Alexandria Journal of Managerial Research & Information Systems

مجلة اسكندرية للبحوث الادارية ونظم المعلومات

Print ISSN : 2974-4318 online ISSN:2974-4326

العلاقة بين معدل حوادث الأمن السيبراني وخبرة مراقب الحسابات بصناعة عميله

دراسة تطبيقية على الشركات المقيدة بالبورصة المصرية[1]

الباحثة

مـــي رمضـــان طلبـــة

باحثة ماجستير

1 البحث مستقل من رسالة ماجستير للباحثة بعنوان "أثر معدل حوادث الأمن السيبراني ومستوي الإفصاح عنها على جودة المراجعة المدركة بالتطبيق علي الشركات المقيدة بالبورصة المصرية".

العلاقة بين معدل حوادث الأمن السيبراني وخبرة مراقب الحسابات بصناعة عميله

دراسة تطبيقية على الشركات المقيدة بالبورصة المصرية

مـــي رمضـــان طلبـــة

ملخص البحث:

استهدف البحث دراسة واختبار العلاقة بين معدل حوادث الامن السيبراني وخبرة مراقب الحسابات بصناعة عميله مع التطبيق علي الشركات المقيدة بالبورصة المصرية .

وفى سبيل ذلك، استخدم الباحث التقارير المالية السنوية وتقارير المراجعة والتقارير المتاحة علي موقع مباشر مصر ومواقع الشركات الموجودة علي الانترنت والتي بلغت 102 شركة في الفترة من 2016 حتي 2023 والتي تمثل فترة اجراء البحث.

وتوصل الباحث في ظل التحليل الأساسي ، الي وجود تأثير سلبي، ولكنه غير معنوي لمعدل حوادث الامن السيبراني علي خبرة مراقب الحسابات بصناعة عميله في الشركات المقيدة بالبورصة المصرية.

كما توصل الباحث في التحليل الإضافي أيضا الي وجود تأثير سلبي، ولكنه غير معنوي لمعدل حوادث الامن السيبراني علي هذه الخبرة .

واخير توصل الباحث في تحليل الحساسية الي وجود تأثير سلبي، ولكنه غير معنوي لمعدل حوادث الامن السيبراني علي هذه الخبرة.

وقد اوصت الدراسة بالعمل علي زيادة خبرة مراقب الحسابات بصناعة عميله بما يخص مجال الامن السيبراني وذلك لان مثل هذه الحوادث تؤثر علي القوائم المالية مجال المراجعة وذلك لتمكن المراجع من معرفة التأثيرات علي القوائم المالية والناتجة عن الحوادث السيبرانية والتى قد تؤدي في النهاية الي التأثير علي رأيه المهني.

الكلمات المفتاحية : خبرة مراقب الحسابات بصناعة عميله، حوادث الامن السيبراني، حجم مكتب المحاسبة والمراجعة، الشركات المقيدة بالبورصة المصرية.

Abstract:

The research aimed to study and test the relationship between the rate of cybersecurity incidents and the auditor's experience in his client's industry, with application to companies listed on the Egyptian Stock Exchange.

For this purpose, the researcher used the annual financial reports, audit reports, and reports available on the Mubasher Egypt website and the companies' websites on the Internet, which amounted to 102 companies in the period from 2016 to 2023, which represents the period during which the research was conducted.

In light of the basic analysis, the researcher concluded that there is a negative, but insignificant, effect of the rate of cybersecurity incidents on the auditor's experience in his client's industry in companies listed on the Egyptian Stock Exchange.

In the additional analysis, the researcher also found that there was a negative, but insignificant, effect of the rate of cybersecurity incidents on this experience.

Finally, in the sensitivity analysis, the researcher concluded that there is a negative, but insignificant, effect of the rate of cybersecurity incidents on this experience.

The study recommended working to increase the experience of the auditor in his client's industry with regard to the field of cybersecurity, because such incidents affect the financial statements in the field of auditing, in order to enable the auditor to know the effects on the financial statements resulting from cyber incidents, which may ultimately lead to affecting his professional opinion.

Keywords: The auditor's experience in his client's industry , cybersecurity incidents, size of the accounting and auditing office, companies listed on the Egyptian Stock Exchange.

1- المقدمة:

لقد تحولت مهنة المحاسبة والمراجعة إلى مهنة رقمية(Friday & Japhet, 2020) .فأصبح هناك حاجة إلى تحسين كفاءة الموارد اللازمة تحقيق الأهداف بحيث يكون لها تأثير على القدرة الرقمية (Khin& Ho,2019). ومع تطور الابتكار الرقمي، اصبح هناك حاجة لتقييم المخاطر بكفاءة بواسطة مراقب الحسابات (Gepp, et al., 2018).

ولقد تم اعتماد القدرة الرقمية على نطاق واسع من قبل العديد من الباحثين مما أدى إلى نمو أداء الأعمال وتجارب المستهلكين الجديدة، والتي تتأثر بشكل إيجابي بالقدرة الرقمية (Chan& Li, 2019; Malchenko, 2020).

ولقد أوضح Raguseo (2018) ان القدرة الموثوقة على تطبيق التكنولوجيا في عمليات المراجعة ستساعد على نجاح استراتيجيات المراجعة في التنبؤ وتحليل المخاطر التي يمكن أن تؤثر علي النتائج التي يتعين متابعتها.

كما أصبح الأمن السيبراني مصدر قلق كبير لمجتمعنا بعد سلسلة من الحوادث السيبرانية سيئة السمعة التي استهدفت الشركات الكبيرة. على سبيل المثال، حدث لشركة ماريوت الدولية (وهي سلسلة فنادق ضخمة)، واحدة من أكبر عمليات اختراق البيانات، حيث تمت سرقة معلومات مثل اسم العميل والعنوان ورقم بطاقة الائتمان وتاريخ السفر لما يصل إلى 500 مليون عميل (Raguseo,2018).

كما أدت هجمات الأمن الإلكترونى على مستوى البيانات الهامة للشركات الكبرى والحكومات إلى لفت إنتباه الشركات إلى الآثار التجارية التى تمثل خرقاً كبيراً فى الشركة يمكن أن تسبب، بما فى ذلك؛ الإضرار بالسمعة، وفقدان الملكية الفكرية، وتعطيل العمليات التجارية الرئيسية، والغرامات والعقوبات التى تفرضها الحكومات، وتكاليف التقاضى، والاستبعاد من الأسواق الاستراتيجية. كما أدى خطر حدوث مثل هذه الآثار إلى إهتمام كبير بشأن الأمن الإلكترونى وإدارته من قبل المستثمرين والعملاء وشركاء الأعمال والمنظمين، ونتيجة لذلك أصبحت إدارة مخاطر الأمن الإلكترونى من الأمور الرئيسية فى مجال الأعمال التى تواجه الإدارة العليا ومجالس إدارات معظم الشركات (فرج،2022).

ووفقًا لأحدث تقرير للتحقيقات في خروقات البيانات، فإن 71 بالمائة من الانتهاكات لها دوافع مالية ويتم تنفيذها بشكل أساسي من قبل جهات خارجية(Verizon, 2019). وتكبد أكثر من 20% من الشركات المتضررة خسارة كبيرة في الإيرادات وفرص الأعمال (Cisco, 2017).

علاوة على ذلك، يكشف تقرير هيئة الأوراق المالية والبورصات الأمريكية SEC عام 2018 أن المجرمين الذين ينتحلون صفة المديرين التنفيذيين للشركات أصدروا تعليمات للموظفين بإجراء تحويلات مالية غير مصرح بها، وهو نوع من الاحتيال عبر الإنترنت الذي دفع الهيئة إلى إصدار تقرير تحقيقي.

هناك أيضًا أدلة على أن المهاجمين يسرقون معلومات حساسة غير عامة من الشركات التي لديها دفاع ضعيف في مجال الأمن السيبراني بسبب التجارة غير القانونية (Berkman et al., 2019). ولذلك،

يُبدي الرؤساء التنفيذيون قلقًا كبيرًا من أن قضية الأمن السيبراني قد تعيق النمو الاقتصادي لشركاتهم (WSJ, 2016).

واستجابة للقلق المتزايد بشأن مخاطر الأمن السيبراني، أصدر قسم تمويل الشركات التابع لهيئة الأوراق المالية والبورصات الأمريكية SEC إرشادات الإفصاح عن الأمن السيبراني في عام 2011 ثم قام بتحديثها لاحقًا في عام 2018، بالتركيز على التزام الشركات علنًا بالكشف عن الحوادث السيبرانية والمخاطر المادية المتعلقة بالأمن السيبراني للمستثمرين (SEC, 2018).

وعلى الرغم من أن هيئة الأوراق المالية والبورصات الأمريكية SEC قامت في البداية بتقييد إجراءاتها ضد الشركات، فإن إنشاء "وحدة إلكترونية" تابعة لقسم الإنفاذ التابع للهيئة يشير بوضوح إلى أن الهيئة التنظيمية أصبحت أكثر جدية (Berman et al., 2019).

كما تتحدى مخاطر الأمن السيبراني الآخذة في التوسع دور المراجع الخارجي في فهم بيئة تكنولوجيا المعلومات الخاصة بالعميل (Yen et al., 2018).

لذلك أصدر مركز جودة المراجعة CAQ (2014)، تلخيصا لمسئوليات المراجعين الخارجيين فيما يتعلق بالأمن السيبراني. كما شكل مجلس الرقابة على أعمال مراجعى الحسابات لجنة لمناقشة قضايا الأمن السيبراني والآثار المحتملة على التقارير المالية والمراجعة (PCAOB,2014) .

ويظل الأمن السيبراني قضية رئيسية في تقرير التفتيش السنوي، فعلى سبيل المثال، تم إدراج مخاطر الأمن السيبراني كمجال رئيسي للتركيز على توقعات عمليات التفتيش التي تقوم بها PCAOB لعام 2019 (PCAOB, 2018a).

وعلى الرغم من أن دور المراجعين محدود للغاية فيما يتعلق بالأمن السيبراني بموجب المعايير الحالية، إلا أن مجلس إدارة PCAOB يدعو المراجعين إلى النظر على نطاق واسع في مخاطر الأمن السيبراني التي يمكن أن يكون لها تأثير مادي على القوائم المالية للشركات، ويتساءل "ما إذا كانت معايير المراجعة الخاصة بـ PCAOB ينبغي أن تتوسع" (PCAOB, 2019a).

2-مشكلة البحث:

تؤكد دراسة(2021),.He Li et al علي أن المراجعين الذين لديهم الخبرة الأكبر في مجال الأمن السيبراني يأخذون فى الاعتبار مخاطر الأمن السيبراني قبل وقوع الحوادث السيبرانية للعملاء. كما أن المراجعين الذين يتمتعون بخبرة في مجال تكنولوجيا المعلومات أكثر قدرة على الاستفادة من خبراتهم في مجال الأمن السيبراني في مساعدة العملاء على منع الحوادث المستقبلية. كما ان قدرة تكنولوجيا المعلومات تسهل على المراجعين تطوير المعرفة المتعلقة بالأمن السيبراني ومعالجة المخاطر السيبرانية في عمليات المراجعة وتشير إلى أن تحسين قدرة تكنولوجيا المعلومات لدى شركات المراجعة أمر ذو قيمة.

ولقد حدد مجلس PCAOB تهديدات الأمن السيبراني كموضوع يثير قلقًا متزايدًا ويستحق اهتمام الشركات العامة ومراقبي الحسابات، وسلطت الضوء على أهمية تقييم مخاطر الأمن السيبراني

.(PCAOB 2018a, 2018b)

كما أكد مجلس PCAOB في مناســـبات متعددة أنه يجب على المراجع النظر في أي مخاطر تتعلق بالأمن السيبراني بغض النظر عما إذا كان قد وقع حادث سيبراني أم لا (PCAOB 2019a, 2019b).

