أثر مخاطر الأمن السيبراني على أتعاب المراجع

عن مراجعة القوائم المالية – دراسة تجريبية

ياسمين داود موسى حمد الطيار
باحثة ماجستير بكلية الأعمال – جامعة اسكندرية
hawa.23eltayar@gmial.com

أ.د/ هانى خليل فرج
أستاذ المحاسبة والمراجعة – كلية الأعمال – جامعة اسكندرية
hany_khalil2007@yahoo.com

د/ محمد وليد قاسم
مدرس المحاسبة والمراجعة – كلية الأعمال – جامعة اسكندرية
Mohamed.walid.kassem@alexu.edu.eg

ملخص البحث

استهدف البحث دراسة واختبار تأثير مخاطر الأمن السيبراني على أتعاب المراجع عن مراجعة القوائم المالية، مع الأخذ في الاعتبار المتغيرات المعدلة، التأهيل العلمي والخبرة المهنية للمراجعين. ويركز البحث على إجراء دراسة تجريبية على عينة من مراجعي الحسابات بمكاتب المراجعة المسجلة لدى الهيئة العامة للرقابة المالية التي تشرف على الشركات المدرجة في البورصة المصرية، وباستخدام منهج تجريبي، تحلل الدراسة البيانات التي تم جمعها من شركات المراجعة المسجلة للتحقيق في العلاقة بين مخاطر الأمن السيبراني وأتعاب المراجعة للقوائم المالية.

وتوصلت الدراسة إلى وجود تأثير إيجابي لمخاطر الأمن السيبراني على أتعاب المراجع عن مراجعة القوائم المالية السنوية، مما يشير إلى أن المخاطر الأعلى تؤدي إلى زيادة تكاليف المراجعة. وعلاوة على ذلك، تؤكد الدراسة أن مؤهلات وخبرة المراجعين تعزز هذه العلاقة، حيث يميل المراجعون الأكثر دراية وخبرة إلى تقييم مخاطر الأمن السيبراني بشكل أكثر فعالية، مما يؤثر على قرارات أتعاب المراجعة الخاصة بهم.وتشمل قيود البحث التركيز على شركات المراجعة العاملة ضمن البيئة التنظيمية المصرية، مما قد يحد من إمكانية تعميم النتائج على سياقات أخرى.

الكلمات المفتاحية: مخاطر الأمن السيبراني، أتعاب المراجع، التأهيل العلمي، خبرة المراجع.

[1] تقديم البحث في 17-3-2025 وقبول نشره في 24-3-2025

The Impact of Cybersecurity Risks on Auditor Fees for Financial Statement Audits - *an Experimental Study*

Abstract

The research aimed to examine the impact of cybersecurity risks on auditor fees for auditing financial statements, taking into account the moderating variables of auditors' academic qualifications and professional experience. The study focused on conducting an Experimental Study on a sample of auditors in audit firms registered with the Financial Regulatory Authority (FRA), which supervises companies listed on the Egyptian Stock Exchange. Using an Experimental approach, the study analyzed data collected from registered audit firms to investigate the relationship between cybersecurity risks and financial statement audit fees.

The study found a positive impact of cybersecurity risks on auditor fees for auditing annual financial statements, indicating that higher risks lead to higher audit costs. Furthermore, the study confirms that auditors' qualifications and experience strengthen this relationship, as more knowledgeable and experienced auditors tend to assess cybersecurity risks more effectively, which influences their audit fee decisions. Limitations of the study include its focus on audit firms operating within the Egyptian regulatory environment, which may limit the generalizability of the findings to other contexts.

Keywords: Cybersecurity risks, audit fees, academic qualification, auditor experience.

1- مقدمة

تواجه معظم الشركات حول العالم تحديات متزايدة بسبب مخاطر الأمن السيبراني، والتي قد تؤثر في النهاية على مصداقية ونزاهة التقارير المالية. وقد أصدر مركز جودة المراجعة (CAQ) تحذيرًا بشأن هذه المخاطر، محددًا مسؤوليات المراجعين، حيث يمكن أن تؤثر بشكل مباشر على جودة عملية المراجعة. وأوصى المركز بأن يكون المراجع مسؤولًا عن التحقق من تقييم الشركة للخسائر المرتبطة بمخاطر الأمن السيبراني، وتحديد تأثيرها على التقارير المالية، بالإضافة إلى مراجعة الضوابط الداخلية الخاصة بتسجيل الأحداث في الوقت المناسب والإفصاح عن المعلومات الضرورية في التقارير المالية (CAQ, 2014).

كما أشارت دراسة على (2022) إلى أهمية تقييم قدرة الشركات على الحفاظ على أمن المعلومات وتقليل احتمالية التعرض للاختراقات والتهديدات المستقبلية، بالإضافة إلى دراسة تأثير مستوى خبرة المراجع ومؤهلاته الأكاديمية. وخلصت الدراسة إلى وجود تأثير إيجابي لمستوى خبرة المراجع ومؤهلاته الأكاديمية، مما يعزز الثقة في قدرة الشركات على الحماية من الهجمات السيبرانية.

علاوة على ذلك، أصدرت هيئة الأوراق المالية والبورصات (SEC) خطابات تحذيرية للتعامل مع تزايد المخاطر السيبرانية التي تواجه الشركات، كما شاركت مؤخرًا في عدة تحقيقات تتعلق بهجمات البيانات، والتي أظهرت أن هذه التهديدات تمثل خطرًا كبيرًا على مستوى الشركات والحكومات. وقد أدت هذه الهجمات إلى خسائر تشمل فقدان الملكية الفكرية، وتضرر السمعة، والغرامات الحكومية، وتعطل العمليات التجارية الأساسية، والاستبعاد من الأسواق التنافسية، وتكاليف التقاضي وغيرها. نتيجة لذلك، أصبح أمن المعلومات وإدارة مخاطر الأمن السيبراني من القضايا الجوهرية التي تواجه مجالس إدارة الشركات، مع تزايد اهتمام المستثمرين والعملاء والشركاء التجاريين بهذه المسألة (Rosati, et al., 2022).

وتشير التقارير الحديثة الصادرة عن مجلس الرقابة على محاسبة الشركات العامة (PCAOB) إلى أن فرق التفتيش تقوم بدراسة كيفية تقييم فرق المراجعة لمخاطر التحريف الجوهري، والهجمات السيبرانية، والضوابط ذات الصلة بالأمن السيبراني، مع استمرار مراقبة ممارسات المراجعين في هذا المجال، وكيفية تحديدهم لأتعاب المراجعة نتيجة لذلك (PCAOB, 2016).

2- مشكله البحث

توصلت دراسة Kamiya, et al. (2021) إلى أن تصاعد الاهتمام بمخاطر الأمن السيبراني أدى إلى زيادة تركيز القطاع المالي في بيئة الأعمال، حيث يمكن لأي خرق لأمن المعلومات المالية خلال فترة زمنية قصيرة أن يتسبب في انهيار الشركات الكبرى. وبناءً على ذلك، شهدت السنوات الأخيرة اهتمامًا متزايدًا من قبل المراجعين الخارجيين، مما دفع واضعي المعايير التنظيمية إلى تكثيف جهودهم لمواجهة تهديدات الأمن السيبراني.

وتعتبر مخاطر الأمن السيبراني تهديدات متعددة الأبعاد، إذ قد لا تظهر آثارها الكاملة على الفور. فقد يتمكن المهاجمون من اختراق معلومات حساسة واستغلال الثغرات الأمنية في مواقع الويب للوصول إلى الأرصدة المالية، والبيانات الشخصية، وتواريخ الميلاد، ومعلومات بطاقات الائتمان. وغالبًا ما تكون العواقب جسيمة، حيث قد تؤدي هذه الهجمات إلى انخفاض أسعار أسهم الشركات بمجرد الكشف عنها، مما يؤثر بدوره على عملية التخطيط للمراجعة ومستوى المخاطر المقبولة لدى المراجعين (Bernard, et al., 2017).

وفي هذا السياق، زاد اهتمام المراجعين بالشركات التي تعرضت لهجمات سيبرانية، الأمر الذي انعكس على فرض أتعاب مراجعة أعلى. وتبين وجود علاقة إيجابية بين أتعاب المراجعة ووقوع المخالفات في الشركات بمختلف أحجامها، حيث يبذل المراجعون جهدًا إضافيًا أثناء تخطيط عمليات المراجعة للشركات التي تعرضت لهجمات إلكترونية (Baongo& Tick, 2021).

بناءً على ما سبق، تتمثل مشكلة البحث في الإجابة عن الأسئلة التالية تجريبيا:

ما هو أثر مخاطر الأمن السيبراني على أتعاب المراجع عن مراجعة القوائم المالية السنوية ؟ وهل يختلف هذا التأثير تبعًا لتأهيل المراجعين وخبراتهم المهنية؟

3- هدف البحث

يهدف البحث الى دراسة واختبار أثر مخاطر الأمن السيبراني على أتعاب المراجع عن مراجعة القوائم المالية السنوية، وكذلك أثر كل من؛ تأهيل، وخبرة المراجع كمتغيرات معدلة للعلاقة محل الدراسة، وذلك من خلال دراسة تجريبيه.

4- أهمية ودوافع البحث

يمكن تتبع أهمية هذا البحث الأكاديمية من خلال تناول موضوع مهم وهو تأثير مخاطر الأمن السيبراني على أتعاب المراجع عن مراجعة القوائم المالية السنوية، والذي سيكون له العديد من الآثار، وهو موضوع مثير للجدل من قبل العديد من الدراسات. حيث يربط بشكل مباشر تأثير مخاطر الأمن السيبراني على أتعاب المراجعة، حيث لا تزال الأبحاث محدودة وقد تصل إلى مستوى القلة خاصة في البيئة المصرية، على حد علم الباحثة، مما يعطي هذا البحث أهمية أكاديمية.

كما يستمد هذا البحث أهميته **العملية** من محاولته الوصول إلى دليل عملي لتلك العلاقة من خلال إجراء تجربة على عينة عشوائية من مكاتب المراجعة المسجلة بالهيئة العامة للرقابة المالية، والتي تقوم بمراجعة الشركات المدرجة في البورصة المصرية.

ورغم **الدوافع** العديدة لهذا البحث إلا أن أهمها ميل الدراسات الأكاديمية في مصر إلى استخدام الدراسات الميدانية باستخدام قوائم الاستقصاء والقليل منها تجريبي، وهو ما تغلبت عليه الباحثة من خلال دراسة تجربية على عينة من مكاتب المراجعة في مصر. كما أن هناك قلة في الأبحاث التي تتعلق بتأثير مخاطر الأمن السيبراني على أتعاب المراجعة بشكل عام. وفي البيئة المصرية على وجه الخصوص، في حدود معرفة الباحثة، مما يترتب عليه محاولة تضيق فجوة البحث المحاسبي في مصر.

5- حدود البحث

وفقا لهدف البحث ومشكلته سوف يقتصر هذا البحث على دراسة واختبار مخاطر الأمن السيبراني على أتعاب المراجعة للقوائم المالية، وكذلك اختبار اثر كل من تأهيل وخبرة مراجع الحسابات على العلاقة الرئيسية محل الدراسة، وذلك من خلال دراسة تجربية. ويخرج عن نطاق البحث المتغيرات المعدلة الأخرى مثل (نوع المراجع، وطبيعة الصناعة، وحجم مكتب المراجعة)، وأخيراً، فإن قابلية تعميم نتائج البحث تتوقف على منهجية الدراسة التجربية بمحدداتها، خاصة محددات اختيار عينة البحث.

إنطلاقا من مشكلة البحث ولتحقيق هدفه فى ضوء حدوده،فسوف يستكمل البحث على النحو التالى:

6- خطة البحث

6-1 مخاطر الامن السيبراني من المنظورين المحاسبى والمهني.

6-2 أتعاب المراجعة ،المفهوم والمحددات.

6-3 تحليل العلاقة بين مخاطر الأمن السيبرانى وأتعاب المراجعة،واشتقاق فروض البحث.

6-4 نموذج و منهجية البحث.

6-5 النتائج والتوصيات وفرص البحث المستقبلية.

6-1 مخاطر الأمن السيبرانى من المنظورين المحاسبى والمهني

يشير الأمن السيبراني إلى "مجموعة من الإجراءات والتقنيات المصممة لحماية الأنظمة، والشبكات، والبرمجيات من الهجمات الإلكترونية التي تستهدف الوصول غير المصرح به إلى المعلومات الحساسة، أو تعديلها، أو إتلافها، مما قد يؤدي إلى خسائر مالية أو تعطل الأعمال داخل المؤسسات" (Von Solms & Van Niekerk, 2013).

ويُستخدم مصطلح "السيبراني" للإشارة إلى كل ما يتعلق بالشبكات الحاسوبية والإنترنت، حيث يشمل الفضاء الإلكتروني بيئة رقمية تفاعلية تتكون من مكونات مادية وغير مادية، مثل الأجهزة الرقمية، وأنظمة الشبكات، والبرامج، والمستخدمين سواء كانوا مشغلين أو مستهلكين. ويُنظر إلى الأمن السيبراني باعتباره

"الذراع الرابع للجيوش الحديثة"[1]، نظرًا لدوره الحيوي في حماية البيانات والخدمات الإلكترونية، بما في ذلك تطبيقات التواصل الاجتماعي، والتحويلات المالية عبر الإنترنت، والتجارة الإلكترونية، وغيرها من الأنشطة الرقمية (Lois,et al.,2021)

ويُعرَّف الأمن السيبراني بأنه "أحد فروع أمن المعلومات، حيث يركز على ضمان سرية البيانات الرقمية وسلامتها وتوافرها (CIA) من أي تهديدات قد تنشأ عبر شبكات الاتصال" (Solms & Solms, 2018). كما يمكن وصفه بأنه "منظومة متكاملة من التقنيات، والإجراءات، والسياسات التي تهدف إلى حماية الأنظمة، وشبكات الكمبيوتر، والبرامج، والأجهزة، والبيانات من الهجمات الإلكترونية، ويُعرف أيضًا بأمن تكنولوجيا المعلومات أو أمن المعلومات الإلكترونية" (الخزاعة، 2021).

وبوجه عام، يُعرَّف الأمن السيبراني بأنه "الحماية الشاملة لكل ما يتصل بالإنترنت، بما في ذلك البرامج، والشبكات، والأنظمة، والبيانات، من خلال وضع سياسات وإرشادات أمنية تهدف إلى الحد من التهديدات الإلكترونية وتعزيز الاستقرار الرقمي للمؤسسات"(العقلاء، وعلى، 2022).

ووفقًا لـ Gao, et al., (2020) يُعرَّف الأمن السيبراني بأنه "مجموعة من الأنشطة أو العمليات أو القدرات أو الإجراءات التي تضمن حماية أنظمة المعلومات والاتصالات وما تحتويه من بيانات ضد التلف أو التعديل غير المصرح به أو الاستغلال".

