5	Q10
Mann-Whitney U	248.500	274.000
Wilcoxon W	524.500	550.000
Z	-1.681	-1.098
Asymp. Sig. (2-tailed)	.093	.272

a Grouping Variable: Exp.

ب-2 نتيجة اختبار فرض الدراسة الثاني الفرعي (H2b):

وفقا لنتيجة اختبار **Mann-Whitney Test يتم قبول فرض العدم ورفض الفرض البديل،** حيث بلغت قيمة P-value للسؤال Q5 والسؤال Q10 (0.152)، (0.561) على التوالي وهي أكبر من 5%، **وبناء عليه يتم رفض الفرض (H2b) ، كما يتضح من الجدول التالي:**

جدول 16: نتائج اختبار الفرض الثاني الفرعي H2b

Test Statistics

	Q5	Q10
Mann-Whitney U	257.500	296.000
Wilcoxon W	533.500	702.000
Z	-1.432	-.582
Asymp. Sig. (2-tailed)	.152	.561

a Grouping Variable: Qualif.

ومن النتائج السابقة، وبمقارنة نتائج التحليل الأساسي بنتائج تحليل الحساسية واختلاف طريق قياس المتغير التابع، **يتضح قبول الفروض** H1,H2,H2a **ورفض** H2b في **التحليل الأساسي، ورفض** جميع الفروض في **تحليل الحساسية،** مما يشير لأفضلية استخدام قيمة سعر السهم التي يتنبأ بها المستثمر في السنة المقبلة في قياس قرارات وأحكام المستثمرين.

7-3 نتائج البحث والتوصيات ومجالات البحث المقترحة

استهدف البحث دراسة واختبار أثر **التوكيد** المهني لمراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر **الأمن السيبراني** على **رغبة وقرارات** المستثمرين في الأسهم، وكذلك اختبار أثر مستوى **الخبرة والتأهيل العلمي** للمستثمر كمتغيرات **مُعدَّلة** على العلاقة محل الدراسة. **وخلص** الباحث إلي مجموعة من النتائج على المستوى **العلمي** الأكاديمي وعلى المستوى **العملي** التطبيقي، والإجابة على أسئلة البحث، بالإضافة إلي اقتراح بعض التوصيات ومجالات البحث المستقبلية، وذلك كما يلي:

7-3-1 نتائج البحث

- **توصلت الدراسة** لوجود اهتمام من قبل المنظمات المهنية والدراسات الأكاديمية وأصحاب المصلحة بأهمية ودور مراقبي الحسابات في التوكيد على إفصاحات عمليات إدارة مخاطر الأمن السيبراني وعلى معلومات الأمن السيبراني التي تُعدها 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)، وأيضًا تقييم مخاطر أحداث 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 **إيجابًا على ثقة ورغبة المستثمرين في الإستثمار في أسهم تلك الشركات.**

- **توصلت الدراسة** إلى وجود تأثير **معنوي إيجابي** لتقرير **التوكيد** المهني لمراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين في الأسهم، وذلك نتيجة **الاتجاه** المتزايد من قبل الشركات نحو الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني، وقيام مراقبي الحسابات بتوفير خدمة توكيد إفصاحات وإدارة 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 الاستثمار** في أسهم تلك الشركات.

- **توصلت الدراسة** إلى وجود تأثير **للخبرة والتأهيل** معًا على العلاقة الإيجابية بين التوكيد المهني على الإفصاح عن عمليات مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين في الأسهم، والذي **يُشير** إلى أن قيام **الإدارة** بالإفصاح عن عمليات إدارة مخاطر الأمن السيبراني **وتوكيد** مراقب الحسابات عليها ينتج عنها تقييمات أكثر ملاءمة لمصداقية الإدارة، وتقييمات أعلى لأسعار الأسهم نتيجة تعزيز مستوى الشفافية وتقليل مستوى عدم تماثل المعلومات، وإضفاء المصداقية على محتوي تقرير الإدارة عن الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني.

- **توصلت الدراسة** إلى وجود تأثير للخبرة على العلاقة الإيجابية بين التوكيد المهني على الإفصاح عن عمليات مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين في الأسهم. مما يعني أن المستثمرين

الأقل والأكثر خبرة يرغبون في وجود تقرير توكيد المهني على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني.

- **توصلت الدراسة** إلى **عدم** وجود **تأثير** للتأهيل العلمي للمستثمر على العلاقة الإيجابية بين التوكيد المهني على الإفصاح عن عمليات مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين في الأسهم، مما يعني أن تقرير **التوكيد** المهني على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني **ليس** له مردود إيجابي على المشاركين الأكثر تأهيلًا مقارنة بالمشاركين الأقل تأهيلًا.
- **توصلت الدراسة** إلي **رفض** جميع الفروض في **تحليل الحساسية** وتغيير طريقة قياس المتغير التابع (بإعطاء القيمة (صفر) في حالة ثبات سعر السهم في السنة المقبلة مقارنة بالسنة الحالية، وإعطاء القيمة (واحد) في حالة توقع انخفاض أو زيادة سعر السهم في السنة المقبلة عن السنة الحالية) مما يشير لأفضلية استخدام قيمة سعر السهم التي يتنبأ بها المستثمر في السنة المقبلة في قياس رغبة وقرارات المستثمرين المستخدم في التحليل الأساسي.

