مجلة البحوث الإدارية والمالية والكمية

Journal of Managerial, Financial

جامعه السويس
كلية التجارة

أثر استخدام تكنولوجيا الأمن السيبرانى على كفاءة أداء عملية المراجعة

(بحث مقبول للنشر كجزء من متطلبات الحصول على درجة الماجستير فى المحاسبة)

إعداد

أسماء مجدى حسين محمود
باحث ماجستير – كلية التجارة – جامعة السويس

الأستاذ الدكتور
منى حسن أبوالمعاطى
أستاذ المحاسبة والمراجعة المساعد
ورئيس قسم المحاسبة والمراجعة
كلية التجارة – جامعة السويس

الأستاذ الدكتور
مها عبدالفتاح محمد
مدرس المحاسبة والمراجعة
كلية التجارة – جامعة السويس

مجلة البحوث الإدارية والمالية والكمية
كلية التجارة – جامعة السويس
المجلد الرابع – العدد الرابع
ديسمبر 2024

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

أثر استخدام تكنولوجيا الأمن السيبرانى على كفاءة أداء عملية المراجعة

الملخص:

هدفت الباحثة من خلال هذه الدراسة إلى التعرف على أثر استخدام تكنولوجيا الأمن السيبرانى على كفاءة أداء عملية المراجعة وذلك من خلال القيام بشرح مفهوم الأمن السيبرانى و الأهداف التى يسعى إلى تحقيقها وأهم تقنياته المستخدمة فى الحد من الهجمات الإلكترونية، وتوضيح العوامل التى تساعد على زيادة كفاءة عملية المراجعة ثم القيام بتوضيح العلاقة التكاملية بين الأمن السيبرانى والمراجعة، كما تم القيام بعمل دراسة ميدانية لتوضيح هل يوجد علاقة بين الأمن السيبرانى وكفاءة عملية المراجعة، حيث اعتمدت الباحثة على اسلوبين فى جمع البيانات وهما المقابلة الشخصية وقائمة الاستقصاء، وتم توزيع قائمة الاستقصاء على فئتين من الدراسة وهما: المراجعون الخارجيون بمكاتب المراجعة حيث تم توزيع عدد (95) قائمة ، والمراجعون الداخليون بالشركات الصناعية وتم توزيع (77) قائمة وذلك بإجمالى (172) قائمة، ومن خلال الدراسة النظرية والميدانية توصلت الباحثة إلى وجود علاقة ذات دلالة إحصائية بين تكنولوجيا الأمن السيبرانى وكفاءة أداء عملية المراجعة.

الكلمات الدالة: الأمن السيبرانى - الهجمات السيبرانية - كفاءة المراجعة

ABSTRACT:

Through this study, the researcher aimed to identify the impact of the use of cyber security technology on the efficiency of the performance of the audit process, by explaining the concept of cyber security, the goals that it seeks to achieve, the most important techniques used in reducing electronic attacks, and clarifying the factors that help increase the efficiency of the audit process, then clarifies the complementary relationship between cyber security and auditing. A field study was also conducted to clarify whether there is a relationship between cyber security and the efficiency of the auditing process. The researcher relied on two methods of collecting data, namely the personal interview and the survey list. The survey list was distributed into two categories of the study. They are: external auditors in audit offices, where a number of (95) lists were distributed, and internal auditors in industrial companies, where (77) lists were distributed, for a total of (172) lists. Through theoretical and field study, the researcher concluded that there is a statistically significant relationship between cyber security technology and efficient performance of the audit process.

Keywords: Cyber security - cyber-attacks - audit efficiency

أولا: الإطار العام للدراسة:

1. المقدمة وطبيعة المشكلة:

لقد ساعدت التكنولوجيا على جعل حياة الإنسان أكثر تطورا ولعبت دورًا حيويًا في إنجاز المهام اليومية بسهولة، حيث إنها ليست مجرد وسيلة للحصول على المعلومات والتواصل فقط ولكنها أيضًا وسيلة لتخزين البيانات، حيث تمكننا من تخزين الكثير من المعلومات المهمة **(Biju,et.al,2019,p1)**

وحيث أن المعلومات المحاسبية تعد من مخرجات النظام المحاسبى فى منظمات الأعمال والتى قد تكون على شكل تقارير أو قوائم مالية تعتمد عليها الإدارة فى تسيير أعمالها، ويقع على عاتقها تأثير كبير فى القرارات المهمة ؛ لذلك يجب أن تكون المعلومات المحاسبية على قدر عالى من الجودة لتؤدى الغاية المطلوبة من إعدادها. **(السرحان،2020،ص.18)**

ولقد أثرت التكنولوجيا على أمن تلك المعلومات والتى قد تتعرض للسرقة أو التلاعب فيها، حيث نجد تطور فى تقنيات السرقة مما نتج عنه زيادة عدد الهجمات الالكترونية والتى لا ينتج عنها فقط خسارة مالية بل أيضًا تسريب للمعلومات الحساسة**(Tariq,2018,p.1)** ،وبالتالى أصبحت الجريمة الإلكترونية قضية أمنية رئيسية في الساحة الدولية؛ حيث يشكل كل من مجرمي الإنترنت والهجمات الإلكترونية التي ترعاها الدول تهديدات للدول التي تحمي بياناتها السرية، وبصرف النظر عن تأثيرها العميق على التقدم الاقتصادي وأنظمة الدفاع فإن هذه التهديدات تصعد التوترات الدبلوماسية مما يؤدي إلى الفوضى في النظام العالمي ، وقد يتأثر السلام العالمي والاستقرار والتنمية من قبل إساءة استخدام تقنية المعلومات والاتصالات.**(Khuda,2020,p.1)**

ولذلك؛ دعت منظمات الأعمال إلى ضرورة إيجاد سياسات وأساليب للحفاظ على مواردها المعلوماتية، فظهرت العديد من السياسات المتعلقة بأمن المعلومات والحفاظ على سريتها، ومن أهم هذه الطرق التى استخدمت هى الأمن السيبرانى، ويستخدم الأمن السيبرانى فى حماية المعلومات المربوطة بشبكات الإنترنت وتكنولوجيا المعلومات، إذ يحافظ على المعلومات من السرقة أو الدخول الغير مصرح به على الأنظمة كما تعزز من جودة مخرجات نظم المعلومات. **(السرحان،2020،ص.18)**

وليس هناك أدل من أهمية دور الأمن السيبراني كبُعد جديد لإدارة المخاطر من التهديدات والمخاطر السيبرانية التى لاقت اهتمامًا كبيرًا من الدول فى جميع أنحاء العالم بسبب المعاناة التى لاقتها الشركات من الهجمات الإلكترونية والمتمثلة فى خسائر اقتصادية وخسائر في سمعتها طويلة الامد **(Haapamaki, sihvonen,2019,P.1)**

وحيث أن عملية المراجعة تهدف إلى تحديد ما إذا كانت الأرقام والمعلومات المفصح عنها فى التقارير المالية والمقدمة لمستخدمى القوائم المالية تعكس بشكل يتسم بالمصداقية المركز المالى الحقيقى للشركة ونتائجها التشغيلية، وبالتالى من شأن تحسين عملية المراجعة أن تعمل على زيادة الثقة فى دقة النتائج المالية المعترف بها ، فى حين يؤدى المستوى المنخفض لجودة المراجعة إلى إنخفاض جودة التقارير المالية . **(الدمنى،2022،ص.1)**

وتأسيسا على ذلك ؛ومع زيادة أتمتة العمليات التجارية والاعتماد المتزايد على البيانات الرقمية كمصدر وحيد للحقيقة بدأ المراجعون الماليون في النظر في أهمية مخاطر الأمن السيبراني فيما يتعلق بالبيانات المالية والتقارير السنوية، وهذا يستدعي تغيير النهج المتبع في عمليات مراجعة تكنولوجيا المعلومات ليشمل تقييمًا للأمن السيبراني قائمًا على المخاطر في المجال التقني للمراجعين، حيث يمثل المتسللون تهديدًا خطيرًا لأنظمة المحاسبة والرقابة الداخلية الحالية لقدرتهم على تجاوز أي تدابير (فعالة) للتحكم في تكنولوجيا المعلومات؛ ونتيجة لذلك يجب على مراجعى تكنولوجيا المعلومات تكييف أسلوبهم ليشمل جمع الحقائق في مجال الأمن السيبراني التقني للمراجعين وأن يتم تجميع نتائج تقييم المخاطر الإلكترونية وإدخالها في خطة المراجعة الشاملة لتحديد التأثير على البيانات المالية والضوابط الداخلية.**(Backer,2022)**

ومن هنا تتضح مشكلة الدراسة الرئيسية والتى تتمثل فى التعرف على "أثر استخدام تكنولوجيا الأمن السيبرانى على كفاءة أداء عملية المراجعة" وذلك من خلال الإجابة على تساؤلات البحث التالية:

1. ماهو الأمن السيبرانى وأهم أهدافه؟
2. ما هى مجالات تطبيق الأمن السيبرانى وتقنياته المستخدمة للحد من الهجمات الإلكترونية؟
3. ما هى أهم العوامل المؤثرة على كفاءة المراجعة؟
4. هل توجد علاقة بين الأمن السيبرانى وكفاءة عملية المراجعة؟

2. الدراسات السابقة:

يمكن تناول الدراسات التى تناولت متغيرات الدراسة على النحو التالى:

1-(Rosati,et.al,2019):

هدفت هذه الدراسة في البحث عن تأثير حوادث الأمن السيبراني على رسوم المراجعة. حيث تقوم اولا بدراسة ما إذا كانت الشركات التي تتعرض لحوادث الأمن السيبراني بيتم تحصيل رسوم مراجعة أعلى منها ام لا. وثانيًا هل المراجعون على دراية بالمشكلات الأمنية المحتملة قبل وقوع أي حادث. وتشير النتائج إلى وجود علاقة إيجابية بين مخاطر الأمن السيبراني ورسوم المراجعة و يمكن تفسير ذلك من خلال الافتراض بأن حوادث الأمن السيبراني والضعف الملحوظ للشركة تجاه مثل هذه الحوادث يؤدي إلى زيادة مخاطر التحريف الجوهري (أي مخاطر المراجعة) نتيجة لذلك ؛ تزيد شركات المراجعة من جهودها لضمان دقة التقارير المالية لعملائها وبالتالى تؤدي هذه الزيادة في النهاية إلى ارتفاع رسوم المراجعة. حيث وجدت الدراسة أن المراجعين يفرضون في المتوسط رسوم مراجعة أعلى بنسبة اثنى عشر بالمائة على الشركات المخالفة ، هذا وتشير النتائج ايضا إلى أن المراجعين يدمجون مخاطر الأمن السيبراني في تقييمهم لمخاطر المراجعة بغض النظر عما إذا كانت حادثة الأمن السيبراني قد حدثت أم لا . وتوصى الدراسة بعمل ابحاث مستقبلية عن كيفية إدراك المراجعين لتقنيات مثل الحوسبة السحابية فيما يتعلق بمخاطر المراجعة وهو ما يمثل تحديا كبيرا للمراجعين خاصة لوجود نقاط ضعف أو خطر الفشل فى إعداد التقارير المالية بسبب أخطاء مقدم الخدمة حيث قد يوفر البحث النوعى والكمى رؤى مفيدة حول تصور المراجعين لهده الاتجاهات الحديثة.