ويرى Cheng, et al., (2022) أن الأمن السيبراني "يُعد جزءًا من أمن تكنولوجيا المعلومات، إذ يشمل التدابير الوقائية لمكافحة الجرائم السيبرانية، ولا سيما محاولات الوصول غير القانوني إلى أنظمة الكمبيوتر والمعلومات المرتبطة بالإنترنت".

ومن هذا المنطلق، يتضمن الأمن السيبراني مجموعة من التقنيات والعمليات والضوابط التي تُستخدم لحماية البنية التحتية الرقمية وضمان سلامة المعلومات المخزنة والمتداولة في الفضاء الإلكتروني. ويشمل الأمن السيبراني مجموعة من التقنيات والإجراءات والضوابط المصممة لحماية الأنظمة والشبكات والبيانات من التهديدات السيبرانية. ويهدف إلى تقليل مخاطر الهجمات الإلكترونية، مما يعزز حماية الأفراد والمنظمات والمجتمعات من الاستغلال غير المصرح به للأنظمة والتقنيات. لذا، يتضمن الأمن السيبراني تأمين المعلومات أثناء معالجتها أو نقلها عبر أنظمة الكمبيوتر (Gordon,et al.,2006).

أما **الهجمات السيبرانية**(Cyber attack) فقد تم تعريفها على أنها "أفعال متعمدة ينفذها مجرمو الإنترنت بهدف سرقة البيانات، أو التلاعب بالمعلومات، أو تعطيل الأنظمة الرقمية الخاصة بالأفراد أو المؤسسات، مما قد يؤدي إلى الإضرار بسمعة المنظمة" (Kamiya, et al.,2021).

[1] مصطلح يشير إلى القوة السيبرانية كأحد الأذرع الرئيسية للجيوش مع تقدم التكنولوجيا والاعتماد المتزايد على الأنظمة الرقمية، أصبحت الحرب السيبرانية عنصرا اساسيا فى الاستراتيجيات العسكرية للدول تستخدم للدفاع والهجوم وجمع المعلومات الاستخباراتية.

كما يمكن تعريفها أيضًا بأنها" استخدام تقنيات الحوسبة والشبكات لإلحاق الضرر أو تعطيل البنية التحتية الحيوية، مثل قطاعات الطاقة والنقل والعمليات الحكومية، أو حتى بهدف ممارسة الضغط على الحكومات أو المدنيين" (لطفي، 2022).

ومن خلال هذه الهجمات، يتمكن مجرمو الإنترنت من الوصول غير القانوني إلى أجهزة الحاسوب واستغلالها وفقًا لأهدافهم الإجرامية. ومع التطور المستمر في المجال، يسعى المهاجمون السيبرانيون إلى ابتكار أساليب جديدة لمواكبة تحديثات الأمن السيبراني.

ومن بين أكثر الهجمات السيبرانية شيوعًا تلك التي أشار إليها (Traina, 2015)، وهى:

- هجمات التصيد الاحتيالي(PHISHING attacks)
- هجمات التصيد الاحتيالي الموجة عبر البريد الألكترونى(SPEAR PHISHING)
- التصيد الاحتيالي المستهدف(WHALE PHISHING)
- التصيد الاحتيالي المرتبط بالبرمجيات الضارة برنامج نصى(DRIVE-BY)
- هجمات برامج الفدية(RANSOMWARE)
- هجمات كلمات المرور (Password attack)
- هجمات التنصت (Eavesdropping)
- هجمات البرامج الضارة(MALWARE attacks)
- حصان طروادة (Trojan Horse)
- هجمات الرجل في المنتصف (MAN-IN-THE-MIDDLE attacks)
- هجمات رفض الخدمة (DoS) ورفض الخدمة الموزعة (DdoS)
- اختطاف الجلسة(Session Hijacking)
- هجمات القوة الغاشمة(BRUTE FORCE)
- هجمات البرمجة النصية عبر المواقع (CROSS-SITE SCRIPTING)
- التهديدات الداخلية (Threats from within)

وبشأن **تأثير الهجمات السيبرانية** تركز بعض الدراسات (Aral, et al., 2013; Hinz, et al., 2015; Ponemon Institute, 2016; Lawrence, et al.,2018) على أن الشركات المخترقة تواجه ردود فعل سلبية في السوق، ويمكن تصنيف تكاليف الاختراق الإلكتروني إلى:

1. **التكاليف قصيرة الأجل:** تشمل الخسائر التجارية، تكاليف جمع الأدلة، انخفاض الإنتاجية، إصلاح الموارد المتضررة، وإبلاغ العملاء وأصحاب المصلحة بالاختراق.
2. **التكاليف طويلة الأجل:** تتضمن خسارة التدفقات النقدية المستقبلية، فقدان العملاء، صعوبة جذب عملاء جدد، تراجع ثقة المستثمرين، ارتفاع تكاليف التأمين، وزيادة تكلفة رأس المال.

هذه الجوانب توضح أهمية تعزيز الأمن السيبراني لتقليل المخاطر المحتملة وحماية البيانات والمؤسسات من التهديدات المستمرة،كما يُسلط هذا المستند الضوء على تأثير مخاطر الأمن السيبراني على ثقة المستثمرين، وتكاليف التأمين، وتكلفة رأس المال للشركات (فرج، 2022).

وفيما يتعلق **بمخاطر الأمن السيبراني**، حددت دراسة أجراها(2018) ,.Lawrence, et al خمسة مخاطر رئيسية يجب أن يكون المحاسبون وأصحاب العمل على دراية بها:

1. الجهل (Ignorance)
2. كلمات المرور (passwords)
3. التصيد الاحتيالي (Phishing)
4. البرامج الضارة (Malware)
5. الثغرات الأمنية (Vulnerabilities Security)

ومن ناحية أخرى، عرّف (2020),.Swift, et al مخاطر الأمن السيبراني بأنها "أي حادث يهدد سرية المعلومات أو سلامتها أو توفرها، أو يؤدي إلى اختراقها من قبل جهة غير مصرح لها".

ونظرًا للخسائر الكبيرة والتأثيرات السلبية المرتبطة بانتهاكات الأمن السيبراني، أصبح الكشف عن هذه المخاطر وطرق إدارتها أمرًا بالغ الأهمية لأصحاب المصلحة. كما تعد مخاطر الأمن السيبراني من بين أكبر التهديدات التي تواجهها البنوك الإلكترونية، كما تؤثر على سمعة الشركات، مما يؤدي إلى ارتفاع التكاليف بسبب تزايد هذه المخاطر وانعكاساتها السلبية على الاستقرار المالي (على، وعلى،2022؛ Tuson, 2021; Kelton,2021)

وتشير الدراسات(Walton, et al.,2021; Nordlund ,2021) إلى أن الإفصاح عن الأمن السيبراني يمكن أن يحمي الشركات من آثار العدوى الناجمة عن الشركات المتصلة بها من خلال سلاسل التوريد أو العلاقات التجارية.

وفي ظل التوترات العالمية الأخيرة والاضطرابات الاقتصادية، شهدت استراتيجيات الدول تحولًا جذريًا فيما يتعلق بالأمن السيبراني، إذ لم يعد مجرد محور مهم في الأجندات الوطنية، بل أصبح عنصرًا حاسمًا في تحديد مستقبل الدول. وقد أدى ذلك إلى تعزيز التدابير الأمنية، والاستفادة من التقنيات المتقدمة، وعلى

رأسها الذكاء الاصطناعي، لمواجهة الهجمات السيبرانية والحد من مخاطرها المحتملة. كما تغيّرت بيئة الأعمال في مختلف القطاعات الاقتصادية، مما أدى إلى زيادة الطلب على تقنيات الحماية الإلكترونية، وارتفاع عدد الشركات المتخصصة في هذا المجال، حيث يُنظر إلى هذه التطورات على أنها فرص يجب استغلالها. وفي عام 2017، وضع المعهد الأمريكي للمحاسبين القانونيين المعتمدين (AICPA) مجموعتين من المعايير ذات الصلة بإدارة مخاطر الأمن السيبراني. تشمل المجموعة الأولى معايير الوصف التي تعتمدها الإدارة عند تنفيذ برامج إدارة المخاطر وإعداد تقاريرها، بينما تتعلق المجموعة الثانية بمعايير الرقابة التي يستخدمها المدققون لتقييم كفاءة تصميم وتشغيل الضوابط الخاصة بإدارة مخاطر الأمن السيبراني (AICPA, 2017).

ويمكن تفسير دوافع الشركات للإفصاح عن مخاطر الأمن السيبراني من خلال عدة نظريات، من بينها:

أولا: نظرية أصحاب المصلحة، تفترض هذه النظرية أن الشركات مطالبة بالتصرف بشكل أخلاقي ومسؤول، وتقديم إفصاحات متوازنة تلبي احتياجات جميع أصحاب المصلحة، وليس فقط تعظيم أرباح المساهمين (Bhat and Abdullah, 2023). وعليه، فإن الشركات تميل إلى توفير كل من المعلومات المالية وغير المالية لتلبية توقعات أصحاب المصلحة (Al-Shaer, et al., 2022).

ثانيا: نظرية الشرعية، تؤكد هذه النظرية أن الشركات بحاجة إلى الإفصاح عن أدائها الاجتماعي والبيئي غير المالي لضمان الحفاظ على شرعيتها أمام المجتمع وأصحاب المصلحة. (Bhat and Abdullah, 2023).

ثالثا: النظرية المؤسسية، تستند هذه النظرية إلى تكامل بين نظريتي أصحاب المصلحة والشرعية، حيث تفترض أن الشركات لا تعمل بمعزل عن غيرها، بل تتفاعل مع مؤسسات تؤثر في سلوكها واستراتيجياتها المستقبلية. لذا، يُتوقع أن تسعى الشركات إلى الإفصاح عن مخاطر الأمن السيبراني للحصول على الموارد الضرورية وتعزيز تفاعلها مع هذه المؤسسات (Campbell, 2007).

رابعًا: نظرية الإشارة، يُتوقع أن تلجأ الشركات إلى الإفصاح عن مخاطر الأمن السيبراني كوسيلة لإيصال رسالة للمجتمع حول مدى التزامها بهذا المجال(Rezaee, et al., 2023).

أخيرًا: استنادًا إلى نظرية الوكالة، يُفترض أن يسهم الإفصاح عن مخاطر الأمن السيبراني في خفض تكاليف الوكالة وتقليل فجوة المعلومات بين مديري الشركة وأصحاب المصلحة (Hassanein and Hussainey, 2015)

ورغم أهمية الإفصاح عن مخاطر الأمن السيبراني، فإن قرار الشركات بشأن إصدار هذه التقارير يختلف تبعًا لعوامل متعددة تؤثر على تبني هذه الممارسة، فضلاً عن كمية ونوعية المعلومات التي يتم الكشف عنها. ويمكن تصنيف هذه العوامل إلى فئتين رئيستين: العوامل الداخلية والعوامل الخارجية. تشمل

العوامل الداخلية حجم الشركة، أداؤها الاقتصادي، التزامها البيئي والاجتماعي، وهيكل الملكية. أما العوامل الخارجية فتشمل طبيعة الصناعة، القوانين والتشريعات، متطلبات الإدراج في البورصة، بلد المنشأ للشركات متعددة الجنسيات، وضغوط أصحاب المصلحة.

وفي مصر، يحظى الأمن السيبراني باهتمام واسع على المستويين العام والخاص، حيث تتبنى الحكومة سياسات صارمة لتعزيز التحول الرقمي في مختلف القطاعات الاقتصادية والحكومية. كما تشهد البلاد توسعًا في تطوير البنية التحتية للاتصالات والإنترنت، إلى جانب إنشاء مراكز بيانات لدعم القطاعات المالية والخدمية، مما يعزز سوق الأمن السيبراني. وتماشياً مع التوجهات الوطنية، تسعى مصر إلى أن تصبح مركزًا إقليميًا لمراكز بيانات التحول الرقمي، وهو ما تدعمه وزارة الاتصالات عبر موقعها الإلكتروني .https://mcit.gov.g

وفيما يتعلق بالجهود الوطنية لحماية الأمن السيبراني، فقد أكد الدستور المصري لعام 2014 (المادة 31) أن الأمن السيبراني جزء أساسي من الأمن الاقتصادي والقومي، مع التزام الدولة باتخاذ التدابير اللازمة لحمايته وفقًا للقانون. وفي هذا السياق، صدر قرار رئيس مجلس الوزراء رقم 2259 لسنة 2014 بإنشاء المجلس الأعلى للأمن السيبراني، بهدف وضع استراتيجية وطنية لمواجهة التهديدات السيبرانية والإشراف على تنفيذها وتحديثها. تبعه قرار رئيس مجلس الوزراء رقم 1631 لسنة 2016 الذي حدد مهام المجلس الأعلى للأمن السيبراني وهيكله التنظيمي، ثم قرار رقم 994 لسنة 2017 الذي ألزم جميع الجهات الحكومية بتنفيذ قرارات المجلس بشأن تأمين البنية التحتية للاتصالات وتقنية المعلومات، وذلك عبر ثلاثة محاور رئيسية، من بينها الاستراتيجية الوطنية للأمن السيبراني، التي تم إطلاقها عام 2018.

المحور الأول: الاستراتيجية الوطنية للأمن السيبراني

المحور الثاني: المركز الوطني للاستعداد للطوارئ الحاسوبية والشبكات

المحور الثالث :المجلس الأعلى للامن السيبرانى.

2-6 أتعاب المراجعة – المفهوم والمحددات

يمكن تعريف أتعاب المراجع الخارجي على أنها "المبالغ المالية التي يتقاضاها نظير تنفيذ عملية مراجعة وفحص البيانات المالية للعميل، وتقديم رأيه الفني بشكل مستقل وموضوعي". (إبراهيم،2018).

وتُعرَّف أتعاب المراجعة على أنها" المبالغ المستحقة للمراجع الخارجي نظير قيامه بعملية المراجعة، حيث يتم تحديدها وفقًا للاتفاق بين المراجع والعميل، مع الأخذ في الاعتبار نوع الخدمة المقدمة والوقت اللازم لأدائها. كما تعكس هذه الأتعاب التكلفة التي يتحملها المراجع أثناء تنفيذ عملية المراجعة وإبداء رأيه في التقارير المالية "(المطارنة، 2006).

كما عرّفت الدراسات (Belina, 2022; Baongo& Tick, 2021; Sun, et al., 2020) أتعاب المراجعة على أنها "التعويض المالي الذي يحصل عليه المراجع مقابل تنفيذ خدمة المراجعة". وتشمل هذه الأتعاب إجمالي تكلفة عملية المراجعة، إلى جانب تعويض مخاطر المراجعة وهامش الربح. وتتكون أتعاب المراجعة من عنصرين رئيسيين: عامل التكلفة وعامل الخسارة المتوقعة. حيث يمثل عامل التكلفة المقياس الكمي للجهود التي يبذلها المراجع أثناء تنفيذ المراجعة، بينما يشمل عامل الخسارة المتوقعة المبالغ الإضافية التي يحصل عليها المراجع نظير مواجهة مخاطر المراجعة ومخاطر التقاضي. ويقوم المراجع ببذل جهود إضافية للحد من التكاليف المحتملة الناجمة عن أي إخفاق في عملية المراجعة.