7-3-2 توصيات البحث

في ضوء ما توصل إليه البحث من نتائج **على المستوى العلمي الأكاديمي وعلى المستوى العملي التطبيقي**، والإجابة على أسئلة البحث، يوصي الباحث بالآتي:

أولاً: بالنسبة لأقسام المحاسبة بالجامعات المصرية: تطوير مقررات ومناهج المحاسبة والمراجعة لتشمل البعد المحاسبي والمهني لتقارير الإفصاح عن مخاطر الأمن السيبراني، وتشجيع الباحثين لإجراء مزيد من البحوث المحاسبية المستقبلية في مجال الإفصاح عن مخاطر الأمن السيبراني والتوكيد عليه وتناول محدداته ومردوده الإيجابي.

ثانيًا: بالنسبة لمكاتب المحاسبة والمراجعة المصرية: تدريب مراقبي الحسابات لديها على خدمة التوكيد المهني على إفصاحات مخاطر الأمن السيبراني، باعتبارها خدمة مهنية جديدة تستلزم تطوير مهاراتهم وقدراتهم المهنية في هذا المجال.

ثالثًا: بالنسبة للهيئة العامة للرقابة المالية: زيادة وعي إدارات الشركات والجهات الرقابية ذات الصلة من خلال المؤتمرات والندوات بأهمية الإفصاح عن مخاطر الأمن السيبراني، وتشجيع وتحفيز الشركات المقيدة بالبورصة على الإفصاح عن مخاطر الأمن السيبراني وإرفاق تقرير توكيد مهني عليه.

رابعًا: بالنسبة للجهات التنظيمية: إصدار إرشادات مهنية كافية خاصة بالتوكيد المهني على إفصاحات مخاطر الأمن السيبراني، وتطوير إطار واضح يوفر إرشادات محددة لإعداد تقارير الإفصاح والتوكيد على مخاطر الأمن السيبراني على غرار الإرشادات والأُطر الدولية في هذا المجال.

7-3-3 مجالات البحث المقترحة

يعتقد الباحث بأن المجالات التالية تحتاج إلى مزيد من البحوث المستقبلية:

- أثر التوكيد على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على قرار منح الائتمان – دراسة تجريبية.
- أثر التوكيد على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على جهد وأتعاب المراجعة.
- أثر التوكيد المهني على حوادث الأمن السيبراني على قرارات الاستثمار والائتمان– دراسة تجريبية.
- أثر التوكيد المهني على حوادث الأمن السيبراني على أسعار الأسهم دراسة تطبيقية على الشركات المقيدة بالبورصة المصرية.
- أثر حوادث الأمن السيبراني على التهرب الضريبي للشركات دراسة تطبيقية على الشركات المقيدة بالبورصة المصرية.
- أثر استخدام تحليلات البيانات الضخمة في توفير خدمة التوكيد المهني على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني.

المراجع

أولاً: المراجع باللغة العربية

الرشيدي، طارق عبد العظيم يوسف؛ السيد، داليا عادل عباس (2019). **أثر الإفصاح عن مخاطر الأمن السيبرانى في التقارير المالية على أسعار الأسهم وأحجام التداول دراسة مقارنة في قطاع تكنولوجيا المعلومات**، مجلة المحاسبة والمراجعة لاتحاد الجامعات العربية، كلية التجارة – جامعة بني سويف، المجلد 8، العدد 2، الصيف 2019، الصفحة 439-487.

الصيرفي، أسماء أحمد (2019). **أثر اختلاف موفر التوكيد ونوع استنتاجه على العلاقة بين التوكيد المهني على الإفصاح عن تقرير لجنة المراجعة وقرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية– دراسة تجريبية**، مجلة البحوث المحاسبية ، كلية التجارة ، جامعة طنطا، المجلد 6، الجزء الثاني العدد2.

بدوي، هبة الله عبد السلام (2018). **أثر المحتوي المعلوماتي لفقرة أمور المراجعة الرئيسية بشأن تقييم الاستثمارات بقيمتها العادلة على جودة قرار الاستثمار – دراسة تجريبية على المستثمرين في مصر**، مجلة الإسكندرية للبحوث المحاسبية، كلية التجارة – جامعة الإسكندرية، العدد الثاني– المجلد الثاني.

رميلي، سناء محمد رزق (2020). **أثر إفصاح الإدارة عن هيكل الرقابة الداخلية وتوكيد مراقب الحسابات عليه على قرار الإستثمار بأسهم الشركات المقيدة بالبورصة المصرية – دراسة تجريبية**، مجلة الإسكندرية للبحوث المحاسبية، كلية التجارة – جامعة الإسكندرية، العدد الأول– المجلد الرابع.

شرف، إبراهيم أحمد إبراهيم (2015). **أثر الإفصاح غير المالي عبر تقارير الأعمال المتكاملة على تقييم أصحاب المصالح لمقدرة الشركة على خلق القيمة – دراسة ميدانية وتجريبية**، رسالة دكتوراة غير منشورة ، كلية التجارة ، جامعة دمنهور.

