مجلة البحوث المحاسبية

https://abj.journals.ekb.eg/

كلية التجارة – جامعة طنطا

العدد : الاول

مارس 2024

القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني – دراسة انتقادية وتجريبية

The Added value of the effectiveness of internal audit consulting and assurance roles in the field of cyber security risk management-A criticism and experimental study

الدكتور

حنان محمد اسماعيل يوسف

أستاذ مساعد بقسم المحاسبة والمراجعة

كلية الأعمال – جامعة الإسكندرية

وأستاذ مشارك في كلية الأعمال، جامعة الإمام محمد بن سعود الإسلامية

المملكة العربية السعودية

Email: Hanan.ismail@alexu.edu.eg

hmyoussef@imamu.edu.sa

ملخص البحث

استهدف البحث دراسة واختبار القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني في بيئة الأعمال المصرية، واعتمد الباحث على تصميم تجريبي (2×2×2)

تم من خلاله محاكاة لشركة افتراضية ذات مخاطر سيبرانية مرتفعة، في ظل حالتين رئيسيتين أحداهما تعكس مستوى فعالية مراجعة داخلية مرتفع، والأخرى مستوى فعالية مراجعة داخلية منخفض، مع مجموعة من المعالجات التي تعكس ضمن الحالتين المتغيرات المعدلة للدراسة وهما التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات (مرتفع/ منخفض)، دعم الإدارة العليا لوظيفة المراجعة الداخلية (مرتفع/ منخفض)، لاختبار الأثر على القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني.

تم استخدام عينة مكونة من (2480) مشاهدة من (62) مشارك من المهتمين بوظيفة المراجعة الداخلية في شركات المساهمة المقيدة بالبورصة المصرية. خلص الباحث إلى وجود أثر إيجابي معنوي احصائياً لفعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني على قيمتها المضافة في مجال إدارة مخطر الأمن السيبراني، وأن "التعاون" بين المراجع الداخلي وموظفي تكنولوجيا المعلومات لم يكن له تأثير على العلاقة محل الدراسة، بينما اتضح وجود تأثير إيجابي معنوي احصائياً لدعم الإدارة العليا لوظيفة المراجعة الداخلية على هذه العلاقة، بما يشير إلى أن الأثر الإيجابي لفعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني على قيمتها المضافة يختلف باختلاف مستوى دعم الإدارة العليا لوظيفة المراجعة الداخلية.

الكلمات المفتاحية: فعالية المراجعة الداخلية، الدوران الاستشاري والتوكيدي للمراجعة الداخلية، القيمة المضافة من فعالية أداء المراجعة الداخلية، إدارة مخاطر الأمن السيبراني.

Abstract:

The research aimed to study and test the added value of the effectiveness of internal audit's performance of its consulting and assurance role in the field of cybersecurity risk management in the Egyptian business environment. The researcher relied on an experimental design (2X2X2) Through a simulation of a hypothetical company with high cyber risks, under two main cases, one of them reflects a high level of internal audit effectiveness, and the other a low level of internal audit effectiveness, with a set of treatments within the two cases reflect the modified variables of the study, which are cooperation between the internal audit and information security functions (High/low), senior management support for the internal audit function (high/low), to test the impact on the added value of the effectiveness of internal audit's performance of consulting and assurance roles in the field of cybersecurity risk management.

The study was conducted on a sample of (2480) observations from 62 participants from the Egyptian Stock Exchange-listed companies interested in the internal audit function. The researcher found that there was a statistically significant positive effect of the effectiveness of the internal audit function's performance of consulting and assurance roles in the field of cybersecurity risk management on its added value in the field of cybersecurity risk management, and that "cooperation" between the internal auditor and IT staff had no effect on the relationship of the study. While there is a statistically significant positive effect of senior management's support for the internal audit function on this relationship, which indicates that the positive impact of the effectiveness of the internal audit function's performance of its consulting and assurance role in the field of cybersecurity risk management on its added value varies according to the level of senior management's support for the internal audit function.