وفيما يخص **العوامل المؤثرة على أتعاب المراجعة**، أشار Smith, et al., (2019) إلى مجموعة من العوامل التي تؤثر في تسعير خدمات المراجعة، والتي حددها كمحددات رئيسية لأتعاب المراجعة. تشمل هذه العوامل حجم شركة المراجعة، وما إذا كانت لديها شراكة مع إحدى شركات المراجعة الكبرى Big 4، بالإضافة إلى حجم الشركة الخاضعة للمراجعة ، ومدى تعقيد عملياتها، وحجم ديونها، وقوة هيكل الرقابة الداخلية لديها. كما تلعب مخاطر أعمال العميل، والميزة التنافسية للمنشأة، وعدد أنشطتها أو فروعها، وشكل ملكيتها، ونوع الصناعة، والأداء المالي، وتقرير الرقابة الداخلية، والتزامها بالحوكمة، وحجم عملية المراجعة، وتأخير إصدار التقرير.

كما تناولت العديد من الدراسات الأخرى (Alali, 2011; Rosati, et al., 2022) عوامل إضافية تؤثر على أتعاب المراجعة، مثل مخاطر المراجعة، وقطاع الشركة الخاضعة للمراجعة، ومعدل دوران المراجعين، ورأي المراجعين، واستمرارية النشاط، وخبرة المراجعين ، وسمعة شركة المراجعة، وتعقيد عملية المراجعة. كما تمت الإشارة إلى مدى تقديم الشركة لخدمات أخرى غير المراجعة، والتخصص الصناعي للمنشأة الخاضعة للمراجعة، كعوامل ذات تأثير على تحديد الأتعاب.

ومن ناحية أخرى، يوضح عبده (2018) أن أتعاب المراجعة تُعد تكلفة اقتصادية يتحملها المراجع، وتتأثر بعدة متغيرات، مثل؛ حجم العميل، ودرجة تعقيده، ومستوى المخاطرة المرتبطة به، بالإضافة إلى نظام الحكومة المطبق عليه. وفي السياق ذاته، يرى Alan, et al., (2001) أن هذه الأتعاب تشكل المصدر الأساسي لإيرادات مكاتب المراجعة، إلا أنها في الوقت نفسه تعد عبئًا ماليًا على الشركات الخاضعة للمراجعة، والتي تحصل بالمقابل على فوائد تبرر هذه الأعباء.

أما دراسة Amba, and Al-Hajeri (2013) فتؤكد أن أتعاب المراجعة تتحدد وفقًا لتفاعل قوى العرض والطلب على المراجعة. ووفقًا للدراسات (Abbott ,2017; Leidner & Lenz ,2017)، فإن أتعاب المراجعة تُعَد التعويض المالي الذي يُدفع للمراجع الخارجي لقاء تنفيذ عملية المراجعة، حيث تشمل التكلفة الفعلية للمراجعة بالإضافة إلى هامش ربح معقول لمكتب المراجعة.

وتجدر الإشارة إلى أن قانون الأخلاقيات والسلوك المهني العام في مصر لا يحدد آلية واضحة لحساب أتعاب المراجع الخارجي (جمعية المحاسبين والمراجعين المصرية، 2015).

ونظرًا لأهمية أتعاب المراجعة، يمكن تصنيفها إلى مجموعتين رئيسيتين: العوامل المتعلقة بمكتب المراجعة، والعوامل المرتبطة بالعميل محل المراجعة. **تشمل العوامل المرتبطة بمكتب المراجعة عدة جوانب، مثل:** حجم المكتب ، وسمعة المكتب ، ومخاطر الحكم المهني، وفترة المراجعة، واستقلالية المراجع، ودرجة المنافسة في السوق(ElGammal & Gharzeddine, 2020).

وتوضح هذه العوامل مدى تعقيد عملية تحديد أتعاب المراجعة، حيث تؤثر عدة متغيرات في عملية التسعير، مما يبرز أهمية الشفافية والاستقلالية في تحديد هذه الأتعاب لضمان جودة خدمات المراجعة واستدامة ثقة المستخدمين في التقارير المالية.

أما العوامل المرتبطة بالعميل الذي يتم مراجعته، فتشمل: حجم شركة العميل،وتعقيد أعمال العميل،ومخاطر بيئة العميل،وجودة المراجعة الداخلية، ونوع الصناعة، والموقف التفاوضي لعميل المراجعة، وهيكل الملكية، وخصائص مجلس الإدارة، وإدارة الأرباح عند العميل، وفعالية هيكل الرقابة الداخلية، ومدى حوكمة الشركات (Axén, 2020).

وتجدر الإشارة إلى أن هناك العديد من العوامل التي ساهمت في تسليط الضوء على قضية تحديد أتعاب المراجعة، من أبرزها غياب معايير واضحة تحقق العدالة بين المراجع والشركة عند تحديد الأتعاب، إضافة إلى المنافسة الشديدة بين مكاتب المراجعة، مما يؤدي إلى خفض الأتعاب بهدف جذب العملاء الجدد. وهذا بدوره قد يثير تساؤلات حول استقلالية المراجع وموضوعيته وكفاءته (حلس، 2003).

6-3 تحليل العلاقه بين مخاطر الأمن السيبراني وأتعاب المراجعة وأشتاق فروض البحث

استعرضت العديد من الدراسات (Masoud and Alutaibi,2022;; Smith,et al., 2019 Rosati,et al.,2022) العلاقة بين مخاطرالأمن السيبراني و أتعاب المراجعة. وتوصلت إلى وجود ارتباط مباشر بين الإفصاح عن هذه المخاطر وارتفاع أتعاب المراجعة، حيث أشارت النتائج إلى أن الشركات التي تعرضت لحوادث أمن سيبراني كانت أتعاب المراجعة الخاصة بها أعلى. ويعود ذلك إلى أن وقوع هذه الحوادث يُعد مؤشرًا على وجود ضعف أساسي في هيكل الرقابة الداخلية، وهو أحد العناصر الرئيسية التي يتم تقييمها خلال عمليات المراجعة. كما يؤدي الضعف في أنظمة التحكم إلى انخفاض جودة التقارير المالية، وزيادة احتمال حدوث الأخطاء الجوهرية في البيانات المالية، مما يتطلب جهدًا إضافيًا من المراجعين. وبالتالي، تزداد أتعاب المراجعة نتيجة الحاجة إلى إجراءات تحقيق إضافية وتوسيع نطاق الفحص.

كما أظهرت دراسة De Arroyabe,et al.,(2024) أنه رغم عدم تحميل المراجع الخارجي مسؤولية وقوع حوادث الأمن السيبراني، فإن تكرار هذه الحوادث يرفع مستوى المخاطر المحتملة، مما يستدعي إجراءات مراجعة أعمق لكشف أي تهديدات أمنية قد تؤثر على البيانات المالية. ومن ثم، تزداد أتعاب المراجعة نظرًا لازدياد الجهود المطلوبة لضمان دقة وسلامة المعلومات المالية.

من جهة أخرى، أكدت الدراسات (Rosati,et al.,2022; Galderon and Gao,2021) أن وقوع حوادث الأمن السيبراني يؤدي إلى ارتفاع مستوى مخاطر المراجعة، والذي يتم تحديده من خلال عاملين رئيسيين: مستوى المخاطر الجوهرية في البيانات المالية، ومستوى مخاطر الاكتشاف، الذي يرتبط بقدرة المراجع على اكتشاف الأخطاء الجوهرية. ويعد ضعف هيكل الرقابة الداخلية أحد العوامل التي تؤدي إلى زيادة مستوى هذه المخاطر، مما يدفع المراجعين إلى تكثيف إجراءات المراجعة، وبالتالي ارتفاع التكاليف المرتبطة بعملية المراجعة، وتؤدي حوادث الأمن السيبراني إلى ارتفاع أتعاب المراجعة، حيث تسعى الشركات إلى تقليل مستوى مخاطر الكشف وإبقاء مخاطر المراجعة ضمن نطاق مقبول.

كما أشارت دراسة Li, et al., (2020) إلى أن مخاطر الأمن السيبراني تؤثر بشكل إيجابي وكبير على أتعاب المراجعة. ويعود ذلك إلى أن هذه الحوادث تزيد من مخاطر الأعمال، بما في ذلك احتمالية تدهور الوضع المالي للشركة وتراجع ثقة العملاء، سواء على المدى القريب أو البعيد. كما تؤدي إلى زيادة احتمال وجود أخطاء جوهرية في البيانات المالية، مما يزيد من مخاطر العميل باعتبارها أحد العوامل المهمة التي تحدد مدى وجود أخطاء جوهرية في التقارير المالية، نتيجة لذلك، يلجأ المراجعون إلى تنفيذ إجراءات واختبارات مراجعة إضافية لتقليل مخاطر المراجعة، وهو ما يؤدي بدوره إلى زيادةاتعاب المراجعة في حال وقوع حوادث أمن سيبراني، يحتاج المراجع إلى بذل جهود أكبر لتحليل المخاطر المرتبطة بها وفحص أنظمة الرقابة الداخلية ومدى تأثيرها على جودة البيانات المالية، مما يؤدي إلى زيادة تكاليف عملية المراجعة.

إضافة إلى ذلك، أوضحت دراسة Baongo& Tick, (2021) أن وقوع حوادث الأمن السيبراني يثير قلق المستثمرين والممولين الخارجيين، مما يزيد من اهتمام الجهات الرقابية بهذه المخاطر. وبناءً على ذلك، يتعين على الشركات المتضررة الإفصاح بشفافية عن حجم الخسائر والالتزامات المالية الناجمة عن هذه الحوادث، مما يزيد من عبء المراجعة ويعزز الحاجة إلى التحقق الدقيق من السجلات المحاسبية لضمان المصداقية والثقة في التقارير المالية.

يتضح للباحثة توافق الدراسات السابقه بشان الافصاح عن مخاطر الأمن السيبرانى وإنعكساته الإيجابية على أتعاب المراجعة .وعلى الرغم من اختلاف البيئات التى تناولت هذه العلاقة ،إلا أن جميعها أشارت الى أن الأفصاح عن هذه الحوادث يرتبط بتحسين مستوى الأمن السيبرانى ،مما يقلل من المخاطر الناتجة

عن نقاط الضعف فى هيكل الرقابة الداخلية .ويؤدى ذلك الى تراجع جودة التقارير المالية وارتفاع احتمالية وجود تلاعبات جوهرية فى القوائم المالية، مما يزيد من مستوى مخاطر المراجعة ، وفي هذه الحالة، يضطر المراجع إلى زيادة ساعات المراجعة وبذل المزيد من الجهد، مما ينعكس على ارتفاع جودة عملية المراجعة.

ومن ناحية أخرى، قد يؤدي ذلك إلى زيادة التلاعب في القوائم المالية، ونظرًا للجدل القائم حول التأثير الإيجابي للإفصاح عن حوادث الأمن السيبراني على ممارسات المراجعة، تسعى هذه الدراسة إلى تحليل مدى تأثير هذا الإفصاح على أتعاب المراجعة.

لذلك، تقترح الباحثة أن مخاطر الأمن السيبراني يمكن أن يكون له تأثير مباشر على مستوى الأتعاب المدفوعة للمراجعين وكذلك على القوائم المالية للشركات. وهذا ما يقودنا إلى الفرضية الأولى للدراسة، والتي تنص على ما يلي:

H_1: تؤثر مخاطر الأمن السيبراني معنويا على أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية.

ويعد **التأهيل العلمي للمراجع** عاملاً رئيسيًا في تكوينه المعرفي، مما يسهم في تحسين جودة تخطيطه للمراجعة وتعزيز إدراكه للعلاقة بين مخاطر الأمن السيبراني وأتعاب المراجعة . فقد أظهرت دراسة Wang et al., (2013) أن استجابة المراجع لهجمات الأمن الإلكتروني تختلف باختلاف القطاع الصناعي، والإجراءات التنظيمية للشركة، ومستوى تأهيله وخبرته. كما توصلت دراسة Navarro & Sutton (2021) إلى أن المعرفة والتأهيل العلمي للمراجع يعززان الطلب على خدماته في إدارة مخاطر الأمن السيبراني، مما يمكنه من اتخاذ قرارات مراجعة أكثر رشادة.

وفي هذا السياق، ينص معيار المراجعة (PCAOB, No. 8) على أن المراجع، لضمان التعبير عن رأي مهني موثوق بشأن القوائم المالية، يجب أن يخطط وينفذ عملية المراجعة بحيث يحصل على تأكيد معقول بأن القوائم المالية خالية من التحريفات الجوهرية، سواء كانت نتيجة خطأ أو احتيال. يتحقق هذا التأكيد عبر تقليل مخاطر المراجعة إلى مستوى مقبول، من خلال الاستفادة من تأهيل المراجع، وخبرته، وممارسته للعناية المهنية، إضافة إلى جمع أدلة مراجعة كافية وملائمة.

وفي ظل التطورات المتسارعة في بيئة الأعمال، أصبحت حوادث اختراق البيانات أكثر تعقيدًا، مما أثار مخاوف عالمية حول كيفية حماية المؤسسات لبياناتها وضمان سلامة قواعدها المعلوماتية. فقد أشار Hsieh, et al., (2020) إلى أن هذه التحديات تستلزم تعزيز الشك المهني لدى المراجعين، خاصة في ظل احتمالية وجود ارتباط اقتصادي بين الشركات والمراجعين فيما يخص الحوادث السيبرانية. ورغم أن

الشركات قد لا تعتبر هذه الحوادث ذات تأثير مباشر على بياناتها المالية من الناحية الكمية، فإن وقوع حادث سيبرانى كبير قد يدفع المراجعين إلى بذل جهود إضافية، بالتعاون مع متخصصين، للتحقيق في الأمر، مما يوسع نطاق مسؤولياتهم خارج حدود مهام المراجعة التقليدية، معتمدين بشكل أساسي على مستوى تأهيلهم.

ومع ازدياد الاعتماد على الأنظمة الرقمية، أصبح الأمن السيبراني يمثل أولوية قصوى للمؤسسات، مما يستلزم وجود مراجعين مؤهلين علميًا ومدربين على أحدث التقنيات لضمان كفاءة عمليات المراجعة والحد من المخاطر السيبرانية. أن هناك علاقة واضحة بين تأهيل المراجعين وقدرتهم على تخطيط وتنفيذ مراجعات فعالة في هذا المجال. على سبيل المثال، تناولت دراسة محمد وآخرون (2023) أثر دور المراجع الداخلى في تعزيز أنظمة الأمن السيبراني لدى الشركات المدرجة في السوق المصري، حيث أكدت نتائج التحليل الإحصائي وجود علاقة إيجابية ذات دلالة إحصائية بين دعم دور المراجع الداخلى وتعزيز أنظمة الأمن السيبراني، وهذا يبرز أهمية تطوير قدرات المراجعين وتزويدهم بالموارد اللازمة لدعم الأمن السيبراني في المؤسسات.