عبدالرحيم، رضا محمود محمد (2020). **أثر التعديلات في شكل ومحتوى تقرير مراقب الحسابات وفقاً لمعيار المراجعة الدولي رقم (570) المعدل لسنة 2015 بشأن الاستمرارية على قراري الاستثمار ومنح الائتمان: دراسة تجريبية**، مجلة الأسكندرية للبحوث المحاسبية ، كلية التجارة – جامعة الأسكندرية، العدد الثاني، المجلد الرابع.

على، نهي محمد زكي محمد (2018). **أثر جودة المراجعة الخارجية على الحد من السلوك الانتهازي للإدارة ومنع الغش بالقوائم المالية– دراسة تطبيقية على الشركات المقيدة بالبورصة المصرية**– رسالة دكتوراه غير منشورة– قسم المحاسبة، كلية التجارة جامعة الإسكندرية.

كعموش، شريف على خميس إبراهيم (2018). **أثر توكيد مراقب الحسابات على الإفصاح عن رأس المال الفكري على أحكام المستثمرين – دراسة تجريبية**، مجلة الإسكندرية للبحوث المحاسبية، كلية التجارة – جامعة الإسكندرية، العدد الثاني– المجلد الثاني.

محمد، عمرو محمد خميس (2020). **أثر توكيد مراقب الحسابات على تقارير الأعمال المتكاملة على قرار الاستثمار بالأسهم – دراسة تجريبية**، مجلة الإسكندرية للبحوث المحاسبية، كلية التجارة – جامعة الإسكندرية، العدد الثالث– المجلد الرابع.

موسي، سعاد زغلول عبده (2018). **أثر توكيد المراجع الخارجي على تقارير الأعمال المتكاملة على قراري الاستثمار ومنح الائتمان – دراسة تجريبية**، رسالة دكتوراة غير منشورة ، كلية التجارة ، جامعة الاسكندرية.

ثانيًا: المراجع باللغة الأجنبية

Aldorisio,J.(2020), Best Practices for Cybersecurity Auditing [a Step-by-Step Checklist], Available at: https://securityscorecard.com/blog/best-practices-for-a-cybersecurity-audit.

American Institute of Certified Public Accountants (AICPA). (2017a). SOC for Cybersecurity: A Backgrounder. ***AICPA, New York, NY***.

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

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.

Arens, A. A., Elder, R. J., Beasley, M. S., & Hogan, C. E. (2016). Auditing and assurance services. Auditing and Assurance Services. Global Edition, Pearson Education Limited, 2016. ***ProQuest Ebook Central***, http://ebookcentral.proquest.com/lib/undip-ebooks/detail. action?docID =5185606.

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. ***Decision Support Systems***, 147,113580.

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).

Bao Ngo, T. N., & Tick, A. (2021). Cyber-security Risks Assessments by External Auditors. Interdisciplinary Description of Complex Systems: ***INDECS***, 19(3), 375-390.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. ***Journal of Accounting and Public Policy***, 37(6), 508-526.

Brown, S. V., Tian, X., & Wu Tucker, J. (2018). The spillover effect of SEC comment letters on qualitative corporate disclosure: Evidence from the risk factor disclosure. ***Contemporary Accounting Research***, 35(2), 622-656.

Brown-Liburd, H., and V. L. Zamora. 2014. The role of corporate social responsibility (CSR) assurance in investors' judgments when managerial pay is explicitly tied to CSR performance. ***Auditing: A Journal of Practice & Theory***, 34(1): 75-96.

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.

Calliess, C., & Baumgarten, A. (2020). Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective. ***German Law Journal***, 21(6), 1149-1179.

Center for Audit Quality. (2016). Understanding cybersecurity and the external audit: A resource for audit committees, investors, management, and others. Available at : https://www.thecaq.org/understanding-cybersecurity-and-external-audit/.

Chartered Professional Accountants Of Canada (CPA Canada).(2018). Reporting Alert CORPORATE REPORTING: Cyber Security: Establishing A Risk Management Program And Continuing To Reassess Disclosure Practices, ***CPA Canada***.

Chartered Professional Accountants Of Canada (CPA Canada).(2018). Cyber Security Risks and Incidents — Reassessing Your Disclosure Practices, ***CPA Canada***.

Cheng, M. M., W. J. Green, & J. C. W. Ko. (2014). The impact of strategic relevance and assurance of sustainability indicators on investors' decisions. ***Auditing: A Journal of Practice & Theory***, 34(1): 131-162.

Cheng, X., & Walton, S. (2019). Do nonprofessional investors care about how and when data breaches are disclosed?. ***Journal of Information Systems***, 33(3), 163-182.

Cheong, A., Yoon, K., Cho, S., & No, W. G. (2021). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. ***Journal of information Systems***, 35(2), 179-194.

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. ***Current Issues in Auditing***, 13(2), C1-C9.

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. ***Journal of Accounting and Public Policy***, 37(6), 564-585.

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.

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. ***International Journal of Accounting Information Systems***, 38, 100468.