لذلك يمكن التعبير عن مشكلة البحث فى كيفية الإجابة عملياً على التساؤل التالي:
ماهو شكل واتجاه العلاقة بين معدل حوادث الأمن السيبراني وخبرة مراقب الحسابات بصناعة عميله في الشركات المقيدة بالبورصة المصرية؟.

3-هدف البحث:

يهدف البحث الي دراسة واختبار العلاقة بين معدل حوادث الأمن السيبراني وخبرة مراقب الحسابات بصناعة عميله ، وذلك لعينة من الشركات المقيدة بالبورصة المصرية في الفترة من 2016-2022

4-أهمية ودوافع البحث:

تكمن **الأهمية الأكاديمية** للبحث فى كونه يركز على قضية هامة وهى تسليط الضوء على أثر معدل حوادث الأمن السيبراني وخبرة مراقب الحسابات بصناعة عميله، فضلا عن قلة البحث الأكاديمي في هذا المجال في مصر (وفقا لمعلومات الباحث)، مما يحد من أوجه القصور الأكاديمية في هذا المجال.

كما تتمثل **الأهمية العملية** للبحث فى مردوده على ترشيد قرارات أصحاب المصالح، خاصة قرار مراقبي الحسابات عند تقديرهم لخطر المراجعة.

ورغم كثرة **دوافع البحث** إلا أن أهمها قلة البحوث المحاسبية فى مصر (وفقا لمعلومات الباحث)، خاصة تلك التي تهتم بدراسة وإختبار الآثار المترتبة على أثر معدل حوادث الأمن السيبراني على خبرة مراقب الحسابات بصناعة عميله، بناءً على أساليب البحث التي تعتمد على التحليلات الأساسية والتحليلات الأخرى.

5-حدود البحث:

وفقاً لهدف البحث ومشكلته سوف يقتصر البحث على دراسة واختبار العلاقة محل الدراسة، وأخيراً، فإن قابلية تعميم نتائج البحث تتوقف على منهجية الدراسة التطبيقية بمحدداتها، خاصة محددات اختيار عينة البحث.

6- خطة البحث:

لمعالجة مشكلة البحث، في ضوء حدوده، وتحقيقا لأهدافه، سيتم تقسيم خطة الدراسة كما يلي:
1/6- الأمن السيبراني، الاتجاهات والأطر.
2/6- خبرة مراقب الحسابات، المفهوم والمردود المهنى.
3/6- تحليل العلاقة بين معدل حوادث الامن السيبراني وخبرة مراقب الحسابات بصناعة عميله واشتقاق فرضى البحث.
4/6- نموذج ومنهجية البحث
5/6- النتائج والتوصيات ومجالات البحث المقترحة

1/6- الأمن السيبراني،الاتجاهات والأطر:

أصبح الأمن السيبراني مصدر قلق كبير خلال السنوات الاخيرة في عالم تكنولوجيا المعلومات. ففي الوقت الحالي، تواجه معظم المنظمات الكثير من المشـــاكل المتعلقة بالجرائم الإلكترونية. وذلك نظرًا لأن المتسللين يقومون باختراق المعلومات الحساسة الرئيسية للمؤسسات، لذا يشعر الأفراد بالقلق الشديد لأن هجوم الأمن السـيبراني يمكن أن يؤدي إلى الاحتيال ويصـل الي ابتزاز الشـركات الكبرى. ويوجد أنواع عديدة من الجرائم الإلكترونية الناشـئة والتي يجب ان يكون الجميع علي دراية بها، وهناك تدابير وأدوات مختلفة يمكن اسـتخدامها لتجنب الجرائم الإلكترونية. ولا يقتصـر التعرض للاختراق على فقدان البيانات السرية فحسب، بل يعني أيضًا فقدان العلاقة مع العملاء في السوق (Bumgarner & Vasarhelyi, 2015).

ويعتبر الإنترنت البنية التحتية الأسرع نمواً في عصرنا هذا. حيث تعمل العديد من التقنيات الجديدة على تغيير البشرية، ولكن بسبب هذه التقنيات الناشئة نكون غير قادرين على حماية معلوماتنا الخاصة بطريقة فعالة، وبالتالي فإن الجرائم الإلكترونية تتزايد بشـــكل كبير على أســـاس يومي. فتتم غالبية المعاملات التجارية والشـخصـية باسـتخدام وسـائل المعاملات عبر الإنترنت، لذلك من المهم أن يكون لديك خبرة تتطلب جودة عالية من الأمان والحفاظ على شـفافية أفضـل للجميع والحصـول على معاملات أكثر أمانًا. حيث تتطلب التقنيات المتقدمة مثل الخدمات السـحابية والهواتف المحمولة والتجارة الإلكترونية والخدمات المصرفية عبر الإنترنت وغيرها معايير عالية من الأمان. وتعتمد جميع الأدوات والتقنيات المستخدمة في هذه المعاملات على معلومات المستخدم الأكثر حساسية وأهمية. لذا فإن توفير الأمن اللازم لهم أمر مهم للغاية. ويعد تحسين الأمن السيبراني وحماية البيانات والبنية التحتية الحساسة أمراً مهمًا لكل من الدولة والمؤسسات (Panchanatham, 2015).

1/1/6-اتجاهات الأمن السيبراني

يلعب الأمن السيبراني دورًا حاسمًا في مجال تكنولوجيا المعلومات، فأصبحت حماية البيانات أكبر صعوبة في يومنا هذا. حيث إن الشيء الرئيسي الذي يداهم الوتر الحساس في مجال الأمن السيبراني هو الجرائم السيبرانية التي تتزايد بشكل كبير خطوة بخطوة (Samuel, & Osman, 2014). حيث تتخذ المنظمات المختلفة العديد من التدابير لمنع هذه الجرائم الإلكترونية. إلا أنه لايزال الأمن السيبراني مصدر قلق كبير للكثيرين. **وفيما يلي بعض الاتجاهات الرئيسية التي تغير الأمن السيبراني:**

1/1/1/6-خوادم الويب

لا يزال خطر الهجمات على تطبيقات الويب لفصل المعلومات أو تعميم التعليمات البرمجية الضارة مستمرًا. فينقل مجرمو الإنترنت أكوادهم البرمجية باستخدام خوادم ويب جيدة قاموا بتبادلها. لذلك تعتبر هجمات الاستيلاء على المعلومات، والتي يحصل الكثير منها على مداولات وسائل الإعلام، تشكل خطرًا كبيرًا. وفي الوقت الحالي، يحتاج الأفراد إلى التركيز على تأمين خوادم الويب وكذلك تطبيقات الويب حيث تعد خوادم الويب بشكل أساسي المرحلة البارزة التي يقوم فيها مجرمو الإنترنت بأخذ المعلومات. وبالتالي، يجب على المنظمات أن تستخدم برامج آمنة إضافية بشكل موثوق، خاصة وسط التبادلات الحيوية حتى لا

تقع مثل هذه الهجمات (Bumgarner, N., & Vasarhelyi, M. A. 2015).

2/1/1/6-التشفير

تشفير الرسائل هى طريقة لايتمكن المبرمجون من فحصها، ففي التشفير، يتم تشفير الرسالة ، وتحويلها إلى محتوى شكلي متحرك. ويكتمل عادةً باستخدام "مفتاح التشفير" الذي يوضح كيفية تشفير الرسالة. ويضمن التشفير عند أقرب مستوى للنقطة المرجعية حماية المعلومات. ويؤدي الاستخدام الإضافي للتشفير إلى المزيد من المشكلات في مجال الأمن السيبراني. فيتم استخدام التشفير لضمان أمن المعلومات، وبالتحديد المعلومات التي يتم تبادلها باستخدام الأنظمة والهواتف المحمولة وأجهزة الراديو اللاسلكية وما إلى ذلك(Sharma, 2012).

3/1/1/6-التهديد المستمر

يعد التهديد المستمر المتقدم (APT) جزءًا كاملاً من برامج الجرائم الإلكترونية لقدرات أمان الشبكة لفترة طويلة. فعلى سبيل المثال، كان لـ IPS أو تصفية الويب تأثير رئيسي في التمييز بين مثل هذه الاعتداءات المركزة. وذلك نظرًا لأن المهاجمين أصبحوا أكثر جرأة ويستخدمون أساليب مشكوك فيها بشكل متزايد، لذا يجب أن يتكامل أمان الشبكة مع المزايا الأمنية الأخرى لتحديد الاعتداءات. وبالتالي، يجب على المنظمة أن تستعيد الإجراءات الأمنية لمواجهة المزيد من المخاطر القادمة. (Bumgarner & Vasarhelyi, 2015).

2/1/6- دور وسائل التواصل الاجتماعي في الأمن السيبراني

أصبحت وسائل التواصل الاجتماعي أسلوب حياة لبعض الأفراد، حيث تستخدم للبقاء على اتصال، والتخطيط للمناسبات، ومشاركة الصور والتعليقات على التطورات الأخيرة. ومع ذلك، كما هو الحال مع أي شيء آخر على شبكة الإنترنت، فمن الضروري أن نتعرف علي المخاطر. فتعد أجهزة الكمبيوتر والهواتف المحمولة والأدوات الأخرى أصولًا لاتقدر بثمن تزود الأشخاص من أي عمر بقدرة غير عادية على الاتصال والتعامل مع أي مكان آخر في العالم. ويمكن للأفراد القيام بذلك بطرق مختلفة، بما في ذلك استخدام وسائل التواصل الاجتماعي أو مواقع التواصل. وبفضل وسائل التواصل الاجتماعي، يمكن للأشخاص مشاركة تأملاتهم أو صورهم أو تمارينهم أو أي جزء من حياتهم. كما يمكنهم إلقاء نظرة على حياة الآخرين، بغض النظر عما إذا كانوا يعيشون في مكان قريب أو في أى مكان فى العالم. وبسبب تزايد الاستخدام أصبحت منصة ممتازة لمجرمي الإنترنت لاختراق البيانات الخاصة والحصول علي البيانات المهمة (Gross et al., 2017).

كما تحتاج المنظمات إلى التأكد من أنها سريعة في التعرف على المخاطر، والرد بشكل مستمر، وتجنب أي اختراق من أي نوع. وبالتالي، يجب على الأفراد اتخاذ التدابير المناسبة خاصة في إدارة وسائل التواصل الاجتماعي للحفاظ على بياناتهم. حيث أن قدرة الأشخاص على نقل البيانات إلى مجموعة من الأشخاص الأخرى هي جوهر الاختبار الدقيق الذي تقدمه وسائل التواصل الاجتماعي للمؤسسات (Cabaj, et al.,2018).

ومع ذلك ، فمن خلال تمكين أي شخص من نشر البيانات الحساسة ماليًا، توفر وسائل التواصل الاجتماعي أيضًا قدرة مماثلة على نطاق البيانات الخاطئة، ويمكن أن يكون مجرد ضرر. ويعد الانتشار

السـريع للمعلومات غير الصـحيحة عبر وسـائل التواصـل الاجتماعي من بين المخاطر المتزايدة. فعلى الرغم من إمكانية استخدام وسائل التواصل الاجتماعي في الجرائم الإلكترونية، إلا أن المنظمات لايمكنها التوقف عن استخدام وسائل التواصل الاجتماعي لأنها تلعب دورًا أساسيًا في اهتمام المنظمة. وبدلاً من ذلك، يجب أن يكون لديهم ترتيبات لإبلاغهم بالمخاطر لإصـلاحه قبل حدوث أي ضـرر فعلي. كما يجب على المنظمات أن تفهم ذلك وتراعي معنى تقسيم البيانات بشكل رئيسي في المداولات الاجتماعية ووضع خطط أمنية جيدة لتجنب المخاطر. ويجب على المنظمة أن تتعاقد مع وسائل التواصل الاجتماعي باستخدام خطط محددة وتقنيات مناسبة(Dervojeda, et al.,2014).