2-دراسة (الزيود،2021):

هدفت الدراسة إلى التعرف على أثر المراجعة الداخلية المتمثل فى (كفاءة المراجعة الداخلية والحيادية والمركز التنظيمى للمراجعة وتخطيط المراجعة) فى الحد من المخاطر السيبرانية فى البنوك التجارية. وتوصلت الدراسة إلى وجود أثر للمراجعة الداخلية المتمثل فى(الكفاءة والمركز التنظيمى والتخطيط) فى الحد من المخاطر السيبرانية وعدم وجود أثر لحيادية المراجعة الداخلية. واوصت الدراسة بضرورة حث إدارة البنوك على زيادة مستوى الوعى والمسؤولية تجاه المخاطر السيبرانية واثرها على ادائها وامكانياتها ،والحث ايضا على الرفع من مستوى الوعى بأهمية دور المراجعة الداخلية فى الحد من المخاطر السيبرانية.

3-دراسة(منصور،2021):

يهدف البحث الى التعرف على اهمية الامن السيبراني من خلال تأثيره على الرقابة الداخلية وقيمة الوحدة الاقتصادية بأعتماد اطار حوكمة تقنية المعلومات**(COBIT5)** ، وتوصلت الدراسة أن هناك تقبل واتفاق بشكل عام على وجود علاقة بين ابعاد ومتطلبات الامن السيبراني(الاستراتيجية، العمليات والاجراءات، الحماية السرية والخصوصية، الامن المنطقي، المخاطر السيبرانية)على قيمة الوحدة الاقتصادية في ظل الاطر الحديثة للرقابة الداخلية، كما اظهر البحث اهمية تكامل عناصر الرقابة الداخلية في ظل اطار عمل COBIT5وضرورة تطبيقها بصورة مجتمعة من اجل تحقيق اهداف الرقابة .وتوصى الدراسة بضرورة قيام الوحدة الاقتصادية بتبني وسائل فعالة للتقويم المستمر للرقابة الداخلية للحفاظ على امن المعلومات بأعتماد الأطر الحديثة للرقابة الداخلية COBIT5وذلك من خلال تكاملية

الاجـراءات والخصـائص فـي ظـل الاطـر الحديثـة لتلافـي وسـائل اختـراق الـنظم الالكترونيـة ومحـاولات التلاعب في معلوماتها.

4-دراسة(Al Bayati,2022):

استهدفت الدراسة توضيح دور الأمن السيبرانى فى تعزيز كفاءة التقارير المالية فى جامعة الفرات الأوسط التقنية، وذلك عن طريق التعرف على مفهوم الأمن السيبرانى وأبعاده الأساسية ، وتوضيح المفاهيم الأساسية للتقارير المالية ومكوناتها والعوامل المؤثرة فيها. وتوصلت الدراسة إلى أن (حوكمة الأمن السيبراني ،و تعزيز ومرونة الأمن السيبراني ، والأمن السيبراني الخارجي ، والأمن السيبراني لأنظمة التحكم) لهم دور في تعزيز كفاءة التقارير المالية في جامعة الفرات الأوسط التقنية وفقًا لعينة الدراسة. وتوصى الدراسة ب:

-الاهتمام المتزايد بوضع استراتيجيات وسياسات واضحة للأمن السيبراني، بالإضافة إلى إنشاء إدارة متخصصة للأمن السيبراني .

-تدريب الموظفين على الأمن السيبراني وكيفية التعامل معه وتعزيز الأمن السيبراني للموارد البشرية والعملاء، ودراسة إدارة الأمن السيبراني.

-التركيز على إطلاق مشاريع مستقلة في الجامعة بالتعاون بين الطلاب والإدارة من أجل دعم الأمن السيبراني .

-تفعيل دور التقارير المالية الإلكترونية وربط الأمن السيبراني بها وتعزيز كفاءة التقارير المالية في الجامعة من خلال الدراسات الدائمة والتحليلات.

-التقييم المستمر والاختبارات الدورية للأمن السيبراني في الجامعة بهدف تحقيق ذلك الحفاظ على المعلومات والبيانات بشكل عام، والبيانات والتقارير المالية بشكل خاص .

5- دراسة(محروس, صالح،2022):

هـدفت الدراسـة إلـى تطـوير أداء المراجعـة الداخليـة لمواجهـة مخـاطر الأمـن السـيبرانى فـى منظمـات الأعمـال المصـرية وذلـك عـن طريـق اسـتخدام المنهجيـة الرشـيقة. وتوصـلت الدراسـة إلـى وجـود زيـادة مسـتمرة فـى مخـاطر الأمـن السـيبرانى بالإضـافة إلـى تأثيراتهـا الكبيـرة علـى منظمـات الأعمـال والاقتصـاد القـومى, وكشـفت الدراسـة عـن وجـود قصـور فـى أداء المراجعـة الداخليـة فـى الوقـت الـراهن لمواجهـة مخـاطر الأمـن السـيبرانى وذلـك بسـبب عـدم مرونـة خطـط المراجعـة وتطبيـق المـنهج التقليـدى فـى المراجعـة وعـدم التواصـل الفعـال بـين المـراجعين الـداخليين والإدارة وأصـحاب المصـالح الرئيسـيين ،وعـدم تـوافر الخبـرات اللازمة فى مجال التكنولوجيا والتحول الرقمى.

كمـا تعـد المنهجيـة الرشـيقة أحـد المنـاهج الملائمـة لتطـوير أداء المراجعـة الداخليـة وبشـكل خـاص فـى مواجهـة مخـاطر الأمـن السـيبرانى نظـرا لانهـا تتـيح درجـة عاليـة مـن المرونـة فـى خطـط المراجعـة ، كمـا إنهـا تطبـق الأسـلوب الاسـتباقى فـى التعامـل مـع المخـاطر وتعتمـد علـى فـرق عمـل متعـددة المهـام والتخصصـات ، وتسـتخدم دورات المراجعـة قصـيرة الأجـل والتـى تسـاعد فـى تقـديم خـدمات المراجعـة فـى أسـرع وقـت. وتوصـى الدراسـة بضـرورة التوعيـة بمخـاطر الأمـن السـيبرانى وتأثيراتهـا السـلبية علـى المنظمـات ، وضـرورة الاسـتفادة مـن المنهجيـة الرشـيقة فـى تطـوير أداء المراجعـة الداخليـة وتـوافر المعرفـة الكافيـة بهـا ونشر ثقافة العمل الرشيق.

6- دراسة(حسين،سالم،2023):

هـدف البحـث إلـى قيـاس أثـر الإفصـاح عـن مخـاطر الأمـن السـيبرانى علـى أتعـاب المراجعـة فـى الشـركات المصـرية، وتوصـلت الدراسـة إلـى وجـود إرتبـاط إيجـابى بـين أتعـاب عمليـة المراجعـة ومخـاطر اختراقـات الأمـن السـيبرانى، حيـث أن مراجعـى الحسـابات عنـدما يجـدون مخـاطر الأمـن السـيبرانى متزايـدة يبـذلون المزيـد مـن الجهـد أثنـاء عمليـة المراجعـة الأمـر الـذى يـؤدى إلـى فـرض أتعـاب مرتفعـة، وتوصـى الدراسـة بضـرورة تطبيـق مـنهج متكامـل لعمليـة ضـمان الأمـن السـيبرانى بكفـاءة وزيـادة الـوعى بمخـاطر الهجمـات السـيبرانية ، بالإضـافة إلـى الاعتمـاد علـى مـنهج تحلـيلات البيانـات وهـو المـنهج الحاسـم لضـمان الأمـن

السيبرانى حيث أن الهدف الرئيسى منه أن تكون المنظمات قادرة على نقل المعلومات بسرعة من خلال الحفاظ على الجودة العالية والأمان.

7-دراسة(يوسف،2024):

هدف البحث إلى دراسة واختبار القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشارى والتوكيدى فى مجال إدارة مخاطر الأمن السيبرانى فى بيئة الأعمال المصرية، وتوصلت الدراسة إلى وجود أثر إيجابى معنوى احصائيا لفعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشارى والتوكيدى فى مجال إدارة مخاطر الأمن السيبرانى على قيمتها المضافة ، كما اتضح وجود تأثير إيجابى معنوى احصائيا لدعم الإدارة العليا لوظيفة المراجعة الداخلية على هذه العلاقة بما يشير إلى أن الأثر الإيجابى بين متغيرات الدراسة يختلف باختلاف مستوى دعم الإدارة العليا لوظيفة المراجعة الداخلية.

ويوصى الباحث:

-اهتمام المنظمات المهنية ومجالس إدارة الشركات بتوفير مناخ ملائم يعزز فعالية المراجعة الداخلية للقيام بدورها الاستشارى والتوكيدى فى مجال إدارة مخاطر الأمن السيبرانى.

-توفير الاستقلال التنظيمى لوظيفة المراجعة الداخلية لما له من أهمية فى تفعيل الدورين الاستشارى والتوكيدى لها.

-العمل بشكل تكاملى بين إدارة المراجعة الداخلية وقسمى إدارة المخاطر وأمن المعلومات بما يوفر رؤية شاملة للمراجع الداخلى عن مخاطر الأمن السيبرانى.

-تطوير نظام التعليم المحاسبى خاصة فى ظل بيئة التحول الرقمى.

تحليل وتقييم الدراسات السابقة:

- اتفقت دراسة **(Rosati,et.al,2019)**،**(حسين،سالم،2023)** إلى وجود علاقة إيجابية بين الهجوم السيبرانى ورسوم المراجعة حيث وجدت أن الشركات التى تتعرض لهجوم تتحمل رسوم مراجعة أعلى من غيرها
- اتفقت دراسة (**الزيود،2021**)، **ودراسة(يوسف،2024)** على أهمية دور المراجعة الداخلية في إدارة مخاطر الأمن السيبرانى.
- توصلت دراسة **(AlBayati,2022)**على أهمية الأمن السيبرانى في رفع كفاءة التقارير المالية وأهمية الإفصاح عن أي هجمات تحدث وهو ما يعمل على زيادة الشفافية وبالتالى جودة التقارير.

3. أهمية الدراسة:

أهمية علمية:

وذلك خلال تناول أحد المواضيع الشائكة ومركز الأهتمام في العصر الحالى وهو الأمن السيبرانى والتعرف على أهميته وتقنياته ودوره في الحد من عمليات الهجمات السيبرانية وتوضيح العلاقة بين الأمن السيبرانى وكفاءة عملية المراجعة.

أهمية عملية:

تعتبر سياسة الأمن السيبرانى ذات أهمية للأنظمة المرتبطة في الشبكات وتكنولوجيا المعلومات؛ فالإلتزام بتطبيق سياسة الأمن السيبرانى يضمن الحفاظ على المعلومات من أي خطر أو تهديد. وإن وجود المعلومات محمية بعيدة عن الغش والاحتيال والتلاعب هو هدف كل منظمة حيث يعمل على زيادة الثقة بين المؤسسة والعملاء وتقليل مستوى الخطر الناتج عن استخدام الفضاء السيبرانى . هذا بالإضافة إلى زيادة الاهتمام بتحقيق أهداف التنمية المستدامة في ضوء رؤية مصر 2030 بأبعادها المختلفة من خلال تعزيز متطلبات الإفصاح والشفافية عن إدارة مخاطر الهجمات السيبرانية.

4. أهداف الدراسة:

يتمثل الهدف الرئيسى للبحث في عرض وتحليل سياسة الأمن السيبرانى وتوضيح أثرها على كفاءة أداء عملية المراجعة وذلك من خلال عرض الأهداف الفرعية التالية:

- بيان ما هو الأمن السيبرانى وأهم أهدافه.
- التعرف على مجالات تطبيق الأمن السيبرانى وتقنياته المستخدمة للحد من الهجمات الإلكترونية.
- توضيح أهم العوامل المؤثرة على كفاءة عملية المراجعة.
- بيان العلاقة بين الأمن السيبرانى وكفاءة عملية المراجعة.

