الدور المقترح لمراجع الحسابات في اضفاء الثقة على تقرير إدارة مخاطرالأمن السيبراني وأثره في دلالة القوائم المالية دراسة تجريبية

إعداد الباحثة

حنان هارون فريد

مدرس بقسم المحاسبة

معهد المستقبل العالي للدراسات التكنولوجية المتخصصة

الملخص:

كأشارات علي ضعف الرقابة الداخلية يمكن ان تمثل حوادث الامن السيبراني عوامل خطر كبيرة لجودة التقارير المالية و نظرا لزيادة عدد حوادث الامن السيبراني وانتشارها لتبني كثيرا من الشركات التحول الرقمي ، ونظرا لتغير طبيعة النشاط في الشركات و خاصة العاملة في قطاع تكنولوجيا المعلومات ،جاء البحث ليناقش الدور المقترح لمراجع الحسابات في اضفاء الثقة علي تقرير ادارة مخاطر الامن السيبراني حتي يستطيع المراجع مواكبة التغير السريع في بيئة الاعمال.

و تتمثل مشكلة البحث في التحديات التي تواجة المراجع متمثلة في حوادث الامن السيبراني ومخاطرها الكبيرة علي البرامج و التطبيقات المالية و صحة التقارير المالية و ما يتبعها من اضرار لاحقة لعملية اختراق البيانات وكيفية مواجهتها بل وعلي الاكثر من ذلك توقع هذة الهجمات و محاولة التخلص منها.

جاء البحث بهدف اظهار دور المراجع في اضفاء الثقة علي تقرير ادارة مخاطر الامن السيبراني ،واثره علي دلالة القوائم المالية ولتحقيق الهدف الرئيسي للبحث قامت الباحثة باستخدم الدراسة التجريبية و هي مناسبة تماما لهذا النوع من البحوث فهي تدرس العلاقة السببية بين متغيرات مستقلة وتابعة ،وبصفه خاصة تأثير الدور المقترح لمراجع الحسابات علي اضفاء الثقة علي تقرير ادارة مخاطر الامن السيبراني ،فالتجارب تعتبر منهجا قويا يمكن للباحثين الاستدلال عن طريقه علي العلاقات السببية ،كما تمكن التجارب من توضيح

التأثيرات الفعلية لانواع مختلفة من المعلومات علي عملية اتخاذ القرارات ،و بما يسمح بتطوير يفيد في تطوير المعرفة في موضوع الدراسة الحالية.
تم اجراء الدراسة التجريبية علي مجتمع واحد و هو مجتمع مراجعي الحسابات العاملين في مكاتب المحاسبة و المراجعة بالمجتمع المصري خلال العام ٢٠٢١ و ٢٠٢٢.
و تكونت العينة من ٤٠٠ مراجع حسابات طبقت عليهم الاستبانة ،و لم يتم استبعاد اي من الردود نظرا لاستخدام النشر الالكتروني للاستبيان عبر موقع Research Gate وهو يحتوي علي مجموعة كبيرة من الفئة المستهدفة للدراسة.
،كما استخدمت الدراسة اربعة متغيرات معدلة يمكن تعريف المتغيرات المعدلة بأنها المتغيرات التي تؤثر في اتجاة او قوة العلاقة بين المتغيرات المستقلة والتابعة ، كما تختلف المتغيرات المعدلة عن المتغيرات الرقابية حيث تؤثر المتغيرات الرقابية علي المتغيرالتابع مباشرة.
و خلصت الدراسة الي وجود تأثير معنوي لاهمية الافصاح عن تقرير ادارة مخاطر الامن السيبراني ،ووجود تأثيرمعنوي للدور المقترح لمراجع الحسابات و اثره علي القوائم المالية .

الكلمات المفتاحية:
الامن السيبراني – مخاطر الامن السيبراني – ادارة مخاطر الامن السيبراني – اضفاء الثقة لمراجع الحسابات – دلالة القوائم المالية.

Abstract:
As Signals of weak internal control, cybersecurity incidents can represent major risk factors for the quality of financial reports, and due to the increase in the number of cybersecurity incidents and their spread, many companies adopt digital transformation, and due to the change in the nature of activity in companies, especially those operating in the information technology sector, the idea of research came to discuss The proposed role of the auditor in giving confidence to the cybersecurity risk

management report so that the auditor can keep pace with the rapid change in the business environment.

The research problem is represented in the challenges that the auditors face, represented in cybersecurity incidents and their great risks to financial programs and applications, the validity of financial reports, and the subsequent damages to the data penetration process, how to confront them, and even more so to anticipate these attacks and try to get rid of them.

The research came with the aim of showing the role of the references in giving confidence to the cyber security risk management report, and its impact on the significance of the financial statements. The proposed role of the auditor is to give confidence to the cybersecurity risk management report. Experiments are considered a powerful approach through which researchers can infer causal relationships. Experiments also enable clarification of the actual effects of different types of information on the decision-making process, allowing for useful development. Knowledge of the topic of the current study.

The experimental study was conducted on one community, which is the community of auditors working in accounting and auditing offices in the Egyptian community during the years 2021 and 2022.

The sample consisted of 400 auditors to whom the questionnaire was applied, and none of the responses were excluded due to the use of electronic publication of the questionnaire through the

Research Gate website, which contains a large group of the target group for the study.

The study also used four modified variables. The modified variables can be defined as the variables that affect the direction or strength of the relationship between the independent and dependent variables. The modified variables differ from the control variables, as the control variables affect the dependent variable directly.

The study concluded that there is a significant impact of the importance of disclosing the cybersecurity risk management report, and that there is a significant impact of the proposed role of the auditor and its impact on the financial statements.

Keywords: Cyber Security - Cyber Security Risks - Cyber Security Risk Management - Confidence in the Auditor - Significance of the Financial Statements.

١ـ المقدمة

يمثل الأمن السيبراني أحد اهم التحديات التي تواجه دول العالم كافة ومن أبرز التحديات التي تظهر نتيجة التطور الرقمي والتكنولوجي السريع الامر الذي يستدعي النهوض بمنظومه الأمن السيبراني، حيث يهتم الأمن السيبراني بالحفاظ على سرية وتكاملية وتوافرية المعلومات من أي تهديد سيبراني للشركة، وذلك بتحسين ضوابطها الأمنية ووضع الاجراءات والتدابير المناسبة وتطوير الاليات الكفء والفعالة لمواجهه التهديدات السيبرانية التي قد تعترضها، وتأمين الحماية اللازمة ضد محاولات الاختراق السيبراني للأنظمة والمعلومات وعمليات القرصنة الإلكترونية (Thomas G. Calderon, et al., 2020). ويتطلب ذلك من الشركات تنظيم الاجراءات والوسائل الواجب اتباعها بما يتماشى مع أفضل الممارسات المتبعة عالميًا بهذا الخصوص لإدارة

المخاطر السيبرانية وتعزيز ضوابط حمايه الأنظمة والبرمجيات والشبكات والأجهزة الشبكية والاستجابة لحوادث الأمن السيبراني الطارئة والتعافي منها.

ويعد تقرير المراجع عن إدارة المخاطر السيبرانية وسيله للشركات لتوصيل جهود إدارة مخاطر الأمن السيبراني إلى اصحاب المصلحة والمهتمين. وهذه التقارير طوعيه ويستلزم التقرير وصفًا سرديًا لبرنامج إدارة مخاطر الأمن السيبراني للشركة وما إذا كانت ضوابط الأمن السيبراني تعمل بشكل فعال خلال الفترة المشمولة بالتقرير والمخاطر الحالية التي تعرضت لها الشركة وسبل ادارتها مع تقييمها من حيث حجم التأثير والمخاطر المحتملة واوجه التصدي لها. الامر الذي يدعو إلى دراسة هذا الموضوع وتحديد مشكله الدراسة وتساؤلاتها والتي يمكن ان تساعد في موضوع الدراسة الحالية. (Jim Peterson, 2022)

٢- مشكلة الدراسة:

يشكل أرتفاع الهجمات السيبرانية مخاطر كبيرة على البرامج والتطبيقات المالية وصحة التقارير التى تنتج عنها، ويتضح هذا بشكل خاص مع استمرار الجهات القائمة بالتهديد في استهداف التطبيقات التجارية الحيوية التي تحتوي على كميات هائلة من البيانات المالية للشركة والموظفين والعملاء وما ينتج عنها من تقارير مالية موثوقة لدى المستثمرين وحملة الاسهم والبنوك والمساهمين وكافة المستفيدين. (محمود أحمد أحمد علي، صالح علي صالح علي، ٢٠٢٢)

وحتي وقت قريب كانت علاقة الامن السيبراني بالبيانات المالية ترتكز على الانشطة الاحتيالية التي تؤثر على صافي أرباح الشركة وتعوق نموها، ومع استمرار تزايد هذه الانتهاكات والهجمات بدأ خبراء الصناعة والمهتمين في ملاحظة أن المراجعين لايقومون بالدور الكافي للنظر في المخاطر التي تسببها هذه الهجمات وهو ما يدفع أعضاء مجلس الإدارة والمديرين وفرق المراجعة الى البدء في دمج الأمن السيبراني في كيفية رؤيتهم للأمتثال للقوانين واللوائح والتشريعات والتفويضات المتعلقة بخصوصية وسياسة الشركات بشأن الحماية لديها، وهو الأمر الذي يتطلب قيام مجالس موثوقة بإصدار مبادرات توجيهية. (Edith Orenstein, 2017)

لذلك فقد زاد اهتمام المجالس التنظيمية والمجالس المعنية بإصدار الارشادات المحاسبية لدعم إفصاح الشركات عن مخاطر الأمن السيبراني وكيفيه إدارة هذه المخاطر. كما إصدارات هيئه البورصة الأمريكية SEC ارشادات حول الإفصاحات عن عوامل خطر الأمن السيبراني الجوهرية في عام ٢٠١١ و٢٠١٨ كما وضع المعهد الامريكي للمحاسبين القانونيين AICPA إطارا للتقرير عن مخاطر الأمن السيبراني لإرشادات الشركات في تعزيز إفصاحاتها المتعلقة بالأمن السيبراني، وأصدرت هيئة سوق المال السعودي CMA دليلا ارشاديا للأمن السيبراني لمؤسسات السوق المالية بهدف تخطيط الضوابط المتعلقة بالأمن السيبراني لمؤسسات السوق السعودي والتي تساعد على تحسين إدارة مخاطر الأمن السيبراني من خلال تبني افضل الممارسات العالمية وتشريعات الأمن السيبراني السعودي. (الدليل الاسترشادي للأمن السيبراني، ٢٠١٩)

وقد اصدر البنك المركزي الاردني في عام ٢٠١٨ تعليمات التكيف مع مخاطر الأمن السيبرانيه كمفتاح رئيسي لرفع كفاءه القطاع المالي والمصرفي في المملكة الأردنية في مواجهه التحديات والمخاطر السيبرانيه. وفي مصر وضع المجلس الاعلى للأمن السيبراني التابع لرئاسة مجلس الوزراء برئاسة وزير الاتصالات وتكنولوجيا المعلومات في عام ٢٠١٧ استراتيجية وطنيه للأمن السيبراني العام (٢٠١٧- ٢٠٢١) وذلك في إطار جهود الدولة لدعم الأمن القومي وتنميه المجتمع المصري. (Mcit.gov.eg/upcont, 2017-2021)

كما أن جميع انواع المخاطر الإلكترونية تتطور بسرعه عالية وبطريقه غير متوقعه، فطبيعة المخاطر السيبرانيه تجعل ادارتها صعبه بشكل خاص وبسبب الطبيعة المتغيرة للمخاطر السيبرانيه تحتاج الشركات إلى تحقيق المرونة والقدرة على الصمود قدر الامكان، هذا ويجب ان يقترن مبدا التصميم السيبراني بنهج للمراجعة الدورية واعاده تقييم المخاطر لتحديد اولويات متطلبات الأمن السيبراني. فالشركات تحتاج أيضًا إلى الاستعداد لاتخاذ قرارات صعبه حيث انها تعمل على تحويل الوعي العام والقلق بشان الجرائم الإلكترونية إلى اجراءات فعالة. وتوجد اسباب مختلفة لذلك منها المعرفة والحوافز الإقتصادية غير

الكافية والتحديات المحددة حول طبيعة المخاطر السيبرانيه. وتحتاج الشركات اليوم إلى الاعتراف بالأمن السيبراني الجيد كضرورة للعمل وتشكيل ادارتها للمخاطر الإلكترونية لتحقيق اقصى قدر من الفوائد. (ICAEW, 2016,)

وتتعلق مسئوليه مراجع الحسابات المستقلة بمراجعة القوائم المالية ومراجعة الرقابة الداخلية على التقارير المالية. وفيما يتعلق بالأمن السيبراني فإن نظم وبيانات تكنولوجيا المعلومات المتعلقة بالتقارير المالية التي قد تكون في نطاق المراجعة الخارجية هي عادة مجموعه فرعيه من النظم والبيانات الكلية التي تستخدمها الشركات لدعم عملياتها التجارية، ويمكن اضافتها والتحكم فيها بشكل منفصل. وبناء على ذلك فان مراجعة القوائم المالية والرقابة الداخلية على التقارير المالية لا تشمل تقييم لمخاطر الأمن السيبراني عبر منصة تكنولوجيا المعلومات بأكملها للشركة. لذلك سيكون مراجع الحسابات مسئولا عن تقييم مخاطر التحريف الجوهري في القوائم المالية للشركة نتيجة الوصول غير المصرح به إلى نظم وبيانات تكنولوجيا المعلومات المتعلقة بالتقارير المالية. كما أن مراجع الحسابات مسؤول عن تقييم المحاسبة التي تقوم بها الشركة عن الخسائر المتعلقة بالأمن السيبراني وعن تقييم الاثر على القوائم المالية للشركة والأفصاحات المالية. (الصيرفي، أسماء أحمد، ٢٠٢٢)

وفي بيئة الاعمال المصرية وبصدد التقرير عن مخاطر الأمن السيبراني افادة الدراسات بضعف الافصاح عن مخاطر الأمن السيبراني وبرامج إدارة مخاطرة في شركات تكنولوجيا المعلومات وكذلك القطاع المالي المصرفي، بالإضافة إلى عدم اصدار اية تنظيمات أو ارشادات للشركات المصرية المسجلة تُدعم الشركات في الافصاح عن مخاطر الأمن السيبراني وبرامج إدارة مخاطرة حيث تعتبر الإستراتيجية الوطنية للأمن السيبراني عامه وغير موجهه للشركات المسجلة في سوق الأوراق المالية. (الرشيدي، طارق عبدالعظيم، عباس، داليا عادل، ٢٠١٩)

وبالرغم من أهمية إدارة انشطه ومخاطر الأمن السيبراني للشركات وبالرغم من الاثار السلبية السيئة المترتبة على اختراقات الأمن السيبراني وضرورة الافصاح عن ذلك للأطراف المعنية داخل وخارج الشركة لم تصدر الهيئة العامة للرقابة المالية أو

البورصة المصرية أو البنك المركزي اية تعليمات لتوجيه الشركات للإفصاح عن انشطه الأمن السيبراني لديها والتهديدات والمخاطر التي تتعرض لها وبرنامج إدارة المخاطر لمواجهه هذه التهديدات. (عبدالمنعم باهي الدين متولي وأخرون، ٢٠٢٢)

وبذلك تتضح أهمية الإجابة علي التساؤل الرئيسي للدراسة وهو ما الدور المقترح لمراجع الحسابات في أضفاء الثقة على تقرير إدارة مخاطر الأمن السيبرانى وأثره في دلالة القوائم المالية؟ ويتفرع عن هذا التساؤل الرئيسي مجموعه من التساؤلات الفرعية وهي:

١- ماهي طبيعة الأمن السيبراني؟ وما هي طبيعة مخاطر الأمن السيبراني وكيفيه ادارتها في الشركات؟
٢- ما هو دور المنظمات المهنية في دعم التقرير عن مخاطر الأمن السيبراني ودعم دور المراجع في اضفاء الثقة على تقرير إدارة مخاطر الأمن السيبراني؟
٣- ما هو التوصيف المهني لخدمه توكيد المراجع عن تقرير إدارة مخاطر الأمن السيبراني؟
٤- ما هو طبيعة تقرير الإدارة عن مخاطر الامن السيبراني فى الشركات المساهمة المصرية؟
٥- ما هو انعكاس دور المراجع على تقرير إدارة مخاطر الامن السيبراني وأثرة في دلالة القوائم المالية؟

٣- مفاهيم الدراسة:

١/٣ الأمن السيبراني: هو مجموعة من التقنيات والعمليات التي تم تصميمها لحمايه (الأنظمة والشبكات والبرامج وقواعد البيانات بما تحويه من بيانات وما تقدمه من خدمات) من الهجمات والوصول غير المصرح به أو تعطيل أو استخدام أو استغلال غير مشروع.

٢/٣ مخاطر الأمن السيبراني: هي المخاطر التي تهدد عمليات الشركة بما في ذلك رؤيه الشركة أو رسالتها أو ادارتها أو صورتها أو سمعتها أو اصول الجهة أو الأفراد بسبب امكانيه الوصول غير المصرح به أو الاستخدام أو الافصاح أو التعطيل أو التعديل أو تدمير المعلومات أو نظم المعلومات.

٣/٣ إدارة مخاطر الأمن السيبراني: تتمثل إدارة المخاطر في تحديد المخاطر وتحليلها والاستجابة لها ومراقبتها واستعراضها باستمرار وذلك بغرض حمايه المعلومات والأنظمة الأمنية التي يمكن ان تُعرض تحقيق أهداف الأمن السيبراني للخطر وتوضيح الاستجابة والتخفيف من الاحداث الأمنية التي لم يتم منعها في الوقت المناسب.

٤/٣ ويعني مفهوم اضفاء ثقة المراجع على تقرير إدارة مخاطر الأمن السيبراني ان يقوم مراجع الحسابات بتقييم والتعبير عن استنتاج من خلال إبداء رأي فني محايد بشان إفصاح الشركة للتقرير عن برنامج إدارة مخاطر الأمن السيبراني بما يتضمنه من عناصر وضوابط من أجل إضفاء مصداقيه على المعلومات الواردة في تلك التقارير وزياده درجه الثقة والاعتماد عليها في اتخاذ القرارات.

٤- هدف الدراسة:

تهدف الدراسة بشكل رئيسي إلى توضيح الدور المقترح لمراجع الحسابات في اضفاء الثقة على تقرير إدارة مخاطر الأمن السيبراني للشركات وأثره في دلالة القوائم المالية، ويتفرع من هذا الهدف مجموعه من الاهداف الفرعية وهي:

١/٤ التعرف على طبيعة مخاطر الأمن السيبراني وكيفيه ادارتها لدي الشركات المساهمة المصرية.

٢/٤ توضيح ما إذا كانت مخاطر الأمن السيبرانى ذات صلة بعمليات مراجعة القوائم المالية، ومدى دور مراجع الحسابات، وهل يحتاج مراجع الحسابات إلى مراعاة مخاطر الأمن السيبراني لعملائه عند التخطيط لعمليه المراجعة وتنفيذها.

٣/٤ توضيح الارشادات المتوفرة حول كيفيه دمج اعتبارات مخاطر الأمن السيبرانى كجزء من تقييم المخاطر اثناء تحديث تخطيط عمليه المراجعة، واستجابات المراجعين المناسبة لمخاطر الأمن السيبراني التي تم تحديدها.

٤/٤ معرفة دور المراجع في اضفاء الثقة على تقرير إدارة مخاطر الامن السيبراني وأثرة في دلالة القوائم المالية.

٥- أهمية الدراسة:

تكتسب هذه الدراسة أهميتها العلمية من حيوية وحداثه الموضوع بالإضافة إلى المبررات الاخرى التالية الداعمة لهذه الأهمية وهي:

١/٥ في ظل الاتجاه نحو التحول إلى رقمنه العمليات وسلاسل التوريد والمعاملات التجارية فمن المتوقع ان تكون الهجمات السيبرانيه احد التهديدات الرئيسية، لذلك يعد الأمن السيبراني الركيزة الأساسية للتحول الرقمي الأمن.

٢/٥ تحول الشركات في ظل الظروف الحالية التي تواجهها الاقتصاديات مثل جائحة كورونا إلى العمل عن بعد لحمايه عمالها مع الاستمرار في خدمه عملائها، حيث نقلت جميع انشطتها إلى بيئة افتراضية، وقد تؤدي بيئة العمل الجديدة هذه إلى تعريض الشركات لنقاط ضعف الكترونيه جديده ومختلفة ينشا عنها مخاطر الإلكترونية.

٣/٥ ندرة الدراسات الأكاديمية التي تناولت بشكل مباشر وتفصيلي دور مراجع الحسابات في اضفاء الثقة على تقرير إدارة مخاطر الأمن السيبراني وأثره في دلالة القوائم المالية.

٤/٥ بتطور الشركات استجابة للمخاطر الجديدة والمتزايدة التي تتعلق بالأمن سيبرانى سيحتاج مراجعي الحسابات إلى تحديث فهمهم لبيئة تكنولوجيا المعلومات وفقا لذلك، ومراجعة تقييمات المخاطر واجراءات المراجعة استجابة لأي مخاطر جديده أو مختلفة للتحريف الجوهري الذي يمكن ان يؤثر على القوائم المالية.