3/1/6- أطر الأمن السيبراني

بالإضـافة الي ما سـبق، تتطلب جوانب السـلامة في الأعمال التجارية ونقل المعاملات الإلكترونية مراجعة أكثر تعقيدًا، لذلك فقد رأت المؤسسات المالية وجود حاجة إلى اعتماد أطر الأمن السيبراني التي يمكن اسـتخدامها لمراجعة تكنولوجيا المعلومات، ويمكن توضـيح الأطر كما يلي: (Jreissat et al., 2018; Osamah et al., 2018).

- **اطار COBIT5 (2012):**

وفقًا لـــ(2015) **ISACA**[2] ، يعد إطار COBIT أداة متكاملة تم تطويرها لمعالجة جميع جوانب تكنولوجيا المعلومات تقريبًا وخاصة حوكمة تكنولوجيا المعلومات. ويركز الاطار على مواءمة تكنولوجيا المعلومات مع الأعمال التجارية. وانتقل الإطار من التركيز علي أهداف المراقبة إلى الإصدار الثالث من COBIT الذي أضـاف مبادئ توجيهية للإدارة (ISACA, 2015) .ومن هناك جاء COBIT 4.0 ثم 4.1 الذي أضـاف عمليات الحوكمة والامتثال. وصـولا إلى إصـدار COBIT 5 الذى يركز بشـكل كامل على حوكمة تكنولوجيا المعلومات وإدارتها، وقد تم اعتماده منذ ذلك الحين باعتباره الإطار المتكامل "الأقوى" لحوكمة تكنولوجيا المعلومات والتحكم فيها (Ndlovu and Kyobe, 2016) .

إن إطار عمل COBIT 5 يتفوق على الباقي لأنه يوفر منهجًا شـاملاً لممارسـات حوكمة تكنولوجيا المعلومات الجيدة. علاوة على ذلك، يذكر الخبراء أن أحد الأسباب الأساسية لاستقبال COBIT من قبل هذه الأعداد الهائلة من المنظمات على مسـتوى العالم هو أنه يدير كل جزء من تكنولوجيا المعلومات (Yeboah, 2013; Jreissat et al., 2018; ISACA, 2019; Otero, 2019).

- **اطار NIST:**

تم إصـدار إطار عمل NIST للأمن السـيبراني بهدف حماية البنية التحتية من الهجمات السـيبرانية، واعتمدت المنظمات منذ ذلك الحين إطار عمل الأمن السيبراني NIST لتعزيز دفاعها السيبراني وتخفيف المخاطر. ولقد تم تصميم الإطار في ثلاثة أجزاء بشكل أساسي؛ جوهر الإطار، ومستويات تنفيذ الإطار، وملف الإطار. ويصـف جوهر الإطار خمس وظائف تعتمد على إدارة المخاطر وأمن المعلومات وهي التحديد والحماية والكشف والاستجابة والاسترداد (Shen, 2014;Jreissat et al., 2018; Ibrahim, et al., 2018)

- **معيار ISO 27000:**

[2] **Information System Audit and Control Association**

هو معيار لأمن المعلومات تم تطويره من قبل المنظمة الدولية للمعايير، ويوفر إرشادات لإعداد أنظمة إدارة لأمن المعلومات من خلال مجموعة معايير، تخدم هذه المعايير غرض الحد من مخاطر الأمن السيبراني من خلال تقديم إرشادات أو توصيات لجميع الضوابط المطلوبة اللازمة لتنفيذ واستخدام نظام إدارة أمن المعلومات (Drljača & Latinovic, 2017;Tamimi et al.,2019) .

ووفقًا لـــــ(2013) Yeboah يتناول إطار عمل ISO قضايا الامتثال من حيث صلتها بالمعايير التنظيمية والمتطلبات القانونية والسياسات والإجراءات الأمنية للمنظمة ونظام إدارة أمن المعلومات الموثق.

- **اطار خدمة الثقة**

تم تطوير هذه الاطار بواسطة مجمع المحاسبين القانونيين الأمريكي (AICPA) وهو يركز على خمس مكونات رئيسية وهي الأمان والإتاحة وسلامة المعالجة والسرية والخصوصية (AICPA, 2017).

بالنسبة للمكون الأول وهو **الأمان؛** يهتم بحماية أصول معلومات المنظمة ضد المتسللين والمستخدمين غير المصرح لهم، كما يضمن أيضًا عدم المساس بسلامة الأنظمة المطبقة والخصوصية والتوافر والسرية إلى الحد الذي تستطيع فيه المنظمة تحقيق أهدافها العامة.

أما فيما يخص المكون الثاني والذي يتمثل في **الإتاحة؛** فيتناول مدى توفر المعلومات والأنظمة للاستخدام، بما في ذلك إمكانية الوصول إلى المعلومات للتشغيل والصيانة والمراقبة.

ويتناول المكون الثالث والذي يتمثل في **سلامة المعالجة؛** الغرض الرئيسي لأنظمة المنظمة. ويثير التساؤل حول ما إذا كانت الأنظمة المطبقة تحقق الغرض الذي صممت من أجل تحقيقه بطريقة صحيحة خالية من الخطأ أو التأخير أو الإغفال أو التلاعب بالمعلومات.

وفيما يتعلق بالمكون الرابع وهو **السرية؛** فيشير إلى الضروريات المتعلقة بجمع البيانات الشخصية واستخدامها والاحتفاظ بها والإفصاح عنها والتخلص منها. وقد تتضمن البيانات السرية بيانات شخصية بالإضافة إلى بيانات أخرى، على سبيل المثال، الملكية الفكرية.

واخير فيما يتعلق بالمكون الأخير وهو **الخصوصية؛** فيتناول كيفية جمع المعلومات الشخصية واستخدامها والاحتفاظ بها والإفصاح عنها والتخلص منها لتحقيق أهداف الكيان. فهناك خط رفيع بين الخصوصية والسرية. في حين تلتزم السرية بأنواع مختلفة من المعلومات الحساسة، تنطبق الخصوصية على المعلومات الشخصية فقط (AICPA,2017).

2/6- خبرة مراقب الحسابات بصناعة عميله، المفهوم والمردود المهني:

تدرك مكاتب المراجعة أهمية خبرة مراقب الحسابات في تقديم عمليات مراجعة عالية الجودة وتقوم بتنظيم ممارسات الجودة الخاصة بها بشكل استراتيجي وفقًا لخطوط الصناعة (Gul et al., 2009). وقبل الانضمام إلى شركة مراجعة، يُطلب من المراجع المحتمل اجتياز اختبارات فنية مختلفة واختبارات أخرى ضرورية لاختبار وتحسين الكفاءة الفنية والمستوى المهني.

بالإضافة إلى ذلك، يذكر Beck and Wu (2006) أن خبرة مراجعي الحسابات لها علاقة إيجابية بجودة المراجعة. فالمراجعون الذين يتمتعون بخبرة في المراجعة لديهم القدرة على اكتشاف المخاطر وتقييمها واتخاذ القرارات الأكثر اتساقًا مع المعايير(Moroney & Simnett 2009).

وتعد خبرة المراجع عنصرًا قيمًا، وهو أمر ضروري لتحسين جودة المراجعة، ويمكن القول أن الخبرة بمثابة دورة للتعلم وتوسيع إمكانية تحسين السلوك من خلال التعليم الرسمي وغير الرسمي ((Saha & Roy, 2017.

وتنبع خبرة المراجع في كيفية قيادة عمليات المراجعة للتقارير المالية من تخصيص الوقت وكمية المهام التي أنجزها المراجعون ، ففي حالة دخول شخص ما في المهنة يجب عليه البحث في البداية عن الخبرة تحت إشراف المراجع الأكثر خبرة (Kuntari, et. al., 2017).

ويمكن تفسير خبرة الشخص على أنها عملية يمكن أن تقود الشخص إلى نمط أعلى من السلوك. وتعتبر خبرة المراجع هي المهارات التي يتمتع بها المراجع في مراجعة القوائم المالية للمنظمة (Chang, et al.,2019).

وكلما زادت خبرة المراجع، زادت قدرته على تقديم أداء أفضل في المهام المعقدة، بما في ذلك إجراء عمليات المراجعة (Saputra, 2019; Cai et al., 2019).

كما يمكن تعريف خبرة المراجع علي انها تراكم كل ما يتم اكتسابه من وجه لوجه والتفاعلات المستمرة مع الأشياء والمواقف والأفكار والإحساس التي تحدث أثناء عملية المراجعة، ومن هذا نجد أن المراجع الذي لديه خبرة أكبر سيكون لديه نسبة خطأ أقل مقارنة بالمراجع الذي لديه خبرة أقل (Saputra, 2019) .

ووفقًا لـ Lehmann & Norman (2006) فيما يتعلق بخبرات المراجعين، فإن المراجع الذي يتمتع بالخبرة سوف يحدد المشكلة بشكل أكثر وضوحًا والذي سيؤثر على حكم المراجع المهني، كما يجب أن يتمتع بالمهارة المهنية العالية، حيث لا يتأثر كل ذلك فقط بالتعليم العالي ولكن أيضًا بعوامل أخرى وهي الخبرة.

علاوة على ذلك، يتم تعريف عملية المراجعة نفسها وفقًا لـ(2003) Arens and Loebbecke على أنها عملية منظمة للتجميع والتقييم الموضوعي للأدلة الخاصة بمزاعم العميل، بشأن نتائج الأحداث والتصرفات الاقتصادية لتحديد مدى تمشي هذه المزاعم مع المعايير المحددة وتوصيل النتائج لمستخدمي القوائم المالية، أصحاب المصلحة في المشروع.

وترتبط الخبرة بمراجعة القوائم المالية من حيث المدة وعدد المهام التي يتم التعامل معها، كما أن الشخص الذي لديه خبرة أكبر مخزنة في ذاكرته يمكنه بسهولة تطوير فهم جيد للأحداث. وفي هذه الحالة، يمكن أن يكون جيدًا في اتخاذ القرارات. (Arens and Loebbecke ,2003).

ويذكر Libby and Frederick (1990) أنه كلما زادت خبرة المراجعين، زادت قدرة المراجعين على إنتاج أنواع مختلفة من التوقعات عند شرح نتائج المراجعة.

وأشار Gaballa and Ning (2011) إلى خبرة المراجع على أنها المهارات التي يتم الحصول عليها من مهام المراجعة فيما يتعلق بمعايير المراجعة ذات الصلة والإرشادات المحاسبية والخبرات الخاصة بالأخطاء المالية، والتي تؤثر على مهمة المراجعة وأداءها.ولذلك يتعين على المراجعين الاستفادة من خبراتهم لتحقيق الفعالية (Gaballa and Ning ,2011).

كما وجدت بعض الدراسات (شحاته،2015؛ بدوى،2018؛ Sila,etal.,2016; Liu, etal.,2017) أنه كلما زادت خبرة مراقب الحسابات زادت كفاءته، ويقصد بالخبرة المهنية هنا أنها الإطار الزمنى المعبر عن مدى توافر التأهيل العلمى والعملى الملائم والمهارات الخاصة الناتجة عن تراكم المعارف العلمية والعملية فى مجال أداء عمليات المراجعة. وتنطوى على معرفة عامة بمجال المراجعة، مع معرفة متخصصة فى مجال صناعة العميل وطبيعة أعماله. حيث أن الخبرة والتخصص الصناعى تزيد من كفاءة أداء مراقب الحسابات، وذلك لأن الخبرة تسمح له بمواجهة ضغوط الإدارة وتساعد على تحقيق جودة ودقة المعلومات التى تعدها الإدارة، كما تساعده على مراجعة أفضل للتقديرات المحاسبية، ومدى تحيز العملاء بشأن تحديد القيمة العادلة. كما توفر الخبرة لدى مراقبى الحسابات نماذج لأفضل الممارسات المحاسبية وقدراته على تقييم المخاطر، وزيادة دقة أحكامه المهنية. ومع مرور الوقت تزيد خبرة مراقب الحسابات والتى تؤدى لتحسين قدراته على حل مشاكل عملية المراجعة وبالتالى تخفيض مخاطر التقاضى.