5. فروض الدراسة:

اعتمادا على التساؤلات التى استندت عليها مشكلة الدراسة يقوم الباحث باختبار الفرض الرئيسى التالى "لا توجد علاقة ذات دلالة احصائية بين تكنولوجيا الأمن السيبرانى وكفاءة أداء عملية المراجعة".

6. منهج الدراسة

في ضوء مشكلة البحث وسعيا نحو تحقيق أهدافه واستخلاص نتائجه؛ اعتمدت الباحثة على كل من المنهج الاستقرائى والاستنباطى وذلك على النحو التالى:

-المنهج الاستقرائى: يعتمد هذا المنهج على دراسة الإطار النظرى للدراسة وكيفية الربط بين المتغيرات عن طريق الاستعانة بالمراجع والرسائل والدوريات العلمية العربية والأجنبية المتاحة على الانترنت ذات الارتباط بموضوع الدراسة .

-المنهج الاستنباطى: تم استخدام هذا المنهج في الدراسة الميدانية بهدف الكشف عن النتائج المنطقية المترتبة على اختبار صحة الفروض الأساسية للدراسة ثم استخلاص النتائج والتوصيات.

7. تقسيمات الدراسة:

انطلاقا من مشكلة الدراسة وتحقيقا لأهدافها تحاول الباحثة في الأجزاء التالية بناء الإطار النظرى للدراسة وذلك من خلال تناول مايلى:

- ماهية الأمن السيبرانى
- أهداف الأمن السيبرانى.
- مجالات تطبيق الأمن السيبرانى.
- تقنيات الأمن السيبرانى المستخدمة في الحد من الهجمات.
- العوامل المؤثرة على كفاءة عملية المراجعة.
- العلاقة التكاملية بين الأمن السيبرانى والمراجعة.

ثانيا: الإطار النظرى للدراسة:

1. ماهية الأمن السيبرانى:

لقد عرف الاتحاد الدولي للاتصالات " InternationalTelecommunication Union" الأمن السيبراني بانه مجموعة من الأدوات والسياسات والمفاهيم الأمنية وضمانات الأمان والمبادئ التوجيهية وأساليب إدارة المخاطر ، والإجراءات والتدريب وأفضل الممارسات، والضمان والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمة والمستخدم, وتتضمن أصول المنظمة المؤسسة, المستخدم, أجهزة الحوسبة المتصلة , الموظفين ,البنية التحتية, التطبيقات, الخدمات , أنظمة الاتصالات ومجموعة المعلومات المرسلة أو المخزنة في البيئة السيبرانية**(ITU,2021)**

وعرفته موسوعة "انفستوبيديا" على إنه التدابير المتخذة للحفاظ على خصوصية المعلومات الإلكترونية وأمانها من التلف أو السرقة، ويتم استخدامه ايضا للتأكد من عدم إساءة استخدام الأجهزة والبيانات، كما عرفه قاموس "oxford"على إنه حالة الأمان من الجريمة الإلكترونية والإجراءات المتخذة لتنفيذ ذلك.**(احمد،اخرون،2022،ص.9)**

وعرف ايضا: بمجموعة من الممارسات التى تهدف إلى حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية أيا كان نوعها، وهذه الممارسات متنوعة إلى تدابير احتياطية إستباقية قبل وقوع الخلل ، وعلاجية بعد وقوع الخلل.**(جاب الله ،2022،ص16).**

ومن خلال المفاهيم السابقة يمكن القول بأن الأمن السيبرانى"هو مجموعة الوسائل التى تهدف إلى الإبقاء على الأجهزة والشبكات دون تلف او تدمير ومنع الوصول الغير مصرح به للبيانات والمعلومات، والحماية من الهجمات الالكترونية والحفاظ على البيانات والمعلومات أمنة.

2. أهداف الأمن السيبرانى:

يمكن حصر أهم أهداف الأمن السيبرانى فيما يلى:

- تعزيزحماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحويه من بيانات.
- التصدى لهجمات وحوداث أمن المعلومات التى تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.
- توفير بيئة آمنة وموثوقة للتعاملات في مجتمع المعاملات.
- صمود البينية الأساسية التحتية ضد الهجمات الإلكترونية.
- الحد من التجسس والتخريب الإلكترونى على مستوى الحكومة والأفراد.
- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حدا سواء من المخاطر المحتملة في مجالات الأنترنت المختلفة .
- تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة.

وبالتالى فأن الهدف العام من الأمن السيبرانى هو : القدرة على مقاومة التهديدات المتعمدة والغير متعمدة على أنظمة المعلومات والأتصالات ، والاستجابة السريعة لرد الأخطار، ودرء الأضرار الناجمة عن تعطيل أو إتلاف المعلومات المخزنة والبيانات الموجودة على أجهزة الكمبيوتر.**(جاب الله،2022،ص.21)**

3. مجالات تطبيق الأمن السيبرانى:

هناك العديد من المجالات التي يتم عليها تطبيق تقنيات الأمن السيبراني للحد من المخاطر الإلكترونية مثل:

خودام الويب: يعتبر التهديد بشن هجمات على تطبيقات الشبكة لاستخراج المعلومات أو لتوزيع التعليمات البرمجية الخبيثة هو احد أشكال الهجمات المستخدمة، حيث بعد أن يقوموا مجرمو الانترنت باختراق شبكة يتم توزيع شفراتهم الخبيثة عليها، وبالتالى اصبح من الضرورة وجود خواد شبكة وتطبيقات أكثر أمانا، حيث تعد خوادم الإنترنت بشكل خاص المنصة الأكثر فعالية لهؤلاء المجرمين الإلكترونيين لسرقة المعلومات ، ومن ثم يجب على الفرد دائمًا استخدام متصفح أكثر أمانًا على وجه الخصوص خلال المعاملات الحيوية حتى لا يقع فريسة لهذه الجرائم.**(Upadhyay,Yadav,2018,p.3)**

- **شبكات المحمول:** يمكننا أن نرى الهاتف المحمول فى أيدى الجميع، حيث يقوم المستخدم بكل نشاط تقريبًا على الهاتف من وسائل التواصل الاجتماعي إلى الخدمات المصرفية ، من الصور إلى مقاطع الفيديو ، دردشة "Whats App' وما إلى ذلك وهو مصدر قلق كبير للأمن السيبراني، وفي هذه الأيام أصبح الفضاء السيبراني والجدران النارية قابلة للاختراق، حيث يستخدم الأشخاص أنواعًا مختلفة من الأجهزة مثل: الهواتف الذكية و IPad والكمبيوتر اللوحي وما إلى ذلك والتي تتطلب جميعها مستوى عالٍ من الأمان وبالتالى ؛ الهواتف المحمولة معرضة بشكل كبير للجرائم الإلكترونية مما يتوجب معه قيام المستخدم بتنزيل أحدث البرامج والتطبيقات لجعل نفسه محميًا من الجرائم الإلكترونية (**(Tabassum,2020,P.2**

- انترنت الاشياء:يشير إنترنت الأشياء إلى الأجهزة المادية بخلاف أجهزة الكمبيوتر والهواتف والخوادم التي تتصل بالإنترنت وتشارك البيانات، حيث تتضمن أمثلة أجهزة إنترنت الأشياء أجهزة تتبع اللياقة البدنية القابلة للارتداء والثلاجات الذكية والساعات الذكية والمساعدات الصوتية مثل Amazon Echo Google Home,، إلا إنه معظم أجهزة إنترنت الأشياء تتمتع بقدرات معالجة وتخزين أقل و قد يجعل ذلك من الصعب استخدام جدران الحماية وبرامج مكافحة الفيروسات وتطبيقات الأمان الأخرى لحمايتها وبالتالى؛ يخلق توسع إنترنت الأشياء (IoT) المزيد من الفرص للجرائم الإلكترونية. (**Kaspersky,2020)**

الحوسبة السحابية وخدماتها:على الرغم من أن الخدمات السحابية تتطور بشكل سريع إلا إنه لا تزال هناك الكثير من المشاكل فيما يتعلق بأمنها وهو ما يمثل تحديًا كبيرًا للأمن السيبراني، نظرًا لتزايد نطاق التطبيقات التي يمكن الوصول إليها داخل السحابة، لذلك يجب أن تتطور الضوابط السياسية لتطبيقات الإنترنت والخدمات السحابية لإيقاف فقدان البيانات القيمة. **(Upadhyay,Yadav,2018,p.3)**

إمكانات الذكاء الاصطناعي (AI) :مما لاشك فيه إن إدخال تقنية الذكاء الاصطناعي والتعلم الآلى في جميع قطاعات السوق أحدثت تغييرات هائلة في الأمن السيبراني، حيث كان للذكاء الاصطناعي دورًا أساسيًا في بناء أنظمة أمان آلية ومعالجة اللغة الطبيعية واكتشاف الوجه والكشف التلقائي عن التهديدات ، وذلك بالإضافة إلى استخدامه أيضًا لتطوير البرامج الضارة والهجمات الذكية لتجاوز أحدث بروتوكولات الأمان في التحكم في البيانات، وبالتالى يمكن لأنظمة الكشف عن التهديدات التي تم تمكينها بواسطة الذكاء الاصطناعي التنبؤ بهجمات جديدة وإخطار المسؤولين عن أي خرق للبيانات على الفور.

الاتمتة: فى ظل التكنولوجيا والتطورات الحديثة اصبح هناك ضغوطا كبيرة على المهنين والمهندسين لتقديم عمل يواكب هذا التطور، وهو ما جعل الاتمتة ذات أهمية كبيرة فى الوقت الحاضر، حيث إنه مع تضاعف حجم البيانات كل يوم اصبح استخدام الأتمتة اكثر امانا ،حيث يعمل على التحكم بشكل افضل فى المعلومات خاصة فى ظل صعوبة حماية تطبيقات الويب الكبيرة والمعقدة مما يجعل الأتمتة وكذلك الأمن السيبراني مفهومًا رئيسيًا لعملية تطوير البرامج.**(Duggal,2023)**

4. تقنيات الأمن السيبرانى للحد من الهجمات الإلكترونية:

مع تطور الأساليب المستخدمة فى عمليات الهجوم الإلكترونى كان لابد من توافر تقنيات للأمن السيبرانى تعمل على حماية الأفراد والشركات والدول من تلك الهجمات ، ومن أهم هذه التقنيات ما يلى:

- التحكم في الوصول وأمان كلمة المرور: يعتبر الأمن الذي يتم توفيره عن طريق اسم المستخدم وكلمة المرور هو طريقة بسيطة لتوفير الأمان للمعلومات الخاصة وذلك حفاظًا على الخصوصية ، وتعد هذه الوسيلة لتوفير الأمن هي واحدة من أكثر مبادرات الأمن السيبراني أهمية.(**(Upadhyay,Yadav,2018,p.4**
- **برامج مكافحة الفيروسات:** مما لاشك فيه أنه يمكن للبرامج الضارة أن تعمل على حذف الملفات أو الكتابة فوقها ، إبطاء و تعطيل النظام وفي بعض الأحيان تساعد المهاجم على اختراق النظام أو الخوادم. ومن أشهر الأمثلة على هذه الفيروسات أحصنة طروادة ,الديدان , برامج الفدية وبرامج التجسس وغيرها ، ويمكن اكتشاف هذه البرامج الضارة باستخدام برامج فحص الفيروسات الضارة المعروفة باسم برامج مكافحة الفيروسات، والتى تتمثل وظيفتها فى تحديد أو حظر أو حذف الملفات المشتبه بها عن طريق فحص النظام بأكمله ،إلا أن هذه البرامج لديها القليل من العيوب مثل زيادة استهلاك ذاكرة الوصول العشوائي .**(Sree,2020,p.4)**
- **جدران الحماية:** وهى عبارة عن حزمة برامج أو أجهزة تساعد على فصل المتسللين والفيروسات والديدان التي تحاول الوصول إلى جهاز الكمبيوتر الخاص بك من خلال الويب. يقوم جدار الحماية بفحص جميع الرسائل الواردة ويحظر تلك التي تفشل في تلبية متطلبات الأمان المتوافقة مع جميع الرسائل وهو دور حيوي للغاية في الكشف عن البرامج الضارة.(**Rajasekharaiah,2020,p.5)**