٥/٥ بالرغم من الاثار السلبية للمخاطر الإلكترونية وتأثيرها في اعداد القوائم المالية ومن ثم على دور المراجع في مراجعة القوائم المالية لم يصدر اي تشريعات تنظم العرض والإفصاح عن هذه المخاطر بالتقارير المالية من قبل الشركات، وطريقه عمل المراجع في أضفاء الثقة على تقارير هذه المخاطر.

٦- فروض الدراسة:

١/٦ لا يوجد تأثير معنوي لأهمية الإفصاح عن تقرير إدارة مخاطر الامن السيبراني.

٢/٦ **لا يوجد تأثير معنوي** لاهمية دور المراجع المقترح على دلالة القوائم المالية مع ثبات الثقة بتقرير ادارة مخاطر الامن السيبراني.

٧- الدراسات السابقة:

١/٧ دراسة National audit office, 2017

"ارشادات للجان المراجعة حول مخاطر الأمن السيبراني".

هدفت هذه الدراسة إلى إصدار توجيهات لمساعده لجان المراجعة في القطاع العام على النظر في المسائل التي تتعلق بالمخاطر المرتبطة بالأمن سيبراني وفي تنظيم مناقشاتها مع ممثلي الإدارة ، وأشارت الدراسة إلى انه إلى جانب الوعي المتزايد بالمخاطر المرتبطة بالأمن السيبراني من قبل لجان المراجعة في القطاع العام فإنه لا يزال هناك قدر كبير من عدم اليقين حول كيفيه معرفه اللجان لمسؤولياتها على افضل نحو في هذا المجال. وواضحت الدراسة انه يجب ان تكون لدي الادارات والهيئات العامة الثقة في سرية بياناتها وسلامتها وتوافرها، وأن تخضع اي بيانات يتم جمعها وتخزينها ومعالجتها من قبل الهيئات العامة أيضًا لمتطلبات قانونيه وتنظيمية محدده، وتشكل الحوادث السيبرانيه تهديدا متزايدا لإدارة الهيئة العامة لمعلوماتها ومن ثم لابد من حمايه الخدمات العامة والمستخدمين خاصه مع استمرار الحملة لجعل الخدمات العامة رقميه.

وفي العديد من المنظمات لم تواكب قدره الموظفين التعامل مع هذه المخاطر، حيث ينشا تعقيد اضافي عندما تحتاج الهيئات العامة إلى تبادل البيانات، وتحتاج المؤسسات إلى ان يكون لها ثقه متبادلة في قدره بعضها البعض على الحفاظ على أمن البيانات واتخاذ الضمانات من إدارة المخاطر الخاصة ببعضها البعض وذلك حتى يتسنى تحقيق فوائد عدم تعرض معلوماتها لخطر متزايد من خلال مشاركتها عبر شبكة أوسع.

- وفي ضوء الدراسة يمكن القول بأن لجان المراجعة لاتزال لديها قدر كبير من عدم اليقين حول المعرفة الكافية بمسئولياتها على افضل نحو في هذا المجال وهو ما يدعو هذه اللجان الى ضرورة دعم سياستها اتجاة وجود ضوابط وتدابير محددة للأمن السيبراني ومطالعة كافة التوجيهات المهنية والارشادات المتعلقة بالموضوع وهو ما ستلقي علية الدراسة الحالية الضوء.

٢/٧ دراسة Rosati, et, al, 2018:

"حوادث الأمن السيبراني والمراجعة الخارجية واحتمال اعادة الصياغة".

قامت الدراسة ببحث كيف يتفاعل المنظمون ومراجعي الحسابات الخارجيين مع حوادث الأمن السيبرانى في العامين التاليين للخرق. حيث أن عدد الحوادث زادت بشكل كبير في السنوات القليلة الماضية بالإضافة إلى التكاليف التي تولدها للشركات المتضررة وعادة ما يلقى اثر هذه الحوادث على الشركات والأفراد المتضررين اهتمامًا كبيرًا من وسائل الاعلام والباحثين على حد سواء. غير ان حوادث الأمن السيبراني تمثل أيضًا مخاوف رئيسيه للجهات التنظيمية ولمراجعي الحسابات الخارجيين للشركات المتضررة . وفي حين ان المنظمين يشعرون بالقلق بشان تأثير ذلك على الاقتصاد العام فان مراجعي الحسابات الخارجيين يواجهون اضرار محتملة في السمعة إذا اسفر الخرق الأمني عن نتائج ماليه مضلله. وأفادت الدراسة بأن الشركات التي تم خرقها تخضع لمزيد من المراجعة من قبل المنظمين ومراجعي الحسابات الخارجيين على حد سواء في اعقاب خرق أمني وهذا يؤدي إلى احتمال ارتفاع جوده المراجعة وانخفاض احتمال اعاده القوائم المالية. واظهرت نتائج الدراسة ان حوادث الأمن سيبراني تمثل احداث بارزه ليس فقط للشركات المتضررة ولكن أيضًا بالنسبة للموظفين ومراجعي الحسابات الخارجيين الذين يحاولون الحد من النتائج السلبية لهذه الحوادث من خلال زياده المراقبة وتعزيز الضوابط.

- وبذلك تفيد هذه الدراسة بأن المراجعين الخارجيين قد ذاد وعيهم نتيجة المخاطر السيبرانية التى تتعرض لها الشركات وهو ما يؤدى الى زيادة جودة اعمال المراجعة للحصول على تقارير مالية أكثر دقة وهو ما يدعم الدراسة الحالية للوصول الى موثوقية ودلالة القوائم المالية في الشركات التى تتعرض لهذه الهجمات وأثرها على المستثمرين والمستفيدين .

٣/٧ دراسة Eaton, et, al, 2019:

"إدارة مخاطر المحاسبة والأمن السيبراني".

أفادت الدراسة بانة مع استمرار ارتفاع عدد حوادث الأمن السيبراني وتزايد قلق اصحاب المصلحة تكرس الشركات موارد كبيره لجهودها في إدارة مخاطر الأمن السيبراني وما يتصل بذلك من الإفصاحات عن الأمن السيبراني، وقامت بوصف كيف ان المحاسبين في وضع فريد لمساعده الشركات في هذه الجهود في مجال الاستشارات والضمانات. فقد ادركت شركات المحاسبة هذه الاتجاهات ووضعت ممارسات استشارية تشمل مجموعه واسعه من الخدمات لمساعده الشركات من جميع الاحجام على استباق التهديدات السيبرانيه والافصاح خارجيا عن جهودها لإدارة مخاطر الأمن السيبراني إلى مستثمريها واصحاب المصلحة الاخرين. وتقوم شركات المحاسبة باستخدام معرفتها بالضوابط الداخلية والافصاح الخارجي وبالتأكيد على ممارساتها في مجال الأمن السيبراني. وهذا يخلق ميزة على الاستشارات غير المحاسبية في مجال الأمن السيبراني ، ومن المتوقع ان تنمو هذه الممارسات بسرعه مع زياده عدد الشركات التي تسعى للحصول على مساعده في حمايه معلوماتهم. كما ينبغي ان يزداد طلب السوق مع بدء الشركات في الافصاح في التقارير الخارجية عن جهود إدارة مخاطر الأمن السيبراني والحصول على توكيد لهذه التقارير. وقدمت الدراسة نموذج لإدارة مخاطر الأمن السيبراني الفعال، واوضحت الدراسة خمس خطوات في تحقيق الإدارة الفعالة لمخاطر الأمن السيبراني. وناقشت كيف يمكن للكفاءات الأساسية للمحاسبين ان تضيف قيمه كبيره في كل مرحله من المراحل الخمس للنموذج. واستخدمت العديد من حوادث الأمن السيبراني كأمثله توضيحيه في كل مرحله من المراحل الخمس والاثار المترتبة على المحاسبين.

- أكدت الدراسة على الدور الفعال للمراجعين الخارجيين في دعم برنامج وسياسة الشركة لمواجهة المخاطر السيبرانية وما اضافة المراجعون من قيمة كبيرة على

النموذج المعد لمواجهة هذه المخاطر وهو ما دفع الباحث للتعرف على الدور المقترح للمراجع لمواجهة مثل هذه الهجمات في بيئة الاعمال المصرية.

٤/٧ دراسة Musaib et al,2020 :

" تأثير للجنة المراجعة في مجال تكنولوجيا المعلومات على موثوقية التقارير المالية"

تهدف الدراسة الى فحص ومعرفة ما اذا كانت خبرة لجان المراجعة في مجال تكنولوجيا المعلومات تؤثر على موثوقية التقارير المالية وحسن توقيتها من عدمة.

وتمثلت عينت الدراسة في عدد من الشركات التي تمتلك جميعها تكنولوجيا معلومات عالية الجودة بشكل عام.

وتوصلت النتائج الى وجود تقليص في احتمالية نقاط الضعف المادية المتعلقة بتكنولوجيا المعلومات والتي تمثل ٥٥% من جميع نقاط الضعف المبلغ عنها لدى الشركات، وكذلك اعلانات الارباح في الوقت المناسب في الشركات التي لديها خبرة في مجال تكنولوجيا المعلومات . وتوصلت النتائج الى أن خبرة للجان المراجعة في مجال تكنولوجيا المعلومات يضفي قدر كبير من الثقة على التقارير المالية . وتعد هذه النتائج قوية للتحكم في سمات تكنولوجيا المعلومات الأخرى للشركة.

- اشارت الدراسة خبرة لجان المراجعة في مجال تكنولوجيا المعلومات واوضحت انها تضيف قدر كبير من الثقة على التقارير المالية ولكنها لم تتعرض الى الأثار السلبية والمخاطر التى يمكن ان تتعرض لها وكذلك دور المراجع في ضوء هذه التكنولوجيا الجديدة وهو ما سيتناولة الباحث في موضوع الدراسة الحالية.

٥/٧ دراسة Pierangelo, et, al, 2020:

"حوادث الأمن السيبراني وجوده المراجعة".

هدفت الدراسة إلى تقييم اثار جوده المراجعة لخروقات البيانات وذلك نتيجة ضعف الرقابة الداخلية واعتبار ان حوادث الأمن السيبراني تمثل خطرا كبيرا لجوده التقارير المالية.

وتمثلت عينة الدراسة في عدد من الشركات الأمريكية وذلك من خلال نهج الاختلاف في الفروق بين الشركات المخترقة وغير المخترقة.

وأشارت النتائج إلى أنه لم يتم التوصل إلى دليل على ان حوادث الأمن السيبراني تؤدي إلى انخفاض جوده المراجعة وعلى العكس تلاحظ وجود تحولات ايجابيه في اربعه وكلاء مستخدمه على نطاق واسع لجوده المراجعة كما توصلت النتائج إلى ان المراجعين قد عوضوا بشكل فعال الزيادات في مخاطر المراجعة من خلال الاختبارات الجوهرية وجهود المراجعة كما اشارت النتائج إلى ان المراجعين قد زاد من وعيهم بمخاطر المراجعة ووضعوا اجراءات مناسبه للتعامل مع عواقب حوادث الأمن السيبراني.

- أكدت الدراسة على ما قدمتة دراسة (Rosati 2018) وهو ذيادة وعي المراجعين اتجاه المخاطر السيبرانية وهو ما يؤدي الى ذيادة جودة عملية والمراجعة وبالتالى انتاج تقارير مالية أكثر دقة وهو مايدعم الدراسة الحالية للحصول على دلالة عالية للقوائم المالية يستفيد منها المستثمرون .

٦/٧ دراسة هبة، ٢٠٢١:

"أثر جودة ومستوى التوكيد على برنامج إدارة مخاطر الأمن السيبراني على قرارات المستثمرين المصريين غير المحترفين".

هدفت الدراسة إلى اختبار وتحليل أثر جودة التوكيد (المقاسة من خلال حجم مكتب المراجعة الذي يوفر هذا التوكيد ، ومكتب مراجعة ينتمي إلى احدي مكاتب المراجعة الاربعة الكبار في مقابل مكتب مراجعة أخر بخلاف هذه المكاتب) ومستوى التوكيد (توكيد معقول في مقابل توكيد محدود)على برنامج إدارة مخاطر الأمن السيبراني على رغبة المستثمرين غير المحترفين في الاستثمار وتقيمهم لأسهمهم.

تكونت عينة الدراسة من ٦٤ طالب دراسات عليا في كلية التجارة جامعة الاسكندرية وجامعة اسلسكا وذلك من خلال بعض التجارب التي اجرتها لإختبار فروض الدراسة.

وتوصلت الدراسة إلى وجود دليلاً على أن لجودة التوكيد المرتفعة ومستوى التوكيد المعقول تأثير جوهري وايجابي على رغبة المستثمرين في الاستثمار وتقيمهم لأسهمهم.

ومع ذلك لم يجد الباحث أختلاف كبيرا في رغبة المستثمرين في الاستثمار أو في تقيمهم لأسهمهم بين الحالة التي يتم فيها توفير تقرير توكيد محدود من قبل مكتب مراجعة ينتمي إلى إحدى مكاتب المراجعة الاربعة الكبار وبين الحالة التي يتم فيها توفير تقرير توكيد معقول من قبل مكتب مراجعة آخر بخلاف إحدى مكاتب المراجعة الاربعة الكبار.

- وبذلك تفيد الدراسة بأن جودة المراجعة ومستوى التوكيد له تأثير جوهري على رغبة المستثمرين في الاستثمار وتقيمهم للأسهم ،كما ان تعرض الشركات للمخاطر السيبرانية دون وضع تدابير لمواجهتها سوف يعوق جودة المراجعة لذلك سوف تتناول الباحثة موضوع التوكيد لدعم دور المراجع في اضفاء الثقة على تقرير إدارة المخاطر وأثرة في دلالة القوائم المالية وهو ما لم تتناولة الدراسة الحالية.

٧/٧ دراسة Prigerson et al ,2021:

"قضايا تتعلق بتوقيت وموثوقية البيانات المالية للشركة وخبرة لجان المراجعة في تكنولوجيا المعلومات".

يعتبر الغرض من الدراسة هو فحص ما اذا كانت خبرة لجان المراجعة في مجال تكنولوجيا المعلومات تؤثر في موثوقية القوائم المالية للشركات وحسن توقيتها أم لا.
واشتملت عينة الدراسة على ٣١٣٨١ ملاحظة سنوية للشركات لتحليل أعادة البيانات و٢٧٤٤٩ ملاحظة سنوية ثابتة لتحليل نقاط الضعف المادية ٢٦٤١١ ملاحظة سنوية ثابتة لأيام تحليل أعلان الارباح.
وتشير نتائج الدراسة الى أن خبرة لجان المراجعة في مجال تكنولوجيا المعلومات مرتبطة بشكل سلبي وكبير بإعادة البيانات المادية ونقاط الضعف المادية المتعلقة بتكنولوجيا المعلومات وتأخر أعلان الارباح، وتشير الدراسة الى انة من غير المرجح أن تؤثر خبرة لجان المراجعة في مجال تكنولوجيا المعلومات في أعادة الصياغة غير المادية وتقاط الضعف المادية غبر المتعلقة بتكنولوجيا المعلومات . ولكن تم التوصل الى أن المستثمرون يستجيبون بشكل أكبر للتقارير المالية في الشركات التي لديها خبرة في شكل لجان مراجعة خبيرة في تكنولوجيا المعلومات وذلك لوجود دلالة على

استجابة اعلى للأرباح، وأن تكلفة رأس المال السهمي أقل في هذه الشركة وأنها أقل عرضة للمقاضاة في دعاوي الدعوى الجماعية المتعلقة بالأحتيال في الأوراق المالية.

- اتفقت الدراسة مع دراسة (Musaib 2020) بأن خبرة لجان المراجعة في مجال تكنولوجيا المعلومات تضيف قدر كبير من الثقة على التقارير المالية ولكنها لم تتناول المخاطر التى من الممكن تتعرض لها نتيجة لإستخدام هذه التكنولوجيا وما سيترتب علية من أثار سلبية تظهرها القوائم المالية في حالة الافصاح عنها وهو ما سوف يؤثر بالسلب على قرارات المستثمرين وجمهور المستفيدين.

٨/٧ دراسة Lankton, et, al, 2021:

"انتهاكات الأمن السيبراني ودور حوكمة تقنيه المعلومات في مواثيق لجنه المراجعة".

تستخدم هذه الدراسة الكفاءة والنظريات المؤسسية للتحقيق في تأثير الانتهاكات الأمنية ولجان التقنية على مستوى مجلس الإدارة في الكشف عن ادوار في ميثاق (ITG) مجموعه التقنيات المتكاملة للجنة المراجعة.

وتمثلت عينة الدراسة في ١٨٩ شركة.

وتشير نتائج الدراسة إلى ان الشركات التي لديها لجنه تكنولوجيا وخرق بيانات اكثر من المحتمل ان تكشف عن أدوار في ميثاق (ITG) مجموعه التقنيات المتكاملة للجنه المراجعة وهذا يشير إلى ان الشركات التي تتعرض لخرق البيانات تدرك مدى ضعفها ومن خلال الاشراف بالفعل على مستوى مجلس الإدارة يكون من الطبيعي بالنسبة لها زياده الاشراف من خلال تعيين أدوار إلى لجنه المراجعة في ميثاق (ITG) التقنيات المتكاملة للجنة المراجعة.

- أكدت الدراسة على أن الشركات التى لديها لجان تكنولوجيا وخرق بيانات يكون لديها قدرة أكبر على مواجهة هذه المخاطر وهو ما يدعم اهمية الدراسة الحالية نحو التعرف على دور مراجع الحسابات في اضفاء الثقة على تقرير إدارة مخاطرالامن السيبراني بأعتبار ان هذه المخاطر احد اسباب استخدام التكنولوجيا والتى يجب على المراجعون مواكبتها حتى يستطيعو مواجهة مخاطرها.

٩/٧ دراسة Eijkelenboom et al, 2021:

" تحليل الأمن السيبراني في التقارير السنوية للشركات الهولندية المدرجة ".

تهدف الدراسة الى محاولة الكشف عن معلومات الأمن السيبراني في التقارير السنوية الهولندية للشركات المدرجة ، مثل تدابير الأمن السيبراني والحوادث السيبرانية ، ثم تحليل للمتطلبات في القانون المالي للكشف عن معلومات الأمن السيبراني في التقارير السنوية ،ثم مناقشة الحوافز المقدمة لمجلس الإدارة فيما يتعلق بالإفصاح عن المعلومات المتعلقة بالأمن السيبراني وتأثيرها على أصحاب المصلحة والمساهمين.

تم عمل دراسة تجريبية استكشافية من خلال التقارير السنوية لعام ٢٠١٨ لعدد ٧٢ شركة من الشركات الهولندية المدرجة في بورصة امستردام.

وتشير نتائج الدراسة بصفة عامة الى أن أكثر من نصف الشركات المدرجة وبما يقارب ٤٠ شركة تشترك في تدابير محددة للأمن السيبراني وبالتالي فهي تفصح عن معلومات أكثر من مجرد ذكر الأمن السيبراني كموضوع مهم كما توصلت الدراسة الى انة أربع شركات فقط هي من تضع ستة تدابير محددة للأمن السيبراني، وعلى النقيض من ذلك فإنة لاتزال بعض الشركات والبنوك لم تكشف عن أي معلومات محددة فيما يتعلق بأستراتيجيتها للأمن السيبراني في حين أنها أكثر عرضة لحوادث الأمن السيبراني وهو ما يعيق حماية الدائنين والمستثمرين وأصحاب المصالح.

- أفادت الدراسة أن أكثر من نصف الشركات الهولندية المدرجة في بورصة امستردام قد وضعت تدابير محددة للأمن السيبراني وتفصح عن المعلومات المتعلقة بالأمن السيبراني وأن الشركات التى لم تكشف عن أي معلومات سوف تواجه مخاطر تعوق حماية الدائنين والمستثمرين وهو ما يدعم دراسة الباحثة لمحاولة الكشف عن مثل هذه المخاطر والتى قد تواجها الشركات المصرية كون المخاطر السيبرانية أصبحت ظاهرة عالمية تعاني منها جميع الشركات على مستوى العالم.