كما هدفت دراسة محروس و صالح(2022) إلى تحليل تأثير تطوير أداء المراجع في الشركات المصرية لمواجهة التحديات المتزايدة في مجال الأمن السيبراني، وخلصت إلى وجود إجماع عام على ضرورة تطوير أداء وتأهيل المراجعين، إذ لم يعد النهج التقليدي في المراجعة كافيًا للتعامل مع هذه التهديدات المستمرة.

أما دراسة شحاته (2022) فقد ركزت على أهمية دور وتأهيل المراجع في تقييم المخاطر السيبرانية لدى الشركات المدرجة في البورصة المصرية، وطرق التعامل معها. وأكدت الدراسة أن تأهيل المراجع يسهم في تعزيز دوره في الكشف المبكر عن المخاطر السيبرانية، واقتراح الحلول المناسبة، مما يعزز حماية الأصول الرقمية للشركات وتحسين جودة المعلومات المالية المقدمة للمستثمرين.

وأشارت بعض الدراسات (Miazee, et al., 2014; Samad, 2017; Gupta, et al., 2018) إلى أن التأهيل العلمي للمراجع، خاصة في المجالات المالية والمحاسبة، يُعد عاملاً أساسيًا يؤثر في عملية اتخاذه للقرارات، كما يساعده في فهم مخاطر الأمن السيبراني.

بناءً على ذلك، تخلص الباحثة إلى أن تأهيل المراجع له تأثير إيجابي جوهري على تحديد اتعاب مراجعة القوائم المالية السنوية التاريخية الكاملة. ومن المتوقع أن يختلف هذا التأثير وفقًا لمستوى مخاطر الأمن السيبراني، ومدى انعكاس ذلك على مراجعة القوائم المالية للشركات المدرجة في البورصة المصرية.

بناءً على ما سبق، يمكن اشتقاق الفرض الثانى للبحث على النحو التالي:

H_2: يختلف تأثير مخاطر الأمن السيبراني معنويا على أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية بإختلاف تأهيل المراجع.

وبشأن أثر **خبرة المراجع** على العلاقه محل الدراسة ، تشير دراسة Price Water House Coopers (2022) إلى أن إدراك مخاطر الأمن السيبرانى يعتمد بشكل أساسي على مستوى معرفة المراجع وفهمه لصناعة العميل، حيث يكتسب المراجع هذه المعرفة من خلال الاطلاع المستمر بالممارسات المحاسبية في القطاع الذي يعمل فيه، إلى جانب إدراكه للمخاطر المحتملة التي قد تؤثر على العميل.

وأشار Krishnan (2003) إلى أن المراجع الذي يتمتع بخبرة واسعة في مجال المراجعة يكون أكثر تخصصًا في فهم الصناعات التي يعمل فيها عملاؤه، مما يمكنه من تقديم خدمات مراجعة ذات جودة أعلى.

وتشير بعض الدراسات إلى أن خبرة المراجع ترتبط ارتباطًا وثيقًا بجودة عمليات التقييم التي يجريها، لا سيما عند إعداد التقارير المالية. فقد توصلت دراسة Dunn and Mayhew (2004) إلى أن خبرة المراجع تؤثر بشكل مباشر على تقييمه للأداء المالي للشركات، كما أظهرت دراسة Carcello & Nagy (2004) أن المراجعين الأكثر خبرة يميلون إلى اكتشاف المخالفات المحاسبية بصورة أسرع مقارنة بالمراجعين الأقل خبرة مما يعزز من جودة التقارير المالية (Balsam, et al., 2003)

وفي سياق الأمن السيبراني، أوضحت دراسة Stanley & DeZoort (2007) أن المراجع الذي يمتلك خبرة متخصصة في تقييم المخاطر السيبرانية يكون أكثر قدرة على تحليل مدى تأثير هذه المخاطر على العمليات المالية للشركة، مما يسهم في تحسين إجراءات وجوده لمراجعة وتقليل المخاطر المحتملة.

كما أكد(2014) Soekrisno أن قدرة المراجع على التقييم لا تقتصر على الجوانب المحاسبية فقط، بل تمتد أيضًا إلى مجالات أخرى، بما في ذلك إدارة المخاطر التجارية، إذ لا يمكنه تطبيق المعايير المهنية بصورة فعالة ما لم يكن لديه معرفة متعمقة وخبرة كافية بأعمال التخطيط للمراجعة، الأمر الذي قد يؤثر على كفاءة خطة المراجعة.

وفي هذا الإطار، توصلت دراسة Kuntari, et al.,(2017) إلى أن خبرة المراجع تلعب دورًا حيويًا في تحديد مدى الإفصاح عن المخاطر السيبرانية، مما يجعل عملية المراجعة أكثر شمولية ودقة.

أما دراسة Wang, et al., (2013) فقد تناولت العلاقة بين خبرة المراجعين وحوادث الأمن السيبراني، وأظهرت النتائج أن المراجعين ذوي الخبرة الواسعة يكونون أكثر قدرة على فهم هذه الحوادث وتحليلها، مما

يسهم في الحد من مخاطر الأمن السيبراني من خلال تعزيز دورهم في عملية المراجعة وتقديم رؤى واضحة حول نقاط الضعف المحتملة في نظم المعلومات.

ومن ناحية أخرى، أكدت دراسة Axén (2020) وجود ارتباط وثيق بين خبرة مكاتب المراجعة ومدى إدراكها لمخاطر الأمن السيبراني. وقد توصلت الدراسة إلى أن المكاتب التي لديها خبرة أكبر تكون أكثر استعدادًا لمواجهة التحديات السيبرانية، حيث يمكنها تطوير استراتيجيات فعالة للتعامل مع المخاطر الإلكترونية، مستفيدةً من مهارات وخبرات مراجعها، مما يسهم في تعزيز جودة التقارير المالية وتقليل احتمالية حدوث اختراقات سيبرانية تؤثر على الشركات التي يتم مراجعتها.

وفي السياق ذاته، هدفت دراسة حماد (2022) إلى تحليل تأثير خبرة مكاتب المراجعة على كفاءة عمليات التخطيط والتنفيذ للمراجعة في ظل التهديدات السيبرانية المتزايدة. وقد أظهرت الدراسة أن المكاتب التي تمتلك خبرة واسعة تكون أكثر قدرة على تطوير إجراءات مراجعة تتماشى مع التطورات التكنولوجية، مما يساعد في تحديد المخاطر السيبرانية المحتملة والتعامل معها بشكل أكثر احترافية.

وفي دراسة حديثة، سعى Vuko, et al.,(2024) إلى تحديد العوامل المؤثرة في كفاءة المراجعة عند تقييم وإدارة مخاطر الأمن السيبراني، وأظهرت النتائج أن المراجعين الذين يمتلكون خبرة متخصصة في الأمن السيبراني يكونون أكثر قدرة على تقييم المخاطر وتطوير استراتيجيات فعالة لإدارتها. كما أشارت الدراسة إلى أهمية تضمين مراجعي الحسابات في عمليات التخطيط الأمني للمؤسسات، من خلال استخدام التقنيات الحديثة مثل الذكاء الاصطناعي وتحليل البيانات الضخمة، لتعزيز دورهم في حماية الأنظمة المالية وسلوكيات الشركات تجاه هذه المخاطر.

بناءً على ذلك، تخلص الباحثة إلى أن خبرة المراجع لها تأثير إيجابي جوهري على تحديد اتعاب مراجعة القوائم المالية السنوية التاريخية الكاملة. ومن المتوقع أن يختلف هذا التأثير وفقًا لمستوى مخاطر الأمن السيبراني، ومدى انعكاس ذلك على مراجعة القوائم المالية للشركات المدرجة في البورصة المصرية.

بناءً على ما سبق، يمكن اشتقاق الفرض الثالث للبحث على النحو التالي:

H_3: يختلف تأثير مخاطر الأمن السيبراني معنويا على أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية بإ ختلاف خبرة مراجع الحسابات.

6-4 نموذج ومنهجية البحث

تعرض الباحثة فى هذه الجزئية أهداف الدراسة التجريبية، ومجتمع وعينة الدراسة، وأدوات وإجراءات الدراسة، وتوصيف وقياس متغيرات الدراسة، ونموذج الدراسة ،والتصميم التجريبى للدراسة، وأخيرا نتائج اختبار الفروض إحصائيا .وذلك على النحو التالى:

6-4-1 أهداف الدراسة التجريبية

تناولت هذه الدراسة بالدرجة الأولى أختبار إمكانية وجود علاقة تأثيرية بين مخاطر الأمن السيبراني وعلى أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية ، وأيضاً تحليل تأثير المتغيرات المعدلة على هذه العلاقة والتي تعكس بوضوح التأهيل العلمي والخبرة لدى مراجعى الحسابات قياساً على (Widodo& Chariri,2021)

6-4-2 مجتمع وعينة الدراسة

يشتمل مجتمع الدراسة على مراجعي الحسابات بمكاتب المراجعة الخاصة المقيدة بسجل الهيئة العامة للرقابة المالية والتي تراجع الشركات المساهمة المقيدة بالبورصة المصرية قياساً على (Navarro & Sutton, 2021). ويبين الجدول التالى الحالات التجريبية التي تم توزيعها على عينة الدراسة.

جدول 1: بيان بالحالات التجريبية الموزعة على عينه الدراسة

التفاصيل	عدد الحالات التجريبية الموزعة	عــدد الحالات التجريبية المستلمة	نسبة الردود الى اجمالي الحالات الموزعة	عدد الحالات التجريبية السليمة	نسبة الردود السليمة الى الحالات المستلمة
عينة تحكمية من مراجعي الحسابات بمكاتب المراجعة الخاصة	110	100	%91	100	%100

6-4-3 أدوات وإجراءات الدراسة

تم استخدام الأساليب الإحصائية الوصفية لدراسة المتغيرات. وإجراء اختبار كرونباخ ألفا Cronbach Alpha لقياس الصدق والثبات. هذا بالإضافة إلى إجراء اختبار الاعتدال Test of normality لتحديد نوع التوزيع للمجتمع الذي يتم سحب العينات منه لتحديد ما إذا كان يجب استخدام اختبار المعلمة Parametric test أو الغير معلمي Non- Parametric test. وعند اختبار فرضيات البحث، تم الاعتماد على اختبار ويلكوكسون Wilcoxon signed- Rank test مع عينتين تابعتين (غير مستقلتين)

لفحص تأثير مخاطر الأمن السيبراني على أتعاب مراجعة القوائم المالية السنوية التاريخية الكاملة للشركات المقيدة بالبورصة المصرية ، وما إذا كانت هذه العلاقة تختلف باختلاف التاهيل العلمى وخبرة المراجع، في حالة اختيار عينة الدراسة من مجتمع لا يتبع التوزيع الطبيعي لأنه اختبار غير معلمي، وإذا تم أخذ عينة الدراسة من مجتمع ذات توزيع طبيعي، يتم استخدام اختبار T- Test كأحد الاختبارات الإحصائية المعلمية :Wilcoxon signed ranks test وهو يمثل احد الأختبارات الأحصائية المعنوية المستخدمه لمعرفة ما إذاكان هناك فروق معنوية بين مجتمعين أو غير مستقلتين، أو مجموعتين من المجموعات التجريبيه. (Kothari,2004;Hashem & Sujud ,2020)

6-4-4 توصيف وقياس متغيرات الدراسة

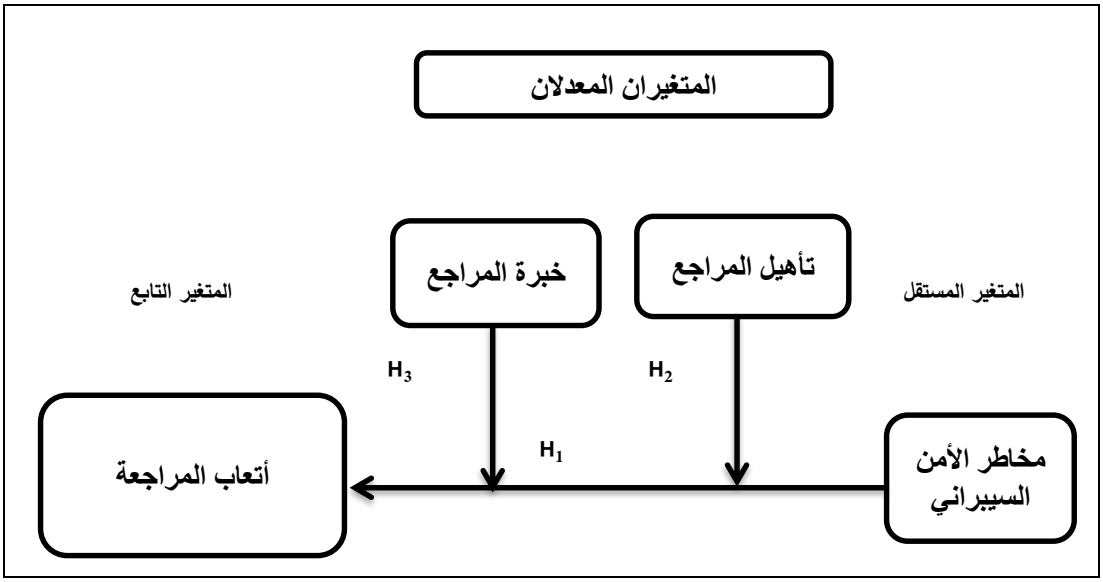
يتضح من خلال فروض البحث، أن متغيرات الدراسة تشكلت من متغير مستقل واحد وهو مخاطر الأمن السيبراني، ومتغير تابع واحد وهو أتعاب مراجعة القوائم المالية، بالأضافة الى متغيرين معدلين وهما التأهيل العلمى، والخبرة لدى مراجعى الحسابات، حيث تم توصيف وقياس المتغيرات بالجدول التالى:

جدول 2: توصيف وقياس متغيرات الدراسة

نوع المتغير	المتغير والرمز	التعريف وطريقه القياس
متغير مستقل	مخاطر الأمن السيبرانى	يشير مفهوم مخاطر الأمن السيبرانى الى التهديدات والضعف فى أنظمه المعلومات والشبكات التى قد تؤدى الى خسائر ماليه وأنتهاكات للخصوصية او تعطيل العمليات التنظيميه، ويتم قياسه باستخدام مقياس ليكارت الخماسى لقياس تصورات المراجعين حول مستوى المخاطر السيبرانية. (NIST,2023)
متغير تابع	أتعاب المراجعة	التكلفه التى تتقضاها شركات المراجعه مقابل خدمات المراجعه المالية ويتم قياسها من خلال الاتعاب المدفوعه للمراجعين خلال السنه المالية مقارنه بين الشركات ذات المخاطر العاليه او هى التى يتحملها عميل المراجعه مقابل قيام منشاه المراجعه بمراجعه القوائم المالية السنويه الكامله، وقد تم قياس هذا المتغير بتقدير الأفراد لأتعاب المراجعة. (Jl,et al.,2018; Sun,et al.,2020)
متغير معدل	التأهيل العلمي لمراجعى الحسابات	يشير الى المستوى التعليمى والمهنى الذى يجب أن يمتلكة المراجع لأداء عملة بكفاءة وفقا للمعايير المهنيه والأخلاقية .ويقاس من خلال مقياس من (1)إلى (5) اذا كان حاصل على دراسات عليا أو شهادات مهنية = 5، أو حاصل على مؤهل محاسبى عادى =1 قياسا على (Pierangelo, et al.,2020)
متغير معدل	مستوى خبرة مراجعى الحسابات	تشير الى مخزون خبرته وفقا لمعايير التقرير المالى الدولية فى مجال مراجعه القوائم الماليه . وسيتم قياسه بعدد سنوات الخبرة فاذا كانت خمس سنوات واكثر يأخذ القيمة (1) وإذا كانت أقل من خمس سنوات يأخذ القيمة (0) قياسا على (Verwey&Asar,2021)

6-4-5 نموذج البحث

بناءٍ على المتغيرات والفروض المحددة فى البحث تم تطوير نموذج البحث فى إطار التحليل الأساسى، مع إضافه العناصر الجديده التى تساهم فى توسيع نطاق الدراسة كما موضح في الشكل رقم (1)



شكل 1: نموذج البحث

المصدر: من اعداد الباحثة

6-4-6 التصميم التجريبي للدراسة

والجدول التالى يوضح التصميم التجريبي للدراسة.