3/6- تحليل العلاقة بين معدل حوادث الامن السيبراني وخبرة مراقب الحسابات بصناعة عميله واشتقاق فرضى البحث:

لقد جعل الاقتصـــاد الرقمي للأمن الســيبراني أولوية قصـــوى على جدول أعمال الجهات التنظيمية. فأصـدر قسـم تمويل الشـركات، التابع لهيئة الأوراق المالية والبورصـات المسـؤول عن الإشـراف على ممارسـات الإفصـاح، إرشـادات إفصـاح تسـلط الضـوء على وجهة نظر القسـم بشـأن متطلبات الإفصـاح المتعلقة بالأمن السـيبراني. وإدراكًا منها أن التوجيهات المسـبقة غير موثوقة، قدمت اللجنة إرشـادات في عام 2018 لتوسيع وتفسير إرشادات الكشف عن الأمن السيبراني لعام 2011 (SEC 2018a, 2018d)، وذلك بهدف تعزيز الإفصـاح الأكثر شـفافية حول مخاطر وحوادث الأمن السـيبراني للمسـتثمرين. وذلك لردع أنشـــطة التداول الداخلي المحتملة الناتجة عن معلومات مادية وغير عامة تتعلق بالأمن الســـيبراني (EY, 2018).

ويتضمن دليل إرشادات الأمن الإلكترونى الخاص بمتطلبات الإفصاح عن الأمن الإلكترونى بواسطة إدارات الشركات قسمين:

القسم الأول: تضمن طبيعة الأمن الإلكترونى وإرشادات الأمن الإلكترونى منذ 2011 وتطوير إرشادات عام 2018 بغرض التوسع فى متطلبات الإفصاح عن إرشادات عام 2011.

القسم الثانى: تضمن مجموعتين؛

المجموعة الأولى: مراجعة قواعد الإفصاح عن مشاكل الأمن الإلكترونى وتشمل:

- **الأهمية النسبية:** يركز على توجيه الإهتمام نحو مخاطر وحوادث الأمن الإلكترونى عند إعداد تقارير الإدارة السنوية، وخاصة الحوادث الهامة من وجهة نظر المستثمرين والأضرار الناتجة عنها، كما يجب أن يستوفى الإفصاح خاصيتى الملاءمة والإكتمال عند الإفصاح عن إدارة مخاطر الأمن الإلكترونى.
- **عوامل المخاطرة:** يجب الإفصاح عن حوادث الأمن الإلكترونى الفعلية والمتوقعة والتى تمثل مخاطر خاصة على الشركة فى سياق الإفصاح عن إدارة مخاطر الأمن الإلكترونى للمستثمرين.
- **المركز المالى ونتائج الأعمال:** يجب الإفصاح عن أى حوادث أمن إلكترونى يكون لها تأثير جوهرى على المركز المالى ونتائج الأعمال.
- **وصف طبيعة الأنشطة:** يجب الإفصاح عن أى حوادث أمن إلكترونى يكون لها تأثير جوهرى على

طبيعة نشاط الشركة والعلاقات مع الموردين أوالعملاء أو أى أطراف خارجية أخرى.

- **الإجراءات القانونية:** يجب الإفصاح عن أى قضايا متعلقة بإدارة مخاطر الأمن الإلكترونى.
- **سياسات الإفصاح فى القوائم المالية:** قد تؤثر حوادث الأمن الإلكترونى على عناصر القوائم المالية من إيرادات أو مصروفات أو تدفقات نقدية، وبالتالى لابد من الإفصاح عن هذه الأثار ضمن الإيضاحات المتممة للقوائم المالية.
- **دور مجلس الإدارة:** يجب الإفصاح عن دور مجلس الإدارة بخصوص برنامج إدارة مخاطر الأمن الإلكترونى والذى يؤثر إيجاباً على المستثمرين.

المجموعة الثانية: السياسات والإجراءات الخاصة بالرقابة على الإفصاح عن إدارة مخاطر الأمن الإلكترونى وتشمل:

- **إجراءات الرقابة:** يجب التأكد من وجود تصميم جيد لضوابط وإجراءات الرقابة على برنامج إدارة مخاطر الأمن الإلكترونى المطبق بالشركة فهى جزء من أعمال لجنة المخاطر بالشركة.
- **المعلومات الداخلية:** يجب أن لايستغل الأطراف الداخلية معرفتهم بأحداث جوهرية حول مخاطر الأمن الإلكترونى فى التعامل على الأوراق المالية.

الإفصـاح الإنتقائى: يجب عدم الإفصـاح عن المعلومات المتعلقة بإدارة مخاطر الأمن الإلكترونى بشـكل إنتقائى وهى المعلومات غير المعلنة للمستثمرين(SEC, 2018).

وحتى اليوم، لم يصدر PCAOB بعد أي أحكام تشريعية خاصة بالأمن السيبراني، ولكنه يراقب عن كثب كيفية تقييم فرق المشـاركة لمخاطر الأخطاء المادية وقضـايا التحكم المرتبطة بها في أعقاب الحادث السيبراني (PCAOB, 2015, 2016).

وتشـير الأبحاث الأكاديمية حول الأمن السـيبراني في مجال المحاسـبة والمالية ،على سـبيل المثال؛ (Goel and Shawky 2009; Hinz et al., 2015; Campbell et al., 2003) على العواقب الاقتصـادية لانتهاكات الأمن السـيبراني وتميل هذه الدراسـات التي تدرس رد فعل السـوق تجاه خروقات البيانات المعلنة علنًا إلى العثور على تأثير سلبى.

ويكشـف كلا من (Hinz et al., 2015; Ettredge & Richardson ,2003) عن وجود تأثيرات غير مباشرة لانتهاكات البيانات، كما تتأثر أسعار أسهم الشركات في نفس الصناعة أو الشركات المماثلة سلبًا.

ومع ذلك، فشلت بعض الأعمال البحثية في العثور على مثل هذا الارتباط (على سبيل المثال، Hilary et al., 2016; Richardson et al., 2019).

بالإضافة الي ما سبق يجادل كل من (Gordon et al., 2011; Richardson et al., 2019) بأن النتائج غير المتناسقة يمكن تفسيرها بالاختلاف في العينة ومعايير الاختيار وطريقة البحث. وبالإضافة إلى دراسـة تقييم السـوق، هناك عدد محدود من الدراسـات التي تبحث في تأثير الحوادث السـيبرانية على المشاركة في المراجعة.

كما تشـير دراسـة Rebecca & Murthy (2021) أن التنبؤ بحادث الأمن الإلكتروني يعكس

تصورات أصحاب المصالح الإيجابية لكفاءة المراجع ويزيد من حساسيتهم لإعاقات الاستقلال المحتملة عندما يتم توفير الأمن السيبراني بشكل مشترك. كما اشارت الدراسة الي أن أصحاب المصالح يكونون أقل رغبة في الاستثمار عندما يتم توفير الفحص بشكل مشترك مقارنة بالمخصصات المنفصلة.

كما تشير دراسة PricewaterhouseCoopers (2002) بأن جودة عملية المراجعة تعتمد على خبرة المراجع وفهمه لطبيعة الصناعة التي يعمل فيها العميل. ويكتسب المراجعون خبرة كبيرة من خلال معرفته بالممارسات المحاسبية والمخاطر بشكل عام وتجربة العمل مع عملاء محددين في الصناعة. ومن المرجح أن يقوم المراجعين ذوى الخبرة بتدريب مراجعيها بمعرفة أكثر خاصة بالصناعة .ويمكن لهؤلاء المراجعين أن يفهموا بشكل أفضل البيئة التي يعمل فيها عملاؤهم (Krishnan, 2003;Curtis, et al., 2009).

ويذكر Soekrisno Agoes (2014) أنه بغض النظر عن مدى قدرة ومعرفة المراجع في المجالات الأخرى ، بما في ذلك المجالات التجارية والمالية ، فإنه مع ذلك لا يمكنه تلبية المتطلبات الواردة في معايير المراجعة ، وذلك إذا كان لم يكن لديه التعليم والخبرة الكافية في مراجعة الحسابات لأن هذا سيكون له تأثير على جودة المراجعة.

ومن ناحية اخري ، يظهر أن خبرة المراجع الكبيرة بالتخصص ترتبط إيجابيًا بجودة الإفصاح عن عمليات العملاء، والتي يتم قياسها من خلال التقييمات التي يضعها المحللين في التقارير وترتبط سلبًا بالاحتيال المالي (Carcello & Nagy, 2004b; Dunn & Mayhew, 2004)

كما وجد Stanley & De Zoort (2007) ان المعرفة والخبرة المكتسبة بالمجال تشمل مخاطر أمن المعلومات، والتشريعات واللوائح المتعلقة بأمن تلك المعلومات، والاتجاهات الخاصة بحوادث أمن المعلومات، وعند امتلاك المراجع لتلك المهارات يقوم بجهد أقل مما هو مطلوب من المراجعين الذين ليس لديهم خبرة بالتخصص. كما وجدت بعض الدراسات (Anis Chariri, 2017 ; Panji & Sukirman ,2017) أن التهديدات السيبرانية قد تؤثر علي مدي معرفة وخبرة المراجع بالصناعة. ومن هنا يمكن اشتقاق الفرض الرئيسى (H_1) للبحث على النحو التالي:

H_1: يؤثر معدل حوادث الامن السيبراني معنويا علي خبرة مراقب الحسابات بصناعة عميله بالشركات المقيدة بالبورصة المصرية.

وبشأن **نسبة الرفع المالى** كمتغير معدل للعلاقة محل الدراسة، فقد وجدت دراسة (Kobelsky et al. 2008) أن مستوى الديون في الشركة له تأثير مباشر على ميزانية تكنولوجيا المعلومات للشركة. لأن الديون تقيد قدرة الإدارة على الاستثمار في مجالات أخرى مثل تكنولوجيا المعلومات؛ ومن ثم، يرتبط الدين سلبًا بمبالغ ميزانية تكنولوجيا المعلومات. وبالتالي، عندما يتم تخصيص الأموال المولدة داخليًا للشركة لالتزامات الديون، يكون لدى الإدارة سلطة تقديرية وقدرة أقل على تخصيص الأموال لنفقات تكنولوجيا المعلومات. ولذلك، فإن نقص الأموال اللازمة لتكنولوجيا المعلومات قد يجبر الشركة على التراجع عن تحديث الأنظمة الحالية، وتوظيف وصيانة موظفي تكنولوجيا المعلومات، وتنفيذ عمليات وتقنيات جديدة لإدارة مخاطر تكنولوجيا المعلومات.

ويؤدي عدم القدرة على توفير خدمات تكنولوجيا المعلومات الكافية والحفاظ عليها بسبب نقص الأموال إلى زيادة تعقيد بيئة تكنولوجيا المعلومات عن طريق تأخير تحديث الأنظمة الحالية إلى إصدار به ضوابط وقائية ورصدية أكثر تقدمًا، والتهرب من إجراءات إدارة التغيير المناسبة بسبب النقص من الموظفين، وبالتالي، الاضطرار إلى مراقبة الأنظمة القديمة، وعدم القدرة على التحكم في تغييرات النظام، والموظفين المثقلين بالعمل سيزيد من تعقيد بيئة تكنولوجيا المعلومات، وبالتالي تتعرض الشركة لمخاطر الأمن السيبراني . إلا أنه كلما زادت خبرة المراجع بنسبة الرفع المالي يسهل من عملية المراجعة، ويساعد فى التعامل مع مخاطر الأنظمة.

ومن هنا يمكن اشتقاق الفرض الثانى(H_2) للبحث علي النحو التالي:

H_2: يختلف التأثير المعنوي لمعدل حوادث الامن السيبراني علي خبرة مراقب الحسابات بصناعة عميله بالشركات المقيدة بالبورصة المصرية باختلاف نسبة الرفع المالي.