Keywords: Internal audit effectiveness, Internal audit Consulting and assurance roles of internal audit, value added from effective internal audit performance, cybersecurity risk management.

1- مقدمة

تعتبر وظيفة المراجعة الداخلية الحديثة Internal Audit Function (IAF) أداة مستقلة من أدوات الرقابة الداخلية المضيفة للقيمة، من خلال أداءها لدورين أساسيين وهما، **الاستشاري Consulting، والتوكيدي Assurance**، وذلك في ثلاث مجالات رئيسية هي؛ إدارة المخاطر والرقابة الداخلية، وحوكمة الشركات، بما يساعد الشركة على تحسين عملياتها وتحقيق أهدافها، مما يساهم في خلق قيمة مضافة للشركة.

ونظرا للتحول الرقمي Digital Transformation (DT)[1] الذي غلب على واقع الأعمال في الفترة الأخيرة وزيادة استخدام تكنولوجيا المعلومات، أصبحت الجرائم السيبرانية متضمنة الهجمات الإلكترونية، خرق البيانات، انقطاع غير مخطط له في تكنولوجيا المعلومات والاتصالات، والحوادث الأمنية، بما يعرف **بمخاطر الأمن السيبراني Cybersecurity Risks**، أحد أهم مخاطر الأعمال المثيرة لقلق الشركات، أصحاب المصالح، الحكومات (Deloitte 2015; Alina et al. 2017; Lois et al. 2021).

يؤدي مجلس الإدارة دوراً رقابياً، بما يساعد في دعم خلق القيمة في الشركة ومنع تدهورها، وقد لعبت إدارة مخاطر الشركة[2] **Enterprise Risk Management (ERM)** دوراً مسانداً قوياً في هذا الشأن، (NIST 2020). وتعد الإدارة هي المسئولة عن تصميم وتنفيذ برنامج إدارة مخاطر الشركة ويقوم مجلس الإدارة بالإشراف والرقابة على كيفية تصميم وتشغيل الإدارة لهذا البرنامج (COSO 2017)، وعليه أصبحت إدارة الشركة في ظل بيئة التحول الرقمي مسئولة بقوة عن تصميم وتنفيذ برنامج إدارة مخاطر الشركة متضمناً مخاطر الأمن السيبراني (NIST 2020).

---

[1] وفقا لدراسة على (2022) يمكن تعريف التحول الرقمي للشركات على أنه" عملية تغيير جذري وتطوير للبنية التحتية لنماذج أداء الأعمال، عن طريق الاعتماد على التقنيات والأدوات التكنولوجية المستحدثة، سواء أكان ذلك بصورة جزئية أو بصورة كلية، لاكتساب ميزة تنافسية وتحقيق قيمة مضافة والسعي نحو تحقيق الأهداف المرجوة من استراتيجيات الأعمال، بصفة عامة".

[2] وفقا لما ورد لتقرير لجنة COSO (2004) عملية إدارة المخاطر هي "عملية تتأثر بأعضاء مجلس إدارة المنشأة، والإدارة ، والأفراد الآخرين، والتي تطبق في إطار عملية وضع إستراتيجية المنشأة، ويتم تصميمها لتحديد الأحداث المحتملة التي قد تؤثر علي المنشأة، وتقوم هذه العملية على التحكم في المخاطر لتكون في الحدود المقبولة للمنشأة، ولتقديم تأكيد معقول فيما يتعلق بتحقيق أهداف المنشأة ".