جدول 3: التصميم التجريبي للدراسة

بدائل مخاطر الامن السيبرانى	مستوى تأهيل المراجع		مستوى خبرة المراجع	
	مرتفع	منخفض	مرتفعة	منخفضه
لاتوجد مخاطر أمن سيبرانى	مدى وطبيعة وتوقيت جمع أدلة المراجعة معالجه (1)	مدى وطبيعة وتوقيت جمع أدلة المراجعة معالجه (2)	مدى وطبيعة وتوقيت جمع أدلة المراجعة معالجه (3)	مدى وطبيعة وتوقيت جمع أدلة المراجعة معالجه (4)
توجد مخاطر أمن سيبرانى	مدى وطبيعة وتوقيت جمع أدلة المراجعة معالجه (5)	مدى وطبيعة وتوقيت جمع أدلة المراجعة معالجه (6)	مدى وطبيعة وتوقيت جمع أدلة المراجعة معالجه (7)	مدى وطبيعة وتوقيت جمع أدلة المراجعة معالجه (8)

وبناءاً على هذا التصميم ستكون هناك (8) معالجات تجريبية على النحو الأتى:

- **المعالجة رقم (1):** لا توجد مخاطر أمن سيبراني/ تأهيل المراجع مرتفع/ ويطلب من مراجع الحسابات تحديد **مدى وطبيعة وتوقيت أدلة المراجعة.**
- **المعالجة رقم(2):** لا توجد مخاطر أمن سيبراني/ تأهيل المراجع منخفض/ ويطلب من مراجع الحسابات تحديد **مدى وطبيعة وتوقيت أدلة المراجعة.**
- **المعالجة رقم(3):** لا توجد مخاطر أمن سيبراني/ المراجع ذو خبرة عالية / ويطلب من مراجع الحسابات تحديد **مدى وطبيعة وتوقيت أدلة المراجعة.**
- **المعالجة رقم (4):** لا توجد مخاطر أمن السيبراني/ المراجع ذو خبرة منخفضة/ ويطلب من مراجع الحسابات تحديد **مدى وطبيعة وتوقيت أدلة المراجعة.**
- **المعالجة رقم (5):** يوجد مخاطر أمن سيبراني/ تأهيل المراجع مرتفع/ ويطلب من مراجع الحسابات تحديد **مدى وطبيعة وتوقيت أدلة المراجعة.**
- **المعالجة رقم (6):** يوجد مخاطر أمن سيبراني/ تأهيل المراجع منخفض/ ويطلب من مراجع الحسابات تحديد **مدى وطبيعة وتوقيت أدلة المراجعة.**
- **المعالجة رقم (7):** يوجد مخاطر أمن سيبراني/ المراجع ذو خبرة عالية/ ويطلب من مراجع الحسابات تحديد **مدى وطبيعة وتوقيت أدلة المراجعة.**
- **المعالجة رقم (8):** يوجد مخاطر أمن السيبراني/ المراجع ذو خبرة منخفضة/ ويطلب من مراجع الحسابات تحديد **مدى وطبيعة وتوقيت أدلة المراجعة.**

ولاختبار فروض الدراسة سيتم إجراء المقارنات التالية:

يتم اختبارالفرض الأول (H_1) في التحليل الأساسي من خلال:

- **المقارنة الاولى:** بين المعالجات **{(1+2+3+4)×(5+6+7+8)}**

ثم يتم إجراء تحليل من خلال إدخال متغيرين تأهيل المراجع، وخبرة المراجع كمتغيرات معدلة لاختبار الأثر على العلاقة محل الدراسة من خلال:

- **المقارنة الثانية:** بين المعالجات (1×5) والمعالجات (2×6) وذلك لاختبار الفرض H_2.
- **المقارنة الثالثة :** بين المعالجات (3×7) والمعالجات (4×8) وذلك لاختبار الفرض H_3.

وذلك لاختبار أثر مخاطر الامن السيبراني باختلاف الاثر المجمع لتأهيل المراجع وخبرة المراجع.

6-4-7 نتائج الدراسة التجريبية

6-4-7-1 الاختبارات الاحصائية المستخدمة في تحليل نتائج الدراسة التجريبية

إعتمدت الباحثة على مجموعة من الأساليب الإحصائية في تحليل البيانات، وبإستخدام جداول برنامج Microsoft Excel تم تفريغ ردود المشاركين في هذه الدراسة، حيث تم إجراء هذه الإختبارات من خلال برنامج التحليل الاحصائي، SPSS وقد إستخدمت الباحثة الإختبارات الإحصائية التي تتلاءم مع طبيعة بيانات الدراسة التجريبية وفرضيات الدراسة على النحو التالي:

6-4-7-2 الإحصاء الوصفي

يوضح الجدول التالي البيانات الإحصائية لمتغيرات الدراسة:

جدول 4: الإحصاء الوصفي لمتغيرات الدراسة

السؤال	المجموعة التجريبية	N	Mean	Median	SD	Min	Max
1- تؤثر مخاطر الأمن السيبراني على قرار تحديد أتعاب المراجعة فى هذه الحالة.	التجربة الاولي	100	1.9600	2	.851	1	3
	التجربة الثانية	100	4.11	4	.851	3	5
	الإجمالي	200	4.25	4	.954	3	5
2- تعرض الشركة لمخاطر الأمن السيبراني سيزيد من أتعاب المراجعة.	التجربة الاولي	100	1.89	2	.815	1	3
	التجربة الثانية	100	4.07	4	.879	3	5
	الإجمالي	200	4.23	4	.811	3	5
3- اذا كانت الأتعاب للشركة عام 2023 كانت 50000 جنيه، فمن المتوقع لهذه الشركة العام القادم أن تكون الأتعاب 0000000 فى هذه الحالة.	التجربة الاولي	100	1.98	2	.803	1	3
	التجربة الثانية	100	4.12	4	.819	3	5
	الإجمالي	200	4.01	4	.745	2	5

من الجدول السابق يتضح ان متوسط تأثير المخاطر على أتعاب المراجعة أكبر سواء كان علي مستوي التجربة الاولي أو التجربة الثانية او العينة ككل.

6-4-7-3 الإختبار الإحصائي الخاص بالصدق والثبات (كرونباخ ألفا)

تم استخدام اختبار كرونباخ الفا لقياس مدي الثبات الداخلي وإمكانية الاعتماد علي إجابات المشاركين في العينة. حيث أن إختبار مدى موثوقية إستجابات مفردات العينة على الأسئلة، وذلك لمعرفة صلاحية وجاهزية بيانات الدراسة للقيام بالتحليل الاحصائي ولمعرفة مدى إمكانية تعميم النتائج التي تم جمعها من العينة على مجتمع الدراسة، حيث تتراوح قيمة هذا المعامل بين الصفر والواحد الصحيح (0-100%)، ففي

حالة ثبات البيانات فإن هذا المعامل سيكون مساوياً للواحد الصحيح، أما إذا كانت قيمة هذا المعامل مساوية للصفر فهذا يدل على عدم ثبات البيانات، وتشير الزيادة في قيمة المعامل عن الزيادة في ثبات البيانات، حيث يعبر هذا الثبات إلى استقرار المقياس وعدم تناقضه،أو من وجهة أخرى أن مقياس كرونباخ الفا يعطي نفس النتائج بإحتمال مساوي لقيمة المعامل في حالة إعادة تطبيقه على العينة ذاتها (موسى،2018).

حيث تم تطبيق الاختبار مع تقسيم الأسئلة الي مجموعتين ويتضح من خلال الجدول التالي أن قيمة معامل Cronbachs Alpha تجاوزت نسبة 70% سواء علي مستوي العينة ككل أو علي مستوي كل تجربة على حدى. وهذا يدل على تمتع الحالات التجريبية والاسئلة الملحقة بها بدرجة عالية من الثبات، ومن ثم يمكن الإعتماد على إجابات المشاركين في التجربة.

جدول 5: معامل كرونباغ الفا

Relitability Statistics

Sample		Cronbachs Alpha	Standard deviation
الحالة الاولي	Q1	0.724	0.008
	Q2	0.845	0.0054
	Q3	0.775	0.041
الحالة الثانية	Q1	0.714	0.002
	Q2	0.859	0.005
	Q3	0.877	0.04
Cronbachs Alpha	0.8954		
STD. Cronbachs Alpha	0.047		

6-4-7-4 إختبار كاي تربيع- Chi- Square (X^2)

هو إختبار إحصائي يستخدم لدراسة العلاقة بين متغيرين في الدراسة لمعرفة ما إذا كانت هناك علاقة بين هذين المتغيرين ام لا. ولتحديد مدى المعنوية في الاسئلة، والغرض من هذا الاختبار إجراء مقارنات بين اجابات العينتين ويمكن صياغة الفرض الإحصائي على النحو الاتي:

فرض العدم: H_0 لاتوجد فروق ذات دلالة احصائية بين إجابات العينة

وكلما زادت قيمة Chi-Square عن الصفر فهذا يدل على وجود فروق بين إجابات العينة، وهذا يعني أن هناك علاقة بين العينتين، فإذا كانت القيمة P-Value اقل من 5% فهذا يعني رفض فرض العدم ويتم قبول الفرض البديل.

ومن خلال هذا الإختبار فقد ظهرت النتائج كما مبين في الجدول رقم (5) أن قيمة P-Value هي اقل من (5%) لجميع الأسئلة المرفقة بالحالة التجربية، ويعني هذا رفض فرض العدم الذي اشار بعدم وجود أي إختلافات بين إجابات العينة، وقبول الفرض البديل الذي أشار إلى وجود اختلافات بين إجابات العينة قياساً على (عبد الرحيم،2020).

جدول 6: نتائج اختبار Chi-Square

Sample	Asymp. Sig
لاتوجد مخاطر أمن سيبرانى	0.000
توجد مخاطر أمن سيبرانى	0.000

6-4-7-5 إختبار الاعتدالية Kolmogorov-Smirnov

استخدم اختبار Kolmogorov- Smirnov لتحديد طبيعة توزيع البيانات بهدف تحديد ما اذا كان سيتم الاعتماد علي الاختبارات المعلمية او اللامعلمية لاختبار الفروض.

إذ أن الإختبارات الاحصائية المعلمية تكون مناسبة عندما تكون البيانات لها توزيع طبيعي معتدل، في حين أن الاختبارات اللامعلمية تكون مناسبة للبيانات التي ليس لها توزيع طبيعي معتدل(موسى،2018).
ويمكن التعبير عن فرض العدم والفرض البديل لهذا الاختبار علي النحو التالي:
فرض العدم: العينة المسحوبة من مجتمع يتبع التوزيع الطبيعي.
الفرض البديل: العينة المسحوبة من مجتمع لا يتبع التوزيع الطبيعي.

جدول 7: نتائج اختبارات توزيع البيانات

Kolmogorov- Smirnov

Sample	Kolmogorov- Smirnov	
	P-Value	Statistic
الحالة الاولي	.00	0.174
الحالة الثانية	.00	0.178

وجاءت جميع قيم P-Value اقل من 5% وبالتالي يتم رفض فرض العدم بان البيانات تتبع التوزيع الطبيعي وقبول الفرض البديل بان البيانات لاتتبع التوزيع الطبيعي وبالتالي سيتم استخدام الاختبارات اللامعلمية.

6-4-7-6 نتائج إختبار فروض البحث في ظل التحليل الأساسي:

تقوم الباحثة بعرض نتائج إختبارات الفروض كلاً على حده وذلك على النحو التالي:

- **نتيجة إختبار فرض البحث الأول:**

لاختبار هذا الفرض تم تحويله الي فرض عدم كالتالي:

H_0: لاتؤثر مخاطر الأمن السيبراني معنويا على أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية.

وتم استخدام اختبار Wilcoxon وذلك علي النحو التالي: 1

جدول 8: نتيجة اختبار الحالة الاولي

RANKS				
		N	Mean Rank	Sum of Ranks
	Negative Ranks	0	.00	.00
Q1-Q3	Positive Ranks	100	45	2190
	Ties	0		
	Total	100		

Test Statistics	
Z	3.56
Sig (2- tailed)	.00

تشير النتائج الي أن قيمة P-Value أقل من 5% لذلك تم رفض فرض العدم وقبول الفرض البديل في ظل الحالة الأولي **بوجود تأثير لمخاطر الأمن السيبراني معنويا على أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية.**

جدول 9: نتيجة اختبار الحالة الثانية

RANKS				
		N	Mean Rank	Sum of Ranks
	Negative Ranks	0	.00	.00
Q1-Q3	Positive Ranks	100	32	2145
	Ties	0		
	Total	100		

Test Statistics	
Z	3.74
Sig (2- tailed)	.00

تشير النتائج الي أن قيمة P-Value أقل من 5% لذلك تم رفض فرض العدم وقبول الفرض البديل في ظل الحالة الثانية **بوجود تأثير لمخاطر الأمن السيبراني معنويا على أتعاب مراجع عن مراجعه القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية.**

- **نتيجة إختبار فرض البحث الثانى:**

لإختبار هذا الفرض على النحو الاتي:

H_0: لايختلف تأثير مخاطر الأمن السيبراني معنويا على أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية بإختلاف تأهيل المراجع.