وعلي نحو اخر اشارت دراسة (Yazan, et al.,2019) الي إمكانية وجود تأثير لحجم مكتب المراجعة علي خبرة مراقب الحسابات ، بجانب معدل حوادث الامن السيبراني. وللتحقق من أثر ذلك يمكن صياغة السؤال التالي لاختبار تأثير المتغير الرقابى:

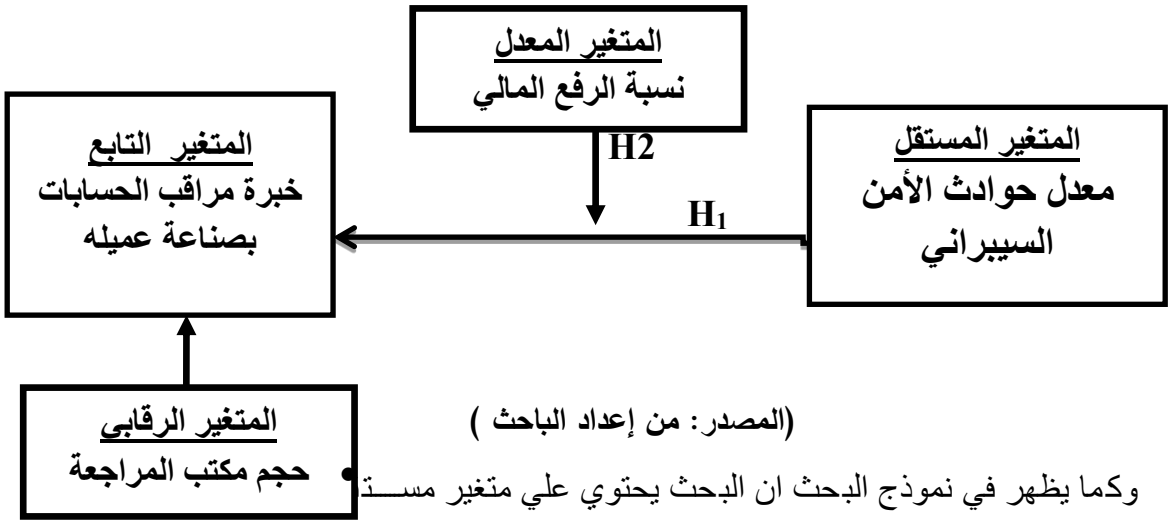
س1: هل يؤثر حجم مكتب المحاسبة والمراجعة معنويا علي خبرة مراقب الحسابات بصناعة عميله في سياق العلاقة التأثيرية بين معدل حوادث الأمن السيبراني وهذه الخبرة؟

4/6- نموذج ومنهجية البحث

لأغراض اختبار العلاقات محل الدراسة، والوصول الي صورة اكثر دقة عن كيفية تأثير مختلف المتغيرات علي بعضها البعض، يستلزم ذلك تناول كل من؛ نموذج البحث، وتوصيف وقياس المتغيرات. وذلك علي النحو التالي:

1/4/6- نموذج البحث:

يظهر التحليل الأساسي للبحث كما في الشكل رقم (1):



(المصدر: من إعداد الباحث)

وكما يظهر في نموذج البحث ان البحث يحتوي علي متغير مستـ

السـيبراني ، ومتغير تابع وهو وخبرة مراقب الحسـابات. ومتغير معدل هو نسـبة الرفع المالي، بالإضـافة الي متغير رقابي هو حجم مكتب المراجعة.

2/4/6-منهجية البحث:

تتناول هذه الجزئية كل من : هدف الدراسة التطبيقية، ومجتمع وعينة الدراسة ، وأدوات وإجراءات الدراسة، وتوصيف وقياس المتغيرات ، نتائج اختبار فروض البحث ، وذلك علي النحو التالي:

1/2/4/6-أهداف الدراسة التطبيقية:

تستهدف الدراسة التطبيقية في المقام الأول اختبار فرضى البحث؛ وذلك للتحقق مما اذا كان هناك تأثير لمعدل حوادث الأمن السيبراني علي خبرة مراقب الحسابات، قياسا على (2020) ,.Chen et al.

2/2/4/6-مجتمع وعينة الدراسة:

يتكون مجتمع الدراسة من الشركات المالية وغير المالية المقيدة بالبورصة المصرية خلال الفترة من 2016 الي 2023. وتم اختيار عينة حكمية من هذا المجتمع مع مراعاة عدة اعتبارات؛ تم اسـتبعاد الشـركات التي خرجت من القيد ببورصـة الأوراق المالية، والشـركات التي لم تكن قوائمها المالية متاحة للباحث خلال فترة الدراسة قياسا على (Abozaid ,et al.,2020)، وبذلك بلغ عدد شركات العينة محل الدراسة101 شركة.

3/2/4/6-ادوات وإجراءات البحث:

فيما يتعلق بأدوات البحث ، فقد تم الاسـتعانة بالبيانات الثانوية الواردة بالتقارير المالية وتقارير الاسـتدامة لشـركات العينة، والاسـتناد أيضـا الي البيانات المتاحة علي موقع مباشـر معلومات الالكتروني بالإضافة إلى الحصول على معايير المحاسبة المصرية ، والقوانين واللوائح المصرية وقواعد قيد وشطب الأوراق المالية ، وموقع البورصة المصرية وهيئة الرقابة المالية.

أما بشـأن إجراءات الدراسـة تم تحليل محتوي التقارير المالية والتي تشـمل القوائم المالية والايضـاحات المتممة وتقارير مراقبى الحسـابات وأيضـا تقارير الاسـتدامة لعينة الشـركات المالية وغير المالية المقيدة بالبورصـة المصـرية. وذلك لتقدير معدل حوادث الأمن السـيبراني، وبعد الانتهاء من تقدير وحسـاب مختلف المتغيرات تم وضـعها في جداول الكترونية باسـتخدام برنامج Excel، وذلك لإجراء الاختبار والتحليل الاحصائي لتلك المتغيرات، قياسا على (زكي، 2018؛أبو العلا،2022).

4/2/4/6-توصيف وقياس المتغيرات:

تم توصيف وقياس تلك المتغيرات علي النحو التالى:

جدول (1): توصيف وقياس متغيرات الدراسة

المتغير والرمز	نوع المتغير	التوصيف	طريقة القياس
معدل حوادث الأمن السيبراني CIR	متغير مستقل	مدي تكرار حدث واحد أو سلسلة من أحداث الأمن السيبراني غير المرغوب فيها أو غير المتوقعة والتي من المحتمل أن تعرض العمليات التنظيمية للخطر (Cyber Coalition,2012)	يقاس بمؤشر حوادث الأمن السيبراني وفقا للمركز الوطني للاستعداد لطوارئ الحاسبات والشبكات الذي يتكون من نسبة الحوادث لكل قطاع من القطاعات المختلفة والواردة في التقرير السنوي لوزارة الاتصالات المصرية. (وزارة الاتصالات المصرية ،2022)
خبرة مراقب الحسابات EXP	متغير تابع	القترة الزمنية التي تعبر عن مقدار المام المراجع الخارجي بمقومات مهنة المحاسبة والمراجعة ، وفهمه المتعمق لطبيعة صناعة عميل المراجعة والتحديدات التشغيلية التي تواجه الصناعات وكيفية تطبيق جميع المعالجات المحاسبية الخاصة بتلك الصناعات، والذي يترتب عن مدي تعود المراجع الخارجي علي أداء مهام المراجعة ودرجة تخصصه الصناعي (Verwey, et al.,2021).	تقاس وفقا لمدي استيفاء مراقب الحسابات لمتطلبات القيد في سجل مراقبي الحسابات لدي الهيئة العامة للرقابة المالية وذلك من واقع بيانات سجل مراقبي الحسابات المتاح لدي الهيئة العامة للرقابة المالية. قياسا على(شحاته،2015)
حجم مكتب المحاسبة والمراجعة AU.FIRM	متغير رقابي	درجة تمكن مكتب المراجع الخارجي على غالبية العملاء في السوق المهنية ، وخاصة العملاء الذين لديهم أصول وايراداتGallizo) &Saladrigues,2016)	تقاس بمتغير وهمي يأخذ القيمة 1 اذا كان مكتب المراجع الخارجي في شراكة مع إحدى منشآت المحاسبة والمراجعة الأربعة الكبرى ، وصفر بخلاف ذلك. قياسا على (Iswari& Hardimi,2017)
نسبة الرفع المالي LEV	متغير معدل	مدي اعتماد الشركة علي الأموال الخارجية في تمويل عملياتها وانشطتها، وتشير أيضا الي المخاطر المحتمل ان تواجها الشركة في حالة عدم قدرتها علي سداد الالتزامات (Dewi, et al,2018).	تقاس وفقا لكل من (Suffian, et al,2015; sengers, 2017: Nouri & Gilaninia,2017; Dewi ,et al,2018) بالمعادلة التالية :اجمالي الالتزامات / اجمالي الأصول

5/2/4/6- أدوات التحليل الإحصائي:

تم استخدم بعض طرق الإحصاء الوصفي لدراسة المتغيرات ومنها؛ المتوسط والانحراف المعياري والوسيط والحد الأدنى والحد الأقصى. ولاختبار الفروض تم الاعتماد على نماذج الانحدار قياسا علي

(Berglund et al.,2018)، وذلك علي النحو التالي:

6/2/4/6-الاحصائيات الوصفية ونتائج اختبار الفروض:

فيما يلي يعرض الباحث الاحصائيات الوصفية يليها نتائج اختبار فروض البحث :

7/2/4/6-الاحصائيات الوصفية:

يوضح الجدول(2) الإحصاءات الوصفية ذات الصلة بالمتغيرات مجال البحث وتتضمن ؛ معدل حوادث الامن السيبراني، وخبرة مراقب الحسابات.

جدول(2) الإحصاء الوصفي

Descriptive Statistics			
	Mean	**Std. Deviation**	**N**
EXP	**101.6597**	**135.46241**	**102**
CIR	**.0774**	**.09828**	**102**

وتشير النتائج الي زيادة الانحراف المعياري لمعدل حوادث الامن السيبراني وخبرة مراقب الحسابات عن الوسط الحسابي لها بمقدار (.02088, 33.80271).

وبشـــأن معاملات الارتباط بين متغيرات الدراســـة يظهر جدول معاملات الارتباط بين هذه المتغيرات كالتالي:

جدول (3) معاملات الارتباط بين متغيرات الدراسة

Correlations			
		EXP	**CIR**
Pearson Correlation	**EXP**	**1.000**	**-.165**
	CIR	**-.165**	**1.000**
Sig. (1-tailed)	**EXP**	**.**	**.049**
	CIR	**.049**	**.**
N	**EXP**	**102**	**102**
	CIR	**102**	**102**

وبتحليل معاملات الارتباط اتضح ان قيم معاملات بيرسون اقل من (1)، كما اتضح ان جميع معاملات الارتباط معنوية عند مســـتوي معنوية اقل من 5% وهذا يعني انه لا يوجد قيم شـــاذة لجميع المتغيرات المستقلة وملاءمتها للقياس .

8/2/4/6نتائج اختبار فرضي البحث في ظل التحليل الأساسي:

قام الباحث بتشـــغيل نماذج الاختبار لاختبار فروض البحث وتحليلها بالاعتماد على معنوية النموذج والتي تشير الي مدي صلاحيته لاختبار العلاقة ذات الصلة بمجال البحث وكذلك معامل β الذي يحدد قوة واتجاه العلاقة بين المتغيرين بناء علي مستوي معنوية P-Value=5% ومستوي ثقة 95% ويتم

قبول او رفض الفرض بناء علي قاعدة القرار وذلك علي النحو التالي:

1/8/2/4/6-نتائج اختبار الفرض الأول (H_1):

لاختبار العلاقة بين معدل حوادث الأمن السيبراني وخبرة مراقب الحسابات بصناعة عميله في الشركات المقيدة بالبورصة المصرية سيتم استخدام نموذج الانحدار التالي:

$$EXP = \beta o + \beta_1 CIR + \varepsilon_{it} \quad (1)$$

حيث : EXP يعبر عن خبرة مراقب الحسابات بصناعة عميله، CIR يعبر عن معدل حوادث الامن السيبراني، وأخيرا ε it يعبر عن الخطأ العشوائي.