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2019). Managing cyber risk in supply chains: A review and research agenda. ***Supply Chain Management: An International Journal***, 25/2, 223–240.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs?. ***Journal of Computer Security***, 19(1), 33-56.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. ***Journal of Accounting and Public Policy***, 25(5), 503-530.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. ***Journal of Cybersecurity***, 1(1), 3-17.

Hampton, C., Sutton, S. G., Arnold, V., & Khazanchi, D. (2021). Cyber Supply Chain Risk Management: Toward an Understanding of the Antecedents to Demand for Assurance. ***Journal of Information Systems***, 35(2), 37-60.

Héroux, S., & Fortin, A. (2020). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. ***Accounting Perspectives***, 19(2), 73-100.

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. ***Information & Management***, 52(3), 337-347.

Hoang, H., & Phang, S. Y. (2021). How does combined assurance affect the reliability of integrated reports and investors' judgments?. ***European Accounting Review***, 30(1), 175-195.

IBM Corporation, (2021). Cost of a Data Breach Report 2021, ***IBM Corporation,New Orchard Road,Armonk, NY 10504***, available at: https://www.ibm.com/security/data-breach .

Jamison, J., Morris, L., & Wilkinson, C. (2018). The future of cyber security in internal audit. the Internal Audit Foundation, formerly The Institute of Internal Auditors Research Foundation (IIARF). available at: https://www.crowe.com/-/media/Crowe/LLP/folio-pdf/The-Future-of-Cybersecurity-in-IA-RISK-18000-002A-update.pdf.

Jr, S. U. & Arnold ,C.(2019). Cybersecurity Is Critical for all Organizations– Large and Small, IFAC, Available at : https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small.

Kaur, J., & Ramkumar, K. R. (2021). The recent trends in cyber security: a review. ***Journal of King Saud University-Computer and Information Sciences***. available at: https://doi.org/10.1016/j.jksuci.2021.01.018.

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

Khari, M., Shrivastava, G., Gupta, S., & Gupta, R. (2017). Role of Cyber Security in Today's Scenario. In Detecting and Mitigating Robotic Cyber Security Risks, ***IGI Global*** ,pp. 177-191.

Knechel, W. R. (2021). The Future of Assurance in Capital Markets: Reclaiming the Economic Imperative of the Auditing Profession. ***Accounting Horizons***, 35(1), 133-151.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. ***Computers & Security***, 105, 102248.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. ***Business Horizons***, 64, 659-671.

Lessambo, F. I. (2018). Auditing, Assurance Services, and Forensics: A Comprehensive Approach, Palgrave Macmillan, Available at: https://doi.org/10.1007/978-3-319-90521-1.

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

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.

Li, H., No, W. G., Cheong, A., & Halterman, C. K.(2021). Data analytics in cybersecurity assurance: should data analytics be an integral part of cybersecurity assurance? Available at: https://zicklin.baruch.cuny.edu/wp-content/uploads/sites/10/2019/12/Data-Analytics-in-Cybersecurity-Assurance-1.pdf.

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

Mercer, M. (2004). How do investors assess the credibility of management disclosures? ***Accounting Horizons***, 18 (3): 185–196.

Modi, S. B., Wiles, M. A., & Mishra, S. (2015). Shareholder value implications of service failures in triads: the case of customer information security breaches. ***Journal of Operations Management***, 35, 21-39.

Moreira, G. P. (2019). Cybersecurity and external audit: the disclosure of risk factors in annual reports, *(**Doctoral dissertation**), **Católica Porto Business Scho**ol.

Morse, E. A., Raval, V., & Wingender Jr, J. R. (2011). Market price effects of data security breaches. ***Information Security Journal**: **A Global Perspective***, 20(6), 263-273.

Navarro, P., & Sutton, S.G.(2021), Investors' Judgment and Decisions after a Cybersecurity Breach: Understanding the Value Relevance of Cybersecurity Risk Management Assurance. Available at SSRN: https://ssrn.com/abstract=3817763 or http://dx.doi.org/10.2139/ssrn.3817763.

Perols, R. R. (2019). Two essays on the impact of cybersecurity risk management examinations on investor perceptions and decisions (***Doctoral dissertation**, **University of South Florida***). Retrieved from https://scholarcommons.usf.edu/etd/8401.

Perols, R. R., & Murthy, U. S. (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.

Pirounias, S., Mermigas, D., & Patsakis, C. (2014). The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. ***Journal of Information Security and Applications***, 19(4-5), 257-271.

Public Company Accounting Oversight Board (PCAOB). (2019). Cybersecurity: Where we are; what more can be done? A call for auditors to lean in. Available at: https://pcaobus.org/News/Speech/Pages/hamm-cybersecurity-wherewe-are-what-more-can-be-done.aspx.

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.

Rea-Guaman, A. M., Mejía, J., San Feliu, T., & Calvo-Manzano, J. A. (2020). AVARCIBER: a framework for assessing cybersecurity risks. ***Cluster Computing***, 23(3), 1827-1843.

Reimsbach, D., Hahn, R., & Gürtürk, 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., 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(03), 1950013.

Rosati, P., Gogolin, F., & Lynn, T. (2020). Cyber-security incidents and audit quality. ***European Accounting Review***, 1-28.