ونتيجة للتغيرات المتسارعة في بيئة الأعمال والممارسة المهنية الحالية في ظل بيئة التحول الرقمي، يمكن لوظيفة المراجعة الداخلية أن تكون أداة فعالة في تحسين حماية المعلومات ومساعدة مجلس الإدارة والمديرين التنفيذين في أداء مسئولياتهم الخاصة بحوكمة الأمن السيبراني، من خلال القيام بدوريها؛ **الاستشاري** الذى يستهدف تقديم المشورة والنصح والإرشاد لمجلس الإدارة بصدد تحديد وتوصيف وقياس مخاطر الأمن السيبراني المحيطة ببيئة عمل الشركة التكنولوجية وكيفية مواجهتها وتفادى أثارها على تحقيق الشركة لأهدافها المرجوة، **والتوكيدي** الذى يستهدف تقديم دليل مستقل عن سياسات الأمن السيبراني ومدى الالتزام بها، وعمليات إدارة المخاطر الالكترونية وضوابط الرقابة الداخلية وفعاليتها في حماية سلامة الأصول وسرية البيانات وتوافرها (Lois et al. 2021; Slapniˇcar et al 2022 ; 2022 شحاتة)

لقد زاد اهتمام الشركات في السنوات الأخيرة، بالدور الذى يمكن تلعبه وظيفة المراجعة الداخلية كأحد الأدوات الرقابية التي من شأنها تحسين ضوابط الأمن السيبراني واتخاذ الإجراءات التصحيحية اللازمة، بما يخفف من نجاح الهجمات السيبرانية المحتملة وتحسين استراتيجية الشركة في إدارة مخاطر الأمن السيبراني (NACD 2020; Hartmann and Carmenate 2021; Lankton et al. 2021)، من خلال قدرتها على توفير استشارات وتأكيدات و مستقلة وموضوعية حول كفاية وفعالية الحوكمة وإدارة المخاطر، والتقرير عن النتائج وتوصيلها إلى الإدارة العليا، بما يعزز التحسين المستمر(IIA 2013; 2017; 2020) ، كما ظهرت أهمية هذا الدور لوظيفة المراجعة الداخلية في الدراسات المحاسبية التي هدفت إلى دراسة وتحليل فعالية المراجعة الداخلية في مجال إدارة مخاطر الأمن السيبراني، وقدرتها على تحقيق النتائج المستهدفة منها (Kahyaoglu and Caliyurt 2018; Shamsuddin et al. 2018; Eaton et al. 2019; Carcello et al. 2020; Slapniˇcar et al. 2022).

2- مشكلة البحث

تلعب وظيفة المراجعة الداخلية دوراً هاماً في مساعدة المؤسسات على تحقيق أهدافها وحماية أصولها، كما أصبحت آلية من من آليات حوكمة الشركات التي تستطيع من خلالها تحقيق رقابة

فعالة على أعمال المؤسسات وإدارة مخاطرها، يجب على المراجع الداخلي المشاركة في تحسين إدارة مخاطر الأعمال والرقابة عليها، استناداً على مدخل منظم قائم على المخاطر(IIA 2009; 2013; Carcello et al 2020; Betti and Sarens 2021)

مؤخراً، تصدرت مخاطر الأمن السيبراني قائمة مخاطر الأعمال كخطر بالغ الأهمية، والذي له أثار مالية جوهرية على الشركة، والاضرار بقيمتها وسمعتها، وأصبحت الجرائم السيبرانية تمثل تهديداً حقيقياً للشركات يؤدى إلى فقدان ثقة أصحاب المصالح، ومن ثم التأثير على أداء الأسهم وقيم الاستثمارات، علاوة على إدراك مراقب الحسابات لمخاطر أعمال أعلي للشركات التي تتعرض لخرق الكتروني وزيادة أتعاب المراجعة(Li et al. 2020; Pacheco–Paredes and Wheatley 2022; Jiang et al. 2022).