١٠/٧ تحليل الدراسات السابقة وإظهار الفجوة البحثية في مجال العلاقة بين المتغيرات البحثية:

- اتفقت معظم الدراسات على انه بالرغم من أهمية التصدي لمخاطر الأمن السيبراني والحوادث السيبرانيه المعترف بها على نطاق واسع الا أنه لا يوجد متطلبات واضحة من قبل المنظمين أو واضعي معايير المراجعة للمراجعين للقيام بذلك وهو ما اكدت علية دراسة National Audit Office, 2017 والتي افادت بانه إلى جانب الوعي المتزايد بالمخاطر المرتبطة بالأمن السيبراني من قبل لجان المراجعة في القطاع العام إلا أنه لا يزال هناك قدر كبير من عدم اليقين حول كيفية ممارسة اللجان لمسؤولياتها على أفضل نحو في هذا المجال،
- اكدت بعض الدراسات على أهمية دور المراجعين في التصدي لمخاطر الأمن السيبراني مثل دراسة Rosati, et, al, 2018 والتي افادت بان الشركات التي تم خرقها تخضع لمزيد من المراجعة من قبل المنظمين ومراجعي الحسابات الخارجيين على حد سواء في أعقاب خرق أمني. وتمثل حوادث الأمن السيبراني أحداث بارزه ليس فقط في الشركات المتضررة ولكن أيضًا بالنسبة للموظفين ومراجعي الحسابات الخارجيين الذين يحاولون الحد من النتائج السلبية لهذه الحوادث من خلال زياده المراقبة وتعزيز الضوابط.
- اتفقت دراسةRosati 2018 ودراسة Pierangelo et al., 2020 على أن خروقات البيانات وحوادث الأمن السيبراني لا تؤدي إلى انخفاض جودة المراجعة وعلى العكس فإنها ادت إلى تحولات إيجابية وعلى نطاق واسع في خدمات المراجعة حيث أن المراجعين قد زاد وعيهم بمخاطر المراجعة ووضعوا الاجراءات المناسبة للتعامل معها.
- وقد بينت دراسة Eaton, et, al, 2019 ان المحاسبين في وضع فريد لمساعده الشركات في هذه الجهود الاستشارات والضمانات، وناقشت كيف يمكن للكفاءات

الأساسية للمحاسبين أن تضيف قيمة كبيرة في كل مرحله من مراحل تحقيق الإدارة الفعالة لمخاطر الأمن السيبراني.

- اتفقت دراسة Musaib 2020 ودراسة Linkton et al 2020 ودراسة Prigerson et al 2021 على أن خبرة لجان المراجعة في مجال تكنولوجيا المعلومات يضيف قدر كبير من الثقة على التقارير المالية حيث أن المستثمرون يستجيبون بشكل أكبر للتقارير المالية في الشركات التي لديها خبرة في شكل لجان مراجعة خبيرة في مجال تكنولوجيا المعلومات.
- تناولت دراسة هبة ٢٠٢١ اختبار وتحليل أثر جودة المراجعة مقاسة من خلال حجم مكتب المراجعة الذي يوفر هذا التوكيد، وقد أكدت على أن جودة التوكيد المرتفعة لها أثر جوهري وايجابي على رغبة المستثمرين في الاستثمار وهو ما يؤكد على دور الدراسة الحالية نحو دور مراجع الحسابات في التوكيد على تقارير إدارة مخاطر الأمن السيبراني.
- أفادت دراسة Eijkelenbom et al 2021 بأن الشركات التي لديها تدابير محددة للأمن السيبراني يكون لديها قدرة على مواجهة مثل هذه الانتهاكات والسيطرة عليها وعلى العكس الشركات التى لم تكشف عن اي معلومات تتعلق بالأمن السيبراني فسوف تكون أكثر عرضة لمثل هذه المخاطر وهو ما يعوق حماية الدائنين والمستثمرين وغيرهم من المستفيدين.

١١/٧ ما يميز الدراسة الحالية عن الدراسات السابقة:

تختلف هذه الدراسة عن الدراسات السابقة حيث تناولت الدراسة دور مراجع الحسابات في اضفاء الثقة على تقرير إدارة مخاطر الأمن السيبرانى واثرة في دلالة القوائم المالية وذلك من حيث:

- تتناول هذه الدراسة على وجه التحديد دور المراجع في اضفاء الثقة على تقرير إدارة مخاطر الأمن السيبراني وأثره في دلالة القوائم المالية بينما تركز الدراسات السابقة ذات الصلة في الغالب على بعض المتغيرات كجودة المراجعة مثل دراسة

(Rosati, et, al, 2018) ودور لجان المراجعة مثل دراسة(musaib 2020 ودراسة prigerson 2021)

- تساهم الدراسة الحالية أيضًا في الأدبيات التي تدعم فكرة ان المراجعين يمكنهم تقليل مخاطر التحريف الجوهري وما يترتب على ذلك من تضليل وعدم مصداقية تقرير إدارة المخاطر من خلال زيادة جهودهم في المراجعة وهو ما لم تتناوله أي من الدراسات السابقة.
- تقدم الدراسة المزيد من الأدلة على أهمية دور المراجع من خلال عرض دور الهيئات التنظيمية في تدعيم دور المراجع لأضفاء الثقة على تقرير إدارة مخاطر الأمن السيبرانى.
- هذا وتفيد الدراسة بان المراجعة الخارجية للحسابات تواجه الحاجة إلى التكييف مره أخرى لمعالجة المخاطر الحرجة المرتبطة بالأمن السيبراني وهو ما يعزز الدراسة الحالية ودور المراجع في اضفاء الثقة على تقرير إدارة مخاطر الأمن السيبراني وأثره في دلالة القوائم المالية لم واجهة ومنع مثل هذه الهجمات والتي قد تكون سبب في مخاطر كبيرة قد تعوق استمرارية الشركة وبقائها.

8- خطة الدراسة:

انطلاقا من مشكلة البحث وتحقيقا لاهدافه ،ولاختبار فروضه تم تقسيم الدراسة إلى:

١/٨ المبحث الأول: مفهوم إدارة مخاطر الأمن السيبراني وتأثيرها على الشركات.
٢/٨ المبحث الثاني: أهمية الإفصاح عن مخاطر الأمن السيبراني وجهود الهيئات التنظيمية لد،عم دور الإدارة والمراجع.
٣/٨ المبحث الثالث: الدور المقترح لمراجع الحسابات في إضفاء الثقة على تقرير إدارة مخاطر الأمن السيبراني وأثرة في دلالة القوائم المالية الدراسة التجريبية.
٤/٨ منهجية البحث
٥/٨ نتيجة اختبار فروض البحث
٦/٨ نتائج البحث و التوصيات و مجالات البحث المقترحة

٧/٨ المراجع

١/٨ المبحث الأول: مفهوم إدارة مخاطر الأمن السيبراني وتأثيرها على الشركات

مع تزايد عدد حوادث الأمن السيبراني كل عام نتيجة الاستخدام المتزايد للإنترنت وتطبيقات الهاتف المحمول والتقنيات الحديثة مثل الحوسبة السحابية (Romanosky Hoffman and Acquisti, Abbasi, sarkex and chiang، ٢٠١٦).

تؤدي حوادث الأمن السيبراني بضرر كبير للشركات التي تتعرض لتلك الحوادث من حيث تكاليف الإصلاح والغرامات وفقد السمعة (Cavusoglu, Misha and et al, 2004, Rosati, Deeney cumminis, et al ٢٠١٩).

وفقاً للتقارير الأخيرة عن الأمن السيبراني أكثر من ٢٠% من الشركات التي تتعرض لاختراق سيبراني تواجه خسارة كبيرة في الإيرادات، وانخفاض في قاعدة عملائهم، وخسارة في فرص الأعمال؛ بتكاليف احتمالية تبلغ حوالي ١٧ مليون دولار أمريكي لكل شركة (cisco 2017, Ponemon Institute، ٢٠١٦).

تصنع الشركات أنظمة رقابة داخلية لتقديم تاكيدات معقولة لبلوغ الأهداف المتعلقة والكفاءة التشغيلية والفعالية والتقارير المالية الموثوقة، والامتثال للقانون واللوائح (Coso، ٢٠٠٤).

قد يكون حادث الأمن السيبراني له تأثير مباشر على الضوابط الداخلية للتقارير المالية (ICFR) للشركة التي تم اختراق أمنها السيبراني.

في هذه الحالة تكون دفاتر وسجلات الشركة قد تغيرت مما قد يؤدي إلى التلاعب في التقارير المالية. تم التأكيد على هذه المشكلة مؤخراً من قبل المنظمين مثل المجلس العمومي للرقابة على الشركة محاسبياً (PCAOB) حيث حذر المجلس على وجه التحديد المراجعين الخارجين أن يأخذوا بعين الاعتبار كيف يمكن لحوادث الأمن السيبراني أن تؤثر على الرقابة الداخلية للتقارير المالية (PCAOB، ٢٠١٠، ٢٠١٣).

ومع ذلك، نظراً للطبيعة المتكاملة لأنظمة الرقابة الداخلية للشركة، فإن حوادث الأمن السيبراني يمكن أن تشكل تهديد على جودة المراجعة من خلال التأثير على

مخاطر الرقابة التشغيلية، أو على وجه الخصوص، ضوابط تكنولوجيا المعلومات (IT) لأن أنشطة إعداد التقارير المالية والتشغيلية تعتمد على ضوابط مشتركة.

إذا تم اعتماد قواعد هيئة الأوراق المالية كما هو مقترح، وستحتاج الشركات العامة إلى:

- التأكد من أن سياسات وإجراءات الاستجابة للحوادث توفر مساراً واضحاً لتصعيد الحوادث إلى قيادة الشركة / أو لجنة الإفصاح، وأن ضوابط وإجراءات الكشف في مكانها الصحيح لتغير التأثير الذي يحدثه مع الشركة حادث الاختراق السيبراني.
- إجراء تقييم للأهمية النسبية في أقرب وقت ممكن عملياً بعد العلم بالحادثة.
- الإبلاغ عن حوادث الأمن السيبراني الجوهرية، بما في ذلك أي تأثير على العمليات التجارية في غضون٤ أيام عمل من تحديدهم أن الحادث جوهري.
- الإفصاح بشكل دوري عن حركة إدارة مخاطر الأمن السيبراني واستراتيجيتها وسياساتها وإجراءاتها، بما في تحديد المسئول عن حوكمة الأمن السيبراني والتأكد من أن هذه البرامج مصممة وفقاً للمخاطر المعروفة وإعادة تقيمها بشكل دوري.
- تحديد خبرة مجالس الإدارة في الأمن السيبراني.

وعن خلفية هذه الاقتراحات فقد أصدرت (SEC) قواعد سبقت تلك الاقتراحات في (٢٠ فبراير، ٢٠١٨).

ارشادات أشارت فيها أنه يجب على الشركات العامة اتخاذ جميع الإجراءات المطلوبة لإبلاغ المستثمرين بمخاطر وحوادث الأمن السيبراني الجوهرية في الوقت المناسب، بما في ذلك الشركات التي تخضع لمخاطر جوهرية للأمن السيبراني، كما أشارت اللجنة إلى أهمية ضوابط وإجراءات الإفصاح التي توفر طريقة مناسبة لتميز التأثير الذي قد تحدثه مثل هذه الأمور على جهة الإصدار وأعمالها ووضعها المالي ونتائج العمليات، بالإضافة إلى بروتوكول لتحديد الأهمية النسبية المحتملة لهذه المخاطر والحوادث.

ومن المرجح أن يؤثر الضعف في أحد المجالات الأخرى. (Lawrence et al؛ ٢٠١٨)

١/١/٨ تأثير ضعف الرقابة الداخلية على التقارير المالية:

نقاط ضعف الرقابة الداخلية، ونقاط ضعف التحكم في تكنولوجيا المعلومات على وجه الخصوص يمكن أن يأثروا سلبياً على جودة التقارير المالية.

(Masli, Richardson and sanchez, 2016)

تشير الأبحاث الحديثة الي ان المراجعين يستجيبون لحوادث الأمن السيبراني من خلال زيادة الجهد في المراجعة وفرض رسوم أعلى على عملائهم.

(Lawrance; Li. No. and Boritz, 2016, Rosati , Gogolin and Lynn, 2019).

هناك أيضاً بعض الادلة التي تشير إلى أن اختراقات الأمن السيبراني يمكن أن تؤدي إلى ارتفاع احتمالية إعادة البيانات المالية خلال سنة من الاختراق السيبراني (Lawrence et al، ٢٠١٨).

٢/٨ المبحث الثاني: أهمية الإفصاح عن مخاطر الأمن السيبراني وجهود الهيئات التنظيمية لدعم دور الإدارة والمراجع في اضفاء الثقة على تقرير إدارة مخاطر الأمن السيبراني:

(في ٩ مارس ٢٠٢٢) اقترحت لجنة الأوراق المالية والبورصات الأمريكية (SEC) تعديلات على قواعدها لتطلب الافصاحات المتعلقة بإدارة مخاطر الأمن السيبراني، الاستراتيجية، والحوكمة، والإبلاغ عن الحوادث من قبل الشركات العامة (available at https:// www sec.gov/rules/proposed/202233-11033,pdf). وفي حالة اعتماد تلك الاقتراحات سوف تتطلب ما يلي:

- التقارير الحالية حول حوادث الأمن السيبراني المادية، والتقارير الدورية لتقييم تحديثات حول حوادث الأمن السيبراني التي تم الإبلاغ عنها سابقاً، بالإضافة إلى الكشف عن حوادث الأمن السيبراني الفردية التي تصبح جوهرية في المجموع.
- تقارير دورية عن:
  - سياسات وإجراءات الشركة لتحديد وإدارة مخاطر الأمن السيبراني.
  - مراقبة مجلس الإدارة لمخاطر الأمن السيبراني.

- دور الإدارة وخبرتها في تقييم وإدارة مخاطر الأمن السيبراني وتنفيذ سياسات وإجراءات الأمن السيبراني.
- إعداد تقارير سنوية حول خبرة مجلس الإدارة في مجال الأمن السيبراني، إن وجدت.

وفي حين أهمية معالجة الأمن السيبراني إلا أنه لا يوجد شرط صريح من قبل حكم المنظمين أو واضعي المعايير للمراجعين للقيام بذلك Li, He; No, wong, Feb 2020، وقد توصلت دراسة (Li & wong) أن رسوم المراجعة تزداد بالنسبة للشركات التي تواجه حادث اختراق سيبراني، كما وجدت الدراسة أن الرسوم المراجعة أقل بالنسبة للشركات التي لديها إفصاح سابق عن مخاطر الأمن السيبراني.

للتعرف على طبيعة الإفصاح عن مخاطر الأمن السيبراني في الشركات المصرية المسجلة في قطاع تكنولوجيا المعلومات حيث انه من القطاعات المعرضة للتهديدات والحوادث السيبرانية فقد أظهرت دراسة (الرشيدي، عباس، ٢٠١٩) ضعف الافصاح عن مخاطر الامن السيبراني ،وبرامج إدارة مخاطره في الشركات المصرية.

١/٢/٨ إطار عمل (COBIT (Control Objective for Information Technologies

أصدرت جمعية مراجعة ورقابة نظم المعلومات ISACA عام ١٩٩٦ النسخة الاولى من إطار COBIT والذي يعتبر إطار عاما لتنفيذ مهام مراجعة تكنولوجيا المعلومات وقد تم تطوير الاطار عام ١٩٩٨ وذلك نتيجة للأدراك المتزايد لأهمية تكنولوجيا المعلومات والحاجة الى رقابة فعالة على هذه التكنولوجيا(محروس، رمضان عارف و صالح ،ابو الحمد مصطفي ،٢٠٢٢) .

وقد قامت جمعية ISACA بتأسيس معهد تكنولوجيا المعلومات ITGI كمركز أبحاث لحوكمة تكنولوجيا المعلومات ، ووفقا لما قدم المعهد ITGI من تصورات وأفكار في تطوير COBIT فقد تم أصدار النسخة الثالثة من إطار COBIT 2000 والتي تضمنت إرشادات الادارة ومنها المقاييس وعوامل النجاح الاساسية ونماذج النضج لعمليات تكنولوجيا المعلومات ، وفي عام ٢٠٠٥ صدرت النسخة الرابعة من إطار COBIT

والذي يهدف الى بناء اطار عمل يلقي قبول عام في مجال حوكمة تكنولوجيا المعلومات كما أحتوت هذه النسخة على العديد من مفاهيم الادارة والحوكمة.

وفي عام ٢٠٠٦ ، ٢٠٠٨ أصدر المعهد التكنولوجي للمعلومات نسختين من إطار عمل VAL IT بالإضافة الى اصدار اطار RISK IT حيث تناولت هذه الاصدارات العمليات والمسئوليات المتعلقة بتكنولوجيا المعلومات ودورها في خلق القيمة وادارة المخاطر ومثلت هذه الاصدارات أعمال تكميلية لكل من COBIT 4 و COBIT 4.1 الصادر في ٢٠٠٧ ، وقد قام المعهد بدمج هذه الاصدارات مع الاطر وتم اصدار COBIT 5 عام ٢٠١٢ كاطار عمل متكامل للممارسات الجيدة لحوكمة وادارة تكنولوجيا المعلومات.

ويهدف COBIT الى تقديم اطار شامل لمساعدة منظمات الاعمال في تحقيق اهدافها لحوكمة وادارة تكنولوجيا المعلوات بالإضافة لكونة يعمل على تقديم وخلق قيمة مثالية من تكنولوجيا المعلومات ، كما انه يساعد في ادارة وحوكمة تكنولوجيا لمعلومات بطريقة شاملة ، بالاضافة لأنه يلائم جميع منظمات الاعمال على أختلاف احجامها سواء كانت تجارية أو غبر هادفة للربح او قطاع عام.

ويقدم اطار COBIT 5 خمسة مبادئ تعمل معا على تمكين منظمات الاعمال من بناء اطار حوكمة وإدارة فعالة مما يعمل على تحسين الاستثمار في المعلومات والتكنولوجيا واستخدامها بما يحقق اهداف اصحاب المصلحة ، وتتمثل الاهداف الخمسة في (تلبية احتياجات اصحاب المصلحة ، تغطية الشركة من البداية للنهاية ، تطبيق اطار واحد ومتكامل ، تمكين المنهج الشمولي ، فصل الحوكمة عن الادارة)

وفي نوفمبر ٢٠١٨ أصدرت النسخة الحالية من الاطار COBIT 2019 والذي يهدف الى توفير فروق أكبر في تنفيذ حوكمة تكنولوجيا المعلومات حيث تضمن تغيير لمبادئ COBIT 5 ، وتحديث لسلسلة الاهداف وادخال بعض العمليات الجديدة ، ومقدمة لمجالات التركيز التي تهدف الى التركيز على مواقف محددة لحل المشكلات ، بالاضافة الى مقدمة لعوامل التصميم التي تهدف الى تسهيل تنفيذ حوكمة تكنولوجيا المعلومات حيث يتميز COBIT 2019 عن غيره من الاطر السابقة في:

- يقدم COBIT 2019 ثلاثة اهداف جديدة للحوكمة والادارة.

- يحدد نظام حوكمة تكنولوجيا المعلومات الفعال
- يقدم سلسلة اهداف تم تحديثها
- يحدد عوامل التصميم التي يجب أخذها في الاعتبار عند تصميم نظام الحوكمة
- يقدم مفهوم مجالات التركيز والذي يهدف الى التركيز على مواقف محددة لحل المشكلات

٢/٢/٨ مقترحات SEC :

تمثل مقترحات لجنة تداول الاوراق المالية والبورصات SEC في مجال الأمن السيبراني عامل هاما وخطوة تاريخية وذلك لما لها من أثار هامة على منظمات الاعمال الامريكية المسجلة بالسوق وكذلك على المنظمات في جميع انحاء العالم ، حيث كشفت اللجنة عن وجود أقتراحين في مجال الأمن السيبراني صدر الاول منها في فبراير ٢٠٢٢(available at https://www sec.gov/rules/news/press-release/February,2022) وهو يركز على مستشاري ومنظمات الاستثمار وصناديق تطوير الاعمال المسجلة بالسوق الامريكية حيث تحتاج منظمات الاستثمار وصناديق التطوير بموجب هذا الاقتراح الى :

- اعتماد وتنفيذ السياسات والاجراءات المكتوبة للأمن السيبراني ، والتي تصمم لمعالجة مخاطر الأمن السيبراني التي قد تؤدي الى الاضرار بالعملاء.
- الافصاح عن حوادث الامن السيبراني الكبيرة التي تؤثر على منظمات وصناديق الاستثمار والتطوير وعملائهم من خلال تقرير يوجه الى SEC.
- الافصاح عن مخاطر وحوادث الأمن السيبراني الكبيرة التي وقعت خلال العامين الماليين السابقيين في كتيبات وقوائم التسجيل الخاصة بهم.

هذا وقد صدر الأقتراح الثاني في مارس ٢٠٢٢ موجها الى جميع منظمات الاعمال العامة المقيدة في السوق الامريكية والذي يهدف الى تعزيز وتوجيه الافصاحات المتعلقة بإدارة مخاطر الامن السيبراني ، والاستراتيجية ، والحوكمة ، والافصاح عن حوادث الأمن السيبراني لمنظمات الأعمال العامة التي تخضع لقواعد الافصاح الخاصة ببورصة الاوراق المالية.

ولتحقيق هذا الأقتراح فقد يتطلب من منظمات الاعمال تقديم افصاحات تتعلق بما يلي :

- سياسات واجراءات المنظمة لتحديد وادارة مخاطر الامن السيبراني من خلال قائمة موسعة ولكنها غير شاملة لأستراتيجيات وسياسات واجراءات المخاطر التي تخضع للافصاح.
- دور الادارة في تنفيذ سياسات واجراءات الأمن السيبراني.
- خبرات مجلس الادارة في مجال الأمن السيبراني واشرافه علة مخاطر الأمن السيبراني.
- حوادث الأمن السيبراني في غضون أربعة ايام عمل كما هو مطلوب لأي حدث جوهري أخر.