Securities and Exchange Commission (SEC). (2018). Commission Statement and Guidance on Public Company Cybersecurity Disclosures Release Nos. 33-10459; 34-82746. Available at: https://www.sec.gov/rules /interp/ 2018/33-10459.pdf.

Tan, H. T., & Yu, Y. (2018). Management's responsibility acceptance, locus of breach, and investors' reactions to internal control reports. ***The Accounting Review***, 93(6), 331-355.

The Committee of Sponsoring Organizations (COSO). (2013). Internal Control—Integrated Framework. ***New York, NY: COSO***.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO).(2019). Managing Cyber Risk in a Digital Age, ***Committee of Sponsoring Organizations of the Treadway Commission (COSO)***. 1234567890 PIP 198765432.

Tosun, O. K. (2021). Cyber-attacks and stock market activity. ***International Review of Financial Analysis***, 76, 101795.

Tysiac, k.(2020). Cybersecurity provides opportunities for auditors to serve, Available at: https://www.journalofaccountancy.com/ news/2020/oct/cybersecurity-opportunities-for-auditors.html.

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. ***Risk Management***, 22(4), 239-309.

Vekez, P. N. (2019). Three Studies on Cybersecurity Disclosure and Assurance ***(Doctoral dissertation, University of Central Florida). Electronic Theses and Dissertations***, 2004-2019. 6541. https://stars. library. ucf.edu/etd/6541.

Walton, S., Wheeler, P., Zhang, Y., & Zhao, X. (2021). An Integrative Review and Analysis of Cybersecurity Research: Current State and Future DirectionsAn Integrative Review and Analysis of Cybersecurity Research. ***Journal of Information Systems***, Vol. 35, No. 1, pp. 155–186.

Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. ***International Journal of Law, Crime and Justice***, 62, 100415.

Yang, L., Lau, L., & Gan, H. (2020). Investors' perceptions of the cybersecurity risk management reporting framework. ***International Journal of Accounting & Information Management***. Vol. 28 No. 1, pp. 167-183.

Yen, J. C., Lim, J. H., Wang, T., & Hsu, C. (2018). The impact of audit firms' characteristics on audit fees following information security breaches. ***Journal of Accounting and Public Policy***, 37(6), 489-507.

ملاحق البحث

الحالات التجريبية

جامعة بني سويف

كلية التجارة

قسم المحاسبة

السيد الأستاذ/ة الفاضل /ـة .....

تحية طيبة وبعد،،،،،،

يقوم الباحث بإعداد بحث في مجال **أثر التوكيد المهني لمراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وجودة قرارت المستثمرين في الأسهم** ، وتمثل الحالات المرفقة أحد أهم أدوات البحث لإجراء الدراسة التجريبية.

والباحث إذ يشكركم مسبقًا على حسن تعاونكم معه. تكرمًا قراءة الحالات التالية والإجابة على أسئلتها ، وسوف تحظى إجاباتكم بالسرية الكاملة ، كما سوف تستخدم لأغراض البحث العلمي.

وتفضلوا سيادتكم بقبول فائق الإحترام والتقدير،،،،،

الباحث/ د. محمد أحمد عبدالعزيز عثمان

أستاذ المحاسبة المساعد

كلية التجارة – جامعة بني سويف

أولاً: البيانات الشخصية

1- **الاسم** (اختياري):.....

2- **الوظيفة** الحالية:.....

3- **جهة العمل**

- **بنك** ( ) (إدارة / قسم).....
- **شركة** تداول أوراق مالية ( )
- **إدارة** صندوق إستثمار ( )
- **أخري** ( )

4- **المؤهل العلمي**

- بكالوريوس في .....
- دبلوم دراسات عليا في .....
- ماجستير أكاديمي أو مهني في .....
- دكتوراة أكاديمية أو مهنية في .....

5- **الشهادات المهنية**

- CPA ( ) - CMA ( )
- CFA ( ) - أخري ( )

6- **عدد سنوات الخبرة في العمل**

- أقل من 5 سنوات ( )
- من 5 سنوات إلي أقل من 10 سنوات ( )
- من 10 سنوات إلي أقل من 15 سنة ( )
- من 15 سنة إلي أقل من 20 سنة ( )
- من 20 سنة فأكثر ( )

ثانياً: مصطلحات البحث الفنية

- **الفضاء السيبراني:** هو المكان الذي يُنشئ فيه الأشخاص والمنظمات وجودًا إلكترونيًّا ويشاركون في أنشطة افتراضية، ويتبادلون المعلومات والمنتجات والخدمات عبر الإنترنت

- **الأمن السيبراني:** هو في الأساس عملية ضمان سلامة الفضاء السيبراني من التهديدات المعروفة وغير المعروفة سواء الداخلية أم الخارجية ، ويشمل مجموعة من التقنيات والعمليات والهياكل والممارسات المستخدمة لحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الوصول غير المصرح به، وضمان سرية وتكامل البيانات وتوافرها.

- **إدارة مخاطر الأمن السيبراني:** هي عملية مستمرة لتحديد وتحليل وتقييم ومعالجة تهديدات الأمن السيبراني للمنظمات، وتتضمن مجموعة من السياسات والعمليات والضوابط الرقابية المصممة لحماية المعلومات والأنظمة من الأحداث الأمنية التي يمكن أن تمنع تحقيق أهداف الأمن السيبراني للكيان واكتشافها والاستجابة لها ومعالجتها في الوقت المناسب.