جدول 10: اختبار فرض البحث الثاني – التجربة الأولي

RANKS				
	التأهيل العلمي	N	Mean Rank	Sum of Ranks
Q1	1	70	66	2254
	0	30	32.67	980
	TOTAL	100		
Q2	1	25	30.7	874
	0	75	70	2841
	TOTAL	100		

RANKS				
	التأهيل العلمي	N	Mean Rank	Sum of Ranks
Q3	1	75	70	2841
	0	25	30.7	874
	TOTAL	100		

	Q1	Q2	Q3
Z	4.20	.201	7.61
Sig (2- tailed)	.00	.007	.00

وتشير النتائج بالجدول السابق الي أن قيمة P-Value أقل من 5%، لذلك يتم قبول الفرض البديل فى الحالة الأولى القائل بأنه **يختلف تأثير مخاطر الأمن السيبراني معنويا على أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية بإختلاف تأهيل المراجع.**

جدول 11: اختبار فرض البحث الثاني- التجربة الثانية

RANKS				
	التأهيل العلمي	N	Mean Rank	Sum of Ranks
Q1	**1**	**25**	**30.7**	**874**
	0	**75**	**70**	**2841**
	TOTAL	**100**		
Q2	**1**	**70**	**66**	**2254**
	0	**30**	**32.67**	**980**
	TOTAL	**100**		
Q3	**1**	**77**	**73**	**2974**
	0	**23**	**28.6**	**748**
	TOTAL	**100**		

	Q1	Q2	Q3
Z	3.00	2.84	4.94
Sig (2- tailed)	.00	.00	.00

وتشير النتائج بالجدول السابق الي أن قيمة P-Value أقل من 5%، لذلك يتم قبول الفرض البديل فى الحالة الثانية القائل بأنه **يختلف تأثير مخاطر الأمن السيبراني معنويا على أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية بإختلاف تأهيل المراجع.**

- **نتيجة إختبار فرض البحث الثالث:**

لإختبار هذا الفرض على النحو الاتي:

H_0: لايختلف تأثير مخاطر الأمن السيبراني معنويا على أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية بإختلاف خبرة مراجع الحسابات.

جدول 1: اختبار فرض البحث الثالث – التجربة الأولى

Ranks				
	خبرة مراجع الحسابات	**N**	**Mean Rank**	**Sum of Ranks**
Q1	1	70	66	2254
	0	30	32.67	980
	TOTAL	100		
Q2	1	25	30.7	874
	0	75	70	2841
	TOTAL	100		
Q3	1	75	70	2841
	0	25	30.7	874
	TOTAL	100		

	Q1	**Q2**	**Q3**
Z	3.25	2.15	4.23
Sig (2- tailed)	.00	.00	.00

وتشير النتائج بالجدول السابق الي أن قيمة P-Value أقل من 5%، لذلك يتم قبول الفرض البديل فى الحالة الأولى القائل بأنه **يختلف تأثير مخاطر الأمن السيبراني معنويا على أتعاب المراجع عن مراجعه القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية بإختلاف خبرة مراجع الحسابات.**

جدول 13: اختبار فرض البحث الثالث – التجربة الثانية

Ranks				
	خبرة مراجع الحسابات	**N**	**Mean Rank**	**Sum of Ranks**
Q1	1	70	66	2254
	0	30	30.67	980
	TOTAL	100		
Q2	1	74	68	2365

	0	26	29.5	875
	TOTAL	100		
Q3	1	75	70	2841
	0	25	30.7	874
	TOTAL	100		

	Q1	Q2	Q3
Z	5.25	4.15	3.03
Sig (2- tailed)	.00	.00	.00

وتشير النتائج بالجدول السابق الي أن قيمة P-Value أقل من 5%، لذلك يتم قبول الفرض البديل فى الحالة الثانية القائل بأنه **يختلف تأثير مخاطر الأمن السيبراني معنويا على أتعاب مراجعة القوائم المالية السنوية التاريخية الكاملة للشركات المقيدة بالبورصة المصرية بإختلاف خبرة مراجع الحسابات.**

6-4-7-7 خلاصة نتائج اختبار الفروض في ظل التحليل الاساسي

جدول 14: خلاصة نتائج اختبار الفروض في ظل التحليل الاساسي

	الفرض في ظل التحليل الاساسي	النتيجة
الفرض الأول	**H_1:** تؤثر مخاطر الأمن السيبراني معنويا على أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية.	قبول
الفرض الثاني	**H_2:** يختلف تأثير مخاطر الأمن السيبراني معنويا على أتعاب مراجعة على أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية بإختلاف تأهيل المراجع.	قبول
الفرض الثالث	**H_3:** يختلف تأثير مخاطر الأمن السيبراني معنويا على أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية بإختلاف خبرة مراجع الحسابات.	قبول

6-4-7-8 نتائج اختبار فروض البحث في ظل التحليلات الأخرى

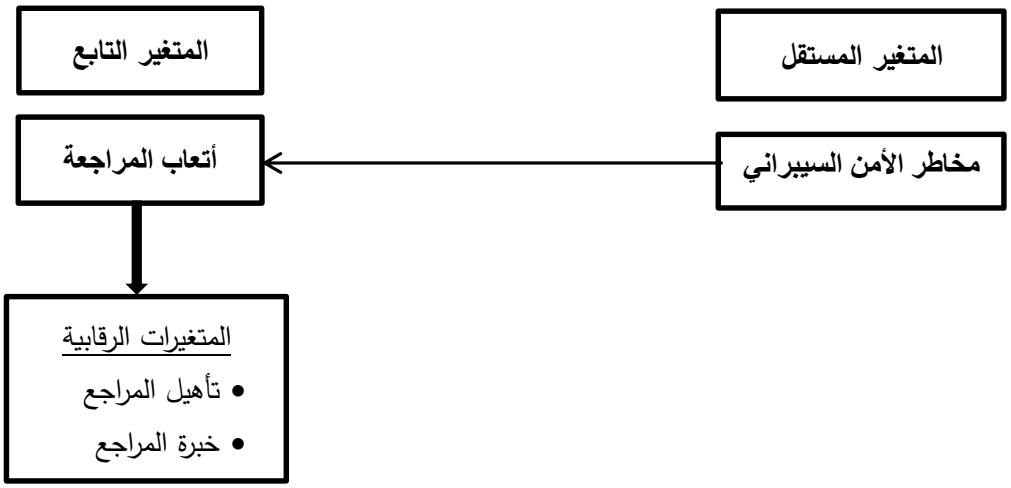
لغرض إضفاء المزيد من الوضوح على العلاقة محل الدراسة ضمن التحليل الأساسي، يتم إجراء تحليل إضافي كإجراءهام لمعالجة أي خلل يمكن أن يكون تضمن فى نموذج البحث الأساسي، من خلال الإعتماد على متغيرات لم يتم التحقق من أثرها من قبل، أو تغيير طرق معالجتها التي تم إختبارها على العلاقة محل الدراسة قياسا على(Khan et al., 2023).

ويعتبر التحليل الإضافي منهجية تستخدم لإعادة اختبار العلاقة محل الدراسة، بعد أن يتم تعديل التحليل الأساسي وذلك بعد إستحداث متغيرات جديدة ومعالجتها (كمتغيرات معدلة أو رقابية) أو أن يتم تغيير طرق

معالجة المتغيرات الجديدة، مع الأخذ فى الإعتبار عدم المساس بالمتغيرات الرئيسية (المتغير التابع أوالمستقل) لأنهم متغيرات رئيسية، ثم إجراء مقارنة بين النتائج الخاصة بالتحليلين الأساسي والإضافي، ولمعرفة مدى الإختلاف بينهما وأثر ذلك على ما تم التوصل اليه.

لذلك تم إعادة إختبار الفرض الثاني والثالث للعلاقة محل الدراسة **(H_2& H_3)** ضمن التحليل الأساسي للدراسة. وبعد ذلك يتم القيام بتحويل طبيعة المتغيرين المعدلين (تأهيل المراجع ،وخبرة المراجع) إلى متغيرين رقابيين، كما يتم القيام بتغيير فرضي الدراسة الثاني والثالث فى التحليل الأساسي إلى سؤالين، لغرض إجراء مقارنة بين نتائج كلا التحليلين ومعرفة مدى الإختلاف الحاصل بينها، وذلك بهدف زيادة وضوح العلاقة الرئيسية محل الدراسة فى التحليل الأساسي، وذلك يساعد على التحقق من التأثير الحاصل على إتجاه وقوة العلاقة محل الدراسة بعد ان يتم إدخال متغيرات رقابية جديدة.

وفي سياق العلاقة التأثيرية بين مخاطر الأمن السيبرانى على أتعاب المراجعة ، حيث إستهدف كل من السؤال الأول والسؤال الثاني إختبار ما إذا كان تأهيل المراجع وخبرته يؤثران أيضاً على أتعاب المراجعة ، ولمعرفة مدى تأثير ذلك تم إختبار أثر المتغيرات الرقابية كل على حده بالإجابة بنعم أو لا على السؤالين الأول والثاني (س1، س2) كما يظهر من نموذج البحث التالي:



شكل 2: نموذج البحث في ظل التحليل الإضافي

المصدر: من اعداد الباحثة

وبشأن نتيجة الإجابة على (س1) بخصوص أثر تأهيل المراجع، تم تصميم السؤال الأول لإختبار ما إذا كان تأهيل المراجع يؤثر على أتعاب المراجعة، في سياق العلاقة التأثيرية بين مخاطر الأمن السيبرانى على أتعاب المراجعة، والجدول الآتي يوضح نتيجة إختبار السؤال إحصائياً.

جدول 15: نتيجه اختبار السؤال الأول فى ظل التحليل الاضافى

السؤال عن الفرض	Q	N	Z	P-Value
س1: هل يؤثر تأهيل المراجع معنويا على أتعاب مراجعة القوائم المالية في سياق العلاقة التأثيرية بين مخاطر الأمن السيبرانى وأتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية؟	Q1	100	5.36	.16
	Q2	100	7.16	.02
	Q3	100	6.02	.00
	الاجمالي	100	3.98	.00

يتضح من الجدول السابق أن قيمة P-Value أقل من 5% وعليه فان تأهيل المراجع يؤثر معنويا على أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة في سياق العلاقة التأثيرية بين مخاطر الأمن السيبرانى وأتعاب مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية.

وتعتقد الباحثة أن المتغير الرقابي (تأهيل المراجع) الذي تم إختياره هو متغير قوي يؤثر بالفعل على المتغير التابع أتعاب المراجعة ، لذلك من البديهي أن تختلف النتيجة عندما يكون هذا المتغير رقابياً عما إذا كان المتغير معدلاً في التحليل الاساسي، حيث أن المتغيرات الرقابية يكون تأثيرها أقوى على المتغير التابع مقارنة بالمتغيرات المعدلة، وهذه النتائج تدعم اختيارات الباحثة للمتغيرات الرقابية وذلك قياساً على (أبو العلا،2021).

وبشأن نتيجة الإجابة على (س2) بخصوص أثر خبرة المراجع على تخطيط إجراءات المراجعة، تم تصميم السؤال الثاني لإختبار ما إذا كانت خبرة المراجع تؤثر على أتعاب المراجعة، في سياق العلاقة التأثيرية بين مخاطر الأمن السيبرانى على أتعاب المراجعة ، والجدول الآتي يوضح نتيجة إختبار السؤال إحصائياً.

جدول 16: نتيجه اختبار السؤال الثانى فى ظل التحليل الاضافى

السؤال عن الفرض	Q	N	Z	P-Value
س2:هل تؤثر خبرة مراجع الحسابات معنويا على أتعاب مراجعة القوائم المالية في سياق العلاقة التأثيرية بين مخاطر الأمن السيبرانى وأتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية؟	Q1	100	8.25	.01
	Q2	100	3.16	.02
	Q3	100	7.02	.00
	الاجمالي	100	1.98	.00

يتضح من الجدول السابق أن قيمة P–Value أقل من 5% وعليه فان خبرة المراجع تؤثر معنويا على أتعاب مراجعة القوائم المالية السنوية التاريخية الكاملة للشركات المقيدة بالبورصة في سياق العلاقة التأثيرية بين مخاطر الأمن السيبرانى وأتعاب مراجعة القوائم المالية السنوية التاريخية الكاملة للشركات المقيدة بالبورصة المصرية.

وتعتقد الباحثة أن المتغير الرقابي (تأهيل المراجع) الذي تم إختياره هو متغير قوي يؤثر بالفعل على المتغير التابع أتعاب المراجعة ، لذلك من البديهي أن تختلف النتيجة عندما يكون هذا المتغير رقابياً عما إذا كان المتغير معدلاً في التحليل الاساسي، حيث أن المتغيرات الرقابية يكون تأثيرها أقوى على المتغير التابع مقارنة بالمتغيرات المعدلة، وهذه النتائج تدعم اختيارات الباحثة للمتغيرات الرقابية وذلك قياساً على (أبو العلا،2021).

6-4-7-9 مقارن نتائج التحليل الأساسي والإضافي

تظهر من خلال الجدول التالي:

جدول 17: مقارنة بين نتائج التحليل الأساسى والإضافى

الفروض وفق التحليل الاساسي	النتائج	الاسئلة وفق التحليل الاضافي	الاجابة
H_2: يختلف تأثير مخاطر الأمن السيبراني معنويا على أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية بإختلاف تأهيل المراجع.	قبول	س1: هل يؤثر تأهيل المراجع معنويا على أتعاب مراجعة القوائم المالية في سياق العلاقة التأثيرية بين مخاطر الأمن السيبرانى على أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية؟	نعم
H_3: يختلف تأثير مخاطر الأمن السيبراني معنويا على أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية بإختلاف خبرة مراجع الحسابات.	قبول	س2:هل تؤثر خبرة مراجع الحسابات معنويا على أتعاب مراجعة القوائم المالية في سياق العلاقة التأثيرية بين مخاطر الأمن السيبرانى على أتعاب المراجع عن مراجعة القوائم المالية السنوية للشركات المقيدة بالبورصة المصرية؟	نعم

6-5 النتائج والتوصيات ومجالات البحث المقترحة

استهدف البحث دراسة واختبار العلاقة بين أثر مخاطر الأمن السيبراني على أتعاب المراجع عن مراجعة القوائم المالية السنوية. وكذلك اختبار أثر تأهيل وخبرة المراجعين على العلاقة محل الاختبار، ولقد

اعتمدت الباحثة على إجراء دراسة تجريبية، على عينة من100 من مراجعى الشركات المقيدة بالبورصة المصرية.

وأجابت الدراسة فى شقها التجريبى على السؤال الأول والخاص بماهو شكل وإتجاه العلاقة بين مخاطر الأمن السيبراني وأتعاب المراجع عن مراجعة القوائم المالية السنوية ؟، حيث تم قبول الفرض الرئيسى H_1

وركز **السؤال الثانى** والخاص بهل تختلف هذه العلاقة بإختلاف مستوى التأهيل والخبرة للمراجع؟، حيث تم قبول الفرض H_2 حيث أن التأهيل العلمى قد يؤثر على توقع أتعاب المراجعة. كما تم قبول الفرض H_3 حيث أن مستوى الخبرة قد يؤثر على توقع أتعاب المراجعة.