ولاختبار هذا الفرض احصائيا تم إعادة صياغته كفرض عدم كما يلي:

H_0: لا يؤثر معدل حوادث الأمن السيبراني معنوياً علي خبرة مراقب الحسابات بصناعة عميله بالشركات المقيدة بالبورصة المصرية.

وفيما يلي نتائج اختبار الفرض الرئيسي الأول للبحث(H_1):

جدول(4) نتائج اختبار الفرض الرئيسي

Variables	B	R2	Adj R2	إحصائية F	Sig.	VIF
CIR	-227.566	.027	.018	2.802	.097	1.000
Constant	119.298				.000	

وبالنظر للجدول يتضح زيادة القيمة المحسوبة لإحصائية F (3.153) عن قيمتها الجدولية[3] (.01) عند مستوي معنوية (.000) اقل من 5% ، بمعني ان النموذج معنوي وصالح لاختبار العلاقة محل الدراسة . وقد بلغت(Adj R2) القوة التفسيرية للنموذج 018. أي ان المتغيرات المستقلة تفسر 018. من التغيرات في المتغير التابع ، ويتضح ان قيمة (VIF) للمتغيرات المستقلة اقل من 10 وهو ما يشير الي عدم وجود مشكلة ارتباط خطي متعدد بين المتغيرات المستقلة.

وبتحليل معاملات الانحدار تبين وجود تأثير سلبي لمعدل حوادث الامن السيبراني علي خبرة مراقب الحسابات الا انه لم يكن معنويا وذلك عند قيمة احتمالية P-Value=.097 ، وقد تم الإشارة الي ذلك في قاعدة قبول او رفض الفرض . وعليه فقد تم قبول فرض العدم ، ومن ثم رفض الفرض البديل H_1 القائل بأنه يوجد تأثير لمعدل معدل حوادث الأمن السيبراني علي خبرة مراقب الحسابات في الشركات المقيدة بالبورصة المصرية.

وتتفق هذه النتيجة مع دراسة (Rebecca R. Perols& Uday S. Murthy ,2021) وتختلف مع

---

[3] تم تحديد القيمة الجدولية لاحصائية F من خلال جدول توزيع F بدرجات حرية للبسط (عدد المتغيرات المستقلة) ، ودرجات حرية للمقام (عدد المشاهدات – عدد معلمات النموذج) وذلك عند مستوي معنوية 05.

دراسة لـ(Soekrisno Agoes ,2014).

ويعتقد الباحث انه علي الرغم من عدم معنوية تأثير معدل حوادث الامن السـيبراني علي خبرة مراقب الحسـابات، الا ان التأثير السـلبي منطقي، وترجع عدم المعنوية الي ان اغلبية المشـاهدات من المؤسـسـات المالية وغير المالية الكبيرة والتي تســعي دائما الي تدريب المراجعين علي كل التطورات التي يمكن ان تحدث في المجال بما في ذلك المخاطر التي يمكن ان تتعرض لها اعمال المراجعة بما فيها حوادث الامن السيبراني باعتبارها خطر يهدد مجال عملية المراجعة.

2/8/2/4/6-نتائج اختبار الفرض الثاني (H_2):

لاختبار ما اذا كانت العلاقة بين معدل حوادث الأمن السيبراني و خبرة مراقب الحسابات بصناعة عميله تختلف باختلاف نسبة الرفع المالي بالشركات المقيدة بالبورصة المصرية سيتم استخدام نموذج الانحدار التالي:

$$EXP= \beta o+ \beta_1 CIR + \beta_2 LEV+ \beta_2 (LEV*CIR)+ \varepsilon_{it} \quad (2)$$

حيث : EXP يعبر عن خبرة مراقب الحسابات بصناعة عميله، CIR يعبر عن معدل حوادث الامن السيبرانيLEV عن نسبة الرفع المالي ،ويعبرLEV*CIR عن المتغير التفاعلي بين نسبة الربع المالي ومعدل الامن السيبراني، وأخيرا ε it يعبر عن الخطأ العشوائي.

ولاختبار هذا الفرض احصائيا تم إعادة صياغته كفرض عدم كما يلي:

H_0: لا يختلف التأثير المعنوي لمعدل حوادث الأمن السـيبراني علي خبرة مراقب الحسـابات بصـناعة عميله بالشركات المقيدة بالبورصة المصرية باختلاف نسبة الرفع المالي.

وفيما يلي نتائج اختبار الفرض (H_2):

جدول (5) نتائج اختبار الفرض (H_2)

Variables	B	R2	Adj R2	إحصائية F	Sig.	VIF
CIR					.095	1.081
LEV	174.399	.121	.095	4.488	.005	1.78
LEV*CIR					.43	1.103
Constant	42.4				.000	

وبالنظر للجدول(5) يتضـح زيادة القيمة المحسـوبة لإحصـائية F (4.488) عن قيمتها الجدولية (10.) عند مستوي معنوية (000.) اقل من 5% ، بمعني ان النموذج معنوي وصالح لاختبار العلاقة محل الدراسة .

وقد بلغت(Adj R2) القوة التفسـيرية للنموذج 095. أي ان المتغيرات المسـتقلة تفسـر 095. من

التغيرات في المتغير التابع ، ويتضـح ان قيمة (VIF) للمتغيرات المسـتقلة اقل من 10 وهو ما يشـير الي عدم وجود مشكلة ارتباط خطي متعدد بين المتغيرات المستقلة.

وبتحليل معاملات الانحدار تبين وجود تـأثير ايجـابي ولكنـه ليس معنوي لمعدل حوادث الأمن السـيبراني علي خبرة مراقب الحسـابات وذلك عند قيمة احتمالية P-Value=.095. وعليه فقد تم رفض الفرض البـديل، ومن ثم قبول فرض العـدم القـائـل بـأنـه يختلف التـأثير المعنوي لمعـدل حوادث الأمن السيبراني علي خبرة مراقب الحسابات للشركات المقيدة بالبورصة المصرية باختلاف نسبة الرفع المالي.

- **ادخال المتغير الرقابي (حجم مكتب المراجعة) الي العلاقة محل الدراسة**

$$EXP= \beta o+ \beta_1 CIR + \beta_2 AU.FIRM + \varepsilon_{it} \quad (1)$$

حيث : EXP يعبر عن خبرة مراقب الحسابات بصناعة عميله، CIR يعبر عن معدل حوادث الامن السيبراني، ويعبر AU.FIRM عن حجم مكتب المراجعة والمحاسبة، وأخيرا ε_{it} يعبر عن الخطأ العشوائي.

ولاختبار هذا الفرض احصائيا تم إعادة صياغته كفرض عدم كما يلي:

H_0: لا يؤثر معدل حوادث الأمن السيبراني خبرة مراقب الحسابات بصناعة عميله بالشركات المقيدة بالبورصة المصرية.

وفيما يلي نتائج اختبار **إدخال المتغير الرقابي على العلاقة الرئيسية محل الدراسة:**

جدول (6)

Variables	B	Sig.	VIF
CIR	-124.386	.184	1.011
AU.FIRM	196.915	.000	1.011
Constant	10.896	.000	
R2	.555		
Adj R2	.546		
إحصائية F	61.725		
Sig.	.000		

وبالنظر للجدول يتضح زيادة القيمة المحسوبة لإحصائية F (61.725) عن قيمتها الجدولية (.01) عند مستوي معنوية (.000) اقل من 5% ، بمعني ان النموذج معنوي وصالح لاختبار العلاقة محل الدراسة . وقد بلغت(Adj R2) القوة التفسيرية للنموذج 546. أي ان المتغيرات المستقلة تفسر 546.من التغيرات في المتغير التابع ، ويتضـح ان قيمة (VIF) للمتغيرات المستقلة اقل من 10 وهو ما يشـير الي عدم وجود مشكلة ارتباط خطي متعدد بين المتغيرات المستقلة.

وبتحليل معاملات الانحدار تبين وجود تأثير سـلبي ولكنه غير معنوي لمعدل حوادث الأمن السـيبراني علي خبرة مراقب الحسـابات وذلك عند قيمة احتمالية P-Value=.184. وعليه فقد تم رفض

الفرض البديل، ومن ثم قبول فرض العدم القائل بأنه لا يوجد تأثير معنوي لمعدل حوادث الامن السيبراني علي خبرة مراقب الحسابات للشركات المقيدة بالبورصة المصرية.

9/2/4/6-التحليلات الأخرى

تم إجراء مجموعة من التحليلات الأخرى وذلك بغرض التأكد من صحة الافتراضات محل الدراسة ، وتحديد مدي صحة النتائج وفقا للتحليل الأساسي. وذلك من خلال عمل ما يلي:

فيما يخص التحليل الإضافي تم إعادة اختبار العلاقة محل الدراسة في ظل ادخال حجم الشركة كمتغير رقابي جديد، والذي يعتبر احدي الخصائص التشغيلية المميزة لدي الشركة، والتي يقصد بها حجم عملياتها واجمالي حجم الأصول. ويتم تحديد قدرة الشركة من خلال الموارد المادية والبشرية والتكنولوجية التي بدورها تسعي لتحقيق الأهداف المالية وغير المالية (التشغيلية). (Chebaane& Othman,2014) وتقاس باللوغاريتم الطبيعي لإجمالي إيرادات النشاط قياسا علي: (Bryan, et al,2018) ولاختبار هذا الفرض احصائيا تم إعادة صياغته كفرض عدم كما يلي:

H_0: لا يؤثر معدل حوادث الأمن السيبراني علي خبرة مراقب الحسابات بصناعة عميله بالشركات المقيدة بالبورصة المصرية.

وفيما يلي نتائج إعادة اختبار العلاقة محل الدراسة في ظل ادخال حجم الشركة كمتغير رقابي جديد

جدول (7)

Variables	B	Sig.	VIF
CIR	-124.613	.186	1.014
AU.FIRM	197.098	.000	1.063
FIRMSIZE	-7.28	.000	1.058
Constant	10.916	.000	
R2	.555		
Adj R2	.541		
إحصائية F	40.736		
Sig.	.000		

وبالنظر للجدول يتضح زيادة القيمة المحسوبة لإحصائية F (40.736) عن قيمتها الجدولية (.01) عند مستوي معنوية (.000) اقل من 5% ، بمعني ان النموذج معنوي وصالح لاختبار العلاقة محل الدراسة . وقد بلغت(Adj R2) القوة التفسيرية للنموذج 541. أي ان المتغيرات المستقلة تفسر 541.من التغيرات في المتغير التابع ، ويتضح ان قيمة (VIF) للمتغيرات المستقلة اقل من 10 وهو ما يشير الي عدم وجود مشكلة ارتباط خطي متعدد بين المتغيرات المستقلة.

وبتحليل معاملات الانحدار تبين وجود تأثير سلبي وغير معنوي لمعدل حوادث الأمن السيبراني علي خبرة مراقب الحسابات وذلك عند قيمة احتمالية P-Value=.186.

اما فيما يخص تحليل الحساسية

تم تغيير طريقة قياس المتغير التابع ليتم قياسه بالاعتماد علي عدد سنوات شغله للوظيفة فاذا كانت 5 سنوات فأكثر يصنف علي انه من ذوي الخبرة ويأخذ القيمة 1، اما اذا كانت اقل من ذلك يعتبر اقل خبرة ويأخذ القيمة صفر (نويجي، 2019) ، بدلا من قياسه وفقا لمدي استيفاء مراقب الحسابات لمتطلبات القيد في سجل مراقبي الحسابات لدي الهيئة العامة للرقابة المالية وذلك من واقع بيانات سجل مراقبي الحسابات المتاح لدي الهيئة العامة للرقابة المالية.