- **تقرير فحص إدارة مخاطر الأمن السيبراني؛** يتضمن المكونات الرئيسية الثلاثة التالية:

- **وصف سردي معد من قبل الإدارة** لبرنامج إدارة مخاطر الأمن السيبراني، وسياسات الأمان الرئيسية والعمليات التي تم تنفيذها وتشغيلها لحماية أصول المعلومات الخاصة بالمنشأة من تلك المخاطر.

- **تأكيد من الإدارة** حول ما إذا كان الوصف مقدمًا وفقًا لمعايير خدمات الثقة للأمان والتوافر والسرية والخصوصية التي طورها المجمع الأمريكي للمحاسبين القانونيين AICPA في 2017 كمعايير رقابية يمكن من خلالها تقييم فعالية الضوابط الرقابية داخل البرنامج لتحقيق أهداف الأمن السيبراني.

- **توكيد مراقب الحسابات وإبداء** رأي حول العرض العادل لوصف وتأكيد الإدارة على فعالية الضوابط الرقابية داخل برنامج إدارة المخاطر السيبرانية، ومدى ملاءمة تصميم ضوابط الرقابة وفعاليتها في تحقيق أهداف الأمن السيبراني.

ثالثًا: الحالات التجريبية

الحالة التجريبية (1)

الشركة (XYZ) شركة مساهمة مصرية مقيدة بالبورصة – خاضعة للقانون 159 لسنة 1981 ولائحته التفيذية والقانون رقم 8 لسنة 1997 قانون ضمانات وحوافز الاستثمار والمعدل بالقانون رقم 72 لسنة 2017، تعمل في مجال الإتصالات والتكنولوجيا أعدت ونشرت القوائم المالية عن السنة المنتهية في 2021/12/31 م وراجعها مكتب الأستاذ / **كامل كمال** والمرخص له بمراجعة الشركات المقيدة بالبورصة – علمًا بأنه يراجع حسابات الشركات المساهمة منذ أكثر من 20 عامًا وشريك مع مكتب KPMG أحد المكاتب الأربع الكبري Big 4، وقد أبدي **رأيًا نظيفًا على القوائم المالية وفق معايير المراجعة المصرية،** وفيما يلي البيانات الخاصة بالشركة:

القوائم المالية (الملخصة)عن السنة المنتهيه في 2021/12/31م

1- قائمة المركز المالي في 2020/12/31م

بيان	2021	2020
الأصول		
إجمالي الأصول طويلة الأجل	1074766461	397991483
إجمالي الأصول المتداولة	432217404	1236228711
اجمالي الأصول	1506983865	1634220194
الالتزامات		
إجمالي الالتزامات طويلة الأجل	47618472	126541852
إجمالي الالتزامات المتداولة	263830365	369931038
اجمالي الالتزامات	311448837	523472890
حقوق الملكية		
رأس المال المدفوع	800000000	800000000
الاحتياطيات	64727152	47489236
الأرباح المرحلة	330807826	263258068
اجمالي حقوق ملكية	1195535028	1110747304
اجمالي الالتزامات وحقوق الملكية	1506983865	1634220194

2- قائمة الدخل(المختصرة) عن السنة المنتهية في 2021/12/31م

بيان	2021	2020
إيرادات النشاط	1264420695	983978558
تكلفة النشاط	(702577315)	(543717790)
مجمل دخل العمليات	561843380	440260768
يضاف ايرادات أخري	42124271	49475383
يطرح مصروفات أخري	(160133634)	(140195929)
صافي الربح قبل الضريبة	443834017	349540222
الضريبة	(99075700)	(76981243)
صافي الربح بعد الضريبة	344758317	272558979

3- قائمة التدفقات النقدية (الملخصة) عن السنة المنتهية في 2021/12/31م

بيان	2021	2020
صافي التدفقات النقدية من أنشطة التشغيل	350029293	247769503
صافي التدفقات النقدية من أنشطة الاستثمار	(218552904)	(98535471)
صافي التدفقات النقدية من أنشطة التمويل	(209267184)	193531358
صافي التغير في النقدية وما في حكمها	(77790795)	342765390
النقدية وما في حكمها أول الفترة	502780870	160015480
النقدية وما في حكمها أخر الفترة	424990075	502780870