- **النسخ الأحتياطى:** ويقصد به عمل نسخة احتياطية من محتويات الحواسيب أو شبكات المعلومات، وحفظ هذه النسخة فى مكان آمن بحيث يمكن الرجوع إليها عند التدمير الكامل للشبكة أو فى حالة اختراقها بهدف محو وتدمير البيانات والمعلومات المتاحة عليها.(**جاب الله،2022،ص35**)
- **تحديث النظام:** لمنع الهجمات المحتملة على البرامج ؛ يجب العمل على تحديث برامج التشغيل الحالية والتى يتم تحديثها من حين لأخر من قبل Windows , Mac Linux ، كما يجب تحديث الأجهزة المحمولة وحماية كلمة المرور وذلك بتنزيل التطبيقات من مصادر موثوقة.
- إدارة إعدادات الوسائط الاجتماعية: عند استخدام وسائل التواصل الاجتماعى يجب الاحتفاظ بالمعلومات الشخصية والخاصة لك فقط ، حيث يراقب مجرمو الإنترنت معلومات وسائل التواصل الاجتماعي ، لذا يجب قفلها وتغيير كلمة المرور الخاصة بها بشكل متكرر، كما يجب أن تشارك قدرًا أقل من المعلومات على الشبكات الاجتماعية حتى لا يتمكن أي شخص من تخمين إجابات الأسئلة الأمنية.
- **أمن الشبكة المنزلية:** يجب أن تحتوي الشبكة المنزلية على كلمة مرور مشفرة قوية وأن يكون لها شبكة افتراضية خاصة"Virtual Private Network" .ويعنى وجود شبكة خاصة افتراضية أن يسمح لك بإنشاء اتصال آمن بشبكة أخرى عبر الإنترنت ، حيث يوفر استخدام VPN مزيدا من الأمان للشبكات الخاصة والعامة.((**Tabassum**,2020,p3)
- التشفير: من الضروري عند تخزين البيانات في الخوادم أن تكون في شكل مشفر بحيث لا يمكن للخصم فك تشفير البيانات المشفرة دون امتلاك المفتاح السري ، حيث يمكن للمرء استخدام إما تشفير المفتاح المتماثل مثل(معيار تشفير البيانات الثلاثي ([31] (DES3) ومعيار التشفير المتقدم ([32] (AES)) ،أو آلية تشفير المفتاح العام على سبيل المثال تشفير المنحنى الإهليلجي ([33] (ECC) , RSA).
- وعى وتدريب المستخدمين: حيث يجب تأهيل المستخدمين وتوعيتهم وتدريبهم على استخدام نظم المعلومات التي تتمتع بمزايا الأمن والسرية؛ لما لذلك من أهمية في الحفاظ على أمن المعلومات وسريتها وحماية المستخدمين أنفسهم من الوقوع في المحظور دون قصد، وعلى المؤسسة وضع التوجيهات الكافية لضمان وعي عام ودقيق بمسائل الأمن، بل أن المطلوب بناء ثقافة الأمن لدى العاملين ، كما أن عليها تحديد ما يتعين على المستخدمين القيام بها وما يحظر عليهم القيام بها في معرض استخدام للوسائل التقنية المختلفة.(**الصحفى،عسكول2019،ص15**)

5. العوامل المؤثرة على كفاءة عملية المراجعة:

هناك العديد من العوامل التى تؤثر على كفاءة أداء عملية المراجعة مثل:

- **التخطيط:** يعتبر التخطيط هو الخطوة الأولى التي يمكن أن تساعد في تحسين كفاءة عملية المراجعة ، ويتضمن تخطيط المراجعة صياغة المبادئ التوجيهية المحددة التي يجب اتباعها عند إجراء المراجعة الفعلية ،حيث يساعد في القضاء على أي مخاطر وتكاليف غير ضرورية وسوء فهم أثناء عملية المراجعة .

وعند التخطيط تحتاج إلى النظر في طبيعة وتوقيت المراجعة مما يساعد المراجع على التعاون مع العميل بطريقة منظمة ، وقضاء وقت أقل ، وبالتالي تحسين كفاءة عملية المراجعة(**Allinson,2021**)

ويجب أخذ العديد من العوامل في الاعتبار عند التخطيط للمراجعة ، مثل :

- المخاطر: تحديد المخاطر المرتبطة بمجال المراجعة مثل المخاطر المالية , والتشغيلية , الأمنية , الاستراتيجية أو المتعلقة بالسمعة .
- إجراءات الاختبار: تطوير إجراءات اختبار شاملة لاختبار الضوابط المطبقة، على سبيل المثال ، فيما يتعلق بخطر اختراق البيانات السرية، تأكد من اختبار الضوابط مثل الوصول (أي الأفراد المصرح لهم فقط من الوصول) والأمن (أي يتم تشفير البيانات السرية).

- الهدف والنطاق: إعداد وتوزيع وثيقة الهدف والنطاق للمراجعة، يمكن أيضًا الإشارة إلى هذا المستند باسم مذكرة التخطيط النهائية وتعمل وثيقة الهدف والنطاق هذه كمحور تركيز المراجعة**(Uniyal,2022)**

- خبرة ومستوى تعليم المراجع:يمكن أن تكون الكفاءة مرتبطة بقدرة الفرد على أداء الوظيفة أو المهمة بشكل صحيح على أساس مستوى التعليم والخبرة المهنية ،وجهود الموظفين والتطوير المهني المستمر. وتساهم الكفاءة في تحسين فعالية المراجعة الداخلية من خلال قدرة المراجعين على أداء وظيفة المراجعة الداخلية بعمليات عالية الجودة**(Zaidan, Neamah,2022,p.6-7)**

وتعنى خبرة المراجع متوسط عدد السنوات فى مجال المراجعة وعدد المهمات السابق إنجازها والتى تعد مؤشر جيد على اتخاذ القرارات المهنية المرجوة |،كما يتطلب معيار المراجعة الدخلية الدولى رقم (1210) الخاص بالكفاءة المهنية للمراجعين الداخليين أن يمتلكوا المعرفة والمهارة والكفاءات الأخرى المطلوبة لأداء مسئولياتهم الفردية**(أحمد،2019،ص.19)**

وبالإضافة إلى التعليم المناسب والخبرة العملية يجب أن يحصل المراجع الجيد على تدريب إضافي في مجال مناسب ؛حيث يحتاج المراجع إلى مهارات تواصل جيدة ومهارات قيادية ، إدارة المشاريع المختلفة والاستعداد جيدًا للبرامج المختلفة التي قد تكون لدى شركات المراجعة، لهذا السبب فإن السعي وراء التدريب يلعب دورًا مهمًا في مهنة المراجعة ويمكننا القول أن التدريب هو عامل محفز هام**(fetai, mjaku,2020,p.6)**

- ضغط ميزانية الوقت وكفاءة المراجعة:يبحث المراجعون دائمًا عن طرق جديدة لجعل المراجعة أكثر فعالية وكفاءة ، وعمليات المراجعة بطبيعتها تستغرق وقتًا طويلاً ومكثفة، و بغض النظر عن الحجم كلما زاد الوقت الذي يقضيه المراجعون في المهام الشاقة والمتكررة إلى حد كبير قل الوقت المتاح لهم لإنفاقه على مهام أكثر قيمة واستراتيجية تتطلب رؤية بشرية(**Association of international certified professional Accounatants,2019)**

وبالتالى يعتبرضغط ميزانية الوقت هو موقف يُطلب فيه من المراجعين إكمال المراجعة في الوقت المحدد والمطالبة بأن يؤدي المراجع كفاءة زمنية مقابل الميزانية الزمنية التي تم إعدادها .

والميزانية الزمنية هي تقدير للوقت المخصص لإنجاز مهام وأنشطة المراجعة ،حيث يتم إعداد ميزانية زمنية مفصلة لكل مرحلة من مراحل عملية المراجعة، وهي بمثابة الأساس لحساب تكاليف المراجعة وتقييم المراجع للنتائج و يعد طريقا لتقييم الأداء للمراجعين(**aswar,et.al**,2021,P.5). ويمكن ضغط الوقت في إجراء عمليات المراجعة المراجع من تحسين الكفاءة في المراجعة بحيث لا تعتمد عملية المراجعة التى يقوم بها المراجع دائمًا على الإجراءات والتخطيط وفقًا للوائح المعمول بها، حيث يُطلب من المراجعين في إجراء عمليات المراجعة أن يكونوا قادرين على إكمال عملهم في الوقت المحدد وفقًا للوقت المتفق عليه مع عميل**(Raditya,2020,p.2)**

- رسوم المراجعة:تعتبر رسوم المراجعة عامل اخر يمكن أن يؤثر على المراجعين فى تحسين جودة ادائهم لواجباتهم، وهى تعنى جميع التكاليف التى تدفعها الشركات لمراجعى الحسابات لخدمات المراجعة وغير المراجعة والتي تتكون من الرواتب ومزايا الموظفين مثل العمل الميداني، ونفقات السفر والتكاليف الأخرى المطلوبة لعمليات المراجعة وما يتصل بها. عادة ما يتم تحديد رسوم المراجعة من قبل بدء عملية المراجعة ويتم تحديدها عند إبرام عقد بين المراجع والعميل.

ويمكن القول أن رسوم المراجعة هي عدد خدمات المراجعة التي يتلقاها المراجع من خلال النظر في مخاطر المهمة والتعقيدات المختلفة والمهارات المطلوبة**(kartini,yolanda,2021,p.2)** ومن الممكن العمل على خفض رسوم المراجعة إذا كان هناك تعاون وتنسيق بين المراجعة الداخلية و الخارجية ، بحيث يمكن أن ينتج عمليات مراجعة عالية الجودة ويكون لها فوائد اقتصادية وبالتالي، يمكن للمراجعين الخارجيين الاعتماد على عمليات المراجعة الداخلية أو المشاركة فيها إذا كانت المراجعة

الداخلية تتمتع بموضوعية وكفاءة كافيين مما يساهم فى توفير الجهد والوقت والتكاليف(**Zaidan, Neamah,2022,p.6**)

- **التنسيق والتعاون بين المراجع الداخلى والخارجى:**لقد أصدرت العديد من المنظمات والهيئات المهنية المنظمة لمهنة المراجعة عدة معايير تهتم بإرشاد المراجع الخارجي عند اعتماده على عمل المراجع الداخلي، كالمعيار الأمريكي رقم(65) الصادر عن معهد المحاسبين القانونين الأمريكي بعنوان" اعتبارات المراجع الخارجي عن كيفية تأثير المراجعة الداخلية على طبيعة وتوقيت ونطاق المراجعة الخارجية"، وكذلك معيار المراجعة الدولي رقم 610 والذي يتعلق بالاستفادة من عمل المراجعين الداخلين في عملية المراجعة الخارجية ، يتطابق معيار المراجعة الدولي رقم 610مع معيار المراجعة المصري رقم " 610دراسة عمل المراجعة الداخلية" ، وإرشاد الإنتوساى للحوكمة رقم " 9150 "التنسيق والتعاون بين الأجهزة العليا للرقابة المالية والمحاسبة والمدققين الداخليين في القطاع العام."، هذا ولا تقتصرعملية التنسيق والتعاون على تبادل الخطط والتقارير ومذكرات الإدارة المتعلقة بعملية المراجعة فحسب، بل تمتد لتشمل أيضا العمل المشترك في وضع الخطط وتبادل البرامج والمستندات المتعلقة بمراجعة كل جهة ، وعقد اجتماعات منتظمة ، وتقاسم التدريب، دون أن يمس ذلك مبدأ استقلالية كل جهة**(محمد،2019،ص.27-28)**

- **التقنيات التكنولوجية الحديثة:**إن زيادة الاعتماد على التكنولوجيا واستخدام الأساليب والأدوات الحديثة للمراجعة وتحليل البيانات في تخطيط وتنفيذ مهام المراجعة يساهم في الوصول إلى استنتاجات أفضل ويقلل من تكاليف أداء أنشطة المراجعة، ويستبعد الأنشطة التي لا تضيف قيمة للمؤسسة، وتمكين المراجعين من توسيع خدماتهم الاستشارية، كما أن استخدام الأساليب والأدوات الحديثة في المراجعة يحقق العديد من المزايا :

- زيادة سرعة وكفاءة عملية المراجعة.
- سهولة التعرف على نماذج البيانات واتجاهاتها والعلاقات فيما بينها، والقدرة على مراقبة المخاطر.
- توفير الوقت والجهد، وتقليل عدد المراجعين اللازمين لتنفيذ عملية التدقيق البرامج.
- زيادة إنتاجية فريق المراجعة، وزيادة جودة الخدمات متاح.
- تطوير الخدمات التي تقدمها مكاتب المراجعة والمحافظة على مكانتها التنافسية وزيادة حصتها في السوق.