٣/٢/٨ مجلس معايير المراجعة والتأمين الاسترالي (AUASB):

نشر مجلس معايير المراجعة والتأمين الأسترالي (AUASB) فيما يتعلق بالنظر في مخاطر الأمن السيبراني في مراجعة التقرير المالي (محروس ،رمضان عارف و صالح ،ابو الحمد مصطفي ،٢٠٢٢). ووفقا لل AUASB يمكن أن يكون للأنتهاكات السيبرانية الأثار المباشرة وغير المباشرة على التقارير المالية من حيث :

- الأعتراف بالمخصصات أو الأفصاح عن الألتزامات الطارئة نتيجة لخرق البيانات وذلك قد يكون نتيجة لغرامات أو عقوبات من المنظمين أو اتخاذ اجراءات قانونية من قبل الأطراف المتأثرة.
- التغيير في القيمة العادلة للأصول نتيجة لحادث الكتروني فعندما يتم أستهداف صناعة معينة أو تتعرض لأزمات أو مشكلات فقد يكون هناك تردد في التعامل مع كيانات داخل تلك الصناعة.
- انخفاض قيمة الأصول بسبب انخفاض التدفقات النقدية التشغيلية نتيجة للهجوم الالكتروني حيث يؤدي الهجوم الالكتروني الى ايقاف العمليات لفترة طويلة من الوقت او قد يؤدي الى الحاق ضرر كبير بالعلامات التجارية.

وتؤكد نشرة معايير المراجعة والتأمين الاسترالي AUASB أنه يقع على عاتق المراجع مسئولية النظر في مخاطر التحريف الجوهري في التقرير المالي كجزء من اجراءات تقييم المخاطر والاستجابة بشكل مباشر عند تحديد مخاطر التحريف الجوهري.

كما أن المسئولون والتنفيذيون في الادارة والحوكمة مسئولون عن وجود عملية تقييم المخاطر بما في ذلك المخاطر الألكترونية وتنفيذ مراقبة الضوابط الداخلية للأستجابة لتلك المخاطر، كما أنه يجب أن يكون التركيز الاساسي للمراجع فيما يتعلق بمخاطر الامن السيبراني على الأنظمة والضوابط التي تتضمن أمن البيانات ذات الصلة بإعداد التقرير المالي.

٤/٢/٨ جهود الأمن السيبراني في مصر:

تكاثفت الجهود المصرية خلال الفترة الأخيرة لمواكبة التطورات الحادثة في مجال تكنولوجيا المعلومات وما يتبعها من مخاطر أصبحت بالفعل تؤثر على أمن واستمرار الشركات ، حيث صدر عن المجلس الأعلى للأمن السيبراني التابع لمجلس الوزراء المصري الاستراتيجية الوطنية للأمن السيبراني .

وتضم الاستراتيجية عدة برامج تهدف الى دعم الشركات في مواجهة المخاطر السيبرانية وتعزيز الثقة في البنية الاساسية للأتصالات والمعلومات وتطبيقاتها وخدماتها في جميع القطاعات الحيوية وتأمينها ، وذلك لتوفير بيئة رقمية أمنة وموثوقة للمجتمع المصري.

وقد حددت الأستراتيجية الوطنية للأمن السيبراني عدة برامج لتحقيق الأمن السيبراني كما يلي:

- تطوير الاطار التشريعي الملائم للأمن السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية والهوية الرقمية من خلال صياغة قواعد تشريعية جديدة وملائمة لمواجهة تلك الجرائم المعاصرة.
- تطوير منظومة وطنية متكاملة لحماية الأمن السيبراني وتأمين البنية الأساسية للأتصالات وتكنولوجيا المعلومات ، وذلك من خلال إعداد وتفعيل فرق الاستجابة للطوارئ أو فرق مواجهة حوادث أمن الحسابات في القطاعات الحيوية

- حماية الهوية الرقمية وتفعيل البنية الاساسية اللازمة لدعم الثقة في التعاملات والخدمات الألكترونية مثل بنية المفتاح المعلن التي يعتمد عليها التوقيع الالكتروني.
- اعداد الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في جميع القطاعات.
- دعم برامج ومشروعات التعاون بين الهيئات البحثية والشركات الوطنية لتطوير وتنمية وصناعة الأمن السيبراني
- نشر التوعية المجتمعية بفرص ومزايا الخدمات الالكترونية وأهمية الأمن السيبراني لحماية تلك الخدمات من المخاطر والتحديات التي تواجها. (المجلس الأعلى للأمن السيبراني التابع لمجلس الوزراء المصري ٢٠٠٧، الاستراتيجية الوطنية للأمن السبراني ٢٠١٧ – ٢٠٢١).

بالأضافة الى جهود المجلس الأعلى للأمن السيبراني وتزامن مع ما قام به لمواكبة التطورات التكنولوجية ومواجهة المخاطر الناتجة عنها فقد قام البنك المركزي المصري بإنشاء مركز الأستجابة لطوارئ الحاسب الألي بهدف توفير الحماية اللازمة للمتعاملين مع البنك وتعزيز الأمن السيبراني في القطاع المصرفي، ويقوم هذا المركز بالتعامل والابلاغ الفوري عن أي مخاطر سيبرانية وتعميم الانذار المبكر والتنبيهات واتخاذ الاجراءات الاحترازية .

كما أشارت توجيهات المركز الى ضرورة القيام بالمراقبة الأمنية وتحديد التهديدات الالكترونية المحتملة وفحص وتقييم المخاطر المرتبطة بالثغرات الامنية والبرمجيات الضارة، بالاضافى الى قيام البنك المركزي بأطلاق مبادرة تعزيز الأمن السيبراني في القطاع المصرفي والتي تهدف الى زيادة اعداد الخبراء المعتمدين دوليا في مجال الأمن السيبراني في القطاع المصرفي. (البنك المركزي المصري ٢٠١٩، تقرير الاستقرار المالي لعام ٢٠١٨)

٥/٢/٨ مجالات مراجعة الأمن السيبراني:

بشكل عام يغطي مراجعة الأمن السيبراني أربعة مجالات رئيسية:

- السياسة والحوكمة: مراجعة سياسات أجراءات المؤسسة للتأكد من أنها كافية للحماية من التهديدات الالكترونية.
- الضوابط الفنية : تقييم الضوابط الفنية للمؤسسة مثل جدران الحماية وانظمة كشف الاختراق للتأكد من فعاليتها.
- الضوابط التشغيلية : عملية تقييم الضوابط التشغيلية للمؤسسة مثل أجراءات ادارة التصحيح للتأكد من أنها كافية.
- أستمرارية الأعمال : استمرارية الاعمال والتعافي من الكوارث ووضع الخطط لمواصلة العمليات في حالة وقوع هجوم الكتروني أو تخريبي أخر.

فوائد مراجعة الأمن السيبراني:

يمكن أن يوفر مراجعة الأمن السيبراني العديد من الفوائد للمؤسسة بما في ذلك:

- تحسين الامان : من خلال تحديد نقاط الضعف في دفاعات المؤسسة ، ويمكن أن يساعد مراجعة الأمن السيبراني في تحسين الوضع الأمني العام.
- قدر أكبر من الطمأنينة : حيث يتمتع المديرون التنفيذيون ومجلس الأدارة في المؤسسة بقدر أكبر من الطمأنينة من خلال تزويدهم بتقييم مستقل لمخاطر الامن السيبراني للمؤسسة.
- زيادة ثقة العملاء : تزداد ثقة العملاء في المؤسسة عندما تأخذ الأمن السيبراني على محمل الجدية.
- تغطية تأمينية محسنة: غالبا ما يساعد مراجعة الأمن السيبراني المؤسسة في الحصول على تغطية تأمينية أفضل للمخاطر.

٣/٨ المبحث الثالث: الدور المقترح لمراجع الحسابات في اضفاء الثقة على تقرير إدارة مخاطر الأمن السيبراني.

يعتبر التركيز على دور المراجعين في المخاطر المتزايدة التي تواجهها الشركات بسبب الاختراق وحوادث الأمن السيبراني من خلال الاهتمام وتوفير رؤى حول كيفية تغير ممارسات المراجعة بسبب الحاجة إلى بيانات الحماية (La Torre et al، ٢٠١٨) من خلال تبني نظرية الممارسة (Schatzki، ٢٠٠٦) سوف توضح الباحثة

تأثير المخاطر المرتبطة بالتحول الرقمي التي يواجهها المراجعين، وكيف يمكن تفعيل دورهم في حماية بيانات الشركة.

١/٣/٨ الواقع والضغوط الخارجية التي تشكل ممارسة حماية البيانات:

يوجد مستوين من الضغوط الخارجية تشكل الحاجة إلى اعتماد تدابير حماية البيانات والأمن السيبراني للشركات.

- يتعلق المستوى الأول بالتغيرات الاجتماعية والتكنولوجية التي تولد مخاوف تتعلق بالخصوصية وأمن البيانات (Haapmakietel. 2019)
- المستوى الثاني يمثل الاعتراف واضفاء الطابع المؤسسي على هذه التغيرات على المستوى التنظيمي للشركة، من خلال تلك الرؤية يمكن تتبع الأحداث والظروف الرئيسية التي تؤثر على ممارسة حماية البيانات.

٢/٣/٨ الخصوصية وأمن البيانات:

مع تطور تكنولوجيا المعلومات وظهور البيانات الضخمة أصبح لخصوصية البيانات منظور جديد على المستويين الفردي والتنظيمي وظهور مشاكل الخصوصية من استخدام التكنولوجيا.

ولأن حدود البحث على المستوى التنظيمي فأننا سوف نعرف الخصوصية على المستوى التنظيمي بأنها حماية وأمن البيانات في الشركات (Messier, et al، ٢٠١٧) والمقصود بالحماية الحفاظ على سرية البيانات وسلامتها وتوافرها (La Torre; Iso, et al، ٢٠١٨).

وبالتالي ترتبط الخصوصية بالظواهر وتتطلب ممارسات فعالة لحماية البيانات داخل المنظمات.

٣/٣/٨ الأهداف والأنشطة: لماذا وكيف يتم تنفيذ حماية البيانات من قبل الشركات؟

نظراً لأهمية حماية البيانات من الاختراق سوف تعرض الباحثة ممارسات حماية البيانات وكيفية تطبيقها في الشركات.

تعني حماية البيانات التحكم في الأشخاص المصرح لهم بالوصول إلى البيانات ومن يمكنهم استخدامها والتأكد منهم ويدعو (Sweeney، ٢٠١٦) إلى ضرورة حماية البيانات والتدريب على الوعي الأمني داخل المنظمة وبين جميع المديرين التنفيذين.

كما يشيرSweeneyإلى أن أنجح نهج لضمان أمن البيانات هو وجود علاقة عمل صحية بين كبير مسؤولي أمن المعلومات (ISO) وبقية الفريق التنفيذي الأول.

كما يرىSweeneyطريقة أخرى وهي تضمين الدفاع ضد اختراقات الأمن السيبراني كجزء دائم من التوصيف الوظيفي لجميع كبار المديرين التنفيذيين وبالتالي تعتبر من الأوجه المعقدة بالشركات أنشطة حماية البيانات.

وإذا انتقالنا من أمن البيانات إلى أمن الشبكات والبنية التحتية الأكبر فأننا نشير إلى إطار عمل الأمن السيبراني وقد حدد المعهد الوطني للمعايير والتكنولوجيا خمسة أنشطة كلية تشكل نظام إدارة الأمن السيبراني (NIST, 2014, pp. 8-9).

ما يتعلق بـ "تحديد" الفهم التنظيمي لإدارة مخاطر الأمن السيبراني على الأنظمة والأصول والبيانات والقدرات.

"الحماية" المتعلقة بتطوير وتنفيذ الضمانات.

"تحديد" ما يتعلق بالأنشطة التي تعرف أحداث الأمن السيبراني

"الرد" بالاطلاع على الأنشطة التي تفسر أحداث الاختراق التي حدثت.

"التعافي" فيما يتعلق بخطط المرونة واستعادة القدرات التي تأثرت من أحداث اختراق الأمن السيبراني.

بالإضافة إلى هذه الوظائف تدعو الباحثة إلى إضافة وظيفة آخري وهي المساءلة، والتي تهدف إلى إبقاء الأطراف المعنية الداخلية والخارجية على إطلاع، والأنشطة التي ذكرت ومنها على سبيل المثال أنشطة الاستخبارات الإلكترونية تحتاج إلى العمل من خلال شبكة واسعة من الشركات والاتصالات، وبالمثل فإن وظيفة المساءلة تتخلل ممارسات حماية البيانات وتهدف إلى جمع المعلومات وإبقاء الجهات الفاعلة وأصحاب المصلحة على علم بالتهديدات الإلكترونية التي تواجهها الشركة.

٤/٣/٨ السؤال التالي الذي يجب معالجته هو: من يقوم بالإجراءات التي تشكل ممارسة حماية البيانات ؟

كان دور الحماية للبيانات تقليدياً على عاتق المديرين التنفيذين لتكنولوجيا المعلومات (Whitman، ٢٠٠٣) ثم تحولت الخصوصية من قضية حرجة الي قضية مهمة بسبب التوسع في استخدام البيانات الضخمة و اوضح كلا من (Wakunuma and Stahl، ٢٠١٤) أن خصوصية البيانات كقضية أخلاقية ينظر إليها" عنصر تكنولوجي يجب التعامل معه فقط في مجالات سياسات التكنولوجيا وليس كجزء من سياسات هيكلية تنظيمية شاملة"؟.

كما أوضح استطلاع رأي بين المديرين التنفيذيين في الولايات المتحدة إلى أن ٤٠ في المائة اعترفوا بأنهم يفتقرون إلى فهم الأمن السيبراني (Sweeney، ٢٠١٦).

وهذا يؤكد واسطورة مفادها أن تكنولوجيا المعلومات فقط التي يمكنها فهم كيفية حماية البيانات.

لذلك يجب أن تمتد ممارسات حماية البيانات في المؤسسات إلى حدود قسم واحد مثل (قسم أمن المعلومات أو تكنولوجيا المعلومات) وأن تشمل الهياكل التنظيمية وحوكمة الشركات بأكملها لأنها تحتاج إلى الوعي والمساءلة من جميع الجهات الفاعلة مثل المديرين التنفيذيين والموظفين (Sweeny, 2016, pp.٣).

٥/٣/٨ الدور المتطور للمراجعين في ممارسة حماية البيانات:

من الاقسام السابقة نستطيع فهم خصوصية المعلومات والمخاطر المرتبطة بها تتطلب معرفة شاملة بمن يتحمل مسئولية ضمان حماية بيانات المؤسسة (Tran Nguen Bao and Andrea Tick، ٢٠٢١).

ومنذ بداية عمليات المراجعة، كان دور المراجع يتقلب استجابة للأحداث والضغوط الخارجية، كما يجب على المراجعين بموجب المعايير الدولية للمراجعة (Hatherly) (ISA، ٢٠٠٩) مراعاة القوانين واللوائح التي لها تأثير جوهري مباشر أو غير مباشر على البيانات المالية في الوقت الحاضر، يطلب من المراجعين

الاستجابة لمزيد من الضغوط الخارجية الناشئة من مطالبة المجتمع بالخصوصية وحماية البيانات.

ونظراً لصعوبة المسئولية الملقاه على عاتق المراجعين فسوف نوضح الدور المتطور للمراجعين لتحديد مهامهم في ضوء الممارسة الحالية والمستقبلية لحماية البيانات.

٦/٣/٨ تغيرات في دور المراجعين في بيئة البيانات الضخمة وممارسة حماية البيانات:

تؤثر الحوسبة المنتشرة على الطريقة التي تعمل بها الشركات حيث تصبح التكنولوجيا الرقمية في كل مكان (Bloern el al, 2014) فالنظر إلى تطور تكنولوجيا المعلومات المتقدمة مع تحليلات البيانات التنبؤية والهواتف الذكية والأتمتة الإدارية التقليدية، وأمور أخرى تلك التي تتعلق بالآلية والأتمتة التي تم تصميمها وتطويرها كبداية للثورة الصناعية، لأن البيانات الضخمة وتحليلات الأعمال تتغلغل بشكل متزايد في جميع جوانب الشركات الكبيرة، فأنها تواجه أيضاً أنظمة المحاسبة والمراجعة التقليدية وجهاً لوجه (Griffin and wright, 2015)، (zheo et al, 2004)، يعتقد أن "الاستخدام الواسع الانتشار لتكنولوجيا المعلومات وقوتها المتزايدة لا يهدد المراجعين فقط ولكنه يوفر أيضاً فرصاً.

حيث تغير دور المراجعين بسبب النظام البيئي للبيانات الضخمة وتهديد الامن السيبراني، واستجابة للحاجة إلى حماية أكبر للبيانات.

٧/٣/٨ محاسبة المراجعين (الأخلاقية) وحماية البيانات:

يشارك المراجعين بشكل مباشر في حماية البيانات لسببين:

أولاً: إمكانية الوصول إلى البيانات الشخصية والحساسة واستخدامها في عملية المراجعة.

ثانياً: دورهم في ضمان المحاسبة في ممارسات حماية البيانات.

بالنسبة للسبب الأول: عند قيام المراجعين بجمع البيانات يطلب منهم التصرف وفقاً للمبادئ الأخلاقية التي قد تتجاوز مسئوليتهم القانونية (Warren et al, 2015) حيث أن أدلة المراجعة يمكن أن تنشأ من مصادر أخرى غير التقليدية: مثل وسائل التواصل الاجتماعي، واجهزة الاستشعار ، وأجهزة تتبع تحديد التردد اللاسلكي ونظام تحديد المواقع العالمي (GPS) (Yoon et al, 2015).

يقع على المراجعين عبء كبير في التحكم ما بين إمكانية الوصول إلى البيانات ما لا يجعل استخدامها انتهاكاً للخصوصية. خصوصاً بعد أن قام الموظفون بربط أجهزتهم المحمولة بشبكات الأعمال.

مما يترتب عليه تدريب المراجعون على استخراج البيانات للحفاظ على الخصوصية لضمان خصوصية استخدام البيانات الحساسة وفقاً لمعايير المهنية الأخلاقية (Gay and simm et al, 2015).

وفي حين أن استخدام البيانات الضخمة تتطلب من المراجعين تعديل مهاراتهم وتطويرها فإنه يوسع مسئولياتهم في الوصول إلى بيانات شخصية أو حساسة معينة واستخدامها، يستدعى المشاركة في حكمهم الأخلاقي.

تعد المساءلة وتحديد المسئول جانباً مهماً من جوانب حماية الخصوصية لأنها يمكن أن تقدم مثالاً واضحاً للجمهور عن الإجراءات التي يقصد بها أن تكون مناسبة في حماية البيانات، والتي ستساعد وفقاً لدراسة (Lawrence and suddaby, 2006) على أما التحقق من صحة أو خطأ السلوك التنظيمي للشركة كمشارك في الحوكمة، يمكن للمساءلة عن حماية البيانات أن تشوه صورة المراجع حيث تمتد مسئولية المراجع ومساءلته عن تقيمه لفعالية أنظمة حماية البيانات الداخلية والأمن السيبراني (Messier et al, 2017).

٨/٣/٨ القواعد والتغيرات في معايير المراجعة

تعتبر معايير المراجعة الحالية والتي تتوفر إلكترونياً لا تزال عبارة عن نموذج ورقي لا فائدة تذكر منه وسيتعين توسيع وإعادة النظر في بعض المعايير وحذف بعض المعايير وسيتطلب أيضاً إضافة بعض المعايير الجديدة لأخذ بيئة المراجعة المتغيرة في الاعتبار (Kranel and Titera, 2015).

مع ظهور البيانات الضخمة ومعالجتها للبيانات والمعلومات بسرعة فائقة اصبحت التقارير التقليدية للمراجعة على أساس سنوي أو ربع سنوي تفقد أهميتها (Appel Baum et al, 2017).

حيث تعمل البيانات الضخمة على تغيير دور المراجع فهي توفر للمراجع بيانات لتقديمها بانتظام في التقرير كما توفر له العرض والتجميع وأخذ العينات المستخدمة في مراجعة البيانات.

تعمل البيانات الضخمة على تغيير دور المراجع من المراجعة لجمع الحقائق إلى دور أكثر تحليلياً (Griffin and wright, 2015).

وسيتطلب ذلك تغير في المعايير مثلا سيحتاج معيار ISA 520 بشأن الإجراءات التحليلية (Gay and Titera, 2015) إلى التغير ليشمل تقنيات تحليلية مناسبة لبيئة البيانات الضخمة ويشير كل من (Titera and krahel, 2015, p. 419) إلى أنه على الرغم من أن المنهجيات التحليلية موجودة إلا أن المراجعين وشركات المراجعة لن تتحمل مسئولية التحليل الإضافية دون أن تكلف بها عن طريق المعايير.

ويبقى السؤال هل معايير المراجعة بحاجة إلى مزيد من التعديلات للكشف عن معلومات أكثر إفادة بالنظر إلى بيئة البيانات (Appelbaum et al, 2017).