وبالرغم من الدور الإيجابي الذي يمكن أن تقدمه وظيفة المراجعة الداخلية في تحسين عمليات إدارة مخاطر الأمن السيبراني. (Alina et al. 2017; Islam et al. 2018; Kahyaoglu and Çaliyurt, 2018; Shamsuddin et al. 2018; Walton et al. 2021; Slapni˘car et al. 2022)، يعتقد الباحث بوجود ندرة في الدراسات الأكاديمية والمهنية التي قامت بتحليل واختبار القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني، وما إذا كان التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات، ودعم الإدارة العليا لوظيفة المراجعة الداخلية، له تأثير على هذه القيمة المضافة من فعالية المراجعة الداخلية، لذا ظهر دافع الباحث في تضيق الفجوة البحثية في هذا الصدد من خلال الإجابة على السؤالين التاليين وفق منهجية بحث انتقادية وتجريبية:

- ما علاقة فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني بقيمتها المضافة؟
- ما أثر التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات، ودعم الإدارة العليا لوظيفة المراجعة الداخلية كمتغيرين معدلين، على العلاقة محل الدراسة؟

3- هدف البحث

يهدف البحث إلى تحليل واختبار، القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني، وأثر كل من

التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات، ودعم الإدارة العليا لوظيفة المراجعة الداخلية على هذه القيمة المضافة، وذلك من خلال تصميم تجريبي (2×2×2) بين المجموعات على عينة من المهتمين بوظيفة المراجعة الداخلية، وتتضمن عينة الدراسة، العاملين بأدوات المراجعة الداخلية (ممثلين لجانب العرض)، وأعضاء كل من مجلس الإدارة ولجنة المراجعة (ممثلين لجانب الطلب).

4- أهمية ودوافع البحث

يكتسب البحث **أهميته** من اسهاماته المتوقعة على المستويين **الأكاديمي والمهني**، فمن جانب **الأهمية العلمية**، يعتبر هذا البحث امتداداً للدراسات التي اهتمت بالقيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني، بالتطبيق على الشركات المقيدة بالبورصة المصرية، والعوامل التي من شأنها التأثير على القيمة المضافة من هذه الفعالية" التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات، دعم الإدارة العليا لوظيفة المراجعة الداخلية" ومن ثم تضيق الفجوة البحثية في هذا الصدد.

ومن جانب **الأهمية العملية**، تتعدد الاسهامات المتوقعة لهذا البحث على مستوى الممارسة المهنية، ولعل أهمها؛ توفير فهم أفضل للقيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني، مما يشجع مجالس إدارة المؤسسات في بيئة الأعمال المصرية، من العمل على تطوير وظيفة المراجعة الداخلية بها لما لها من مردود إيجابي، في تحقيق أهدافها الحالية والمستقبلية، والعمل على إرساء التعاون بين وظيفتي المراجعة الداخلية ووظيفة أمن المعلومات، وتقديم الدعم الكامل لوظيفة لمراجعة الداخلية بما في ذلك توفير الاستقلال والموارد اللازمة لها، وتنفيذ توصياتها بشأن إدارة مخاطر الأمن السيبراني.

وتتمثل أهم دوافع البحث في محاولة الباحث المساهمة الأكاديمية لموضوع أعطته الدولة المصرية أهمية على المستوى القومي، فقد نصت المادة 31 من الدستور المصري على أن "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذى ينظمه القانون" (دستور جمهورية مصر العربية 2014)، كما يعد من دوافع البحث تضيق فجوة البحث المحاسبي، فيما يتعلق بفعالية أداء

المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني وما يوفره من قيمة مضافة، من خلال دراسة مشكلة البحث، واختبار فرضياته، وفق منهجية علمية تجريبية منضبطة، تتلافى قدر الإمكان سلبيات الدراسات الاستقصائية، والتوصل إلى نتائج قد تسهم في تحسين الدور الذي ينبغي أن تؤديه المراجعة الداخلية في إدارة مخاطر الأمن السيبراني في بيئة الأعمال المصرية.

5- حدود البحث

يقتصر البحث على دراسة واختبار القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني في الشركات المقيدة في البورصة المصرية، وبذلك يخرج عن نطاق البحث أثر هذه القيمة المضافة من أداء المراجعة الداخلية لدوريها على مجال إدارة مخاطر الأعمال الأخرى بخلاف إدارة مخاطر الأمن السيبراني، مصدر تقديم خدمة المراجعة الداخلية، وأخيراً فإن إمكانية تعميم نتائج البحث مشروطة بضوابط اختيار عينة الدراسة والتصميم التجريبي المستخدم في هذا البحث.