-إعادة اختبار الفرض الأول في حالة تغيير قياس المتغير التابع

لإعادة اختبار اثر معدل حوادث الامن السيبراني علي خبرة مراقب الحسابات بصناعة عميله في الشركات المقيدة بالبورصة المصرية سيتم استخدام نموذج الانحدار التالي:

$$EXP = \beta o + \beta_1 CIR + \varepsilon_{it} \quad (1)$$

حيث : EXP يعبر عن خبرة مراقب الحسابات، CIR يعبر عن معدل حوادث الامن السيبراني، وأخيرا ε_{it} يعبر عن الخطأ العشوائي.

ولاختبار هذا الفرض احصائيا تم إعادة صياغته كفرض عدم كما يلي:

H_0: لا يؤثر معدل حوادث الامن السيبراني معنوياً علي خبرة مراقب الحسابات بصناعة عميله بالشركات المقيدة بالبورصة المصرية.

وفيما يلي نتائج اختبار الفرض الرئيسي للبحث(H_1):

جدول(8) نتائج إعادة اختبار الفرض الرئيسي (H_1)

Variables	B	R2	Adj R2	إحصائية F	Sig.	VIF
CIR	-124.613	. 925	.922	40.5	.114	1.063
Constant					.000	

وبالنظر للجدول يتضح زيادة القيمة المحسوبة لإحصائية F (40.5) عن قيمتها الجدولية (.01) عند مستوي معنوية (.000) اقل من 5% ، بمعني ان النموذج معنوي وصالح لاختبار العلاقة محل الدراسة . وقد بلغت(Adj R2) القوة التفسيرية للنموذج 922. أي ان المتغيرات المستقلة تفسر 922. من التغيرات في المتغير التابع ، ويتضح ان قيمة (VIF) للمتغيرات المستقلة اقل من 10 وهو ما يشير الي عدم وجود مشكلة ارتباط خطي متعدد بين المتغيرات المستقلة.

وبتحليل معاملات الانحدار تبين وجود تأثير سلبي وغير معنوي لمعدل حوادث الامن السيبراني علي خبرة مراقب الحسابات وذلك عند قيمة احتمالية P-Value=.000 ، وقد تم الإشارة الي ذلك في قاعدة قبول او رفض الفرض . وعليه فقد تم رفض الفرض البديل ، ومن ثم قبول فرض العدم القائل بأنه لا يوجد تأثير لمعدل حوادث الامن السيبراني علي خبرة مراقب الحسابات في الشركات المقيدة بالبورصة المصرية وتتفق هذه النتيجة مع نتائج التحليل الأساسي.

4/6-النتائج والتوصيات ومجالات البحث المقترحة

استهدف البحث دراسة واختبار العلاقة بين معدل حوادث الامن السيبراني وخبرة مراقب الحسابات مع التطبيق علي الشركات المقيدة بالبورصة المصرية .

ومن اجل ذلك استخدم الباحث التقارير المالية السنوية وتقارير المراجعة والتقارير المتاحة علي موقع مباشر مصر ومواقع الشركات الموجودة علي الانترنت والتي بلغت 102 شركة في الفترة من 2016 حتي 2023 والتي تمثل فترة اجراء البحث.

وتوصل الباحث في ظل التحليل الأساسي، الي وجود تأثير سلبي ولكنه غير معنوي لمعدل حوادث الامن السيبراني علي خبرة مراقب الحسابات بالشركات المقيدة بالبورصة المصرية.

كما توصل الباحث في التحليل الإضافي أيضا الي وجود تأثير سلبي ولكنه غير معنوي لمعدل حوادث الامن السيبراني علي خبرة مراقب الحسابات بالشركات المقيدة بالبورصة المصرية

واخير توصل الباحث في تحليل الحساسية الي وجود تأثير سلبي ولكنه غير معنوي لمعدل حوادث الامن السيبراني علي خبرة مراقب الحسابات بالشركات المقيدة بالبورصة المصرية.

وعند ادخال المتغير الرقابي حجم مكتب المحاسبة والمراجعة علي العلاقة الرئيسة محل الدراسة، تبين وجود تأثير لذلك المتغير علي المتغير التابع محل الدراسة.

وفي ضوء اهداف البحث وحدوده ومشكلته وما انتهي اليه من نتائج في شقيه النظري والتطبيقي ، يوصي الباحث بما يلي:

بالنسبة للشركات:

- ضرورة الإفصاح عن حوادث الامن السيبراني ومعدلاتها كل عام حتي تتمكن الشركات من اخذ الحذر قبل وقوع الحادث السيبراني.

بالنسبة للجهات المهنية:

- ضرورة الزام الشركات بتطبيق الإفصاح عن مخاطر الامن السيبراني
- ضرورة عمل ورش تدريبية لتوعيتهم بخطورة الحادث السيبراني والمساعدة علي التدريب للحد من هذا الخطر

في ضوء ما سبق يقترح الباحث المجالات البحثية التالية مستقبلا :

- اثر معدل حوادث الامن السيبراني علي جودة المراجعة الداخلية
- اثر الإفصاح عن حوادث الامن السيبراني علي اتعاب المراجعة
- اثر معدل حوادث الامن السيبراني علي هيكل الرقابة الداخلية

مراجع البحث

أولا:المراجع العربية:

- أبو العلا، أسامة مجدي فؤاد محمد.2022 . إستخدام جودة هيكل الرقابة الداخلية في تفسير العلاقة بين المعاملات مع الأطراف ذوي العلاقة وقيمة الشركة : دراسة تطبيقية . ***المجلة العلمية للدراسات والبحوث المالية والتجارية، كلية التجارة – جامعة دمياط،*** 3(1)ج 2 .201 -261 .
- المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات. ***وزارة الاتصالات المصرية*** 2022. متاح علي الموقع الإلكتروني: https://www.egcert.eg/ar.

- بدوى، هبة الله عبدالسلام.2018. أثر خطرى المراجعة وأعمال عميل المراجعة على قرار مراقب الحسابات بشأن قبول التكليف بمراجعة الحسابات: دراسة تجريبية. ***مجلة كلية التجارة للبحوث العلمية***، كلية التجارة- جامعة اسكندرية:1-49.
- فرج،هانى خليل.2022. أثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بالأسهم - دراسة تجربية. ***مجلة المحاسبة والمراجعة***، اتحاد الجامعات العربية – كلية التجارة، جامعة بنى سويف، العدد الثانى: 129-209.
- زكي، نهي محمد.2017.دراسة واختبار العلاقة بين جودة المراجعة الخارجية وخلو القوائم المالية للشركات المقيدة بالبورصة المصرية من الغش. ***مجلة الإسكندرية للبحوث المحاسبية- جامعة الإسكندرية- كلية التجارة***، 2(1):1111-1152.
- زكي، نهى محمد. 02018.***أثر جودة المراجعة الخارجية علي الحد من السلوك الانتهازي للإدارة ومنع الغش بالقوائم المالية: دراسة تطبيقية علي الشركات المقيدة بالبورصة المصرية***. رسالة دكتوراه غير منشورة، كلية التجارة، جامعة الإسكندرية.
- شحاته،شحاته السيد.2015. أثر خبرة مراقب الحسابات وحجم منشأته على جودة المراجعة الخارجية - دراسة تجريبية. ***مجلة كلية التجارة للبحوث العلمية***، كلية التجارة- جامعة اسكندرية، العدد الثاني- المجلد الثاني والخمسون : 1-32.
- نويجي، حازم محفوظ محمد. ٢٠١٩. أثر درجة تعقد التقديرات المحاســبية علي تخطيط إجراءات المراجعة وتقرير مراقب الحسـابات- دراسـة تجريبية. ***مجلة الإسكندرية للبحوث المحاسبية- جامعة الإسكندرية- كلية التجارة***، 3(3): 395-461.

ثانيا: المراجع الأجنبية :

-Arens, Alvins, Loebbecke, James. 2003. Auditing an Integrated Approach. Eight Edition. ***New Jersey: Prentice Hall***.

- Abozaid, E. M., Elshaabany, M. M., and Diab, A. A. 2020. The impact of Audit Quality on Narrative Disclosure: Evidence from Egypt. ***Academy of Accounting and Financial Studies Journal,*** 24(1):1-14.

- Aicpa. 2017. Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

- Anis Chariri.2017. The Effect of Auditor Ethics, Auditor Experience, Audit Fees and Auditors Motivation on Audit Quality. ***SIJDEB***,12: 203-218.

- Berkman, H., J. Jona, G. Lee, and N. S. Soderstrom. 2019. Digital insiders and informed trading before earnings announcements. ***Working paper***.

- Berman, S., I. Roffman, and M. Todman. 2019. Year in review: the SEC and cybersecurity.

- Bryan, D., Mason, T. and Reynolds, J.K. 2018. "Earnings autocorrelation, earnings volatility, and audit fees", Auditing: ***A Journal of Practice and Theory,***37(3): 47-69.

-Beck, P., & Wu, M. 2006. Learning by doing and audit quality. ***Contemporary Accounting Research***, 23(1):1- 30.

-Bumgarner, N., & Vasarhelyi, M. A. 2015. Continuous auditing — a new view audit analytics and continuous audit: looking toward the future. New York: ***AICPA*** :3–51.
- Berglund, N. R., Eshleman, J. D., and Guo, P. 2018. Auditor size and going concern reporting. Auditing: A ***Journal of Practice and Theory***, 37(2):1-25.
-Cabaj, K., Kotulski, Z., Księżopolski, B., & Mazurczyk, W. 2018. Cybersecurity: trends, issues, and challenges. ***EURASIP Journal on Information Security.***
- Cai, C., Zheng, Q., & Zhu, L. 2019. The effect of shared auditors in the supply chain on cost stickiness. ***China Journal of Accounting Research***, 12 (4): 337–355. https://doi.org/10.1016/j.cjar.2019.09.001.
- Carcello, J.V., Nagy, A.L., 2004b. Client size, auditor specialization and fraudulent financial reporting. ***Manager. Audit. J,*** 19 (5):651–668.
- Chang, Y., Chen, H., Cheng, RK, & Chi, W. 2019. Journal of Contemporary Accounting & Economics The impact of internal audit attributes on the effectiveness of internal control over operations and compliance.***Journal of Contemporary Accounting & Economics,*** 15(1):1–19.
- Chebaane, S., and Othman, H. B. 2014. The impact of IFRS adoption on value relevance of earnings and book value of equity: the case of emerging markets in African and Asian regions. ***Procedia-Social and Behavioral Sciences***,145:70-80.
- Chen, T., Barbarossa, S., Wang, X., Giannakis, G. B., & Zhang, Z. L.2019. Learning and Management for Internet of Things: Accounting for Adaptivity and Scalability. ***Proceedings of the IEEE***.
- Colonel Terrence L. Howard.2012. Forming a Cyber Coalition. ***United States Army War College,***8-98.
-Campbell, K., L. A. Gordon, M. P. Loeb, and L. Zhou.2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. ***Journal of Computer Security*** ,11 (3):431-448.
- Curtis, M.B., Jenkins, J.G., Bedard, J.C., Deis, D.R., 2009. Auditors' training and proficiency in information systems: a research synthesis. ***J. Info. Syst,*** 23(1):79–96.
- Cisco. 2017. Annual cybersecurity report.
-Center for Audit Quality (CAQ).2014.CAQ Member Alert: Cyber security and the External Audit.
-Dervojeda, K., Verzijl, D., Nagtegaal, F., Lengton, M., & Rouwmaat, E. 2014. Innovative Business Models: Supply chain finance. Netherlands: Business Innovation Observatory; ***European Union.***
- Drljača, D., & Latinović, B.2017. Frameworks for Audit of an Information System in Practice. JITA - ***Journal of Information Technology and Applications (Banja Luka) - APEIRON***, 12(2).
- Dunn, K., Mayhew, B., 2004. Audit firm industry specialization and client