6. العلاقة التكاملية بين الأمن السيبرانى والمراجعة

تحتاج تقدم مهنة المراجعة إلى التكامل مع التكنولوجيا للمساعدة في تحسين جودة أداء المراجعة وجعلها أكثر تقدمًا ودقة وموثوقية، حيث وجد أن أكبر خطر يواجهه المراجعون في عشرينيات القرن الحادي والعشرين هو أمن البيانات والأمن السيبراني، ومن خلال اعتماد إطارالمعهد الوطنى للمعايير والتكنولوجيا (NIST)للأمن السيبراني كعنصر من عناصر مراجعة المخاطر ووضع إطار عمل للأمن السيبراني يمكن تحسين أداء المراجع ليكون أكثر انفتاحًا على المخاطر المتعلقة بعملية التكنولوجيا.

(kurniawan, mulyawan,2023,p1,8)

وبما أن التقارير المالية هي المنتج النهائي لعلم المحاسبة في المنظمات فإن تلك التقارير يجب أن تكون دقيقة وأن تتميز بجودة وكفاءة عالية، حيث تعمل العديد من المنظمات ذات الصلة على تحديد المخاطر التي تؤثر على كفاءة إعداد تقاريرها المالية والعمل على حلها مثل مخاطر الأمن السيبراني، وبالتالي فإن معظم المنظمات تولى اهتمامًا كبيرًا بالأمن السيبراني نظرًا لأهميتها الكبيرة في ضمان عدم التلاعب بالبيانات المالية أو حذفها وبالتالى ؛ نجد أن للأمن السيبرانى تأثير واضح على التقارير المالية حيث يعزز من كفاءتها من خلال العمل على حفظها ومنع التلاعب بها عن طريق:

-الحفاظ على المعلومات والبيانات الأساسية للمنظمة من التلاعب والسرقة والقرصنة.
- حماية الأجهزة التي يستخدمها المحاسبون من الاختراق والقرصنة.
- .الاحتفاظ بنسخ احتياطية للبيانات خالية من القرصنة والعبث.
-حماية التقارير المالية النهائية من الاحتيال والتلاعب بعد نشرها إلكترونيًا.

- توفير الموارد البشرية العاملة في إعداد التقارير المالية(albayati, 2022, p.1, 6)

وبالتالى يمكن توضيح العلاقة بين الأمن السيبرانى والمراجعة وكيف يمكن أن يكون لتقنيات الأمن السيبرانى دور فى كفاءة عملية المراجعة من خلال شرح تفصيلى للعلاقة بين الأمن السيبرانى والمراجعة الداخلية ولجان المراجعة والمراجعة الخارجية وذلك كما يلى:

- **الأمن السيبرانى والمراجعة الداخلية:**

فى ظل العصر الرقمى الحالى نجد تطور وتحول سريع فى مهنة المراجعة الداخلية، حيث يعتبر أحد المحركات الرئيسية لهذا التحول هو الأمن السيبرانى؛ حيث إنه مع تزايد اعتماد المؤسسات على البنية التحتية والبيانات الرقمية أصبحت المخاطر المرتبطة بالتهديدات السيبرانية مصدر قلق كبيرمما جعل موضوع الأمن السيبرانى في طليعة وظائف المراجعة الداخلية مما ترتب عليه إعادة تشكيل استراتيجياتها ومنهجياتها ومتطلباتها من المهارات.

وهنا يظهر دور المراجعة الداخلية فيما يتعلق بإدارة المخاطر السيبرانية والحد من تلك المخاطر، حيث يجب على مدير إدارة المراجعة تقديم النصح والإرشاد لمجلس الإدارة بصدد تحديد وتوصيف وقياس مخاطر الأمن السيبرانى المحيطة ببيئة أعمال المنشأة التكنولوجية وكيفية مواجهتها والحد من اثارها بما يدعم تحقيق أهداف المنشأة.(أمير هم،2022،ص.17)

ويمكن ايضا تقديم الاستشارة والنصح عن طريق القيام بالتحديث والمتابعة الدورية لمختلف مخاطر الأمن السيبرانى ، فضلا عن وضع وتطوير الإطار المستند عليه فى عملية إدارة مخاطر الأمن السيبرانى ومساعدة إدارة الشركة في وضع توصيات بشأن كلا من الحد الأدنى المقبول لمستوى مخاطر الأمن السيبرانى وكيفية تحسين عمليات إدارة المخاطر فى ذلك الصدد، والمقترحات اللازمة لمواجهة مخاطر الأمن السيبرانى وتفاديها والاستجابة السريعة لها.

كما يمكن ايضا بلورة الدور التوكيدى في مجال إدارة مخاطر الأمن السيبرانى والذى يرتكز في الأساس على قيام مدير إدارة المراجعة الداخلية بتقديم تقرير بشأن مدى صدق التقارير المعدة من قبل المسئولين عن إدارة مخاطر الأمن السيبرانى بالشركة ويشمل: التقرير عن مدى فاعلية تصميم وتشغيل عميلة إدارة مخاطر الأمن السيبرانى، التقاريرالمعدة من قبل المسئولين عن عملية إدارة مخاطر الأمن السيبرانى (كالتقرير عن كيفية تحديد وتقييم وإدارة مخاطر الأمن السيبرانى الجوهرية، والتقرير عن كيفية تحديد وتقييم وإدارة مخاطرالأعمال الرئيسية خاصة فيما يتعلق بالأمن السيبرانى،)، التقرير عن تنفيذ الاستراتيجيات الموضوعة لإدارة مخاطر الأمن السيبرانى التى حدثت بالفعل، وأخيرا التقرير عن تحديد وتقييم مخاطر عدم وفاء الشركة بمتطلبات الالتزاماتها التعاقدية خاصة فيما يتعلق بالعقود الذكية فى ظل بيئة التحول الرقمى.(شحاته،2022،ص.9)

وفى سياق متصل، تعمل جودة المراجعة الداخلية على تمكين إدارات المنشأت من تصميم خطوط دفاع قوية لمواجهة مخاطر الأمن السيبرانى طبقا لطبيعة واحتياج البيئة التكنولوجية ونوعية وكثافة المخاطرالتي تواجه المنشأة والتي تتمثل في :

- تقييم الوعى بالأمن السيبراني : والذى يتمثل في تحديد الفجوات في الوضع الحالي للأمن السيبراني، هذا علاوة على فهم محددات وأبعاد نقاط الضعف المطلوب التركيز عليها .

-مراجعة التكنولوجيا الجديدة :حيث تقدم منصات التكنولوجيا الناشئة والتي تضم (السحابة ،والشبكات الاجتماعية ،والجوال ،والبيانات الضخمة وأنظمة الذكاء الاصطناعي وغيرها) مخاطر الكترونية جديدة تستدعي القيام بعمليات مراجعة خاصة تشتمل على مراجعة عنصر الأمان قبل وبعد تنفيذ التكنولوجيا الجديدة.(أمير هم،2022،ص.17)

ويمكن توضيح كيفية تعامل المراجعة الداخلية مع الهجمات السيبرانية فى كل مرحلة من المراحل التالية كما يلى:

- **مرحلة الحماية:** تساعد المراجعة الداخلية فى هذه المرحلة من خلال العمل مع إدارة المنظمة وإدارة المخاطر فى تطوير برنامج حوكمة تكنولوجيا المعلومات، ويتضمن استراتيجيات وسياسات الأمن السيبرانى الخاصة بالمنظمة، وتقييم واختبار مخاطر الأمن السيبرانى وتقييم خطط الأمن السيبرانى ومدى فعاليتها فى الحد من هذه المخاطر.
- **مرحلة الكشف عن المخاطر:** تقوم المراجعة الداخلية فيها بتقييم ضوابط الرقابة على الأمن السيبرانى ، وتقدم تقاريرها إلى الإدارة التنفيذية ولجنة المراجعة حول فعالية هذه الضوابط والتهديدات المحتملة ، والتحقق من فعالية الإجراءات المطبقة للكشف عن أية مخاطر.
- **مرحلة استمرار النشاط:** حيث تساعد المراجعة الداخلية فى تقييم برامج الاستجابة للمخاطر السيبرانية، وبرامج استمرار النشاط للصمود ضد الهجمات السيبرانية ، كما تساعد فى التحقق من توافر إجراءات وخطط بديلة فعالة لاستمرار النشاط فى حالة وقوع هجوم سيبرانى.
- **مرحلة رد الفعل:** تقييم دى ملاءمة طرق الاستجابة للمخاطر التى اتبعتها إدارة المنظمة؛ حيث تحتاج منظمات الأعمال لإعداد برنامج لإدارة الأزمة كأحد أجزاء إدارة استمرار النشاط ، ويعد تقييم المخالفات والثغرات وإيجاد طرق الاستجابة المناسبة لها هى الخطوة الأولى فى التعامل مع الهجمات السيبرانية.
- **مرحلة التطوير:** تضيف المراجعة الداخلية فى هذه المرحلة قيمة عالية من خلال إبداء الرأى فى كل من النشاط بشكل كامل وإجراءات الأمن المتبعة ، واستراتيجيات التعامل مع المخاطر واقتراح التحسينات اللازمة لضمان الاستعداد لأية هجمات سيبرانية.(على ،2023،ص15)

هذا ومع استمرار تطور التهديدات السيبرانية فإن دور المراجعة الداخلية سيتطور أيضًا؛ حيث سيحتاج المراجعون إلى مواكبة أحدث اتجاهات الأمن السيبراني ونواقل التهديد، وسيحتاجون أيضًا إلى العمل بشكل وثيق مع فرق تكنولوجيا المعلومات والأمن السيبراني في مؤسستهم لفهم ملف تعريف المخاطر السيبرانية للمؤسسة وتوفير ضمانات بشأن فعالية ضوابط الأمن السيبراني الخاصة بها.

هذا بالإضافة إلى التأكيد على أن التحول نحو الأمن السيبراني سوف يؤدى إيضا إلى تغيير مجموعة المهارات المطلوبة للمراجعين الداخليين ؛ حيث بالإضافة إلى فهم المخاطر المالية والتشغيلية يجب أن يكون لدى المراجعين الداخلين الآن فهم قوي لتكنولوجيا المعلومات، ومخاطر الأمن السيبراني، ولوائح خصوصية البيانات، يتضمن ذلك فهم الجوانب الفنية للأمن السيبراني، مثل أمن الشبكات والتشفير وأنظمة كشف التسلل.