وأكدت التحليلات الأخرى نتائج التحليل الأساسى بشأن أثر إختلاف مستوى التأهيل والخبرة للمراجع على هذه العلاقة.

وفى ضوء أهداف البحث وحدوده ومشكلته وما إنتهى إليه من نتائج، توصى الباحثة بمايلى:

- الزام الشركات المقيدة بالبورصة المصرية للافصاح عن مخاطر الأمن السيبرانى.
- الزام الشركات المقيدة بالبورصة المصرية بإنشاء إدارات لمواجهة مخاطر الأمن السيبرانى.
- تركيز المناهج بالجامعات على تدريس الأمن السيبرانى.
- تطوير أداء مراجعى الحسابات من الناحية التكنولوجية للتعرف على مخاطر الأمن السيبرانى وتأثيرها على عملية المراجعة.

وفى ضوء ماسبق تقترح الباحثة المجالات البحثية التالية مستقبلاً:

- أثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن السيبرانى على قرار منح الإئتمان – دراسة تجريبية.
- أثر الافصاح عن توكيد المراجع الداخلى على مزاعم الإدارة عن إدارة مخاطر الأمن السيبرانى على قرار الاستثمار بالأسهم – دراسة تجريبية.
- أثر الإفصاح عن إدارة مخاطر الأمن السيبرانى فى التقارير المالية على أسعار الأسهم وأحجام التداول فى البورصة– دراسة تطبيقية.
- دور إدارة المراجعة الداخلية التوكيدى والاستشارى فى إدارة مخاطر الأمن السيبرانى فى التقارير المالية– دراسة تجريبية.
- أثر الافصاح عن مخاطر الأمن السيبرانى على تقرير المراجع الخارجى – دراسة تطبيقية.
- أثر إدماج مخاطر الأمن السيبرانى فى نموذج خطر المراجعة على تخطيط واجراءات المراجعة الخارجية – دراسة تجريبية.

المراجع

أولا: المراجع باللغة العربية

إبراهيم، زينب خليل (2018). **مخاطر التدقيق والأهمية النسبية وأثرهم على عملية التدقيق**، رسالة الدبلوم العالي في تدقيق ومراجعة الحسابات في المحاسبة، *https://www.researchgate.net/publication/324706323*

ابو العلا، اسامة مجدي فؤاد (2021). خبرة مراقب الحسابات وقيده لدى الهيئة العامة للرقابة المالية كمحددين للعلاقة بين ممارسته للعصف الذهني وكفاءته في كشف الغش بالقوائم المالية: دراسة تجريبية، **مجلة الاسكندرية للبحوث المحاسبية، قسم المحاسبة والمراجعة**، 3(5): 301-373.

الاستراتيجية الوطنية للأمن السيبراني(2018). متاحة على الموقع: *https://mcit.gov.eg/Ar/Publication/Publication_Summary/6132*

التحول الرقمي – وزارة الاتصالات وتكنولوجيا المعلومات متاحة على الموقع: *https://mcit.gov.eg › Digital Government*

الخزاعلة، عبير (2021). مفهوم الأمن السيبراني. متاحة على الموقع: *https://mawdoo3.com/cite_note-*

العقلاء، رؤى احمد صالح، وعلى، نور الدين ادم (2022). درجة الوعى بمفاهيم الأمن السيبرانى لدى معلمى ومعلمات الحاسب الألى بمدينة حائل. **مجلة كلية التربية**، جامعه حائل المملكة العربية السعودية.العدد(2):284- 315.

المطارنه، غسان فلاح (2006). لأسباب المحتملة لتغيير مدقق الحسابات الخارجي في الشركات المساهمة العامة الأردنية: دراسة ميدانية، **جامعه أسيوط – مركز دراسات المستقبل**، العدد، س8 ع، 123-151

جمعية المحاسبين والمراجعين المصرية(2015). **الميثاق العام المصرى لأداب وسلوكيات مهنة المحاسبة والمراجعة**. متاح على الموقع *http://www.esaaegypt.com*

حلس، سالم عبدالله (2003). العوامل المؤثرة فى تحديد أتعاب المراجعة فى فلسطين. **مجلة الجامعة الاسلامية**، العدد(1)، 248-275.

حماد، ماجدة عزت حسين(2022). أثر العلاقة بين خبرة وحجم مكتب المراجعة وإدراكه لفرص وتحديات عملية المراجعة في ظل تكنولوجيا الحوسبة السحابية وانعكاس ذلك على إجراءات تخطيط عملية المراجعة: دراسة تجريبية. **المجلة العلمية للدراسات التجارية والبيئية**، المجلد 13، العدد 3.

شحاته، شحاته السيد(2022)."نحو دور فاعل للمراجع الداخلي في إدارة مخاطر الأمن السيبراني". **المجلة العلمية للدراسات والبحوث المالية والإدارية**، كلية التجارة – جامعة مدينة السادات. المجلد 13، العدد 2، 26-37.

عبد الرحيم، رضا محمود محمد(2020). اثر التعديلات في شكل ومحتوى تقرير مراقب الحسابات وفقاً لمعيار المراجعة الدولي رقم (570) المعدل لسنة 2015 بشأن الاستمرارية على قراري الاستثمار ومنح الائتمان: دراسة تجريبية، **مجلة الاسكندرية للبحوث المحاسبية**، قسم المحاسبة والمراجعة كلية التجارة جامعة الاسكندرية، 2(4)،1-94.

عبده، إيمان محمد السعيد(2018). أثر خطر التقاضى وخصائص مجلس الإدارة على أتعاب المراجعة الخارجية وإنعكاسها على توقيت إصدار تقرير المراجعة – دراسة تطبيقية على الشركات الصغيرة والمتوسطة المتداولة ببورصة النيل المصرية. **مجلة الفكر المحاسبى**، جامعة عين شمس:1-63.

على، محمود أحمد أحمد، وعلي، صالح علي صالح (2022). أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية –دراسة تجريبية، **المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة بعنوان تحديات وأفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين**، كلية التجارة – جامعة الإسكندرية.

على، محمود أحمد(2022). أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية- دراسة تجريبية، **رساله ماجستير**، كليه التجارة- جامعه بنى سويف.

فرج، هانى خليل(2022). أثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الإستثمار بالأسهم- دراسة تجربية، **مجلة المحاسبة والمراجعة**، اتحاد الجامعات العربية – كلية التجارة، جامعة بنى سويف،2022 العدد الثانى، 129-209.

قرار رئيس مجلس الوزراء رقم 994 لسنة 2017 بالتزام الجهات الحكومية بتنفيذ قرارات وتوصيات المجلس الأعلى للأمن السيبراني.

لطفى، وفاء (2022). الجهود الدوليه فى مجال مكافحة جرائم الارهاب السيبرانى:التجربة الماليزية نموذجاً، مجلة كلية الأقتصاد والعلوم السياسية، مجلد23، العدد 1، 159-201.

محروس، رمضان عارف رمضان، وصالح، أبو الحمد مصطفى (2022). استخدام المنهجية الرشيقة في تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني. **مجلة البحوث المالية والتجارية**، جامعة بورسعيد، المجلد 23، العدد 3.

محمد، هيام عيد عطية، ودياب، محمد عبد القادر، وحسن، حنان جابر(2023). أثر دعم دور المراجعة الداخلية على تعزيز أنظمة الأمن السيبراني،دراسة ميدانية. **مجلة كلية التجارة** – جامعة عين شمس،71-120.

موسى، سعاد زغلول عبده (2018). اثر توكيد المراجع الخارجي على تقارير الاعمال الكاملة على قراري الاستثمار ومنح الائتمان: دراسة تجريبية، **رسالة دكتوراه غير منشورة**، كلية التجارة، جامعة الاسكندرية.

ثانيا: المراجع باللغة الأجنبية

Abbott, L. (2017). The Impact of Litigation Risk on Auditor Pricing Behavior: Evidence from Reverse Mergers. *Contemporary Accounting Research*, 34, No. 2, 1103–1127.

Alali, F. (2011). Audit Fees and Discretionary Accruals: Compensation Structure Effect. *Managerial Auditing Journal*, 26,90-113.

Alan, V., G. Pratt, and J. Stevenson.(2001). The Determinants of Audit Fees—Evidence from the Voluntary Sector. *Managerial Auditing Journal*: 243-274.

Al-Shaer, H., Albitar, K. and Hussainey, K. (2022). Creating Sustainability Reports that matter: an investigation of factors behind the narratives. *Journal of Applied Accounting Research*, Vol. 23, No. 3: 738-763. https://doi.org/10.1108/JAAR-05-2021-0136.

Amba, S. and F. Al-Hajeri, (2013). Determinants of audit fees in Bahrain: An empirical study. *Journal of Finance and Accountancy*, 13: 1-10.

American Institute of Certified Public Accountants (AICPA).(2017). Trust Services Criteria Crosswalk. Available at: *http://www. aicpa.org.*

Aral, S., C. Dellarocas and D. Godes. (2013). Introduction to the special issue-social media and business transformation: A framework for research. *Information Systems Research*, 24(1),3-13.

Axén, L.(2020). Determinants of audit fees and the management of corporate disclosures. *Doctoral thesis,* Linköping Studies in Arts and Sciences, ISSN 0282-9800.

Balsam, S., J. Krishnan, J.S. Yang. (2003). Auditor industry specialization and earnings quality. *Auditing: A Journal of Practice and Theory*, 22 (2), 71–97.

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

Belina, H. (2022). Surprise" material weakness disclosures: Effects on audit fees and audit report lags. *Journal of Accounting and Public Policy*, 41(6), 106979. *https://doi.org/10.1016/j.jaccpubpol.*

Bernard, T., T. Hsu, N. Perl Roth, and R. Lieber. (2017). Equifax Says Cyber-Attack May Have Affected 143 Mil-lion in the U.S. New York Times, RetrievedDecember8, *Available at: https://www.nytimes.com /2017/09/07/ business/equifax -cyberattack.html.*

Bhat, S. and Abdullah, M. (2023). Factors Influencing Sustainability Reporting Practices among Listed Companies in Oman. *International Journal of Economics and Financial Issues*, Vol. 13, No. 3: 74-83. *https://doi.org/ 10.32479/ijefi.13912.*

Campbell, J. (2007). Why Would Corporations Behave in Socially Responsible Ways? An Institutional Theory of Corporate Social Responsibility. *Academy of Management Review*, Vol. 32, No. 3: 946-967. *http://www.jstor.org/stable/20159343.*

Carcello, J.V. & A.L. Nagy. (2004). Client size, auditor specialization and fraudulent financial reporting. Manage. *Audit. J*, 19 (5):651–668.

Center for Audit Quality (CAQ).2014. CAQ Member Alert: Cyber security and the External Audit. Available at: *http://www. thecaq.org/wpcontent /uploads/2019/03/caqalert_2014_03.pdf.*

Cheng, X., Hsu, C., & Wang, T. D. (2022). Talk too much? The Impact of Cyber Security Disclosures on Investment Decisions. *Communications of the Association for Information Systems*, 50 (1).

De Arroyabe, J, I. De Arroyabe, M. Arroyabe and C. Arranz.(2024). Navigating Cybersecurity Implementation: Exploring the Influence of Environment on

Standards Adoption and Board Involvement, *Available at SSRN: https://ssrn.com/abstract=4762075 or http://dx.doi.org/10.2139/ssrn.4762075*

Dunn, K., and B. Mayhew. (2004). Audit firm industry specialization and client disclosure quality. *Rev. Account. Stu*, 9 (1),35–58.

ElGammal, W. and M. Gharzeddine.(2020). Determinants of audit fees in developing countries: Evidence from Egypt. *Corporate Ownership & Control,* 17, 2,142-156.

Galderon, Thomas G. and Lei Gao.(2021). Cybersecurity Risks Disclosure and Implied Audit Risks: evidence from Audit Fees, *International Journal of Auditing*, Vol.25,24-39.

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

Gordon, L., M. Loeb, W. Lucyshyn, and T. So hail. (2006). The impact of the Sarbanes-Oxley act on the corporate disclosures of information security activities, *Journal of Accounting and Public Policy*: 115-133.

Gupta, G., J. Mahaud, and B. Debata. (2018). Impact of CEO's characteristics on investment decisions of Indian listed firms: does crisis make any difference, *available* at *https:// doi.org/ 10.1080/ 23322039.*

Hashem, B., & Sujud, H. (2020). The Impact of Using It on The Quality of Auditing in Lebanon, *International Research Journal of Finance and Economics*, Issn 1450-2887 Issue 178:131-143.

Hassanein, A. and Hussainey, K. (2015), Is forward-looking financial disclosure really informative? Evidence from UK narrative statements, *International Review of Financial Analysis*, Vol. 41; 52-61. *https://doi.org/10.1016/j.irfa.2015.05.025.*

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

Hsieh, T. S., Kim, J. B., Wang, R. R., & Wang, Z. (2020). Seeing believes? Executives' facial trustworthiness, auditor tenure, and audit fees. *Journal of Accounting and Economics*, 69: 10-12.

Ji, Xu Dong, Wei Lu and Wen Qu .2018. Internal Control Risk and Audit Fees: Evidence from China, *Journal of Contemporary Accounting & Economics*, Vol.14:266-287.

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

Kelton, A. 2021. How to Reduce the Cyber Security Breach Contagion Effect? *Current Issues in Auditing*, 15 (2), 1-9.

Khan, A. S., Nejad, M. Y., & Kassim, A. A. M. (2023). The Effect of Audit Qualityon Fraud Reduction: A Moderating Role of International Financial Reporting Standards (IFRS) Adoption in Malaysia and Indonesia. *International Journal of Professional Business Review*, 8(6), 1- 22.

Kothari, C. (2004). *Research Methodology: Methods & Techniques,* Second Revised Edition, New Delhi, New Age International (P) Limited, Daryaganj.

Krishnan, G., (2003). Does Big 6 auditor industry expertise constrain earnings management? *Accounting Horizons*, 17,1–16.

Kuntari, Y., Chariri, A., and Nurdhiana, N. (2017). The Effect of Auditor Ethics, Auditor Experience, Audit Fees and Auditors Motivation on Audit Quality. *SIJDEB*, 12,203-218.

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

Leidner, J. and H. Lenz. (2017). Client's Business Risk, Public-Interest Entities, and Audit Fees: The Case of German Credit Institutions. *International Journal of Auditing*, Vol. 21,324–338.

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

Lois, P., G. Drogalas, A. Karagiorgos, and A. Vrontis. (2021). Internal Auditing and Cyber Security: Audit Role and Procedural Contribution. *Int. J. Managerial and Financial Accounting*, 13 (1), 25-47.