ومعايير جديدة تنظم درجة العلاقة بين الكشف عن المخاطر وانتهاك الخصوصية، كما ستحتاج بعض المعايير إلى معالجة: كيفية التعامل مع البيانات غير المهيكلة لكل من مرحلتي التخطيط والتنفيذ للمراجعة (Krahal and titera, 2015)، وتوفير أدلة من مصادر بديلة مثل وسائل التواصل الاجتماعي (Appelbaum at el, 2017) كما يمكن تطوير المعايير الجديدة إلى الاعتراف بمساءلة المراجعين ودورهم المتطور لمحاربة حماية البيانات.

٤/٨ منهجية الدراسة

مقدمة:

تهدف الدراسة إلى التعرف على الدور المقترح لمراجع الحسابات في إضفاء الثقة على تقرير إدارة مخاطر الامن السيبراني واثره على دلالة القوائم المالية ، وتوصيف البيانات الأولية في قائمة الاستقصاء التي اعتمدت عليها الباحثة علاوة على ذلك توضيح أدوات التحليل الإحصائي المستخدمة في تحليل الاستقصاء وكذلك اختبار مقياس الدراسة بغرض الحصول على النتائج التي توضح مدى صحة أو خطأ فروض

الدراسة . ولتحقيق ذلك الهدف سوف يعتمد الباحث على بعض الأساليب الإحصائية الوصفية وبعض الأساليب الإحصائية الاستدلالية .

تناقش هذة الجزئية من البحث اختبار فروض البحث تجريبيا وفي سبيل تحقيق هذا الهدف تتناول الباحثة كلا من هدف الدراسة التجريبية ،ومجتمع وعينة الدراسة ،توصيف وقياس متغيرات الدراسة ،نموذج البحث،وادوات واجراءات الدراسة التجريبية ،والتصميم التجريبي المستخدم ،والمعالجات والمقارنات التجريبية وذلك علي النحو التالي:

١/٤/٨ هدف الدراسة:

تستهدف الدراسة التجريبية اختبار العلاقة التأثيرية بين اهمية الافصاح عن تقرير ادارة مخاطر الامن السيبراني.

،وكذا اختبار العلاقة التأثيرية بين الدور المقترح لمراجع الحسابات ودرجة الثقة التي يضفيها علي تقرير ادارة مخاطر الامن السيبراني.

،كما تستهدف الدراسة اختبار العلاقة التأثيرية بين الدور المقترح لمراجع الحسابات في اضفاء الثقة علي تقرير ادارة مخاطر الامن السيبراني ودلالة القوائم المالية، وذلك في ضوء انتماء او عدم انتماء الشركة التي يعمل بها المراجع للمكاتب الأربعة الكبرى وأيضا خبرة المراجع كمتغيرات معدلة.

(١) ملاحظات: تناسب التجارب الميدانية كطريقة للبحث العلمي طبيعة البحث الحالي ،حيث يستهدف البحث دراسة علاقة سببية بين متغ يرات مستقلة وتابعة ،وبصفه خاصة تأثير الدور المقترح لمراجع الحسابات علي اضفاء الثقة علي تقرير ادارة مخاطر الامن السيبراني ،فالتجارب تعتبر منهجا قويا يمكن للباحثين الاستدلال عن طريقه علي العلاقات السببية ،كما تمكن التجارب من توضيح التأثيرات الفعلية لانواع مختلفة من المعلومات علي عملية اتخاذ القرارات ،و بما يسمح بتطوير يفيد في تطوير المعرفة في موضوع الدراسة الحالية.

(٢) يمكن تعريف المتغيرات المعدلة بأنها المتغيرات التي تؤثر في اتجاة او قوة العلاقة بين المتغيرات المستقلة والتابعة ، كما تختلف المتغيرات المعدلة عن المتغيرات الرقابية حيث تؤثر المتغيرات الرقابية علي المتغيرالتابع مباشرة (موسي ، ٢٠١٨) .

٢/٤/8 مجتمع وعينة الدراسة:

اولا: عينة الدارسة:

تم اجراء الدراسة التجريبية علي مجتمع واحد و هو مجتمع مراجعي الحسابات العاملين في مكاتب المحاسبة و المراجعة بالمجتمع المصري خلال العام ٢٠٢١ و ٢٠٢٢) .

(١) و تكونت العينة من ٤٠٠ مراجع حسابات طبقت عليهم الاستبانة ،و لم يتم استبعاد اي من الردود نظرا لاستخدام النشر الالكتروني للاستبيان عبر موقع Research Gate وهو يحتوي علي مجموعة كبيرة من الفئة المستهدفة للدراسة.

والذي قام بتجميع الردود ليصبح حجم العينة المستخدم في الدراسة ٤٠٠ مراجع بنسبة استجابة ١٠٠% و هو مناسب لحجم عينة الدراسة الحالية بناءا علي العلاقة الرياضية التالية التي اوضحت ان حجم العينة يجب الا يقل عن ٣٨٤ مشارك، كما ان العينة كانت متفاوتة التأهيل وسنوات الخبرة وان بعضهم مقيد وبعضهم غير مقيد لدي هيئة الرقابة المالية .

$$n = \frac{z^2}{e^2} f(1-f)$$

حيث ان:

z : هي القيمة المعيارية عند مستوى ثقة ٩٥% وهى تساوى ١.٩٦

e : هو الخطأ المعياري المسموح به وهو يساوى ٠.٠٥

f : هو درجة الاختلاف بين مفردات المجتمع وقد تم افتراضها بـ ٠.٥ وذلك بالاعتماد على الدراسات السابقة.

ثانيا: الأساليب الإحصائية المستخدمة :

(أ)- <u>الأساليب الإحصائية الوصفية</u> :

تم الاعتماد على معامل الاتساق الداخلي ومعامل الثبات وذلك لقياس مدى صلاحية واعتمادية استمارة الاستقصاء المستخدمة في قياس استجابات مفردات عينة البحث ، وكذلك تم الاعتماد علي الوسط الحسابي والإنحراف المعياري لقياس متوسطات استجابات عينة البحث حول متغيرات الدراسة مع قياس مدى التشتت في تلك الإجابات.

- معامل ألفا (كرونباخ):

يمثل معامل ألفا متوسط المعاملات الناتجة عن تجزئة الأختبار إلي أجزاء بطرق مختلفة وبذلك فإنه يمثل معامل الارتباط بين أي جزئين من أجزاء الاختبار. فقد اعتمدت الباحثة على معامل كرونباخ ألفا بهدف دراسة معامل الثبات (درجة الاعتمادية) وذلك على مستوي جميع الأبعاد الخاصة باستمارة الاستقصاء.

- معامل الارتباط Correlation Coefficient

ويستخدم معامل الارتباط لقياس درجة الارتباط بين متغيرين. وتعبر قيمة هذا المعامل- بصرف النظر عن الإشارة- عن قوة العلاقة بين المتغيرين ورغم أنه لا توجد علاقة محددة لوصف درجة العلاقة بين المتغيرين بناء على قيمة معامل الارتباط إلا أنه يمكن استخدام بعض المؤشرات التقريبية للحكم على درجة هذه العلاقة. فإذا كانت قيمة معامل الارتباط تقع بين (0,0.5) دل ذلك على ضعف العلاقة بينما إذا كانت قيمته تقع بين (0.5,1) دل ذلك على قوة هذه العلاقة. وتنعدم العلاقة بين المتغيرين إذا كان معامل الارتباط صفرا، بينما تدل القيمة واحد لمعامل الارتباط على وجود علاقة تامة بين المتغيرين. وتدل إشارة معامل الارتباط عادة على اتجاه العلاقة بين المتغيرين، فإذا كانت الإشارة موجبة دل ذلك على وجود علاقة طردية بين المتغيرين بمعنى أن القيم الكبيرة للمتغيرين تميل أن تحدث معا والقيم الصغيرة أيضاً تميل أن تحدث معا. أما إذا كانت إشارة معامل الارتباط سالبة دل ذلك على وجود علاقة عكسية بين المتغيرين بمعنى أن القيم الكبيرة لأحد المتغيرين تميل أن تحدث مع القيم الصغيرة للمتغير الآخر.

وبرنامج SPSS يعطي قيمة الدلالة P-Value حيث نقوم بمقارنتها بقيمة المعنوية ٥% فإذا كانت قيمة الدلالة أصغر من قيمة المعنوية ٥% إذا نقبل الفرض القائل بوجود علاقة بين المتغيرين والعكس صحيح.

(ب) – الأساليب الإحصائية الإستدلالية :

١- اختبار ويلكوكسون للرتب:

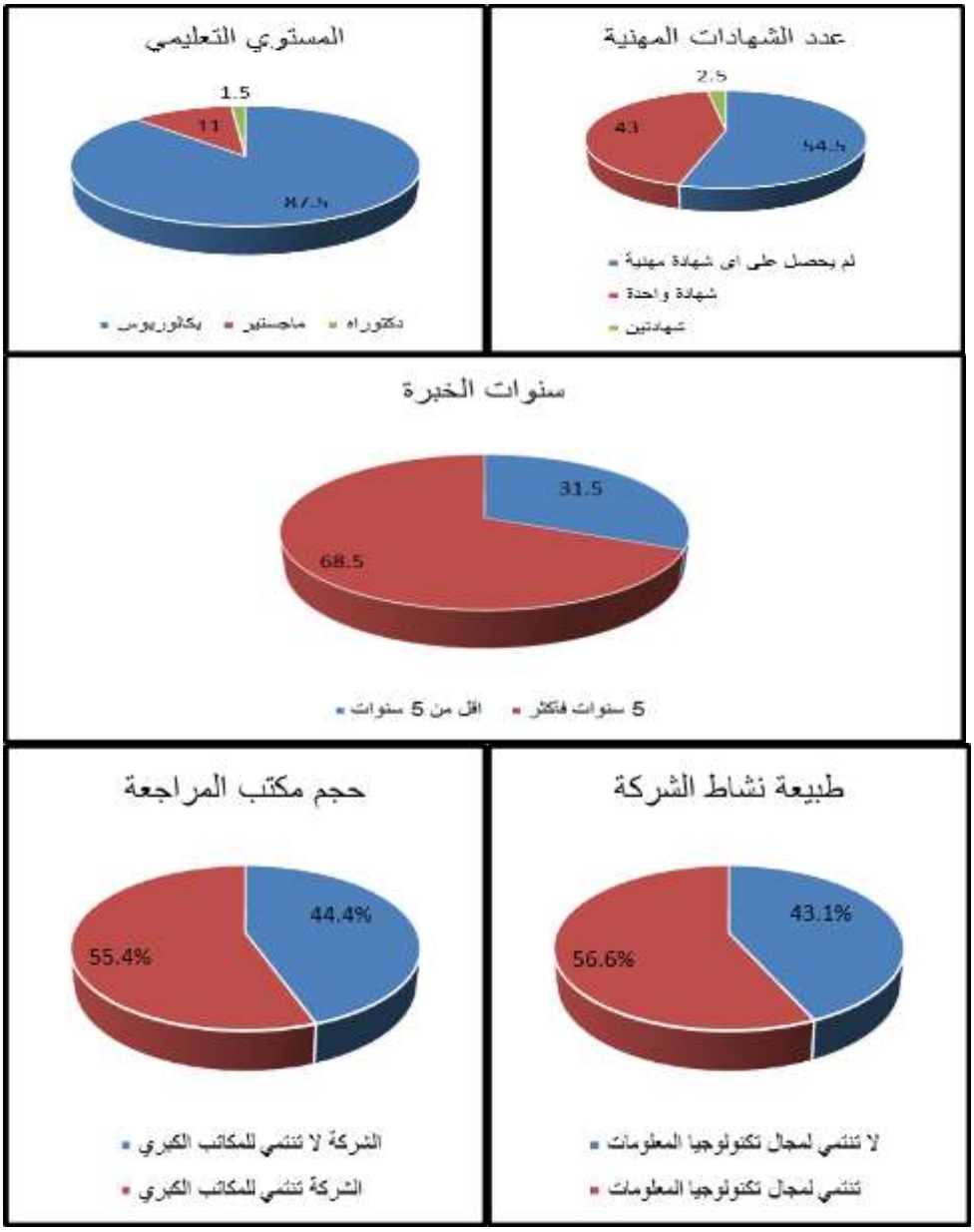
وهو اختبار لا معلمي تم استخدامه لقياس معنوية تأثير المتغيرات المستقلة على المتغيرات التابعة ويعطي برنامج SPSS قيمة الدلالة P-Value للمجاهيل للاختبار فإذا كانت قيمة الدلالة أصغر من قيمة المعنوية ٥% هذا يعني وجود تأثير معنوي للمتغير المستقل على المتغير التابع.

ثالثا: الجداول التكرارية والنسبية Frequency Tables

استخدم الباحث هذه الجداول لاستنتاج عدد ونسبة الاستجابات من المبحوثين ووضعها في جدول من ثلاثة اعمدة يمثل الأول العدد والثاني النسبة من حجم العينة والثالث هو النسبة التراكمية كما هو موضح في الجداول التالية.

جدول (١) يوضح عدد ونسبة المبحوثين في العينة

		العدد	%	النسبة التراكمية
المستوي التعليمي	بكالوريوس	350	87.5	87.5
	ماجستير	44	11.0	98.5
	دكتوراه	6	1.5	100.0
عدد الشهادات المهنية	لم يحصل على اى شهادة مهنية	218	54.5	54.5
	شهادة واحدة	172	43.0	97.5
	شهادتين	10	2.5	100.0
سنوات الخبرة	اقل من ٥ سنوات	126	31.5	31.5
	٥ سنوات فأكثر	274	68.5	100.0
حجم مكتب المراجعة	الشركة لا تنتمي للمكاتب الكبري	178	44.4%	44.4%
	الشركة تنتمي للمكاتب الكبري	222	55.4%	100.0
طبيعة نشاط الشركة	لا تنتمي لمجال تكنولوجيا المعلومات	173	43.1%	43.1%
	تنتمي لمجال تكنولوجيا المعلومات	227	56.6%	100.0


المستوي التعليمي
1.5
11
87.5
دكتوراه
ماجستير
بكالوريوس
عدد الشهادات المهنية
2.5
43
54.5
لم يحصل على اى شهادة مهنية
شهادة واحدة
شهادتين
سنوات الخبرة
31.5
68.5
5 سنوات فاكثر
اقل من 5 سنوات
حجم مكتب المراجعة
44.4%
55.4%
الشركة لا تنتمي للمكاتب الكبري
الشركة تنتمي للمكاتب الكبري
طبيعة نشاط الشركة
43.1%
56.6%
لا تنتمي لمجال تكنولوجيا المعلومات
تنتمي لمجال تكنولوجيا المعلومات

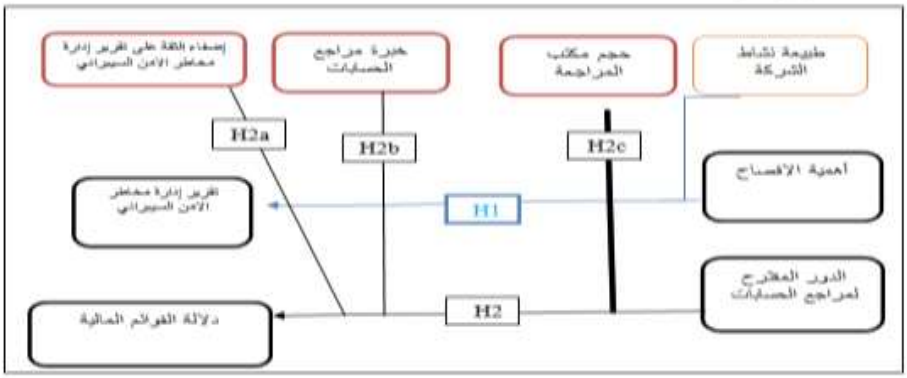
رابعا: توصيف وقياس متغيرات الدراسة

تشمل متغيرات الدراسة في التحليل الاساسي متغيرين مستقلين و متغيرين تابعين واربعة متغيرات معدلة ،وتم توصيف المتغيرات وقياسها كما يتضح من الجدول التالي:

المتغير	نوعه	توصيفة	قياسه	التأثير المتوقع
اهمية الافصاح عن تقرير ادارة مخاطر الامن السيبراني	مستقل	الافصاح عن مخاطر الامن السيبراني من انواع الافصاح الاختياري حيث ان سوق المال المصري لايلزم الشركات بالافصاح عن ادارة مخاطر الامن السيبراني (وهبة ،اماني احمد ،٢٠٢٢) وتختلف اهمية الافصاح عن مخاطر الامن السيبراني تبعا لطبيعة النشاط الذي تنتمي اليه الشركة حيث ان الشركات التي تعمل بمجال تكنولوجيا المعلومات يكون الافصاح عن تقرير ادارة مخاطر الامن السيبراني اكثر اهمية بالنسبة اليها و في المقابل الشركات التي لا تنتمي لمجال تكنولوجيا المعلومات.	استخدمت الباحثة دراسة تجريبية وتم توجية اسئلة للمراجعي الحسابات لمجموعة من الشركات التي تنتمي لمجال تكنولوجيا المعلومات و التي لديها مخاطر امن سيبراني مرتفعة ،و في المقابل تم توجية نفس الاسئلة لمراجعي الحسابات في مجموعة الشركات التي لا تنتمي لمجال تكنولوجيا المعلومات والتي لديها مخاطر امن سيبراني منخفضة.	ايجابي في المجموعة الاولي وسلبي في المجموعة الثانية
الدور المقترح لمراجع الحسابات	مستقل	حيث ان طبيعة المخاطر التي تواجه الشركة تغيرت مع تغير اسلوب العمل و الاتجاة المتزايد نحو التحول الرقمي ،لذا اصبح للمراجع دور جديد بخلاف المتطلبات التقليدية التي اوضحتها معايير المهنة وهو التقرير عن ادارة المخاطربصفة عامة ومخاطر الامن السيبراني بصفة خاصة، (الصيرفي ، اسماء احمد ، ٢٠٢٢)	قامت الباحثة بقياس الدور المقترح لمراجع الحسابات باستخدام الاسلوب التجريبي(٢×٢×٢)و توجية مجموعة من الاسئلة لمعرفة اثره علي دلالة القوائم المالية اذا كانت درجة الثقة التي يضفيها علي تقرير ادارة مخاطر الامن السيبراني معقولة و في المقابل توجية نفس الاسئلة للمبحوثين اذا كانت درجة الثقة محدودة .وكذلك توجية نفس الاسئلة اذا كانت خبرة مراجع الحسابات طويلة و في المقابل اذا كانت خبرة مراجع الحسابات قليلة (من اعداد الباحثة)	ايجابي اذا كانت درجة الثقة معقولة و الخبرة طويلة و سلبي في المقابل اذا كانت درجة الثقة محدودة والخبرة قليلة.
تقرير ادارة مخاطر الامن السيبراني	تابع	يمكن تعريف ادارة مخاطر الامن السيبراني بأنها مجموعة من السياسات والعمليات و الاجراءات الرقابية المصممة لحماية المعلومات و الانظمة الالكترونية من الحوادث الامنية التي تعرض امن الشركة السيبراني لمخاطر عدم تحقيق اهدافه، كما تساعد تلك الاجراءات علي اكتشاف الهجمات الامنية و الاستجابة لها و التخفيف من اثارها (الصيرفي ، اسماء احمد، ٢٠٢٢) و التقرير عن ادارة تلك المخاطر يعتبر من الاهمية بمكان لاتقل عن التقرير عن المخاطر المرتبطة بالتقارير المالية (ISCA،٢٠١٨)	باستخدام الاسلوب التجريبي (٢×٢) توجية اسئلة للمبحوثين لمجموعة مراجعي الحسابات في شركات تنتمي لنشاط تكنولوجيا المعلومات في مقابل مجموعة من مراجعي الحسابات في شركات لاتنتمي لمجال تكنولوجيا المعلومات لتحديد وقياس اهمية الافصاح عن هذا التقرير. (من اعداد الباحثة)	ايجابي اذا كانت الشركة تنتمي لمجال تكنولوجيا المعلومات و سلبي اذا كانت لاتنتمي لمجال تكنولوجيا المعلومات.