وبالتالى يظهر تأثير الأمن السيبراني على مستقبل عمليات المراجعة الداخلية، حيث حول دور المراجعة الداخلية من التركيز المالي والتشغيلي التقليدي إلى دور أوسع يشمل توفير الضمانات بشأن مخاطر الأمن السيبراني، وهذا التحول ليس ضروريًا فحسب، بل يمثل أيضًا فرصة للمراجعين الداخليين للعب دور حاسم في تعزيز وضع الأمن السيبراني لمؤسساتهم .**(Baidoo,2023)**

- **<u>الأمن السيبرانى ولجان المراجعة:</u>**

يمكن أن تختلف درجة مشاركة لجنة المراجعة في قضايا الأمن السيبراني بشكل كبير حسب الصناعة والأعمال،ففي بعض المنظمات يتم إسناد مهمة إدارة تهديدات الأمن السيبراني إلى لجنة المراجعة مباشرة، في حين يتم تشكيل لجان منفصلة للمخاطر من قبل منظمات أخرى للتعامل معها، حيث أن الشركات التي تعتمد بشكل كبير على التكنولوجيا في عملياتها التجارية غالبًا ما تنشأ لجنة مخصصة للأمن السيبراني تركز فقط على الأمن السيبراني، ومع ذلك و بغض النظر عن الهيكل الرسمي المعتمد؛ فإن النمو السريع في اعتماد التكنولوجيا وتوليد البيانات إلى جانب المخاطر التي ينتج عنها عمليات الخروقات الأمنية، يظهر مدى أهمية فهم الأمن السيبراني باعتباره مطلبا تجاريًا جوهريًا على مستوى المؤسسة.

وبالتالى ؛ من الضروري أن تكون لجان المراجعة على دراية بالاتجاهات الحديثة للأمن السيبراني فضلاً عن التهديدات والمخاطر السيبرانية الرئيسية التي تهدد الأعمال، ويرجع ذلك إلى حقيقة أن المخاطر المتعلقة بالتطفل وانتهاكات البيانات يمكن أن تؤدي إلى عواقب اقتصادية وتجارية

واقتصادية شديدة تؤثر على أصحاب المصلحة بطريقة كبيرة ، كما ستساعد المناقشات والتفاعلات المنتظمة مع قادة الأعمال الذين يركزون على التكنولوجيا لجنة المراجعة على فهم الجوانب المتعلقة بالأمن السيبرانى بشكل أفضل ، وتشمل بعض الجوانب التي يجب أن تأخذها لجان المراجعة في الاعتبار لمناقشتها مع فريق الإدارة فيما يتعلق بالأمن السيبراني ما يلي :

- الخطة الشاملة والاستراتيجية لحماية الأصول .
- قوة الاستجابة للحوادث وخطط الاتصال الخاصة بالمنظمة .
- الأصول الهامة التي سيتم تأمينها.
- نقاط الضعف والمخاطر التي تم تحديدها.
- الضوابط الموضوعة لمراقبة الموردين والشبكات السحابية، إلى جانب البرامج التي تعمل على الأجهزة.
- تدريب وخبرة الموظفين في التنبؤ بالتهديدات السيبرانية.
- إمكانية الوصول إلى معلومات وبيانات الشركة.

هذا بالإضافة إلى مسؤولية لجنة المراجعة من التأكد من قدرة المراجع الداخلي على تطوير خارطة طريق للمستقبل من أجل التعامل مع التهديدات والمواقف المختلفة للأمن السيبراني ، ولذلك، تلعب لجنة المراجعة دورًا حيويًا في استراتيجيات الأمن السيبراني للمؤسسة.**(Jadhav,2023,p.4)**

- **<u>الأمن السيبرانى والمراجعة الخارجية:</u>**

مما لاشك فيه أن المراجع الخارجى مطالب بتحديد وتقييم مخاطر التحريف الجوهري في البيانات المالية ، وذلك من خلال فهم المنشأة وبيئتها بما في ذلك الرقابة الداخلية للمنشأة، ومن خلال الفهم المتعمق لأعمال وبيئة الكيان (بما في ذلك تكنولوجيا المعلومات الخاصة بالكيان والبيئة الإلكترونية) فإنه يمكّن للمراجع تحديد المخاطر وتصميم وتنفيذ استجابات مراجعة مناسبة لمعالجة تلك المخاطر المحددة, كما أن الشركات التى تتعرض لهجمات إلكترونية تتكبد تكاليف باهظة وتتعرض لأضرار جسيمة ؛لذلك يجب على المراجع فهم طبيعة وسبب الحادث والنظر بعناية في التكاليف وأي عواقب سلبية تنشأ عن الحادث السيبراني وتقييم التأثير على البيانات المالية، و تقييم تأثير الهجوم على الإيرادات المستقبلية للكيان وتكاليف حماية الأمن السيبراني والتدفقات النقدية المستقبلية**(Nexia-Sabt&T,2018)**

هذا و يتطلب معيار المراجعة رقم (12) لمجلس الرقابة المحاسبية من المراجع صراحة الحصول على فهم لكيفية استخدام تكنولوجيا المعلومات , تأثير تكنولوجيا المعلومات على البيانات المالية، تقييم تهديدات الأمن السيبرانى فى نموذج مخاطر المراجعة الخاصة بهم , مراجعة الرقابة الداخلية على إعداد التقارير المالية وتقييم مخاطر التحريف الجوهرى الناتج عن الوصول الغير مصرح به إلى الأنظمة, كما يخضع المراجعون الخارجيون لضغوط متزايدة من المنظمين وواضعى المعايير فيما يتعلق بالأمن السيبراني على سبيل المثال, أبرز مركز جودة المراجعة مرارا وتكرار حقيقة أنه يجب على المراجعين إيلاء اهتماما خاصا لهذه الأنواع من الحوادث وأن المراجعين يمكنهم لعب دورا مهما فى منع أو التخفيف من آثار هذه الحوادث من خلال ضمان اضافى حول ضوابط تكنولوجيا المعلومات لعملائها ,كما زادت لجنة التبادل الأمنى من متطلبات الإفصاح الخاصة بها فيما يتعلق بالأمن السيبرانى, وأكد تقرير مجلس مراقبة حسابات الشركات العامة أن الأمن السيبرانى يمثل خطرا متطورا للمراجعين ويتطلب تركيزا مستمرا**(Rosati,Et.Al,2019,p.5-6)**

هذا و سواء وقع حادث إلكتروني أم لا، فإنه يجب على المراجع أثناء عملية التخطيط إجراء تقييم للمخاطر، ويجب أن يأخذ هذا التقييم في الاعتبار أي مخاطر محتملة تتعلق بالأمن السيبراني يكون لها تأثير جوهري على البيانات المالية للشركة، وهو ما يترتب عليه زيادة رسوم المراجعة استجابةً لمخاطر

الأمـــن الســـيبراني للعميـــل والطريقـــة التـــي يـــتم بهـــا معالجـــة تلـــك المخـــاطر والكشـــف عنها.**(Calderon,Gao,2020,p.3)**

حيث إنه فيما يتعلق برسوم المراجعة ؛ فعادةً يتم تحديدها من خلال مقدار العمل الذي يجب على المراجع القيام به (أي جهد المراجعة) ومخاطر المراجعة, وهي دالة لعاملين أولا:خطر التحريف الجوهري وهو خطر أن البيانات المالية محرفة بشكل جوهري قبل المراجعة ، ثانيا: مخاطر الكشف وهي مخاطر عدم اكتشاف المراجع للتحريفات الفردية أوالمجمعة ، وبالتالى فإن المراجعين يتصدون للزيادة في مخاطر التحريف الجوهري من خلال زيادة جهودهم في المراجعة لتقليل مخاطر الكشف مما يؤدي إلى زيادة رسوم المراجعة**(Rosati,Et.Al,2019,p.10)**, ونظرا لان الشركات التى تتعرض لحوادث الأمن السيبرانى تتزايد فيها معدلات الخطر فهناك علاقة حول تأثير حوادث الأمن السيبراني على استجابة المراجعيين الخارجيين من خلال رسوم المراجعة ،حيث تم إكتشاف أنه بيتم فرض رسوم مراجعة أعلى على الشركات التى تتعرض لقرصنة الأمن السيبرانية**(Ngo,Tick,2021,p.5)**

ثالثاً: الدراسة الميدانية لاختبار "أثر استخدام تكنولوجيا الأمن السيبراني على كفاءة أداء عملية المراجعة"

1. أهداف الدراسة الميدانية:

تهدف الدراسة الميدانية إلى دعم ما توصلت إليه الباحثة من نتائج نظرية حتى يمكن استخلاص بعض الأدلة العملية التي تساهم في تحقيق أهداف الدراسة والتي تتمثل أهمها في استطلاع آراء مفردات العينة حول بعض متغيرات الدراسة تمهيداً لاختبار مدى صحة الفرض التالي:

"لا توجد علاقة ذات دلالة احصائية بين تكنولوجيا الأمن السيبراني وكفاءة أداء عملية المراجعة"

2. أداة جمع البيانات:

اعتمدت الباحثة في جمع البيانات اللازمة لإجراء الدراسة الميدانية على أسلوبين هما:

الأسلوب الأول: المقابلة الشخصية:

لجأت الباحثة إلى أسلوب المقابلة الشخصية من خلال إجراء العديد من المقابلات الشخصية مع بعض مفردات العينة لاستطلاع آرائهم والإجابة على استفساراتهم حول أهداف الدراسة والاستفادة من آرائهم في تعديل تصميم أسئلة قائمة الاستقصاء كأحد الأساليب الرئيسية للحصول على البيانات وذلك للتأكد من مدى وضوحها وشمولها وسهولة فهمها من قبل المستقصي منهم.

الأسلوب الثاني: قائمة الاستقصاء:

اعتمدت الباحثة على أسلوب قائمة الاستقصاء كأحد الأساليب الرئيسية للحصول على البيانات الأولية اللازمة للدراسة، حيث تم إعداد تلك القائمة في شكل أسئلة يمكن من خلال دراسة وتحليل استجابات مفردات العينة تجاهها استخلاص البيانات التي يمكن استخدامها في قياس متغيرات الدراسة تمهيداً لاختبار الفروض التي استندت إليها.

وقد تم تصميم قائمة الاستقصاء في ضوء مجموعة من الاعتبارات التي تساهم في تحقيق أهداف الدراسة الميدانية تتمثل أهمها فيما يلي:

- عرض الأسئلة بشكل مبسط وواضح، مما يجعلها قابلة للفهم من قبل مفردات العينة.
- صياغة الأسئلة بشكل يساهم في تغطية متغيرات الدراسة على نحو متكامل.

وقامت الباحثة بتقسيم قائمة الاستقصاء إلى قسمين أساسيين وهما:

- **القسم الأول:** يحتوي على بعض الخصائص الديموغرافية لمفردات العينة كالمؤهل العلمي والمسمى الوظيفي وسنوات الخبرة، وذلك للاطمئنان على مستوى القائمين بملىء استمارة الاستقصاء.

- **القسم الثاني:** يحتوي على مجموعة من الأسئلة التي يمكن من خلالها قياس متغيرات الدراسة، حيث تم صياغتها على نحو يغطي عدة جوانب تعبر عن تلك المتغيرات، وتتمثل في الأسئلة التالية:
  - **السؤال الأول (أهداف تكنولوجيا الأمن السيبراني):** هدفت الباحثة من خلال هذا السؤال إلى استطلاع آراء فئات الدراسة حول الأهداف التي تحققها تكنولوجيا الأمن السيبراني كالتصدي لمخاطر أمن المعلومات والحماية من الهجمات الإلكترونية.
  - **السؤال الثاني (العوامل التي تؤثر على كفاءة أداء عملية المراجعة):** وكان الهدف منه التعرف على أهم العوامل التي تساهم في زيادة كفاءة عملية المراجعة وخاصة تلك المتعلقة باستخدام التقنيات التكنولوجية الحديثة لما قد توفره من انعكاسات إيجابية على إجراءات عملية المراجعة.