6- خطة البحث

انطلاقاً من مشكلة البحث وهدفه وفى ضوء حدوده سوف يتم استكماله على النحو التالي:

1/6 إدارة مخاطر الأمن السيبراني من منظور مهني وأكاديمي

2/6 فعالية وظيفة المراجعة الداخلية، المفهوم والمقاييس

3/6 تحليل الدراسات السابقة واشتقاق فروض البحث

4/6 منهجية البحث

5/6 نتائج الدراسة التجريبية

6/6 الخلاصة والتوصيات وأهم مجالات البحث المستقبلية المقترحة

1/6 إدارة مخاطر الأمن السيبراني من منظور مهني وأكاديمي

أصبحت مخاطر خرق البيانات أكثر تعقيداً وشيوعا في بيئة الأعمال المعاصرة[3]، وقد أثارت زيادة الجرائم السيبرانية Cyber–crime[4] حول العالم وتبعياتها الاقتصادية مخاوف واهتمام المنظمات بشأن كيفية حماية المعلومات والحفاظ على سلامة قواعد البيانات (Pacheco–Paredes and Wheatley 2022)، فقد عكس خطاب مفوض SEC لويس أجيلار في بورصة نيويورك عن هذه المخاوف، فقد صرح بأنه قد يمتد تأثير الهجمات السيبرانية إلى ما هو أبعد من التكاليف المباشرة المرتبطة بالاستجابة الفورية للهجمات، فبالإضافة إلى الضرر غير المقبول للعملاء، تشمل الأثار الثانوية لتلك الهجمات الضرر والتأثير على السمعة، الذى يؤثر بشكل جوهري على أرباح الشركة (Li et al. 2020)، إضافة إلى انتشار الأثار الاقتصادية السلبية للشركة المخترقة إلى الشركات بالصناعة بما يعرف بأثار عدوي الصناعة industry contagion effects (Kelton and Pennington 2020) كما أشار Janvrin and Wang (2022) إلى أن الجرائم السيبرانية لها أثار على المحاسبين والمراجعين لأنها قد تؤدى إلى انخفاض أداء الشركة، والقيمة السوقية لها، وزيادة المخاطر التشغيلية، والمعلومات المفقودة.

ونتيجة زيادة مخاوف الشركات، والقلق المتزايد من التبعيات الاقتصادية للهجمات السيبرانية، زاد اهتمام الشركات **بالأمن السيبراني**، ويعرف الأمن السيبراني بأنه "مجموعة من الأدوات والسياسات ومفاهيم وضمانات الأمن، والمبادئ الإرشادية، ومداخل إدارة

---

[3] تعرضت العديد من الشركات حول العالم لهجمات الكترونية، علي سبيل المثال، في 2013 استطاع مخترقي البيانات الكترونيا (الهكر) الوصول إلي بيانات بطاقات الائتمان والمعلومات الشخصية للملايين من الأشخاص من خلال اكتشاف نقاط الضعف في نظم نقاط البيع لشركة Target ، وفي 2014 نشرت مجموعة الهكر بيانات سرية لشركة Sony Pictures Entertainment تضمنت معلومات شخصية لموظفي الشركة، ورسائل البريد الالكتروني بين الموظفين، ومعلومات عن رواتب المديرين التنفيذين بالشركة، ونسخ من أفلام سوني التي لم يتم عرضها بعد، وفي عام 2017 أعلنت شركة Equifax عن تعرضها لهجمة الكترونية من المحتمل أن تؤثر على ما يقرب من 143 مليون مستهلك في الولايات المتحدة (Li et al. 2020)