Masoud, N. and G. Alutaibi.(2022). The Determinants of Cybersecurity Risk Disclosure in Firms Financial Reporting: Empirical Evidence, *Research in Economics*, Vol.76, 131-140.

Miazee, M., A. Shareef, and M. Hasan. (2014). Fundamentals knowledge of investor and its influence on investment in capital market- A study from Dhaka stock exchange. *Research Journal of Finance and Accounting*, 5 (24), 192-204.

Navarro, P. and S. Sutton. (2021). Investors' Judgment and Decisions after a Cyber Security Breach: Understanding the Value Relevance of Cyber Security Risk Management Assurance, (February,1),1-52. *Available at http://dx.doi.org/10.2139/ssrn.3817763*

NIST Conference Papers Fiscal Year 2023.

Nordlund, J. (2021). The disclosure of cyber security risk. *www. SSRN.com*

Pierangelo R., F. Gogolin and T. Lynn. (2020). Cyber-Security Incidents and Audit Quality. *European Accounting Review*: 15-34.

PCAOB Audit Risk. (2016). Wiley Practitioner's Guide to GAAS 2015: Covering all SASs, SSAEs, SSARSs, PCAOB Auditing Standards, and Interpretations,881-882. *https://www.researchgate.net/publication/319533469_PCAOB_8_Audit_Risk DOI:10.1002/9781118979037.ch71*

Ponemon Institute. (2016). Cost of Cyber Crime Study &the Risk of Business Innovation, Benchmark Study of 237 Global Companies *Ponemon Institute*, October.

PriceWaterHouseCoopers, (2022). Mandatory Rotation of Audit Firms: Will It Improve Audit Quality? PricewaterhouseCoopers LLP, New York, NY. The central role of the propensity score in observational studies for causal effects. *Biometrika*, 70 (1), 41–55.

Rezaee, Z., Homayoun, S., Rezaee, N. and Poursoleyman, E. (2023). Business sustainability reporting and assurance and sustainable development goals. *Managerial Auditing Journal*, Vol. 38, No. 7: 973-996. *https://doi.org/10.1108/MAJ-10-2022-3722.*

Rosati, P., M. Cummins, P. Deeney, F. Gogolin, L. Werff, and T. Lynn. (2022).The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis,* V.49,146-154.

Samad, A. 2017.Relationship and Impact of Risk Aversion & Financial Knowledge on Individual Investment's Decision, *available at https://www.linkedin.com.*

SEC.(2011).CF Disclosure Guidance. *Available at: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2 .htm.*

Seltman, Howard. (2018). Experimental Designs and Analysis, *available at http://www.stat.cmu.edu.*

Smith, T., J. Higgs, and R. Pinsker. (2019). Do Auditors Price Breach Risk in Their Audit Fees? *Journal of Information Systems*, 33(2):177–204. *Available at: https://doi.org/10.2308/isys-52241.*

Soekrisno, A. (2014). Influence of auditor independence, audit tenure, and audit fee on audit quality of members of capital market accountant forum in Indonesia. *Procedia Social & Behavioral Science*, 164:324 – 331.

Solms B. and R. von Solms.(2018). Cyber security and information security – what goes where? *Information and Computer Security*, Vol. 26. No. 1:1- 29.

Stanley, J., F. DeZoort. (2007). Audit firm tenure and financial restatements: an analysis of industry specialization and fee effects. *J. Account. Publ Policy*, 26: 131–159.

Swift, O., Colon, R., & Davis, K. (2020). The impact of cyber breaches on the content of cyber security disclosures. *Journal of Forensic and Investigative Accounting*, 12 (2),197-212.

Sun, Zhengjie, Huang, Feiqi & Li, He. (2020).The Effect of Auditor Cybersecurity Expertise on Audit Fees and Cyber Incidents. Pace University. *Retrieved from: fhuang@pace.edu*

Traina, L. (2015). 5 Steps CPAs can take to fight hackers, journal of accountancy, *Available at*: https://www. cpa2biz.com

Tuson, O.,.(2021). Cyber-attacks and Stock Market Activity, *International Review of Financial Analysis*: 1-15.

Verwey, I., and S. Asare. (2021). The joint effect of ethical idealism and trait skepticism on auditors' fraud detection. *Journal of Business Ethics*, 171(2),1-15.

Von Solms, R. and J. Van Niekerk. (2013). from information security to cyber security. *Computers and Security*, Vol.38:97-102.

Vuko, Tina, Slapnicar, S., Cular, M., & Drascek, M. (2024). Key Drivers of Cybersecurity Audit Effectiveness. *International Journal of Auditing*. Retrieved from: http://wileyonlinelibrary.com/journal/ijau.

Walton, S., Wheeler, P. R., Zhang, Y. I., & Zhao, X. R. (2021). An integrative review and analysis of cyber security research: Current state and future directions. *Journal of Information Systems*, 35 (1), 155-186.

Wang, Y., K. Kannan, and J. Ulmer. (2013).The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, Vol. 24, No. 2: 201-218.

Widodo, N. and Chariri, A. (2021). The relationship between audit proce-dures, auditors'experience and auditors' responsibility for fraud de-tection. Diponegoro *Journal of Accounting*, 10 (1), 1-10.

ملحق البحث

الحالتان التجريبيتان

الاستاذ الفاضل/

السلام عليكم ورحمة الله وبركاته

تحية طيبه وبعد...

تقوم الباحثة بإعداد رسالة ماجستير في المحاسبة والمراجعة بعنوان (أثر إدراك مراجعى الحسابات لمخاطر الأمن السيبرانىعلى تخطيط إجراءات المراجعة– دراسة تجريبية) بالتطبيق على مكاتب المراجعه الخاصة المقيدة لدى الهيئه العامه للرقابة المالية التى تراجع الشركات المقيدة فى البورصه المصرية.

وتقدر الباحثة تعاونكم في مراجعة الحالة التجريبية والإجابة على الأسئلة الواردة فيها، كما تؤكد لكم أن هذه الدراسة تجرى لأغراض البحث العلمي فقط وأن إجاباتكم ستعامل بسرية تامة. وأخيراً نشكركم على تعاونكم، ونعتذر لكم عن أي إزعاج قد يسببه لكم ذلك.

تفضلوا بقبول تحياتنا واحترامنا

الباحثة

ياسمين داود موسى

كلية التجارة– جامعه الاسكندرية

القسم الاول: البيانات الشخصية

المسمى الوظيفي

1.مراجع مبتدئ ☐

2.مراجع متوسط الخبرة ☐

3.مراجع رئيسي ☐

4.مدير مراجعة ☐

آخر (يرجى التحديد): .....

عدد سنوات الخبرة في مجال المراجعة

1.أقل من 5 سنوات ☐

2.من 5-10 سنوات ☐

3.أكثر من 10 سنوات ☐

نوع الشركات التي تقوم بمراجعتها (يمكن اختيار أكثر من إجابة)

1.صناعية ☐

2.خدمية ☐

3.مالية ☐

أخرى (يرجى التحديد): .....

المؤهلات الدراسية

1.بكالوريوس محاسبة ☐

2.دبلومات الدراسات العليا ☐

3.ماجستير ☐

4.دكتوراه ☐

5.عضوية وزمالة المنظمات المهنية المصرية والدولية

- أذكرها:.....

هل سبق لك التعامل مع قضايا تخص الأمن السيبراني أثناء المراجعة؟

1.نعم ☐

2.لا ☐

مصطلحات فنية:

- **مخاطر الأمن السيبرانى:** هى القدرة على تدمير أو تعطيل أو التهديد بتقديم الخدمات الأساسية أو استغلال الثغرات للسطو على المعلومات والأموال والتى تسبب خسائر مالية أو فقدان الشركة لسمعتها عند تعطل أحد أنظمة المعلومات بها.
- **جهود المنظمات الدولية لمواجهة مخاطر الأمن السيبرانى:**

1- **مجمع المحاسبين القانونيين الأمريكىAICPA:** وضع عام 2017 إقتراح للتقرير عن إدارة مخاطر الأمن السيبرانى وكيفية إفصاح الشركات عنها.

2- **لجنة البورصة الأمريكية SEC:** أصدرت عام 2018 دليلاً استرشادياً عن متطلبات الإفصاح عن إدارة مخاطر الأمن السيبرانى.

- **الجهود المصرية لمواجهة مخاطر الأمن السيبرانى:**

نص الدستور المصرى 2014 – مادة (31) على أن: أمن الفضاء المعلوماتى جزء أساسى من منظومة الإقتصاد والأمن القومى، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذى ينظمه القانون.

القسم الثانى: الحالة التجريبية الأولى

حالة تتضمن عدم إفصاح الادارة عن حدوث مخاطر الأمن السيبرانى وتحديد أثر ذلك على أتعاب المراجعة السنوية للشركات المساهمة المقيدة بالبورصة المصرية

بإفتراض أن إحدى شركات تكنولوجيا المعلومات ش. م. م. خاضعه لقانون 159 لسنه 1981 ومقيدة بالبورصة المصرية لاتواجه مخاطر أمن سيبرانى، وكانت الايضاحات المتممة للقوائم المالية على النحو التالى:

الإيضاحات المتممة:

- تم إعداد القوائم المالية المجمعة فى 31 ديسمبر 2020 طبقا لمعايير المحاسبة المصرية وفى ضوء القوانين واللوائح المصرية ذات العلاقة.
- أعدت القوائم المالية على أساس التكلفة التاريخية باستثناء بعض أنواع الإستثمارات المالية والتى يتم تقييمها بالقيمة العادلة وفقا لمعايير المحاسبة المصرية.
- تم عرض القوائم المالية بالجنيه المصرى والذى يمثل عملة التعامل للشركة.
- تتطلب إعداد القوائم المالية وفقا لمعايير المحاسبة المصرية قيام الإدارة بعمل تقديرات وإفتراضات والتى تؤثرعلى تطبيق السياسات المحاسبية وعلى قيم الأصول والإلتزامات والايرادات والمصروفات. ويتم مراجعة التقديرات والإفتراضات بشكل دورى مستمر.

- تدار أنشطة التشغيل الخاصة بالشركة عن طريق قطاعات تشغيلية على مستوى أنشطة الشركة ككل كأنشطة متكاملة وذلك على اساس طبيعة الخدمة المقدمة.

ويتم اعداد التقارير القطاعية وفق ثلاث قطاعات:

الأول: قطاع الاتصالات والكوابل البحرية والبنيه التحتية.

الثانى: قطاع خدمات الانترنت الثابت.

الثالث: قطاع خدمات التعهيد.

- **رأس مال الشركة:** راس المال المصدر والمدفوع بالكامل 17070716 الف جنيه مصرى مقسم لأسهم قيمة السهم الإسمية 10 جنيه مصرى.
- المخاطر التى تواجهها الشركة:
- **خطر الائتمان:** يتمثل فى خطر عدم وفاء أحد أطراف الأدوات المالية لالتزاماته، ويعرض الطرف الاخر لخسائر مالية، وينشأ هذا الخطر بصفة رئيسية من عملاء الشركه والمدينين الاخرين.
- **خطر السيولة:** يتمثل فى خطر عدم وفاء الشركة إلتزاماتها فى تاريخ استحقاقها.
- **خطر السوق:** يتمثل فى خطر التغيرات فى أسعار السوق مثل أسعار صرف العملات الأجنبية وسعر الفائدة وأسعار أدوات حقوق الملكية.

وعلمت أن:

- الشركة لديها إجراءات فعالة لحماية بياناتها من التهديدات السيبرانية.
- يتم تدريب الموظفين بانتظام على مواجهة التهديدات السيبرانية.
- يتم إجراء اختبارات دورية على أنظمة الشركة الأمنية.
- الشركة لم تتعرض لهجمات سيبرانية كبيرة في السنوات الأخيرة.
- هناك تواصل مستمر بين الإدارة وفريق تقنية المعلومات لضمان حماية الأنظمة.

فى ضوء قراءة الايضاحات المتممة السابقة، أجب عن الأسئلة التالية:

1. تؤثر مخاطر الأمن السيبراني على قرار تحديد أتعاب المراجعة فى هذه الحالة.

أوافق تماما	أوافق بدرجة كبيرة	أوافق	لا أوافق إلى حد ما	لا أوافق تماما

2. تعرض الشركة لمخاطر الأمن السيبراني سيزيد من أتعاب المراجعة.

أوافق تماما	أوافق بدرجة كبيرة	أوافق	لا أوافق إلى حد ما	لا أوافق تماما

3. اذا كانت الأتعاب للشركة عام 2023 كانت 50000 جنيه، فمن المتوقع لهذه الشركة العام القادم أن تكون الأتعاب 0000000 فى هذه الحالة.

القسم الثالث: الحالة التجريبية الثانية

حالة تتضمن إفصاح الادارة عن حدوث مخاطر الأمن السيبرانى وتحديد أثر ذلك على تخطيط إجراءات المراجعه السنوية للشركات المساهمة المقيدة بالبورصة المصرية

إفترض فى الحالة السابقة مايلى:

أن إدارة الشركة أفصحت عن وجود نظام لإدارة مخاطر الأمن السيبرانى، وأفصحت ضمن الايضاحات المتممة عما يلى:

- **مخاطر الأمن السيبرانى:** تتمثل فى أن الهجمات الالكترونية يمكن أن تؤدى الى تخفيض الايرادات أو زيادة المصروفات أو إلحاق الضرر بسمعة الشركة، ويوجد تطور للتهديدات الالكترونية بإستمرار وليس لدى الشركه حاليا القدرة على كشف بعض الثغرات الأمنية مما قديؤدى إلى تعطيل أمان النظم مما قد يضعف قدرة الشركة على تقديم خدماتها للعملاء وحماية الخصوصية لديهم.

وعلمت أن:

- الشركة تتعرض بشكل متكرر لهجمات سيبرانية.
- الشركة لديها ضعف واضح في البنية التحتية التكنولوجية.
- هناك فجوات في سياسات وإجراءات أمن المعلومات داخل الشركة.
- الشركة لا تُحدث أنظمتها الأمنية بشكل دوري.
- الشركة تُظهر عدم كفاية في تدريب الموظفين على التعامل مع التهديدات السيبرانية.

فى ضوء قراءة الايضاحات المتممة السابقة، أجب عن الأسئلة التالية:

1. تؤثر مخاطر الأمن السيبراني على قرار تحديد أتعاب المراجعة فى هذه الحالة.

أوافق تماما	أوافق بدرجة كبيرة	أوافق	لا أوافق إلى حد ما	لا أوافق تماما

2. تعرض الشركة لمخاطر الأمن السيبراني سيزيد من أتعاب المراجعة.

أوافق تماما	أوافق بدرجة كبيرة	أوافق	لا أوافق إلى حد ما	لا أوافق تماما

3. اذا كانت الأتعاب للشركة عام 2023 كانت 50000 جنيه، فمن المتوقع لهذه الشركة العام القادم أن تكون الأتعاب 0000000 فى هذه الحالة.