وقد اعتمدت الباحثة في تصميم أسئلة القسم الثاني من قائمة الاستقصاء على نظامين هما:

- **نظام الأسئلة ذات النهاية المغلقة (الاستقصاء المغلق):**

من خلال تحديد مجموعة من الإجابات المحتملة للأسئلة يختار المستقصي منه من بينهم، وقد أعتمد الباحث على نظام الاستقصاء المغلق لما يتميز به من سهولة الترميز، وإمكانية الثقة فيه بصورة أكثر لشموله على أسئلة يسهل إدارتها وفهمها من قبل فئات المستقصي منهم، كما أنه يحتوي على إجابات محددة لتلك الأسئلة.

- **نظام الأسئلة ذات النهاية المفتوحة:**

وذلك لإعطاء المستقصي منهم مجالاً لأي إضافات يرونها هامة فيما يتعلق بمتغيرات الدراسة والتي تضفي مزيد من الأهمية على الدراسة.

كما تم استخدام مقياس ليكرت (Likert) المتدرج ذي الخمس نقاط لتحديد وترميز إجابات أفراد العينة، حيث يختار المستقصي منه إجابة من خمس إجابات يكون لكل منها وزن رقمي (أهمية نسبية) يمكن بيانها على النحو التالي:

الإجابات	غير موافق تماماً	غير موافق	محايد	موافق	موافق تماماً
أوزان الإجابات	(1)	(2)	(3)	(4)	(5)

3. مجتمع وعينة الدراسة:

1/3. مجتمع الدراسة:

تحقيقاً لأهداف الدراسة الميدانية، قامت الباحثة بتحديد مجتمع الدراسة في فئتين من المعنيين بمهنة المراجعة بمحافظتي القاهرة والسويس وهم:

- **الفئة الأولى: المراجعون الخارجيون بمكاتب المراجعة،** وتم الاعتماد عليهم لما يمتلكون من خبرة عملية ودراية بأهم العوامل التي تساهم في تحسين كفاءة أداء عملية المراجعة، مما يجعل لآرائهم بالغ الأثر في التوصل إلى نتائج تتسم بالدقة والموضوعية حول أثر استخدام تكنولوجيا الأمن السيبراني على كفاءة عملية المراجعة.
- **الفئة الثانية: المراجعون الداخليون بالشركات الصناعية،** باعتبارهم أن طبيعة عملهم تجعلهم على وعي وإدراك بالتقنيات التكنولوجية الحديثة وانعكاساتها المختلفة على أدائهم المهني ومن ثم على كفاءة أداء عملية المراجعة، وبالتالي ستنعكس آرائهم إيجابياً على نتائج الدراسة.

2/3. عينة الدراسة:

نظراً لصعوبة استقصاء جميع مفردات مجتمع الدراسة نتيجة عامل الوقت والجهد والتكلفة، فضلاً عن صعوبة حصر جميع مفردات المجتمع اعتمدت الباحثة على أسلوب العينة العشوائية الحكمية في الحصول على البيانات اللازمة من خلال توزيع قائمة الاستقصاء على عدد من المفردات الممثلة لكل فئة من فئات الدراسة بشكل تحكمي، وقد روعي في هذه العينة أن تكون ممثلة للمجتمع محل الدراسة وأن تنطبق عليها المواصفات المطلوبة لأغراض الدراسة، لذا قامت الباحثة بتوزيع (95) قائمة على الفئة الأولى من المراجعين الخارجيين، و(77) قائمة على الفئة الثانية من المراجعين الداخليين بإجمالي (172) قائمة، وتم توزيع تلك القوائم من خلال المقابلة الشخصية وكذلك الوسائل الإلكترونية، وكانت الاستجابة جيدة من قبل مفردات العينة حيث بلغ عدد الاستجابات الواردة (155) قائمة بنسبة (90.1%) وتم استبعاد (11) قائمة منها لعدم صلاحيتها بسبب عدم استكمال البيانات، ومن ثم تم الاعتماد في إجراء التحليل الإحصائي اللازم على عدد (144) قائمة من الاستجابات الصحيحة بنسبة (92.9%)، كما هو موضح بالجدول التالي:

جدول (1)
استجابات فئات الدراسة

فئات الدراسة	عدد الاستمارات الموزعة	الاستمارات الواردة		الاستمارات المستبعدة		الاستمارات الصحيحة	
		العدد	النسبة	العدد	النسبة	العدد	النسبة
المراجعون الخارجيون	95	86	%90.5	7	%8.1	79	%91.9
المراجعون الداخليون	77	69	%89.6	4	%5.8	65	%94.2
الإجمالي	172	155	%90.1	11	%7.1	144	%92.9

4. الأساليب الإحصائية المستخدمة:

قامت الباحث بتفريغ بيانات قوائم الاستقصاء الصحيحة تمهيداً لتحليلها إحصائياً باستخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS, Version 26)، وذلك من خلال الاعتماد على الأساليب الإحصائية التالية:

- **معامل ارتباط ألفا كرونباخ (Cronbach's Alpha Correlation):** حيث يستخدم لتحديد قيمة معامل الثبات لأسئلة الاستقصاء، وذلك لتقييم مدى ثبات واعتمادية أو مصداقية المقاييس المستخدمة في الدراسة، ومن ثم تحديد مدى إمكانية الاعتماد على نتائج قائمة الاستقصاء، وكذلك تحديد معامل الصدق الذاتي للعبارات الممثلة لأسئلة الاستقصاء لتحليل ثبات الاتساق الداخلي لاستجابات مفردات العينة والتأكد من عدم وجود تحيز أو تحريف في النتائج عند التحليل.
- **تحليل الانحدار البسيط (Simple Regression Analysis):** يتم الاعتماد على نموذج الانحدار البسيط لقياس مدى وجود علاقة بين متغيرين أحدهما مستقل والأخر تابع، وكذلك التعرف على اتجاه وقوة العلاقة بينهما.

5. نتائج التحليل الإحصائي واختبار فرض الدراسة:

1/5. تحليل الاعتمادية والمصداقية (اختبار الصدق والثبات):

اعتمدت الباحثة على استخدام معامل آلفا كرونباخ (Cronbach's Alpha) لتحديد معاملي الثبات والصدق الذاتي لعبارات قائمة الاستقصاء التي تعبر عن متغيرات الدراسة، وذلك لاختبار مدى مصداقية تلك العبارات وثباتها واتساقها

داخلياً ومن ثم إمكانية الاعتماد عليها في استخلاص نتائج الدراسة والتحقق من عدم وجود تحريف أو تحيز في تلك النتائج. فإذا زادت قيمة مقياس آلفا عن (0.6) أمكن الاعتماد على نتائج الدراسة وتعميمها على المجتمع. ويوضح الجدول (2) معاملي الثبات والصدق الذاتي لمتغيرات الدراسة على النحو التالي:

جدول (2)
اختبار الصدق والثبات لمتغيرات الدراسة

متغيرات الدراسة	رمز المتغير	عدد الفقرات	معامل الثبات (Alpha)	معامل الصدق الذاتي
تكنولوجيا الأمن السيبراني	X	7	0.732	0.856
كفاءة أداء عملية المراجعة	Y	7	0.624	0.79

يتضح من الجدول السابق أن معاملات آلفا كرونباخ لمتغيرات الدراسة تجاوزت الحد الأدنى المقبول ويبلغ (0.6)، حيث تراوحت بين (0.624) و(0.732)، كما تراوحت قيم معامل الصدق الذاتي بين (0.79) و(0.856)، مما يشير إلى ارتفاع مستوى اعتمادية ومصداقية الأسئلة المستخدمة للتعبير عن متغيرات الدراسة وارتفاع درجة الاتساق الداخلي بين محتوياتها ومن ثم إمكانية الاعتماد على هذه المتغيرات في إجراء الدراسة الميدانية وتعميم النتائج على مجتمع الدراسة.

2/5. اختبار فرض الدراسة:

"لا توجد علاقة ذات دلالة احصائية بين تكنولوجيا الأمن السيبراني وكفاءة أداء عملية المراجعة"

ولاختبار ذلك الفرض تم استخدام نموذج الانحدار البسيط (Simple Regression Model) الذي يستخدم لقياس وجود أو عدم وجود علاقة بين متغير واحد مستقل ومتغير واحد تابع، وذلك للتعرف على اتجاه وقوة العلاقة بين المتغير المستقل **(تكنولوجيا الأمن السيبراني "X")** والمتغير التابع **(كفاءة أداء عملية المراجعة "Y")**. ويوضح الجدول التالي رقم (3) أهم نتائج هذا التحليل:

جدول رقم (3)
نتائج تحليل الانحدار لاختبار فرض الدراسة
"لا توجد علاقة ذات دلالة احصائية بين تكنولوجيا الأمن السيبراني وكفاءة أداء عملية المراجعة"

المتغير التابع / المتغير المستقل	كفاءة أداء عملية المراجعة (Y)				
	قيمة معامل الانحدار (Beta)	T. Test		F. Test	
		القيمة	مستوى المعنوية (Sig)	القيمة	مستوى المعنوية (Sig)
تكنولوجيا الأمن السيبراني (X)	0.711	18.420	0.000	339.291	0.000
معامل الارتباط (R)					0.840
معامل التحديد (R^2)					0.705
مستوى الدلالة الإحصائية					0.05

درجات الحرية عند (F)	(142-1)

ويمكن تفسير نتائج هذا التحليل على النحو التالي:

- **القوة التفسيرية للنموذج:**
  - بلغت قيمة معامل الارتباط (R) (0.840)، الأمر الذي يشير إلى وجود علاقة طردية بين المتغير المستقل (تكنولوجيا الأمن السيبراني) والمتغير التابع (كفاءة أداء عملية المراجعة).
  - بلغت قيمة معامل التحديد (R^2) التي تدل على قوة العلاقة بين المتغير المستقل والمتغير التابع (0.705)، الأمر الذي يشير وجود علاقة ارتباط قوية بين المتغير المستقل والمتغير التابع، كما يشير أيضاً إلى أن تكنولوجيا الأمن السيبراني كمتغير مستقل تفسر 70.5% من التغير الكلي في المتغير التابع (كفاءة أداء عملية المراجعة)، وأن باقي النسبة (29.5%) قد ترجع إلى الخطأ العشوائي في المعادلة أو لعدم إدراج متغيرات مستقلة أخرى كان من المفترض إدراجها ضمن نموذج الانحدار.

- **المعنوية الكلية للنموذج:**
  - يتضح من اختبار (F Test) المستخدم لتحديد معنوية متغيرات نموذج الانحدار ككل، ارتفاع قيمة (F) المحسوبة وتبلغ (339.291) عن قيمة (F) الجدولية وتبلغ (3.91) عند درجات حرية (1)، (142) ومستوى المعنوية المقبول بالأدب المحاسبي (5%)، وأيضاً اقتراب مستوى المعنوية عند (F) من الصفر، الأمر الذي يشير إلى أن نسبة -الخطأ في قبول هذا النموذج تقترب من الصفر، وهذا يدل على أن نموذج الانحدار ذو دلالة إحصائية.
  - يتضح من اختبار (T Test) المستخدم لتحديد معنوية المتغير المستقل، ارتفاع قيمة (T) المحسوبة وتبلغ (18.42) عن قيمة (T) الجدولية (1.98) عند درجة حرية (143) ومستوى المعنوية المقبول بالأدب المحاسبي (5%)، وأيضاً اقتراب مستوى المعنوية عند (T) من الصفر، الأمر الذي يشير إلى أن المتغير المستقل معنوي التأثير على المتغير التابع.