[4] عرف Asthana et al. (2021) الجرائم السيبرانية بأنها "جريمة ترتكب باستخدام أجهزة الكمبيوتر أو الانترنت لتعطيل أو تدمير أو التحكم بشكل ضار في بيئة الحوسبة أو البنية التحتية للهدف أو تدمير سلامة البيانات، أو سرقة الرقابة على المعلومات"، ويقدر أن تكلف الجرائم السيبرانية الاقتصاد العالمي ما يقرب من 6 ترليون دولار بحلول عام 2025 (Kelton and Pennington 2020)

المخاطر، والأفعال والتصرفات، والتدريب، وأفضل الممارسات، والتوكيد، والتكنولوجيا، التي يمكن استخدامها لحماية أصول معلومات المنظمة ضد التهديدات الداخلية والخارجية" (Saudi Arabian Monetary Authority 2017) ووفقاً لإطار الأمن السيبراني Saudi Arabian Monetary Authority (2017) تشمل أهداف الأمن السيبراني بصفة عامة ثلاثة أهداف رئيسية وهم؛ **السرية confidentiality** : المعلومات متاحة فقط للأشخاص المصرح لهم بالوصول لها، **السلامة integrity** : أي أن تكون المعلومات دقيقة وكاملة وتم معالجتها بشكل صحيح، ومحمية من التعديل غير المصرح به، أو التدمير لنظام تكنولوجيا المعلومات بصورة جزئية أو كلية، **الإتاحة availability:** المعلومات محمية من الانقطاع غير المصرح به. كما عرف AICPA (2017) الأمن السيبراني بأنه" مجموعة التقنيات والعمليات والإجراءات المصممة لحماية أجهزة الكمبيوتر وقواعد البيانات والشبكات والتطبيقات، وما تحتويه من بيانات وخدمات من الهجمات الالكترونية، والوصول غير المصرح به، والتغيير أو التعطيل وسوء الاستخدام، أو الاستغلال غير المشروع، كما أكدت دراسة Kahyaoglu and Caliyurt (2018) على أن الأمن السيبراني هو" أنشطة أو عمليات أو قدرات أو حالة تكون المعلومات أو أنظمة الاتصال والمعلومات المرتبطة بها محمية أو يتم الدفاع عنها ضد التخريب أو استخدام غير مصرح به، أو التعديل، أو سوء الاستغلال"، وفي نفس السياق عرفت دراسة Li et al. (2020) الأمن السيبراني بأنه "الحفاظ على سرية، تكامل، وتوافر المعلومات في البيئات المعقدة، نتيجة تفاعل الأفراد والبرامج والخدمات على الانترنت باستخدام أجهزة تكنولوجيا المعلومات والشبكات المتصلة"، وفي نفس السياق أشارت دراسة Shamsuddin et al. (2018) إلى أنه يعتبر الأمن السيبراني من أولويات الشركات، نتيجة كثرة الاختراقات والخوف من الهجمات السيبرانية وفشل الأمن بما يؤثر علي في الاقتصاد العالمي، فقد نما الانفاق السنوي على الأمن السيبراني حول العالم بنسبة 64%، من 75.6 بليون دولار في 2015 إلى 124 مليار دولار في 2020، الانفاق العالمي علي الحلول الأمنية سيحقق معدل نمو سنوي تراكمي (CAGR) 9.2% للفترة من 2018 – 2022، وتصل إلى 133.8 بليون دولار في 2022 (Lee 2021).