دلالة القوائم المالية	تابع	تتأثر بعض البنود في القوائم المالية نتيجة اعداد المراجع لتقرير عن ادارة مخاطر اللامن السيبراني وقد حددت الباحثة من هذة البنود عوائد الاسهم ،وزيادة المخزون.	استخدمت الباحثة الاسلوب التجريبي (٢×٢) بتوجية اسئلة للمبحوثين في حالة ان تقرير ادارة مخاطر الامن السيبراني تأكد تعرض الشركة لمخاطر امن سيبراني مرتفعة واثر ذلك علي عوائد الاسهم وزيادة المخزون وفي المقابل توجية نفس الاسئلة في حالة ان تقرير ادارة المخاطر يؤكد تعرض الشركة لمخاطر امن سيبراني منخفضة واثر ذلك علي كلا من عوائد الاسهم وزيادة المخزون . (من اعداد الباحثة)	سلبي في حالة ان التقرير يؤكد تعرض الشركة لمخاطر امن سيبراني مرتفعة ،و ايجابي في حالة تعرض الشركة لمخاطر امن سيبراني منخفضة
درجة الثقة التي يضفيها تقرير ادارة مخاطر الامن السيبراني	معدل	تختلف درجة الثقة التي يضفيها تقرير ادارة مخاطر الامن السيبراني وفقا لتفعيل دور مراجع الحسابات اثناء قيامه بأعداده لذا تختلف هذة الدرجة و قد حددت الباحثة لاجراء الدارسة التجريبية درجتين لقياس هذة الثقة معقولة ومحدودة لامكانية قياس هذا التأثير ،(بدوي، هبة عبد السلام،٢٠٢٢)	استخدمت الباحثة الاسلوب التجريبي لقياس درجة الثقة التي يضفيها الدور المقترح علي تقرير ادارة مخاطر الامن السيبراني (٢×٢×٢) بتوجية اسئلة لمراجعي الحسابات اذا تم اعداد هذا التقرير من مراجعي حسابات ينتمون للمكاتب الاربعة الكبري و توجية نفس الاسئلة للمبحوثين في المقابل اذا كان التقرير تم اعداده من مراجعي حسابات لا ينتمون للمكاتب الاربعة الكبري ،و كذلك توجية اسئلة للمبحوثين اذا تم اعداده من مراجعي حسابات لهم خبرة طويلة في مقابل خبرة قليلة.(من اعداد الباحثة)	تأثير ايجابي في حالة تم الاعداد من قبل احد المكاتب الاربعة و للمراجع خبرة طويلة و تأثير سلبي اذا تم اعداده من خارج المكاتب الاربعة وخبرة المراجع قليلة
حجم مكتب المراجعة	معدل	مدي ما يتمتع به مكتب المراجعة من امكانيات فنية و مادية وبشرية لتأدية مهامه بشكل افضل وجودة عالية لعدد من العملاء لهم وزن نسبي عالي في السوق.(بدوي، هبة عبد السلام ، ٢٠٢٢)	استخدمت الباحثة (٢×٢) الاسلوب التجريبي بتوجية اسئلة للمبحوثين في حالة ان حجم مكتب المراجعة الذي اعد تقرير الامن اسيبراني من المكاتب الاربعة وفي المقابل توجيه نفس الاسئلة اذا كان مكتب المراجعة الذي اعد التقرير خارج المكاتب الاربعة(من اعداد الباحثة)	ايجابي في حالة ان حجم المكتب كبير و سلبي اذا كان حجم المكتب صغير
خبرة مراجع الحسابات	معدل	هي المخزون المعرفي لمراجع الحسابات الناتج عن ممارسة المهنة (بدوي ، هبة عبد السلام، ٢٠٢٢)	استخدمت الباحثة (٢×٢) الاسلوب التجريبي بتوجية اسئلة للمبحوثين في حالة ان المراجع الذي اعد تقرير الامن اسيبراني له خبرة مهنية طويلة وفي المقابل توجيه نفس الاسئلة اذا المراجع الذي اعد التقرير له خبرة مهنية قليلة (من اعداد الباحثة)	ايجابي في حالة المراجع له خبرة مهنية طويلة و سلبي اذا كان المراجع له خبرة مهنية قليلة.
طبيعة نشاط الشركة	معدل	تختلف طبيعة نشاط الشركة طبقا لدراسة البحث الي شركات تعمل في مجال تكنولوجيا المعلومات و اخري تعمل خارج هذا المجال و بالتالي تختلف اهمية الافصاح عن مخاطر الامن السيبراني وفقا لاختلاف طبيعة نشاط الشركة (بدوي ، هبة عبد السلام، ٢٠٢٢)	استخدمت الباحثة الاسلوب التجريبي (٢×٢) بتوجية اسئلة للمبحوثين في حالة ان الشركة التي يتم الافصاح عن تقرير ادارة مخاطر الامن السيبراني تعمل في مجال تكنولوجيا المعلومات وفي المقابل تم توجية نفس الاسئلة للمبحوثين اذا كانت الشركة تعمل خارج مجال تكنولوجيا المعلومات (من اعداد الباحثة)	اهمية الافصاح تكون اكثر اهمية للشركات العاملة في مجال تكنولوجيا المعلومات و اقل اهمية في الشركات التي لاتعمل في هذا المجال

خامسا: نموذج الدراسة



سادسا: صلاحية واعتمادية الأداة المستخدمة في قياس نتائج الدراسة

لتحديد درجة صلاحية ومدي الاعتماد على الأداة المستخدمة في قياس استجابات مفردات العينة، قام الباحث باستخدام كل من:

١- الصدق الظاهري (صدق المحكمين): Face Validity

حيث تم عرض الاستبانة على عدد من المحكمين الخبراء والمتخصصين في المجال وطلب منهم دراسة الاستبانة وإبداء آرائهم فيها من حيث: مدى ارتباط كل عبارة من عباراتها بالمجال المنتمية إليه، ومدى وضوح العبارات وسلامة صياغتها اللغوية وملاءمتها لتحقيق الهدف الذي وضعت من أجله، واقتراح طرق تحسينها وذلك بالحذف أو الإضافة أو إعادة الصياغة، وقد قدم المحكمون ملاحظات قيمة أفادت الدراسة، وآثرت الاستبانة، وساعدت على إخراجها بصورة جيدة.

٢- معامل الاتساق الداخلي Interconsistancy :

يقيس درجة مصداقية النتائج المحققة لكل بند من بنود الاستقصاء، والذي يعتمد في المقام الأول على معامل الارتباط، وبالتالي فمن الضروري أن يكون المعيار الأساسي هو اختبار لمعنوية معامل الارتباط.

٣- معامل كرونباخ ألفا (α) : Cronbach's Alpha

الصدق الداخلي للعناصر

أولا: الصدق الداخلي لعناصر المجموعة الأولى

بُعد اهمية الافصاح

يوضح الجدول (٢) نتائج التحليل الإحصائي الخاصة ببُعد **اهمية الافصاح**.

جدول (٢) نتائج صلاحية واعتمادية ببُعد اهمية الافصاح

م	عناصر بُعد اهمية الافصاح	معامل الاتساق الداخلي (معامل الارتباط)	المعنوية
١	الافصاح عن اسلوب اجراءات الامن السيبراني في الوحدة الاقتصادية	.750**	أقل من ٠.٠١
٢	الافصاح عن الخسائر المالية التي تترتب عن انتهاكات الفضاء السيبراني للشركة	.796**	أقل من ٠.٠١
٣	الافصاح عن الدرات التدريبية (مبالغها) المنعقدة داخل خارج الشركة	.858**	أقل من ٠.٠١
٤	الافصاح عن السجلات الخاصة بالموجودات المعلو ماتية و التقنية وفقا للمتطلبات التشريعية و المعاهدات المحلية الد ولية	.825**	أقل من ٠.٠١

** تشير إلي معنوية معامل الارتباط عند مستوي معنوية ٠.٠١

أكدت نتائج الجدول السابق على صلاحية جميع العناصر الخاصة ببعد **اهمية الافصاح** حيث أكدت على ذلك قيم معاملات الارتباط وقد جاءت جميعها معنوية عند مستوي ٠.٠٥.

ثانيا: الصدق الداخلي لعناصر المجموعة الثانية

بُعد حوكمة الامن السيبراني

يوضح الجدول (٣) نتائج التحليل الإحصائي الخاصة ببُعد **حوكمة الامن السيبراني**

جدول (٣) نتائج صلاحية واعتمادية ببُعد حوكمة الامن السيبراني

م	عناصر بُعد حوكمة الامن السيبراني	معامل الاتساق الداخلي	المعنوية
١	عدد التقارير المرفوعة للادارة العليا من قبل المراجع عن حالات الاختراق	.818**	أقل من ٠.٠١
٢	عدد الحالات التي اسهمت بها المراجعة الداخلية في ادارة مخاطر الانترنت	.870**	أقل من ٠.٠١
٣	توظيف مستشار بأختصاص برمجيات الحاسوب	.782**	أقل من ٠.٠١

**** تشير إلي معنوية معامل الارتباط عند مستوي معنوية ٠.٠١**

أكدت نتائج الجدول السابق على صلاحية جميع العناصر الخاصة ببعد **نتائج حوكمة الامن السيبراني** حيث أكدت على ذلك قيم معاملات الارتباط وقد جاءت جميعها معنوية عند مستوي ٠.٠٥.

ثالثا: الصدق الداخلي لعناصر المجموعة الثالثة

بُعد حماية الامن السيبراني

يوضح الجدول (٤) نتائج التحليل الإحصائي الخاصة ببُعد **حماية الامن السيبراني**

جدول (٤) نتائج صلاحية واعتمادية ببُعد حماية الامن السيبراني

م	عناصر بُعد حماية الامن السيبراني	معامل الاتساق الداخلي	المعنوية
١	ادارة الاصول السيبرانية	.837**	أقل من ٠.٠١
٢	ادارة صلاحيات استعمال الاجهزة الالكترونية	.795**	أقل من ٠.٠١
٣	ادارة الفضاء الخارجي	.744**	أقل من ٠.٠١
٤	حماية البريد الالكتروني ووسائل التواصل الرقمي الذي تعتمده الشركة و الموقع الالكتروني الرسمي	.822**	أقل من ٠.٠١
٥	ادارة النسخ الاحتياطية	.837**	أقل من ٠.٠١
٦	اختبارات الاختراق و التشفير و الحماية للسجلات الرقمية	.795**	أقل من ٠.٠١

**** تشير إلي معنوية معامل الارتباط عند مستوي معنوية ٠.٠١**

أكدت نتائج الجدول السابق على صلاحية جميع العناصر الخاصة ببعد **نتائج حماية الامن السيبراني** حيث أكدت على ذلك قيم معاملات الارتباط وقد جاءت جميعها معنوية عند مستوي ٠.٠٥.

رابعا: الصدق الداخلي لعناصر المجموعة الرابعة

بُعد إدارة المخاطر السيبرانية

يوضح الجدول (٥) نتائج التحليل الإحصائي الخاصة ببُعد **إدارة المخاطر السيبرانية**

جدول (٥) نتائج صلاحية واعتمادية ببُعد الاستراتيجية

م	عناصر بُعد إدارة المخاطر السيبرانية	معامل الاتساق الداخلي	المعنوية
١	الموقع الالكتروني للوحدة الاقتصادية	.965**	أقل من ٠.٠١
٢	الادارة الامنية السيبرانية وفق التشريعات و التعليمات الاستراتيجية المعتمدة في البلد المعني	.964**	أقل من ٠.٠١

**** تشير إلي معنوية معامل الارتباط عند مستوي معنوية ٠.٠١**

أكدت نتائج الجدول السابق على صلاحية جميع العناصر الخاصة ببعد **نتائج إدارة المخاطر السيبرانية** حيث أكدت على ذلك قيم معاملات الارتباط وقد جاءت جميعها معنوية عند مستوي ٠.٠٥.

خامسا: الصدق الداخلي لعناصر المجموعة الخامسة

بُعد إضفاء الثقة على تقرير إدارة مخاطر الامن السيبراني

يوضح الجدول (٦) نتائج التحليل الإحصائي الخاصة ببُعد **إضفاء الثقة على تقرير إدارة مخاطر الامن السيبراني**

جدول (٦) نتائج صلاحية واعتمادية ببُعد إضفاء الثقة على تقرير إدارة مخاطر الامن السيبراني

م	عناصر بُعد إضفاء الثقة على تقرير إدارة مخاطر الامن السيبراني	معامل الاتساق الداخلي	المعنوية
١	تقرير ادارة مخاطر الامن السيبراني الذي يعده المراجع ضمن الد و ر المقترح للمراجع بالدراسة يعد بضمان احد المكاتب الاربعة	.877**	أقل من ٠.٠١
٢	تقرير ادارة مخاطر الامن السيبراني الذي يعده المراجع ضمن الد و ر المقترح للمراجع بالدراسة يعد بضمان مراجع من خارج المكاتب الاربعة	.927**	أقل من ٠.٠١
٣	تقرير ادارة مخاطر الامن السيبراني الذي يعده المراجع ضمن الد و ر المقترح للمراجع بالدراسة يعد من قبل مراجع له خبرة مهنية طويلة	.933**	أقل من ٠.٠١
٤	تقرير ادارة مخاطر الامن السيبراني الذي يعده المراجع ضمن الد و ر المقترح للمراجع بالدراسة يعد من قبل مراجع له خبرة مهنية قصيرة	.920**	أقل من ٠.٠١

**** تشير إلي معنوية معامل الارتباط عند مستوي معنوية ٠.٠١**

أكدت نتائج الجدول السابق على صلاحية جميع العناصر الخاصة ببعد **نتائج إضفاء الثقة على تقرير إدارة مخاطر الامن السيبراني** حيث أكدت على ذلك قيم معاملات الارتباط وقد جاءت جميعها معنوية عند مستوي ٠.٠٥.

سادسا: الصدق الداخلي لعناصر المجموعة السادسة

بُعد إضفاء الثقة على تقرير إدارة مخاطر الامن السيبراني

يوضح الجدول (٧) نتائج التحليل الإحصائي الخاصة ببُعد **إضفاء الثقة على تقرير إدارة مخاطر الامن السيبراني**

جدول (٧) نتائج صلاحية واعتمادية ببُعد إضفاء الثقة على تقرير إدارة مخاطر الامن السيبراني

م	عناصر بُعد إضفاء الثقة على تقرير إدارة مخاطر الامن السيبراني	معامل الاتساق الداخلي	المعنوية
١	وصف الامن السيبراني ومخاطر المعلومات المتاحة	.921**	أقل من ٠.٠١
٢	عدد التقارير المرفوعة الي الادارة العليا من قبل لجنة ادارة المخاطر عن حالات الاختراق	.917**	أقل من ٠.٠١
٣	تقرير ادارة مخاطر الامن السيبراني الذي يعده المراجع ضمن الد و ر المقترح للمراجع بالدراسة يعد بضمان احد المكاتب الاربعة	.839**	أقل من ٠.٠١
٤	تقرير ادارة مخاطر الامن السيبراني الذي يعده المراجع ضمن الد و ر المقترح للمراجع بالدراسة يعد بضمان مراجع من خارج المكاتب الاربعة	.912**	أقل من ٠.٠١
٥	تقرير ادارة مخاطر الامن السيبراني الذي يعده المراجع ضمن الد و ر المقترح للمراجع بالدراسة يعد من قبل مراجع له خبرة مهنية طويلة	.933**	أقل من ٠.٠١
٦	تقرير ادارة مخاطر الامن السيبراني الذي يعده المراجع ضمن الد و ر المقترح للمراجع بالدراسة يعد من قبل مراجع له خبرة مهنية قصيرة	.926**	أقل من ٠.٠١

**** تشير إلي معنوية معامل الارتباط عند مستوي معنوية ٠.٠١**

أكدت نتائج الجدول السابق على صلاحية جميع العناصر الخاصة ببعد **نتائج إضفاء الثقة على تقرير إدارة مخاطر الامن السيبراني** حيث أكدت على ذلك قيم معاملات الارتباط وقد جاءت جميعها معنوية عند مستوي ٠.٠٥.

سابعا: الصدق الداخلي لعناصر المجموعة السابعة

بُعد تقييم الاسهم

يوضح الجدول (٨) نتائج التحليل الإحصائي الخاصة ببُعد **تقييم الاسهم**

جدول (٨) نتائج صلاحية واعتمادية بُعد تقييم الاسهم

م	عناصر بُعد تقييم الاسهم	معامل الاتساق الداخلي	المعنوية
١	تقرير ادارة مخاطر الامن السيبراني الذي يعده المراجع يعد بضمان احد المكاتب الاربعة يكون هناك تأثير علي قيمة اسهم الشركة	.626**	أقل من ٠.٠١
٢	تقرير ادارة مخاطر الامن السيبراني الذي يعده المراجع يعد بضمان مراجع من خارج المكاتب الاربعة يكو ن هناك تأثير علي قيمة اسهم الشركة	.602**	أقل من ٠.٠١
٣	تقرير ادارة مخاطر الامن السيبراني الذي يعده المراجع يعد من قبل مراجع له خبرة مهنية طويلة يكون هناك تاثير علي قيمة اسهم الشركة	.731**	أقل من ٠.٠١
٤	تقرير ادارة مخاطر الامن السيبراني الذي يعده المراجع يعد من قبل مراجع له خبرة مهنية قصيرة يكون هناك تاثير علي قيمة اسهم الشركة	.633**	أقل من ٠.٠١

**** تشير إلي معنوية معامل الارتباط عند مستوي معنوية ٠.٠١**

أكدت نتائج الجدول السابق على صلاحية جميع العناصر الخاصة ببعد **نتائج تقييم الأسهم** حيث أكدت على ذلك قيم معاملات الارتباط وقد جاءت جميعها معنوية عند مستوي ٠.٠٥.

ثامنا: الصدق الداخلي لعناصر المجموعة الثامنة

بُعد زيادة المخزون

يوضح الجدول (٩) نتائج التحليل الإحصائي الخاصة ببُعد **زيادة المخزون**

جدول (٩) نتائج صلاحية واعتمادية بُعد زيادة المخزون

م	عناصر بُعد زيادة المخزون	معامل الاتساق الداخلي	المعنوية
١	تقرير ادارة مخاطر الامن السيبراني الذي يعده المراجع يعد بضمان احد المكاتب الاربعة يك ون هناك تأثير علي زيادة المخز ون	.807**	أقل من ٠.٠١
٢	تقرير ادارة مخاطر الامن السيبراني الذي يعد ه المراجع يعد بضمان مراجع من خارج المكاتب الاربعة يكو ن هناك تأثير علي زيادة المخز ون	.801**	أقل من ٠.٠١
٣	تقرير ادارة مخاطر الامن السيبراني الذي يعده المراجع يعد من قبل مراجع له خبرة مهنية طويلة يكون هناك تاثير علي زيادة المخز ون	.509**	أقل من ٠.٠١
٤	تقرير ادارة مخاطر الامن السيبراني الذي يعده المراجع يعد من قبل مراجع له خبرة مهنية قصيرة يكون هناك تاثير علي زيادة المخز ون	.347**	أقل من ٠.٠١

**** تشير إلي معنوية معامل الارتباط عند مستوي معنوية ٠.٠١**

أكدت نتائج الجدول السابق على صلاحية جميع العناصر الخاصة ببعد **نتائج زيادة المخزون** حيث أكدت على ذلك قيم معاملات الارتباط وقد جاءت جميعها معنوية عند مستوي ٠.٠٥.

معامل ألفا كرونباخ لقياس الثبات لأبعاد الدراسة

جدول (١٠)

المجموعة	عدد العناصر	معامل ألفا كرونباخ
المجموعة الأولى: نتائج اهمية الافصاح	٤	٠.٨٢٠
المجموعة الثانية: نتائج حوكمة الامن السيبراني	٣	٠.٧٥٩
المجموعة الثالثة: نتائج حماية الامن السيبراني	٦	٠.٨٩١
المجموعة الرابعة: نتائج الاستراتيجية	٤	٠.٦٣٣
المجموعة الخامسة: نتائج إدارة مخاطر الامن السيبراني	٢	٠.٩٢٥
المجموعة السادسة: نتائج إضفاء الثقة على تقرير إدارة مخاطر الامن السيبراني	٤	٠.٩٣٥
المجموعة السابعة: نتائج تقييم الاسهم	٤	٠.٥٤١
المجموعة الثامنة: نتائج زيادة المخزون	٤	٠.٤٩١
المقياس	٣١	٠.٩٤٥

يتضح من الجدول السابق ما يلي:

١- بالنسبة للمجموعة الأولى معامل كرونباخ ألفا (α =٠.٨٢٠) أي أن عناصر **بُعد نتائج اهمية الافصاح يمكن** الاعتماد عليها بشكل كبير في قياس المحور.

٢- بالنسبة للمجموعة الثانية معامل كرونباخ ألفا (α =٠.٧٥٩) أي أن عناصر **بُعد نتائج حوكمة الامن السيبراني يمكن** الاعتماد عليها بشكل كبير في قياس المحور.

٣- بالنسبة للمجموعة الثالثة معامل كرونباخ ألفا (α =٠.٨٩١) أي أن عناصر **بُعد نتائج حماية الامن السيبراني يمكن** الاعتماد عليها بشكل كبير في قياس المحور.

٤- بالنسبة للمجموعة الرابعة معامل كرونباخ ألفا (α =٠.٦٣٣) أي أن عناصر **بُعد نتائج الاستراتيجية يمكن** الاعتماد عليها بشكل كبير في قياس المحور.

٥- بالنسبة للمجموعة الخامسة معامل كرونباخ ألفا (α =٠.٩٢٥) أي أن عناصر **بُعد نتائج إدارة مخاطر الامن السيبراني يمكن** الاعتماد عليها بشكل كبير في قياس المحور.

٦- بالنسبة للمجموعة السادسة معامل كرونباخ ألفا (α =٠.٩٣٥) أي أن عناصر **بُعد نتائج إضفاء الثقة على تقرير إدارة مخاطر الامن السيبراني يمكن** الاعتماد عليها بشكل كبير في قياس المحور.

٧- بالنسبة للمجموعة السابعة معامل كرونباخ ألفا (α =٠.٥٤١) أي أن عناصر **بُعد نتائج تقييم الاسهم يمكن** الاعتماد عليها في قياس المحور.