مما سبق تخلص الباحثة إلى قبول الفرض البديل وهو:

توجد علاقة ذات دلالة احصائية بين تكنولوجيا الأمن السيبراني وكفاءة أداء عملية المراجعة

رابعا: النتائج والتوصيات:

1.نتائج الدراسة: توصلت الباحثة من خلال الدراسة النظرية والميدانية إلى مجموعة من النتائج يمكن توضيحها فيما يلى:

1/1. وجود العديد من الأهداف التى يسعى الأمن السيبرانى إلى تحقيقها من تطبيقه وتتمثل فى توفير بيئة آمنة وموثوقة للتعاملات في المجتمع ، صمود البنية الأساسية التحتية ضد الهجمات الإلكترونية، الحد من التجسس والتخريب الإلكترونى على مستوى الحكومة والأفراد وحماية المواطنين والمستهلكين على حدا سواء من المخاطر المحتملة في مجالات الأنترنت المختلفة .

2/1.تتعدد العوامل التى تساعد على زيادة كفاءة عملية المراجعة مثل: التخطيط والذى يتم من خلاله التعاون بين المراجع والعميل بطريقة منظمة وبالتالى قضاء وقت أقل وتكلفة أقل مما يعمل على تحسين كفاءة المراجعة، وخبرة المراجع ومستوى تعليمه، رسوم المراجعة ، التعاون بين المراجع الداخلى والخارجى بالإضافة إلى التقنيات التكنولوجية الحديثة والتى تساهم في زيادة سرعة وكفاءة عملية المراجعة.

3/1.أظهرت الدراسة النظرية والميدانية أن هناك ارتباط وعلاقة بين استخدام تكنولوجية الأمن السيبرانى وتحسين وزيادة كفاءة عملية المراجعة.

2.التوصيات: في ضوء النتائج التى تم التوصل إليها من خلال الدراسة النظرية والميدانية توصى الباحثة بما يلى:

1/2. زيادة اهتمام المنظمات والشركات والمؤسسات المالية بتطبيق تقنيات الأمن السيبرانى وذلك للحد من عمليات التخريب والهجمات الإلكترونية.

2/2.ضرورة العمل بشكل متعاون بين المراجعين وإدارة المخاطر وامن المعلومات في الشركات حتى يمكن توفير أقصى درجات الأمن والحفاظ على سرية المعلومات وعدم التلاعب.

3/2. مع التقدم السريع وزيادة وتنوع الأساليب التكنولوجية في العصر الحديث لابد من زيادة وعى جميع أفراد المجتمع بخطورة الأضرار التى تنتج من الاستخدام المتزايد للتكنولوجيا ومحاولة استخدام اساليب الأمن السيبرانى للحفاظ على أمن وسلامة جميع افراد المجتمع ويمكن تحقيق ذلك من خلال الاهتمام بالمجال التكنولوجي في المدارس والجامعات وعمل ندوات وابحاث علمية توضح مزايا ومخاطر التكنولوجية وكيف يمكن التقليل من تلك المخاطر.

قائمة المراجع

اولا: المراجع العربية:

- الصحفى، مصباح احمد حامد؛عسكول، سناء صالح. (2019). "مستوى الوعى بالأمن السيبرانى لدى الحاسب الألى للمرحلة الثانوية بمدينة جدة"،**دار المنظومة**، ص493-534.
- السرحان، حنين عبد المهدى سالم.(2020). " اثر تطبيق سياسة الأمن السيبرانى على جودة المعلومات المحاسبية فى البنوك التجارية الاردنية"،**دار المنظومة**، ص 1-99.
- الزيود، محمود سليمان سعود.(2021). "أثر التدقيق الداخلى فى الحد من المخاطر السيبرانية فى البنوك التجارية الأردنية"، **دار المنظومة**، ص 1-105.
- الدمنى، عمار محمد عادل.(2022). "أثر جودة عملية المراجعة فى ظل عمليات الرقمنه على جودة التقارير المالية بسوق دمشق للأوراق المالية" ، **المجلة العلمية للدراسات والبحوث المالية والإدارية** ،المجلد الثالث عشر، العدد الثانى، ص 1-21.
- أحمد ، محمد أحمد عباس.(2019)." أثر العوامل الشخصية والتنظيمية على كفاءة وفعالية أداء المراجع الداخلى لتحسين جودة المراجعة الداخلية المبنية على المخاطر"، **مجلة البحوث المالية والتجارية**، العدد الأول، ص52-87.
- أحمد، فاطمة على إبراهيم؛ وأخرون.(2022)."الأمن السيبرانى والنظافة الرقمية"، **المجلة المصرية لعلوم المعلومات**، المجلد 9، العدد الثانى، ص 390-422.
- أميرهم، جيهان عادل.(2022). "أثر جودة المراجعة الداخلية فى الحد من مخاطر الأمن السيبرانى وإنعكاساته على ترشيد قرارات المستثمرين"، **مجلة البحوث المالية والتجارية**، المجلد 23، العدد الثالث، ص1-53.
- جاب الله،عادل موسى عوض.(2022)."وسائل حماية الأمن السيبرانى :دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة"،**مجلة كلية الشريعة والقانون بأسيوط** ، المجلد 3، العدد 34، ص 2230-2296.
- حسين،مصطفى زكى.،سالم،حسين عبدالعال.(2023)." قياس تأثير الإفصاح عن مخاطر الأمن السيبرانى على أتعاب المراجعة الخارجية"،**www.researchgate.com**، ص 1-71.
- شحاته، السيد شحاته.(2022). "نحو دور فاعل للمراجع الداخلى فى إدارة مخاطر الأمن السيبرانى فى الشركات المقيدة بالبورصة المصرية"، **المجلة العلمية للدراسات والبحوث المالية والإدارية**، المجلد 13،العدد الثانى،ص26-37.
- على، هيام عيد عطيه محمد.(2023). " أثر دعم دور المراجعة الداخلية على تعزيز أنظمة الأمن السيبرانى : دراسة ميدانية"، **دار المنظومة**، ص71-120.

- محمد، أمال ابراهيم.(2019)." العوامل المؤثرة على فعالية وظيفة المراجعة الداخلية فى الوحدات الحكومية المصرية"، **المجلة العلمية للإقتصاد والتجارة**، ص1-52.
- منصور، آمنه محمد.(2021). "تأثير الأمن السيبرانى على الرقابة الداخلية وانعكاسها على الوحدة الاقتصادية-دراسة استطلاعية لأراء عينة من المدققين والمحاسبين فى وزارة التعليم العالى والبحث العلمى"، **دار المنظومة**،ص1-16.
- محروس،رمضان عارف رمضان.،صالح،أبو الحمد مصطفى.(2022)."استخدام المنهجية الرشيقة فى تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبرانى"، **مجلة البحوث المالية والتجارية**، المجلد 23، العدد الثالث،ص1-60.
- يوسف، حنان محمد اسماعيل.(2024)."القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشارى فى مجال إدارة مخاطر الأمن السيبرانى –دراسة انتقادية وتجريبية"، **مجلة البحوث المحاسبية**، جامعة طنطا، العدد الأول، ص 1-71.

ثانيا: المراجع الأجنبية:

Periodicals:

- Allinson, M.(2021)."4 ways to Improve the efficiency of your auditing process", **https://robotics and automation news.com.**
- Al Bayati,Q.A. O.(2022)."the role of cyber security in the efficiency of financial reports in Iraqi universities: a field study on workers at the al-furat aswat technical university", **social science journal**, P.1-16.
- Aswar,K.,et.al.(2021)."determinants of audit quality: role of time budget pressure",**problems and perspectives in management**,volum 19,issue2,P.1-13.
- Biju,J.M.,et.al.(2019)."Cyber Attacks And Its Different types",**international Research Journal Of Engineering And Technology**,Volume: 06,issue:3,P.1-4.
- Backer,T.(2022)." Cybersecurity risks in the financial statement audit", **https:// kpmg.com**.
- Baidoo,D.K.(2023)."the impact of cyber security on the future of internal audit",**https://www.linkedin.com/pulse/impact-cybersecurity-future-internal-audit-daniel.**
- Calderon,T. g.,Gao,L.(2020)."cybersecurity risks disclosure and implied audit risks: Evidence from audit fees", **wiley online library**,P.1-16.
- Duggal, N.(2023)."Top 10 Cybersecurity Trends To Watch Out For In 2023", **Www.Simplilearn.Com.**
- Fetai,B.,mjaku,G.(2020)." the determinants and efficiency of auditing in the republic of Kosovo", **www.researchgate.com**, P.1-13.
- Haapamaki, E., sihvonen, J .(2019)."cyber security in accounting research", ,**managerial auditing journal**,vol.34. no.7,P.1-27.
- Jadhav,K.d.(2023)."the role of cyber security audits",**www.researchgate.com**,P.1-8.
- Khuda,K.E.(2020)."Cyber Security And It's Reality In Bangladesh: An Analysis Of Existing Legal Frameworks",**International Journal On Emerging technology,**P.1-7.
- Kartini,G. t.,Yolanda,A.M .W.(2021)."determinants of audit Quality at public accounting firms",**gatr journal of finance and banking review**,P.1-10.

- Kurniawan,Y.,mulyawan,A.N.(2023)."the role of external auditors in improving cybersecurity of the companies through internal control in financial reporting", **journal of system and management sciences**,vol.13,No.1,pp.485-510.
- Ngo,T.N.B.,Tick,A.(2021)."cyber security risks assessment by external auditors",**www.researchgate.net**, P.1-16.
- Rosati,P,et.al.(2019). audit firm assessments of cyber security risk:evidence from audit fees and sec comments", **international journal of accounting**,P.1-76.
- Raditya,G. A .G.(**2020). the influence of time budget pressure,audit complexity and audit fee on audit quality(case study at public accounting firms in bali province)",journal of business and management,vol 2, issue 1,**PP27-32.
- Rajasekharaiah K.M ,Et.al.(2020)."Cyber Security Challenges and its emerging trends on Latest Technologies",**www.researchgate.net**,P.1-8.
- Sree,K .(2020)."Cyber security and It's importance",**researchgate.net**,p.1-5.
- Tariq, N.(2018). " Impact Of Cyberattacks On Financial Institutions", **Journal of internet Banking And Commerce,**vol.23,no.2,p.1-11.
- Tabassum, L.(2020)."Cyber Security And Safety Measures", **International Research Journal, of Modernization in Engineering Technology and Science**, vol.2,Issue.6,**P.1-4.**
- Upadhyay, V., Yadav,S.(2018)."study of cyber securitychallenges it's Emerging trends:current technologie",**International Journal of Engineering Research And Management**",volume 5,issue7,p.1-5.
- Uniyal,S.(2022)."the top-five audit essentials for driving efficiency and value ,**https://www.isaca.org**.
- Zaidan, A. M., Neamah, I .S.(2022)." the effect of the quality of internal audit function to improve the operational efficiency of companies",http://www.webology.org,volume 19,N.1, P.1-30.

Others:

- Association of international certified professional Accounatants, "Welcome to the new era of audit efficiency", **www.cpa.com**, 2019.
- Definition Of Cybe Security"_**https://www.itu.int/en/ITU-t/study_groups/com17/Pages Cybersecurity.aspx**,2021.
- Top Ten Cybersecurity Trends",**Www.Kaspersky.Com**.
- external auditor's responsibility to consider cyber security",**Www.Nexia-Sabt&t** ,2018.