disclosure quality. Rev. ***Account. Stu,***. 9 (1):35–58.
- Dewi, T. H. S., Gunarhadi, & Riyadi, K. 2018. The Important of Learning Media Based on Illustrated Story Book For Primary School. ***Proceeding of International Conference On Child-Friendly Education, Universitas Muhammadiyah Surakarta***, 233–236.
- EY. 2018. Understanding the Cybersecurity Threat: The Board's Role. ***New York: Corporate Governance Advisor,*** 26:9-17
- Friday, I., & Japhet, I. 2020. Information technology and the accountant today: What has really changed? ***Journal of Accounting and Taxation***.
- Gaballa, A. S. M, & Ning, Z. 2011. An analytical study of the effects of experience on the performance of the external auditor. ***International Conference on Business and Economics Research***, 1: 169 -173.
- Gallizo, J. L., and R. Saladrigues., 2016,. An analysis of determinants of going concern audit opinion: Evidence from Spain stock exchange. ***Intangible Capital,*** 12(1):1-16.
- Gepp, A., Linnenluecke, M. K., O'Neill, T. J., & Smith, T. 2018. Big data techniques in auditing research and practice: Current trends and future opportunities. ***Journal of Accounting Literature***, 40:102–115.
- Gross, M. L., Canetti, D., & Vashdi, D. R. 2017. Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. ***Journal of Cybersecurity***, 3(1): 49–58.
-Gul, F. A., Fung, S. Y. K., & Jaggi, B. 2009. Earnings quality: Some evidence on the role of auditor tenure and auditors' industry expertise. ***Journal of accounting and Economics***, 47(3): 265-287.
- Gordon, R.; Carrigan, M. and Hastings, G.2011. A Framework for Sustainable Marketing. ***Marketing Theory***, 11 (2):143-163.
- Goel, S. and Shawky, H.A. 2009. Estimating the Market Impact of Security Breach Announcements on Firm Values. ***Information & Management,*** 46:404-410.
-He Li and Sungjin Yoo and William J. Kettinger.2021. The Roles of IT Strategies and Security Investments in Reducing Organizational Security Breaches. ***Journal of Management Information Systems*** , 38(1): 222-245.
- Hinz, N., M. Coolbaugh, L. Shevenell, G. Melosh, W. Cumming, and P. Stelling, 2015. Preliminary Ranking of Geothermal Potential in the Cascade and Aleutian Volcanic Arcs, Part III: Structural tectonic settings of the Volcanic Centers. ***Geothermal Resources Council Transactions,*** 39:717- 725.
-Ibrahim, A., Valli, C., Mcateer, I., & Chaudhry, J.2018. A security review of local government using NIST CSF: A case study. ***Journal of Supercomputing***, 74(10): 5171- 5186.
- Iswari and Y. Hardini. 2017. The Moderating Effect of Public Accounting Firm Size on Correlation of Organizational-Professional Conflict and Auditor Judgment.

Review of Integrative Business and Economics Research, 6(1):427-436.
-ISACA.2015. Cyber security audit. ***Isaca Journal***, 6.
- ISACA. 2019. Test your skills and take your career to the next level. Trends, challenges and audit in a rapidly changing landscape, 6.
- Jreissat, E. R., Gall, J. M., & Doheir, M. 2018. A Review of IT Audit, ITG / ISG and Cobit Frameworks on Institutions in " MENA " Region. ***International Journal of Pure and Applied Mathematics***, 119(18):525–541
- Khin, S. and Ho, T. C. F. 2019, Digital technology, digital capability and organizational performance: A mediating role of digital innovation, ***International Journal of Innovation Science***, 11(2): 177–195.
- Kuntari, Chariri, & Nurdhiana.2017. The Effect of Auditor Ethics, Auditor Experience, Audit Fees and Auditor Motivation on Audit Quality. ***International Journal of Dynamic Economics and Business***,1(2): 203-218.
-Krishnan, G., 2003. Does Big 6 auditor industry expertise constrain earnings management? Account. ***Horizons***, 17:1–16.
- Kusuma Panji & Sukirman .2017. The Effect of Emotional Intelligence and Auditor's Experience on Audit Quality with Independence as A Moderating Variable. ***Accounting Analysis Journal*** , (3) : 370-379.
- Lehmann, C. M, & Norman, C. S. 2006. The Effects of experience on complex problem representation and judgment in auditing: An experimental investigation. ***Behavioral Research in Accounting***, 18:65–83.
- Li, T. (Carol), & Chan, Y. E. 2019. Dynamic information technology capability: Concept definition and framework development. ***Journal of Strategic Information Systems.***
-Libby & Frederick. 1990. Experience and the Ability To Explain Audit Findings. ***Journal of Accounting Research,*** 28 (2).
-Liu, L., X. Xie, Y. Chang, and D. Forgione. 2017.New Clients, Audit Quality, and Audit Partner Industry Expertise: Evidence from Taiwan, ***International Journal of Auditing***: 1-16.
-Michael L. Ettredge& Vernon J. Richardson.2003. Information Transfer among Internet Firms: The Case of Hacker Attacks. ***Journal of Information Systems*** ,17 (2): 71–82.
- Moroney, R., & Simnett, R. 2009. Differences in industry specialist knowledge and business risk identification and evaluation. ***Behavioral Research in Accounting,*** 21(2): 73-89.
- Malchenko YA .2020. From digital divide to consumer adoption of smart city solutions: a systematic literature review and bibliometric analysis.19(3):316–335.
- Ndlovu, S. L., & Kyobe, M. E. 2016. Challenges of CoBIT 5 IT Governance Framework Migration. In CONF-IRM: 58.
- Nouri, S., and B. Gilaninia. 2017. The Effect of Surplus Free Cash Flow and Audit

Quality on Earnings Management. ***International Journal of Economics and Financial Issues*** 7(3):270-275.
- Osamah, A., Mazen, S., & Helal, I. 2018. Cyber Security Tools for IS auditing. In the 6th international conference on enterprise systems. Cyprus: ***Research gate.***
- Otero, A. R. 2019. Information Technology Control and Audit. taylor & francis group. ***https://doi.org/10.1201/9780429465000.***
-Panchanatham, D. N. 2015. A case study on Cyber Security in E-Governance. ***International Research Journal of Engineering and Technology***.
- PricewaterhouseCoopers, 2002. 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.
- Public Company Accounting Oversight Board (**PCAOB**)2018b. Standing advisory group meeting.
- Public Company Accounting Oversight Board (**PCAOB**)2019b. Cybersecurity: where we are; what more can be done? A call for auditors to lean.
- Public Company Accounting Oversight Board (**PCAOB)** 2018a. Inspections outlook for 2019.
- Public Company Accounting Oversight Board (**PCAOB**). 2014. Standing advisory group meeting.
- Raguseo, E. 2018. Big data technologies: An empirical investigation on their adoption, benefits and risks for companies. ***International Journal of Information Management***, 38(1):187–195.
-Richardson, M., A. Hunt, J. Hinds, R. Bragg, D. Fido, D. Petronzi, L. Barbett, T. Clitherow, et al. 2019. A measure of nature connectedness for children and adults: Validation, performance, and insights. Sustainability, 11: 3250.
-Rebecca R. and U. Murthy. 2021. The Impact of Cybersecurity Risk Management Examinations and Cybersecurity Incidents on Investor Perceptions and Decisions. ***AUDITING: A Journal of Practice & Theory*** ,40 (1): 73–89.
- Securities and Exchange Commission ***(SEC)***. 2018a. Commission statement and guidance on public company cybersecurity disclosures.
- Securities and Exchange Commission ***(SEC)***. 2018b. Public companies should consider cyber threats when implementing internal accounting controls.
- Securities and Exchange Commission ***(SEC)***. 2018c. Report of investigation pursuant to Section 21(a) of the Securities Exchange Act of 1934 regarding certain cyber-related frauds perpetrated against public companies and related internal accounting controls requirements.
- Securities and Exchange Commission ***(SEC).*** 2018d. Statement on cybersecurity interpretive guidance.
- Saha, S.S. & Roy, M.N. 2017. Quality control procedures for statutory financial

audit: An empirical study. **Emerald Publishing, Bingley**.
-Sharma, R. 2012. Study of Latest Emerging Trends on Cyber Security and its challenges to Society. ***International Journal of Scientific & Engineering Research***, 3(6).
- Shen, L. 2014. The NIST cybersecurity framework: Overview and potential impacts. ***SciTech Lawyer,*** 10(4): 16.
- Sila, M., B. Subroto, Z. Baridwan, and A. Rahman. 2016. The Effect of Knowledge and Experience on Professional Auditor's Judgment: Study on State Auditor in Indonesia, ***International Journal of Management and Administrative Science****s*, Vol. 3, Issue 10: 98-106.
- Suffian, Mohd, Taufik, Mohd, Mohd Sanusi, Zuraidah, dan Mastuki, Nor'azam. 2015. Real earnings management and firm value: Empirical evidence from Malaysia/Mohd Taufik Mohd Suffian, Zuraidah Mohd Sanusi and Nor'Azam Mastuki. ***Malaysian Accounting Review***, 14(1): 26-47.
- Saputra, KAK, Juniariani, NMR, Jayawarsa, AAK, &Darma, IK (2019). Conflict of Interest and Auditor Independence in Public Accounting Firms in Bali. I***nFestation*** , 15 (1), 1– 9.
-Samuel, K. O., & Osman, W. R.2014. Cyber Terrorism Attack of The Contemporary Information Technology Age: Issues, Consequences and Panacea. ***International Journal of Computer Science and Mobile Computing***, 3(5):1082-1090.
-Soekrisno Agoes. 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.
- Stanley, J.D., De Zoort, F.T., 2007. Audit firm tenure and financial restatements: an analysis of industry specialization and fee effects. ***J. Account. Publ Policy,*** 26: 131–159.
- Southall, Jane and Wason, Hilary.2016. Evaluating the use of synoptic assessment to engage and develop lower level Higher Education students within a Further Education setting. ***Practitioner Research in Higher Education***,10 (1):192-202.
- Sengers, T. 2017. **The Effect of Audit Partner and Firm Tenure on audit quality**. Published Thesis to Fulfillment of the Requirements for the Degree of Master of Economics, Radboud University.
- Tamimi, M., Aljohani, R., Alzahrani, A., & Alharbi, B.2019. SECURITY REVIEW BASED ON ISO 27000/ ISO 27001/ ISO 27002 STANDARDS: A CASE STUDY RESEARCH. **At Istanbul, Turkey: Proceedings of Researchfora 48th International Conference.**
- Verwey, I. G., and Asare, S. K. 2021. The joint effect of ethical idealism and trait skepticism on auditors' fraud detection. ***Journal of Business Ethics***, 171(2):1-15.
- Verizon: 2019 Data Breach Investigations Report (2019).

- WSJ. 2016. Cybersecurity and the board: 8 issues keeping directors up at night. ***Wall Street Journal.***
- Yazan Y A, Wan S Y, Muhammad A. and Anas N.G.2019.The Effect of Audit Tenure and Audit Firm Size on the Audit Quality :Evidence from Jordanian Auditors. ***International Journal of Business and Technopreneurship***,9(1):15-24.
- Yeboah, T. 2013. A Proposed Information Technology Audit Framework for Microfinance Kumasi. ***Journal Of Engineering, Computers & Applied Sciences***, 2(8):1-7. Retrieved from ***https://www.borjournals.com.***
- Yen, J.-C., J.-H. Lim, T. Wang, and C. Hsu. 2018. The impact of audit firms' characteristics on audit fees following information security breaches. ***Journal of Accounting and Public Policy*** 37 (6):489-507.