٨- بالنسبة للمجموعة الثامنة معامل كرونباخ ألفا (α =٠.٤٩١) أي أن عناصر **بُعد نتائج زيادة المخزون يمكن** الاعتماد عليها في قياس المحور.

٩- بالنسبة للمقياس معامل كرونباخ ألفا (α =٠.٩٤٥) أي أن أداة الدراسة **يمكن** الاعتماد عليها بشكل كبير في قياس اهداف وفرضيات الدراسة.

سابعا: التصميم التجريبي والمعالجات التجريبية

حالة شركة وطريقة المراجعة فيها				حجم مكتب المراجعة			
				ينتمي الى المكاتب الأربعة الكبري		لا ينتمي الى المكاتب الأربعة الكبري	
				سنوات الخبرة		سنوات الخبرة	
				طويلة	قليلة	طويلة	قليلة
الدور المقترح لمراجع الحسابات	مفعل	درجة الثقة في تقرير إدارة المخاطر	معقولة	معالجة رقم (١)	معالجة رقم (٢)	معالجة رقم (٣)	معالجة رقم (٤)
			محدودة	معالجة رقم (٥)	معالجة رقم (٦)	معالجة رقم (٧)	معالجة رقم (٨)
	غير مفعل	درجة الثقة في تقرير إدارة المخاطر	معقولة	معالجة رقم (٩)	معالجة رقم (١٠)	معالجة رقم (١١)	معالجة رقم (١٢)
			محدودة	معالجة رقم (١٣)	معالجة رقم (١٤)	معالجة رقم (١٥)	معالجة رقم (١٦)

ويشمل التصميم التجريبي السابق ١٦ معالجة يمكن توضيحهم على النحو التالي:

معالجة رقم (١):

الدور المقترح المفعل لمراجع الحسابات اذا كان مراجع الحسابات ينتمي لأحد المكاتب الكبار وله خبرة طويلة في المهنة، كما ان درجة الثقة في تقرير إدارة المخاطر لدي المبحوثين معقولة

معالجة رقم (٢):
الدور المقترح المفعل لمراجع الحسابات اذا كان مراجع الحسابات ينتمي لأحد المكاتب الكبار وله خبرة قليلة في المهنة، كما ان درجة الثقة في تقرير إدارة المخاطر لدي المبحوثين معقولة

معالجة رقم (٣):
الدور المقترح المفعل لمراجع الحسابات اذا كان مراجع الحسابات لا ينتمي لأحد المكاتب الكبار وله خبرة طويلة في المهنة، كما ان درجة الثقة في تقرير إدارة المخاطر لدي المبحوثين معقولة

معالجة رقم (٤):
الدور المقترح المفعل لمراجع الحسابات اذا كان مراجع الحسابات لاينتمي لأحد المكاتب الكبار وله خبرة قليلة في المهنة، كما ان درجة الثقة في تقرير إدارة المخاطر لدي المبحوثين معقولة

معالجة رقم (٥):
الدور المقترح المفعل لمراجع الحسابات اذا كان مراجع الحسابات ينتمي لأحد المكاتب الكبار وله خبرة طويلة في المهنة، كما ان درجة الثقة في تقرير إدارة المخاطر لدي المبحوثين محدودة

معالجة رقم (٦):
الدور المقترح المفعل لمراجع الحسابات اذا كان مراجع الحسابات ينتمي لأحد المكاتب الكبار وله خبرة قليلة في المهنة، كما ان درجة الثقة في تقرير إدارة المخاطر لدي المبحوثين محدودة

معالجة رقم (٧):
الدور المقترح المفعل لمراجع الحسابات اذا كان مراجع الحسابات لا ينتمي لأحد المكاتب الكبار وله خبرة طويلة في المهنة، كما ان درجة الثقة في تقرير إدارة المخاطر لدي المبحوثين محدودة

معالجة رقم (٨):
الدور المقترح المفعل لمراجع الحسابات اذا كان مراجع الحسابات لاينتمي لأحد المكاتب الكبار وله خبرة قليلة في المهنة، كما ان درجة الثقة في تقرير إدارة المخاطر لدي المبحوثين محدودة

معالجة رقم (٩):
الدور المقترح الغير مفعل لمراجع الحسابات اذا كان مراجع الحسابات ينتمي لأحد المكاتب الكبار وله خبرة طويلة في المهنة، كما ان درجة الثقة في تقرير إدارة المخاطر لدي المبحوثين معقولة

معالجة رقم (١٠):
الدور المقترح الغير مفعل لمراجع الحسابات اذا كان مراجع الحسابات ينتمي لأحد المكاتب الكبار وله خبرة قليلة في المهنة، كما ان درجة الثقة في تقرير إدارة المخاطر لدي المبحوثين معقولة

معالجة رقم (١١):
الدور المقترح الغير مفعل لمراجع الحسابات اذا كان مراجع الحسابات لا ينتمي لأحد المكاتب الكبار وله خبرة طويلة في المهنة، كما ان درجة الثقة في تقرير إدارة المخاطر لدي المبحوثين معقولة

معالجة رقم (١٢):
الدور المقترح الغير مفعل لمراجع الحسابات اذا كان مراجع الحسابات لاينتمي لأحد المكاتب الكبار وله خبرة قليلة في المهنة، كما ان درجة الثقة في تقرير إدارة المخاطر لدي المبحوثين معقولة

معالجة رقم (١٣):
الدور المقترح الغير مفعل لمراجع الحسابات اذا كان مراجع الحسابات ينتمي لأحد المكاتب الكبار وله خبرة طويلة في المهنة، كما ان درجة الثقة في تقرير إدارة المخاطر لدي المبحوثين محدودة

معالجة رقم (١٤):
الدور المقترح الغير مفعل لمراجع الحسابات اذا كان مراجع الحسابات ينتمي لأحد المكاتب الكبار وله خبرة قليلة في المهنة، كما ان درجة الثقة في تقرير إدارة المخاطر لدي المبحوثين محدودة

معالجة رقم (١٥):
الدور المقترح الغير مفعل لمراجع الحسابات اذا كان مراجع الحسابات لا ينتمي لأحد المكاتب الكبار وله خبرة طويلة في المهنة، كما ان درجة الثقة في تقرير إدارة المخاطر لدي المبحوثين محدودة

معالجة رقم (١٦):
الدور المقترح الغير مفعل لمراجع الحسابات اذا كان مراجع الحسابات لاينتمي لأحد المكاتب الكبار وله خبرة قليلة في المهنة، كما ان درجة الثقة في تقرير إدارة المخاطر لدي المبحوثين محدودة

قطاعات متغيرات الدراسة:
قبل التطرق الى التحقق من صحة او خطأ فرضيات الدراسة تم استخدام التحليل العنقودي السريع k-mean cluster analysis والهدف من ذلك هو تقسيم متغيرات الدراسة الى عنقودين بحيث يتم دراسة كل متغير في حالتين مختلفتين. بالإضافة الى تحليل التباين الأحادي المصاحب للتحليل العنقودي السريع والذي يهتم بدراسة المعنوية بين العنقودين المقسمين.

- **سنوات الخبرة**

تم الاعتماد بشكل مبدئي على تقسيم سنوات الخبرة الى عنقودين باعتبار ان كل عنقود متجانس ومختلف عن العنقود الاخر، حيث تم تسمية العنقود الأول سنوات الخبرة الطويلة وهو يتضمن أصحاب الخبرة ذوي ال ٥ سنوات واكثر، والعنقود الثاني سنوات الخبرة القليلة وهو يتضمن أصحاب الخبرة الأقل من ٥ سنوات.

- **حجم مكتب المراجعة**

تم الاعتماد بشكل مبدئي على تقسيم حجم مكتب المراجعة الى عنقودين باعتبار ان كل عنقود متجانس ومختلف عن العنقود الاخر، حيث تم تسمية العنقود الأول حجم مكتب المراجعة الكبير وهو ينتمي الى احد المكاتب الأربعة الكبري، والعنقود الثاني حجم مكتب المراجعة الصغير وهو لا ينتمي الى احد المكاتب الأربعة الكبار

- **الدور المقترح للمراجع**

تم الاعتماد بشكل مبدئي على تقسيم الدور المقترح للمراجع الى عنقودين باعتبار ان كل عنقود متجانس ومختلف عن العنقود الاخر، حيث تم تسمية العنقود الأول الدور المقترح للمراجع المفعل، والعنقود الثاني الدور المقترح للمراجع الغير مفعل

- **درجة إضفاء الثقة بتقرير إدارة المخاطر**

تم الاعتماد بشكل مبدئي على تقسيم درجة إضفاء الثقة الى عنقودين باعتبار ان كل عنقود متجانس ومختلف عن العنقود الاخر، حيث تم تسمية العنقود الأول درجة إضفاء الثقة المعقولة، والعنقود الثاني درجة إضفاء الثقة المحدودة، وذلك كما هو موضح بالجدول التالي :

المتغير		حجم العينة	المراكز المبدئية للعناقيد	المراكز النهائية للعناقيد	المسافة بين المراكز النهائية للعناقيد		F	Sig.
					العنقود الاول	العنقود الثاني		
الدور المقترح للمراجع	العنقود الاول	١٤٩	١.٠	١.٨١	٠.٠٠	٠.٨٥	٨٠٧.٧١٢	0.000
	العنقود الثاني	٢٥١	٣.٠	٢.٦٦	٠.٨٥	٠.٠٠		
درجة إضفاء الثقة بتقرير إدارة المخاطر	العنقود الاول	٢١٦	١.٠	١.٥١	٠.٠٠	١.٣	١٠٨٨.٦٩٩	0.000
	العنقود الثاني	١٨٤	٣.٠	٢.٨١	١.٣	٠.٠٠		

يوضح الجدول السابق وجود اختلاف معنوي ودال احصائيا لجميع متغيرات الدراسة والتي تعزي الى العنقودين الأول والثاني مما يؤكد على اختلاف العناقيد التي تم تقسيمها بالتحليل العنقودي عن بعضها البعض، وذلك بدرجة ثقة ٩٥%

٥/٨ نتائج اختبار فروض البحث

ف١: لا يوجد تأثير معنوي لأهمية الافصاح على تقرير إدارة مخاطر الامن السيبراني

جدول اختبار تبعية متغيرات الفرض الأول للتوزيع الطبيعي

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
افصاح شركة تنتمي لمجال تكنولوجيا المعلومات لتقرير ادارة المخاطر	.285	401	.000	.809	401	.000
افصاح شركة لا تنتمي لمجال تكنولوجيا المعلومات لتقرير ادارة المخاطر	.345	401	.000	.759	401	.000

a. Lilliefors Significance Correction

يوضح الجدول السابق ان جميع متغيرات الفرض الاول لا تتبع التوزيع الطبيعي لذلك تم استخدام الاختبار اللامعلمي Wilcoxon Signed Ranks Tes للتحقق من الفرض الاول كما يلي:

للتحقق من هذا الفرض تم استخدام اختبار Wilcoxon Signed Ranks Test، حيث يشير الفرض العدمي الى عدم وجود تأثير معنوي لأهمية الافصاح على تقرير إدارة مخاطر الامن السيبراني، وكانت نتيجته موضحة كما يلي:

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The median of differences between افصاح شركة تشي لسجل تكنولوجيا المعلومات and افصاح شركة لا تشي لسجل تكنولوجيا المعلومات لتقرير ادارة المخاطر equals 0.	Related-Samples Wilcoxon Signed Rank Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

وضح الجدول السابق ان القيمة الدلالية للاختبار ٠.٠٠٠ وهي اقل من مستوي المعنوية ٠.٠٥ مما يعنى رفض الفرض العدمي وقبول الفرض البديل الذي ينص على وجود تأثير معنوي لأهمية الافصاح على تقرير إدارة مخاطر الامن السيبراني.

ف٢: لا يوجد تأثير معنوي لأهمية دور المراجع المقترح على دلالة القوائم المالية

للتحقق من الفرض الثاني للدراسة تم اجراء المقارنات التالية بين المعالجات:

المقارنة الأولى:

$\{(16:9)x(8:1)\}$ وذلك لقياس أثر أهمية تفعيل دور المراجع المقترح على دلالة القوائم المالية ومن ثم الإجابة على الفرض الرئيسي الثاني.

المقارنة الثانية:

$\{(16:13)+(8:5)\}x\{(12:9)+(4:1)\}$ وذلك لقياس اثر إضفاء الثقة بتقرير مخاطر الامن السيبراني على العلاقة بين أهمية دور المراجع المقترح ودلالة القوائم المالية، ومن ثم الإجابة على الفرض الفرعي الثاني

المقارنة الثالثة:

$\{(14:10)+(6:2)\}x\{(13:9)+(5:1)\}$ وذلك لقياس اثر خبرة المراجع الطويلة على العلاقة بين أهمية دور المراجع المقترح ودلالة القوائم المالية، ومن ثم الإجابة على الفرض الفرعي الثاني

المقارنة الرابعة:

$\{(16:12)+(8:4)\}x\{(15:11)+(7:3)\}$ وذلك لقياس اثر حجم مكتب المراجعة على العلاقة بين أهمية دور المراجع المقترح ودلالة القوائم المالية، ومن ثم الإجابة على الفرض الفرعي الثاني

اختبار تبعية المتغيرات للتوزيع الطبيعي

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
المالية القوائم بدلالة مفعل غير دور	.392	400	.000	.697	400	.000
المالية القوائم بدلالة مفعل دور	.266	400	.000	.792	400	.000
المقترح الدور بدلالة قليلة خبرة المالية القوائم على	.413	400	.000	.668	400	.000
المقترح الدور بدلالة طويلة خبرة المالية القوائم على	.214	400	.000	.867	400	.000
المقترح الدور بدلالة كبير مكتب المالية القوائم على	.293	400	.000	.810	400	.000
المقترح الدور بدلالة صغير مكتب المالية القوائم على	.339	400	.000	.762	400	.000
المقترح الدور بدلالة محدودة ثقة المالية القوائم على	.261	400	.000	.802	400	.000
المقترح الدور بدلالة معقولة ثقة المالية القوائم على	.337	400	.000	.752	400	.000
تكنولوجيا لمجال تنتمي الشركة المعلومات	.376	400	.000	.630	400	.000
تكنولوجيا لمجال تنتمي لا الشركة المعلومات	.376	400	.000	.630	400	.000
لمجال تنتمي شركة افصاح ادارة لتقرير المعلومات تكنولوجيا المخاطر	.285	400	.000	.809	400	.000
لمجال تنتمي لا شركة افصاح ادارة لتقرير المعلومات تكنولوجيا المخاطر	.344	400	.000	.760	400	.000
للمخزون مفعل غير دور	.389	400	.000	.704	400	.000
للمخزون مفعل دور	.266	400	.000	.790	400	.000

الاسهم لتقييم مفعل غير دور	.388	400	.000	.706	400	.000
الاسهم لتقييم مفعل دور	.264	400	.000	.801	400	.000
المقترح الدور بدلالة محدودة ثقة المخزون على	.262	400	.000	.801	400	.000
المقترح الدور بدلالة محدودة ثقة الاسهم تقييم على	.258	400	.000	.799	400	.000
المقترح الدور بدلالة معقولة ثقة المخزون على	.337	400	.000	.750	400	.000
المقترح الدور بدلالة معقولة ثقة الاسهم تقييم على	.336	400	.000	.753	400	.000
المقترح الدور بدلالة طويلة خبرة المخزون على	.215	400	.000	.865	400	.000
المقترح الدور بدلالة طويلة خبرة الاسهم تقييم على	.211	400	.000	.870	400	.000
المقترح الدور بدلالة قليلة خبرة المخزون على	.413	400	.000	.666	400	.000
المقترح الدور بدلالة قليلة خبرة الاسهم تقييم على	.411	400	.000	.666	400	.000
المقترح الدور بدلالة كبير مكتب المخزون على	.293	400	.000	.807	400	.000
المقترح الدور بدلالة كبير مكتب الاسهم تقييم على	.291	400	.000	.813	400	.000
المقترح الدور بدلالة صغير مكتب المخزون على	.339	400	.000	.760	400	.000
المقترح الدور بدلالة صغير مكتب الاسهم تقييم على	.336	400	.000	.761	400	.000

a. Lilliefors Significance Correction

يوضح الجدول السابق ان جميع متغيرات الفرض الثاني لا تتبع التوزيع الطبيعي لذلك تم استخدام الاختبار اللامعلمي Wilcoxon Signed Ranks Tes للتحقق من الفرض الرئيسي الثاني كما يلي:

للتحقق من هذا الفرض تم استخدام اختبار Wilcoxon Signed Ranks Test، حيث يشير الفرض العدمي الى عدم وجود تأثير معنوي لأهمية دور المراجع المقترح على دلالة القوائم المالية، وكانت نتيجته موضحة كما يلي:

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The median of differences between دور مفعل بدلالة القوائم المالية and دور غير مفعل بدلالة القوائم المالية equals 0.	Related-Samples Wilcoxon Signed Rank Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

يوضح الجدول السابق ان القيمة الدلالية للاختبار ٠.٠٠٠ وهي اقل من مستوي المعنوية ٠.٠٥ مما يعنى رفض الفرض العدمي وقبول الفرض البديل الذي ينص على وجود تأثير معنوي لأهمية دور المراجع المقترح على دلالة القوائم المالية **بالنسبة للمخزون**

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The median of differences between دور مفعل للمخزون and دور غير مفعل للمخزون equals 0.	Related-Samples Wilcoxon Signed Rank Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

يوضح الجدول السابق ان القيمة الدلالية للاختبار ٠.٠٠٠ وهي اقل من مستوي المعنوية ٠.٠٥ مما يعنى رفض الفرض العدمي وقبول الفرض البديل الذي ينص على وجود تأثير معنوي لأهمية دور المراجع المقترح على المخزون
بالنسبة لتقييم الاسهم

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The median of differences between دور غير مفعل لتقييم الاسهم and دور مفعل لتقييم الاسهم equals 0.	Related-Samples Wilcoxon Signed Rank Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

يوضح الجدول السابق ان القيمة الدلالية للاختبار ٠.٠٠٠ وهي اقل من مستوي المعنوية ٠.٠٥ مما يعنى رفض الفرض العدمي وقبول الفرض البديل الذي ينص على وجود تأثير معنوي لأهمية دور المراجع المقترح على تقييم الأسهم.

ف٢/a: لا يوجد تأثير معنوي لدرجة الثقة بتقرير إدارة المخاطر على العلاقة بين أهمية دور المراجع المقترح ودلالة القوائم المالية

للتحقق من هذا الفرض تم استخدام اختبار Wilcoxon Signed Ranks Test، حيث يشير الفرض العدمي الى عدم وجود تأثير معنوي لدرجة الثقة بتقرير إدارة المخاطر على العلاقة بين أهمية دور المراجع المقترح ودلالة القوائم المالية، وكانت نتيجته موضحة كما يلي:

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The median of differences between ثقة محدودة بدلالة الدور المقترح على القوائم المالية and ثقة محققة بدلالة الدور المقترح على القوائم المالية equals 0.	Related-Samples Wilcoxon Signed Rank Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

يوضح الجدول السابق ان القيمة الدلالية للاختبار ٠.٠٠٠ وهي اقل من مستوي المعنوية ٠.٠٥ مما يعنى رفض الفرض العدمي وقبول الفرض البديل الذي ينص على وجود تأثير معنوي لدرجة الثقة بتقرير إدارة المخاطر على العلاقة بين أهمية دور المراجع المقترح ودلالة القوائم المالية

بالنسبة للمخزون

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The median of differences between ثقة محدودة بدلالة الدور المقترح على المخزون and ثقة محققة بدلالة الدور المقترح على المخزون equals 0.	Related-Samples Wilcoxon Signed Rank Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

يوضح الجدول السابق ان القيمة الدلالية للاختبار ٠.٠٠٠ وهي اقل من مستوي المعنوية ٠.٠٥ مما يعنى رفض الفرض العدمي وقبول الفرض البديل الذي ينص على وجود تأثير معنوي لدرجة الثقة بتقرير إدارة المخاطر على العلاقة بين أهمية دور المراجع المقترح والمخزون

بالنسبة لتقييم الاسهم

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The median of differences between ثقة محدودة بدلالة الدور المقترح على تقييم الاسهم and ثقة معقولة بدلالة الدور المقترح على تقييم الاسهم equals 0.	Related-Samples Wilcoxon Signed Rank Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

يوضح الجدول السابق ان القيمة الدلالية للاختبار ٠.٠٠١ وهي اقل من مستوي المعنوية ٠.٠٥ مما يعنى رفض الفرض العدمي وقبول الفرض البديل الذي ينص على وجود تأثير معنوي لدرجة الثقة بتقرير إدارة المخاطر على العلاقة بين أهمية دور المراجع المقترح وتقييم الاسهم

ف٢/b: لا يوجد تأثير معنوي لخبرة المراجع الطويلة على العلاقة بين أهمية دور المراجع المقترح ودلالة القوائم المالية

للتحقق من هذا الفرض تم استخدام اختبار Wilcoxon Signed Ranks Test، حيث يشير الفرض العدمي الى عدم وجود تأثير معنوي لخبرة المراجع الطويلة على العلاقة بين أهمية دور المراجع المقترح ودلالة القوائم المالية، وكانت نتيجته موضحة كما يلي:

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The median of differences between خبرة طويلة بدلالة الدور المقترح على القوائم المالية and خبرة قليلة بدلالة الدور المقترح على القوائم المالية equals 0.	Related-Samples Wilcoxon Signed Rank Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

يوضح الجدول السابق ان القيمة الدلالية للاختبار ٠.٠٠٠ وهي اقل من مستوي المعنوية ٠.٠٥ مما يعنى رفض الفرض العدمي وقبول الفرض البديل الذي ينص على وجود تأثير معنوي لخبرة المراجع الطويلة على العلاقة بين أهمية دور المراجع المقترح ودلالة القوائم المالية

بالنسبة للمخزون

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The median of differences between خبرة طويلة بدلالة الدور المقترح على المخزون and خبرة قليلة بدلالة الدور المقترح على المخزون equals 0.	Related-Samples Wilcoxon Signed Rank Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

يوضح الجدول السابق ان القيمة الدلالية للاختبار ٠.٠٠٠ وهي اقل من مستوي المعنوية ٠.٠٥ مما يعنى رفض الفرض العدمي وقبول الفرض البديل الذي ينص على وجود تأثير معنوي لخبرة المراجع الطويلة على العلاقة بين أهمية دور المراجع المقترح والمخزون.