4- الإيضاحات المتممة للقوائم المالية

- **غرض الشركة:** تقديم خدمات التشغيل المتخصصة لأنظمة تكنولوجيا المعلومات والاتصالات سواء داخل أو خارج جمهورية مصر العربية.
- **يتم إعداد القوائم المالية** وفقًا لافتراض الاستمرارية ومبدأ التكلفة التاريخية فيما عدا الأصول والالتزامات المالية التي يتم إثباتها بالقيمة العادلة والتكلفة المستهلكة.
- **تم إعداد القوائم المالية** للشركة وفقًا لمعايير المحاسبة المصرية الصادرة بقرار وزير الاستثمار رقم 110 لسنة 2015 والمعدلة في سبتمبر 2019 بقرار وزيرة الاستثمار رقم 69 لسنة 2019 والقوانين واللوائح السارية.
- **يتطلب إعداد القوائم المالية** قيام الإدارة بعمل أحكام وتقديرات تؤثر على قيم الإيرادات والمصروفات والأصول والالتزامات المدرجة بالقوائم المالية وما يصاحبها من إفصاحات.
- **أثناء عملية تطبيق** السياسات المحاسبية للشركة اتخذت الإدارة بعض الأحكام التي لها تأثير كبير على المبالغ المعترف بها في القوائم المالية.
- **يتحمل مجلس إدارة الشركة** مسؤولية وضع إطار لإدارة المخاطر التي تتعرض لها الشركة والإشراف عليه، وتتحمل الإدارة العليا بالشركة وضع وتتبع سياسات إدارة المخاطر ورفع تقارير إلي مجلس الإدارة تتناول أنشطتها على أساس منتظم.
- **تم مراجعة** القوائم المالية للشركة (المنشورة في **2021/3/25م)** وأبدى مراقب الحسابات **رأيًا نظيفًا** بتاريخ **2021/3/25م** على القوائم المالية وفق معايير المراجعة المصرية.

تقرير الإدارة عن برنامج وضوابط إدارة مخاطر الأمن السيبراني:

تقرير الإدارة عن برنامج وضوابط إدارة مخاطر الأمن السيبراني

السادة/ مساهمو الشركة

هيئة الرقابة المالية

إدارة البورصة المصرية

برنامج إدارة مخاطر الأمن السيبراني هو مجموعة من السياسات والعمليات والضوابط الرقابية المصممة لحماية المعلومات والأنظمة من الأحداث الأمنية التي يمكن أن تمنع تحقيق أهداف الأمن السيبراني للشركة واكتشافها والاستجابة لها ومعالجتها في الوقت المناسب. لقد وضعنا أهداف الأمن السيبراني لشركة XYZ، وحددنا أيضًا المخاطر التي من شأنها أن تمنع تحقيق هذه الأهداف وقمنا بتصميم وتنفيذ وتشغيل ضوابط رقابية لمواجهة تلك المخاطر.

تأكيد

نؤكد أننا أجرينا تقييمًا لفعالية الضوابط الرقابية المدرجة في برنامج إدارة مخاطر الأمن السيبراني طوال الفترة من 1 يناير 2021 إلى 31 ديسمبر 2021، باستخدام معايير خدمات الثقة للأمان والتوافر والنزاهة والسرية والخصوصية كمعايير رقابية. بناءً على هذا التقييم، نؤكد أن الضوابط كانت فعالة طوال الفترة من 1 يناير 2021 إلى 31 ديسمبر 2021، لتحقيق أهداف الأمن السيبراني للشركة بناءً على معايير الرقابة.

عضو مجلس الإدارة المنتدب

2021/12/31م

وفي ضوء تحليلك وقراءتك للقوائم المالية للشركة وإيضاحاتها المتممة، وتقرير إدارتها عن برنامج إدارة مخاطر الأمن السيبراني. يُرجي الإجابة عن الأسئلة التالية:

1- هل توافق على أن تقرير الإدارة عن برنامج إدارة مخاطر الأمن السيبراني يوفر لك معلومات مفيدة يمكن الاعتماد عليها في اتخاذ قرار الاستثمار

موافق تمامًا	موافق	محايد	غير موافق	غير موافق تمامًا
( )	( )	( )	( )	( )

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:

موافق تمامًا	موافق	محايد	غير موافق	غير موافق تمامًا
( )	( )	( )	( )	( )

3- ما هو احتمال استثمارك في أسهم هذه الشركة:

أكبر من 75%	أكبر من 50% وأقل من 75%	محايد	أكبر من 25% وأقل من 50%	أقل من 25%
( )	( )	( )	( )	( )

4- من وجهة نظركم هل توافق على أن إخضاع تقرير الإدارة عن برنامج إدارة مخاطر الأمن السيبراني للتوكيد من قبل مراقب حسابات الشركة سيكون له أثر أكبر على اعتمادكم على هذا التقرير عند اتخاذ قرار الاستثمار

موافق تمامًا	موافق	محايد	غير موافق	غير موافق تمامًا
( )	( )	( )	( )	( )

5- إذا كان سعر إقفال سهم الشركة XYZ في 2020/12/31 يبلغ 17.89 جنيهًا، وسعر إقفال السهم في 2021/12/31 كان 19.95 جنيهًا، فإن سعر الإقفال المتوقع من وجهة نظركم في 2022/12/31

سوف يقل عن 19.95 جنيهًا	سوف يثبت عند 19.95 جنيهًا	سوف يزيد عن 19.95 جنيهًا
( )	( )	( )
ليصبح ..... جنيهًا		ليصبح ..... جنيهًا

الحالة التجريبية (2)

بافتراض أن إدارة شركة XYZ قررت تكليف "كامل كمال – KPMG" لفحص فعالية الضوابط الرقابية ضمن برنامج إدارة مخاطر الأمن السيبراني، وبعد إجراء الفحص المطلوب، أصدر السيد / كامل كمال شريك مع KPMG تقرير التالي:

تقرير توكيد مراقب الحسابات بشأن تأكيد الإدارة على فعالية الضوابط الرقابية داخل برنامج إدارة المخاطر السيبرانية

إلي السادة/ مساهمي شركة XYZ

هيئة الرقابة المالية

إدارة البورصة المصرية

مجلس إدارة الشركة

تم تكليفنا لتوفير توكيد معقول بشأن تأكيد الإدارة على فعالية الضوابط الرقابية داخل برنامج إدارة المخاطر السيبرانية لشركة XYZ كما هي في 2021/12/31، وتتمثل مسؤوليتنا في إبداء الرأي، بناءً على فحصنا حول ما إذا كانت الضوابط الرقابية داخل هذا البرنامج فعالة لتحقيق أهداف الأمن السيبراني للشركة بناءً على معايير الرقابة. وتم إجراء فحصنا وفقًا لإطار لإعداد تقارير الأمن السيبراني ومعايير التصديق التي وضعها المعهد الأمريكي للمحاسبين القانونيين (AICPA). تتطلب هذه المعايير أن نقوم بتخطيط وإجراء الفحص للحصول على تأكيد معقول حول ما إذا كانت الضوابط داخل البرنامج، من جميع الجوانب الهامة، فعالة لتحقيق أهداف الأمن السيبراني للكيان بناءً على معايير الرقابة. تضمن فحصنا ما يلي: (1) الحصول على فهم لأهداف الأمن السيبراني للشركة وبرنامجها لإدارة مخاطر الأمن السيبراني ، و(2) تقييم المخاطر وأن الضوابط داخل هذا البرنامج كانت فعالة ، و (3) تنفيذ الإجراءات للحصول على أدلة حول ما إذا كان كانت الضوابط فعالة. تضمن فحصنا أيضًا إجراء الإجراءات الأخرى التي رأيناها ضرورية في هذه الظروف.

وبسبب القيود المتأصلة في الضوابط الرقابية، ربما لا تمنع أو تكشف الضوابط الرقابية كل التحريفات الجوهرية، وأيضًا فإن تقييم الفعالية للفترات المستقبلية يخضع لمخاطر أن ضوابط الرقابة قد تصبح غير ملائمة بسبب تغير الظروف. نعتقد أن الأدلة التي حصلنا عليها كافية ومناسبة لتوفير أساس معقول لرأينا.

الإستنتاج

في رأينا، أن الضوابط الرقابية المصممة داخل هذا البرنامج كانت سارية من جميع الجوانب الهامة طوال الفترة من 1 يناير 2021 إلى 31 ديسمبر 2021، وفعالة في تحقيق أهداف الأمن السيبراني للشركة، بناءً على معايير خدمات الثقة للأمان والتوافر والنزاهة والسرية والخصوصية كمعايير رقابية.

السيد/ كامل كمال

شريك KPMG

القاهرة في 25 مارس 2021

وفي ضوء تحليلك وقراءتك للقوائم المالية للشركة وإيضاحاتها المتممة، وتقرير إدارتها عن برنامج إدارة مخاطر الأمن السيبراني، وتقرير توكيد مراقب الحسابات عليه، يُرجي الإجابة عن الأسئلة التالية:

1- هل توافق على أن تقرير الإدارة عن برنامج إدارة مخاطر الأمن السيبراني وتقرير توكيد مراقب الحسابات يوفر لك معلومات مفيدة يمكن الاعتماد عليها في اتخاذ قرار الاستثمار:

موافق تمامًا	موافق	محايد	غير موافق	غير موافق تمامًا
( )	( )	( )	( )	( )

2- هل توافق على أن هذه الشركة سيكون لها أولوية أكبر عند دراسة قرار الاستثمار في الأسهم مقارنة بالشركات التي لم تقدم إفصاحًا وتوكيدًا عن برنامج إدارة مخاطر الأمن السيبراني:

موافق تمامًا	موافق	محايد	غير موافق	غير موافق تمامًا
( )	( )	( )	( )	( )

3- ما هو احتمال استثمارك في أسهم هذه الشركة:

أكبر من 75%	أكبر من 50% وأقل من 75%	محايد	أكبر من 25% وأقل من 50%	أقل من 25%
( )	( )	( )	( )	( )

4- من وجهة نظركم هل توافق على أن تقرير توكيد مراقب الحسابات على تقرير الإدارة عن برنامج إدارة مخاطر الأمن السيبراني سيكون له أثر أكبر على اعتمادكم على هذا التقرير عند اتخاذ قرار الاستثمار:

موافق تمامًا	موافق	محايد	غير موافق	غير موافق تمامًا
( )	( )	( )	( )	( )

5- إذا كان سعر إقفال سهم الشركة XYZ في 2020/12/31 يبلغ 17.89 جنيهًا ، وسعر إقفال السهم في 2021/12/31 كان 19.95 جنيهًا، فإن سعر الإقفال المتوقع من وجهة نظركم في 2022/12/31:

سوف يقل عن 19.95 جنيهًا	سوف يثبت عند 19.95 جنيهًا	سوف يزيد عن 19.95 جنيهًا
( )	( )	( )
ليصبح ..... جنيهًا		ليصبح ..... جنيهًا