بالنسبة لتقييم الاسهم

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The median of differences between خبرة طويلة بدلالة الدور المقترح على تقييم الاسهم and خبرة قليلة بدلالة الدور المقترح على تقييم الاسهم equals 0.	Related-Samples Wilcoxon Signed Rank Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

يوضح الجدول السابق ان القيمة الدلالية للاختبار ٠.٠٠٠ وهي اقل من مستوي المعنوية ٠.٠٥ مما يعنى رفض الفرض العدمي وقبول الفرض البديل الذي ينص على وجود تأثير معنوي لخبرة المراجع الطويلة على العلاقة بين أهمية دور المراجع المقترح لتقييم الاسهم.

ف٢/c: لا يوجد تأثير معنوي لحجم مكتب المراجعة على العلاقة بين أهمية دور المراجع المقترح ودلالة القوائم المالية

للتحقق من هذا الفرض تم استخدام اختبار Wilcoxon Signed Ranks Test، حيث يشير الفرض العدمي الى عدم وجود تأثير معنوي لحجم مكتب المراجعة على العلاقة بين أهمية دور المراجع المقترح ودلالة القوائم المالية، وكانت نتيجته موضحة كما يلي:

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The median of differences between مكتب كبير جلالة الدور المقترح على القوائم المالية and مكتب صغير جلالة الدور المقترح على القوائم المالية equals 0.	Related-Samples Wilcoxon Signed Rank Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

يوضح الجدول السابق ان القيمة الدلالية للاختبار ٠.٠٠٠ وهي اقل من مستوي المعنوية ٠.٠٥ مما يعنى رفض الفرض العدمي وقبول الفرض البديل الذي ينص على وجود تأثير معنوي لحجم مكتب المراجعة على العلاقة بين أهمية دور المراجع المقترح ودلالة القوائم المالية

بالنسبة للمخزون

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The median of differences between مكتب كبير دلالة الدور المقترح على المخزون and مكتب صغير دلالة الدور المقترح على المخزون equals 0.	Related-Samples Wilcoxon Signed Rank Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

يوضح الجدول السابق ان القيمة الدلالية للاختبار ٠.٠٠٠ وهي اقل من مستوي المعنوية ٠.٠٥ مما يعنى رفض الفرض العدمي وقبول الفرض البديل الذي ينص على وجود تأثير معنوي لحجم مكتب المراجعة على العلاقة بين أهمية دور المراجع المقترح والمخزون

بالنسبة لتقييم الاسهم

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The median of differences between مكتب كبير دلالة الدور المقترح على تقييم الاسهم and مكتب صغير دلالة الدور المقترح على تقييم الاسهم equals 0.	Related-Samples Wilcoxon Signed Rank Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

يوضح الجدول السابق ان القيمة الدلالية للاختبار ٠.٠٠٠ وهي اقل من مستوي المعنوية ٠.٠٥ مما يعنى رفض الفرض العدمي وقبول الفرض البديل الذي ينص على وجود تأثير معنوي لحجم مكتب المراجعة على العلاقة بين أهمية دور المراجع المقترح وتقييم الأسهم

٦/٨ النتائج والتوصيات و مجالات البحث المقترحة

١/٦/٨ النتائج:

فيما يتعلق بالامن السيبراني:

١-يتعلق بشكل اساسي بأدارة المخاطر المستقبلية و الاستجابة للحوداث الحالية و الماضية.

٢-تتطلب ادارة المخاطر المستقبلية نظرة ثاقبة لنقاط الضعف الحالية والمستقبلية ،وكيفية منعها اوالحد منهاو احتمالات التهديد ،و التكاليف المرتبطة بالنتائج المحتملة وكيفية التخفيف منها .

٣-تتطلب الاستجابة للحوادث و الهجمات الحالية و السابقة معرفة ما حدث و طرق منع حوادث مماثلة في المستقبل و الاجراءات القانونية و غيرها من الاجراءات العلاجية الممكنة ضد الجناة.

فيما يتعلق بالدور المقترح للمراجعين:

١- لا يقتصر كون المراجع مستشارا موثوقا للامن السيبراني علي معرفة المفاهيم الاساسية لمخاطر الامن السيبراني ،و التعاون ببساطة مع موظفي تكونولوجيا المعلومات لتتوفر لديه الخبرة في مجال الامن السيبراني.

٢- يجب علي المراجعين توسيع قدراتهم في مراجعة تكنولوجيا المعلومات لتقديم روئ استباقية و بهذة الطريقة يمكنهم تقديم توصيات ذات قيمة مضافة للادارة.

٣- يجب علي المراجعين ان يكونوا علي معرفة عملية قوية بالتغيرات القادمة في اللوائح ذات الصلة و المتطلبات الجديدة و الاتجاهات الصناعية الاخري.

٤- يجب ان يحدد المراجعين بحذر كفاءات الامن السيبراني للرئيس التنفيذي للمراجعة و المراجعين الداخليين من خلال ادارة المواهب الفعالة ،و برامج

التطوير المهني بناءا علي معايير معهد المراجعين و الاستفادة بشكل استراتيجي من المصادر المشتركة لتوفير كفاءات مناسبة.

فيما يتعلق بأدارة المخاطر:

١- لا يقتصر ان يصبح المراجع مستشارا الكترونيا موثوقا به علي اجراء تقييم للمخاطر لتحديد احتمالية وتأثير المخاطر الالكترونية ،و ادراك كيفية تعامل المنظمة مع الامن السيبراني و الاجراءات التي اتخذتها الادارة للتخفيف من المخاطر ذات الصلة او مراجعة تقاريرمراجعة ،وبدلا من ذلك يجب علي المراجعين فهم التاثير الكامل للتهديدات الالكترونية علي المنظمة.

٢- يجب عليهم تضمين ذلك بشكل خاص في خطة المراجعة القائمة علي المخاطر الخاصة بهم في وقت واحد.

٣- يجب ان يكون المراجعين الداخلين مؤهلين للتعرف بشكل استباقي علي مخاطر الامن السيبراني الناشئة ولتحقيق ذلك يجب علي المراجعين فهم مدي قابلية المنظمة للمخاطر لمكافحة التهديدات الالكترونية من خلال اجراء مراجعة مستمرة علي ضوابط الامن السيبراني للادارة.

٤- يجب علي المراجعين ان يكون لديهم شراكة مستمرة مع مزودي الخدمات الكترونية.

فيما يتعلق باضفاء الثقة علي تقرير ادارة مخاطر الامن السيبراني:

١- لا يقتصر ان يصبح المراجع موثوقا به علي تقييم الامتثال للسياسات و الاجراءات المتعلقة بالفضاء الالكتروني لتوفير ضمانات بشأن برامج الامن السيبراني للمنظمة ، بل يجب ايضا توفير ضمانات بشأن الاستجابة للحوادث و التعافي من الكوارث و حفظ استمرارية الاعمال.

٢- الابلاغ عن نتائج المشاركة المتعلقة بالامن السيبراني الي الادارة و مجلس الادارة و لجنة المراجعة.

٣- يجب علي المراجعين تقديم مراجعة مستقلة لاستراتيجية الامن السيبراني قبل وضع السياسات و الاجراءات.

٤- يجب ان يكون المراجعين جزءا من فرق تنفيذ المشروع التكنولوجي لضمان معالجة المخاطر الالكترونية و دمجها بدلا من اضافتها لاحقا الي العملية ذات الصلة.

٦/٨ /٢ التوصيات:

١- ضرورةاهتمام الشركات التي تبنت التحول الرقمي بأدارة مخاطر الامن السيبراني.

٢- ضرورة قيام الهيئات الرقابية المصرية بوضع ضوابط وارشادات تساعد الشركات عند القيام بممارسات الافصاح عن مخاطر الامن السيبراني

٣- ضرورة اهتمام الجهات المنوط بها اصدار المعايير باصدار معيار ينظم جوانب الافصاح المحاسبي عن انشطة و مخاطر الامن السيبراني و برامج ادارة مخاطر الامن السيبراني

٤- ضرورة قيام الجامعات بتضمين المقررات الدارسية المتخصصة بالموضوعات الحديثة مثل ادارة مخاطر الامن السيبراني و ذلك بمرحلتي البكالوريوس و الدراسات العليا

٥- ضرورة تفعيل الدور المقترح لمراجع الحسابات في اضفاء الثقة علي تقرير ادارة مخاطر الامن السيبراني

٣/٦/٨ مجالات البحث المقترحة:

١- الدور المقترح للمراجع الخارجي في الشركات التي تنبت التحول الرقمي ولديها ادارة لمخاطر الامن السيبراني

٢- اثر الافصاح عن ادارة مخاطر الامن السيبراني علي اسعار الاسهم وحجم تداولها.

٣- اثر قيام الشركات بأدارة مخاطر الامن السيبراني علي اتعاب المراجعة و جهد المراجع

٤- دراسة واختبار اثر قيام المراجعة الداخلية بدورها الاستشاري و التوكيدي في مجال انشطة ادارة مخاطر الامن السيبراني علي قيمة الشركة

٧/٨ المراجع:

١. الاستراتيجية الوطنية للأمن السيبراني (٢٠١٧-٢٠٢١)، المجلس الأعلى للأمن السيبراني، رئاسة مجلس الوزراء، جمهورية مصر العربية، ص ١-١٩، متاح على الرابط: www.mcit.gov.eg/upcont, 2017-2021
٢. الدليل الاسترشادي للأمن السيبراني لمؤسسات السوق المالية،٢٠١٩،هيئة السوق المالية، السعودية، ص ص ١-٤٧.
٣. الرشيدي، طارق عبدالعظيم، عباس، داليا عادل ،(٢٠١٩)،"أثر الافصاح عن مخاطر الأمن السيبراني في التقارير المالية على اسعار واحجام التداول – دراسة مقارنة في قطاع تكنولوجيا المعلومات"، مجلة المحاسبة والمراجعة، وكلية التجارة، جامعة بني سويف، مجلد ٨، العدد٢، ص ص ٤٣٩- ٤٨٧.
٤. الصيرفي، أسماء أحمد، (٢٠٢٢)، "أثر تطبيق الشركات لإدارة مخاطر الأمن السيبراني على جودة المراجعة الخارجية"، كلية التجارة، جامعة الإسكندرية، مجلة البحوث المحاسبية، مارس.
٥. المجلس الأعلى للأمن السيبراني التابع لمجلس الوزراء المصري ٢٠٠٧.
٦. الاستراتيجية الوطنية للأمن السبراني ٢٠١٧ – ٢٠٢١.
٧. البنك المركزي المصري ٢٠١٩، تقرير الاستقرار المالي لعام ٢٠١٨.
٨. بدوى، هبة الله عبدالسلام،٢٠٢١،" أثر جودة ومستوى التوكيد على برنامج إدارة مخاطر الأمن السيبراني على قرارات المستثمرين المصريين غير المحترفين ،مجلة الاسكندرية للبحوث التجارية، كلية التجارة، جامعة الاسكندرية، المجلد ٥،العدد٣،ص ص١-٥٦.
٩. عبدالمنعم باهي الدين وأخرون، (٢٠٢٢)، دور المراجع الداخلي في مواجهة خطر الأمن السيبراني وخطر الغش في الاستعانة بمصادر خارجية في عمليات التأمين: دراسة استطلاعية"، مجلة الإسكندرية للبحوث المحاسبية، سبتمبر، العدد الثالث.
١٠. محمود أحمد أحمد علي، وصالح علي صالح علي، (٢٠٢٢)، "أثر الإفصاح عن تقرير إدارة الأمن السيبراني على قرار الاستثمار بأسهم السندات المقيدة بالبورصة المصرية: دراسة تجريبية"، مجلة إسكندرية للبحوث المحاسبية، العدد الثالث، سبتمبر.
١١. محمد موسى، رمضان عارف، صالح أبو الحمد مصطفى، (٢٠٢٢)، "استخدام المنهجية الرشيقة في تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني، مجلة البحوث المالية والتجارية، كلية التجارة، جامعة جنوب الوادي، المجلد ٢٣، العدد ٣، ص ص ٤٣٢ – ٤٩٠.

12. E.V.A. Eijkelenboom, B.F.H. Niewesteeg,2019, An Analysis Of Cyber Security In Dutch Annual Reports Of Listed Companies, Computer Law& Security Review, V.40.
13. Musaib ashraf, paul n michas, dan russomanno,202 0, the impact of audit committee information technology expertise on the reliability and timeliness of financial reporting, the accounting review,95(5),pp23-56..
14. Pierangelo Rosati, fabian gogolin, theo lynn, 2020, cyber security incidents and audit quality, European accounting review, pp1-28.
15. Rosati, P; lynn,tg;andgogolin,f;2018; cyber security incident, external monitoring and probability of restatements, pp1-44.
16. Eaton,t, V; Grenier,j, H and Layman,d;2019; accounting and cyber security risk management, American accounting association, vol.13, no.2, pp 1-9.
17. ICAEW, 2016, Audit Insights Cyber Security Taking Control of The Agenda. icaew.com/auditinsights.
18. Li, He; No, Wong, Gyun, Bority, JEfrim. Are External auditor Concerned about cyber security Incidents?
19. Nancy Lankton, Jean B Price, Mohamed Karim, 2021, Cyber Security Breaches And The Role of Information Technology Governance in Audit Committee Charters, Journal of Information Systims, 35(1), Pp101-119.
20. National audit office, (NAO)2017,cyber security and information risk guidance for audit committees, pp 1-16. www.isca.org.sg
21. Prigerson Carolyn,Gene Rainey, Aba Elena,2021, Issues On The Timelines And Reliability Of Corporate Financial Statement And The Expertise Of Audit Committee Information Technology, Review Of Business Accounting & Finance (RBAF), V.1,N.5,PP 392-414.

22. Release No. 33-11038, Cybersecurity Risk Management, strategy Governance, and Incident Disclosure (Mar 9, 2022) avaliable at https://www.sec.gov/rules/Proposed/2022/33-11038.pdf.
23. Abbasi, A., sarker, s. and chiang, R. H. (2016) Big Data Research In Information system: Toward an Inclusive Research Agenda- Journal of Association For Information System, 17 (2), 1-22.
24. Appelbaum, D.A., Kogan, A. and vas arhelyi, M. A. 2013 "Big data and analytics in the modern audit. engagement: Research needs", Auditing: A Journal of practice and theory, Vol36, No. 4, pp. 1-27.
25. Bloem, J. Van Doom, M. Duivestein, S. Excoffier, D.. Maas, R. and Van Ommeren, E. (2014), The Fourth. Industrial revolution", Things Tighten.
26. Cavusog lu, H., Mishra, B., and el al, (2004), The Effect of Internet security breach announcements on market value: Capital market reactions For breached Firms and Internet security developers. International Journal of Electronic Commerce, 9 (1) 70-104.
27. Cisco (2017) Cisco 2017 Annual Cyber Security Report. Available at:
28. Commission statement and Guidance on. Public Company Cyber security Disclosure, Release No 33- 104 59 (Feb. 26, 2018).available at http://www.sec.gov/rules.interp//2018-33-10459.pdf.
29. Committee of sponsoring organization of the Tread way Commission (coso) (2004).
30. Edith Orenstein,2017, Aicpa Issues Final Standards For Auditor, Management Reporting On Cybersecurity, Available At: www.macpa.orgl/aicpa-issues- /Agement Reporting On Cybersecurity.
31. Enterprise Risk Management - Integrated Framework. Durham, NC AICPA.
32. Gay G. E. and Su simontt, R., (2015) " Auditing and Assurance Services in Australia, Mc Grand_ Hill Book Company.

33. Griffin, P. A. and Wright, A.M. (2015), “Commentaries on big Data's importance for accounting and auditing", Accounting Horizon, VOL.29 No.2, PP. 377-379.
34. Gvidence from audit Fees. Auditing; Sarasota vol, 39 Iss 1 Feb, 2020.
35. Haapmaki, Elina, Sihvonen, Jakka," Cyber security (2019) in accounting research", Managerial Auditing Journal, Bradford, vol 34, Iss 7, pp. 808-834.
36. Haapmaki, Elina, sihvonen, Ju kka. (2019), cybersecurity in accounting, Manageriaf Auditing Journal Brad ford vol 34, Issu 7, 808-834.
37. Hatherly, D.J. (2009)" Travelling Audit 's Fault lines: a new arch architecture for cuditing standais Managerial auditing Journal, vol. 24. No. 2, pp.204-215.
38. http://www.cisco.com/c/m/en_au/products/security/offersl/annual-Cybersecurity- Report.
39. Jim Peterson , (2022), "The Future of External Audit: Issues and Questions", International Journal of Auditing, Vol.26, Issue 1, Jan., pp.14-17.
40. Krahel, J.P. and Titern, W.R. (2015)," Lon sequences. of big data and formalization on accounting and auditing standards", Accounting Horizon, vol. 29 No. 2, PP. 408-422.-
41. La Torre, H. Dumay, J. and Rea, M. A. (2018) "Breaching intellectual Capital, critical reflection on big Data -Security", Meditari Accountancy Research, vol 26 No.3 pp. 463 482.
42. Lawrance and, T. B. and suddaby, R. (2006) "Institutions and Institutional work" in alegy S. R., Hardy C., Nord, W. R. and Lawrence, T.B. (Eds) SAGE publication, London, pp. 215-254.
43. Lybersecurity Incident and audit quality, Rosati Pierangelo; Gogolin, Fabian lynn, Theo, European Accounting Review; Vol. 31, Iss. 3 (Jul 2022) 701-728.

44. Matteo La torre, Botes Vida Lucia, Dumay John, edendaal, Elja.
45. Messier, f., Glover, S. and Prawitt, D. (2017), "Auditing and Assurance Services: A systematic Approach, the Grow Hill New York, NY.
46. Protecting a new Achilles heel: The Role of auditors within the practice of data protect is Managerial auditing Journal, Bradford vol 36 Iss 2 (2021) 218-239.
47. Public company Accounting oversight Board (PCAOB) (2010). Identifying AND Assessing Risk of Material Misstatement. As No. 12.
48. Romanosky, S., Hoffman, D., and Acquisit, A. (2014) "Empirical analysis of data breash litigation, Journal of Emplrical legal studies, 11 (1), 64-74.
49. Rosati, P., Deeney, P. Cummins, M. et al. (2019). Social media and stock price Reaction to data breach announcement: Evidence From Us. listed companies. Research in International Business and finance, 47, 458-469.
50. Schatzki, T.R. (2006), "on organizations as They happen", organization studies, vol. 27. No. 12, pp. 1863-1872.
51. Thomas G. Calderon Lei Gao, (2020), "Cyber Security Risks Disclosure and Implied Audit Risks: Evidence from Audit Fees", International Journal of Auditing, Vol.25, Issue 1.
52. Tran Nguen. B. and A ndrea. T., (2021)," cyber Security Risks Assessment By External Auditors Interdisciplinary Description-Complex systems pp. 375- 390.
53. Wak unuma, k. J. and stahl, B. C. (2014), " Tamarrow's ethics and today's response: an investigation into the ways. information Systems professionals perceive and address emerging ethical issues", Information systems form Frontiers, Vol 16 No. 3, PP 383-397.
54. Whitman, M.E. (2003), "Enemy at the gate", Communications of the ACM, vol. 46 No.8 PP. 91-95.

55. Yeen, K., Hoogduin, L. and Zhang; L. (2015), "Big data as complementary audit evidence", Accounting Horizon, vol. 29. No.2, PP. 431-438.
56. Zhao, N., Yen, D. C. and change, I. C., (2004), Auditing in the e. Commerce era", Information management and Computer Security, vol.12, No.15, pp. 389-400.
57. Securities and Exchange Commission (SEC), Securities and Exchange Proposes Syber Security Risk Management Rules and Amendments for Regis Tered Investment Advisers and Funds Press Release, February 9, http://www.sec.gov/news/press-release/2022.