مع التطورات المستمرة في تكنولوجيا المعلومات، يواجه الأمن السيبراني أساليب وتقنيات جديدة تهدف إلى الاستفادة من نقاط الضعف في أدوات الرقابة علي تكنولوجيا المعلومات (Lee 2021)، بما يعرف **باختراق الأمن السيبراني،** وهو خسارة سرية المعلومات أو سلامتها أو اتاحتها، بما في ذلك أي ضرر ناتج عن سلامة معالجة المعلومات أو النظم، سلامة أو إتاحة مدخلات أو مخرجات النظام، والذى له تأثير سلبي على تحقيق أهداف والتزامات الأعمال، بما في ذلك التزامات ومسؤوليات الأمن السيبراني (AICPA 2017)، كما عبرت PCAOB (2020) عن مخاوفها حول الأمن السيبراني حيث أكدت أن أهم أهداف الخطة الاستراتيجية 2020-2024 هو تقييم التغيرات في بيئة أمن المعلومات وفهم المخاطر ذات الصلة، كما أشارت PCAOB (2020) إلى أن الدخول غير المصرح به، لنظم المعلومات وقواعد البيانات، يمكن أن يؤدى إلى التلاعب في البيانات، وفقدان الملكية للمعلومات الحساسة، وتدمير النظم والإضرار بالسمعة، وينبغي مراقبة هذه المخاطر وتقييم تأثير أنشطة الإشراف والرقابة عليها.

وفيما يتعلق بالجهود المصرية في التصدي والتخفيف من مخاطر السيبراني الأمن السيبراني، أطلق المجلس الأعلى للأمن السيبراني (2017)، الاستراتيجية الوطنية للأمن السيبراني (2017-2021) التي تهدف إلى رصد ومواجهة المخاطر السيبرانية وتعزيز الثقة في البني التحتية للاتصالات والمعلومات وتطبيقاتها وخدماتها، من أجل التنمية في شتي القطاعات الحيوية وتأمينها من أجل تحقيق بيئة رقمية آمنة وموثوقة للمجتمع المصري بمختلف أطيافه.

تعتبر مخاطر الشبكات من المخاطر التي لا يمكن تجنبها، ولكن يمكن إدارتها (Kahyaoglu and Caliyurt 2018، لذلك أصبح من الهام إدارة مخاطر الأمن السيبراني Cyber Security Risk Management (CSRM) من جانب الشركات (على 2022)، وقد وصف AICPA (2017) إدارة مخاطر الأمن السيبراني كعملية تنفيذ وتشغيل الأساليب الرقابية، وأنشطة إدارة المخاطر الأخرى، لحماية المعلومات والنظم من الأحداث الأمنية التي يمكن أن يتعرضوا لها، واكتشاف الأحداث الأمنية والاستجابة لها والتخفيف منها عندما

الأحداث الأمنية لا يتم منعها. وفي نفس السياق عرف Annarelli et al. (2020) إدارة مخاطر الأمن السيبراني بأنها مدخل منظم لتقييم مخاطر أمن النظام.

يوجد نوعين من الرقابة الداعمة لإدارة مخاطر الأمن السيبراني وهما؛ الرقابة الداخلية: وهى عملية يتم تنفيذها من قبل مجلس إدارة، والإدارة، والموظفين الآخرين، وتكون مصممة لتقديم توفير معقول عن أن الأهداف تم تحقيقها(COSO 2017)، **الرقابة الأمنية:** تمثل الضمانات أو الإجراءات المنصوص عليها في نظام المعلومات لحماية السرية، والسلامة، والإتاحة للنظام ومعلوماته، توفر الرقابة الأمنية الأساليب الإدارية والتقنية للإدارة للاستجابة لمخاطر الأمن السيبراني من خلال الردع deterring، الاكتشاف detecting، المنع preventing أو تصحيح التهديدات ونقاط الضعف Corrective (Stine et al. 2020)

كما أشارت العديد من الدراسات إلى ضرورة التوكيد الداخلي على الأمن السيبراني Kahyaoglu and Caliyurt (2018); Lois et al. (2021); Drašček et al. (2022) وتبنى الشركات إطار عمل للتوكيد على الأمن السيبراني، وفي هذا الشأن يوجد بعض الأُطر الأكثر استخداماً والتي يمكن أن تكون قابلة للتطبيق على المنظمات المختلفة منها وهي؛

- **أهداف الرقابة للمعلومات والتكنولوجيا المرتبطة بها (COBIT):** إطار حددته منظمة ISACA بحيث يساعد الإدارة في تخفيض الفجوة بين متطلبات الرقابة، والعناصر التكنولوجية، ومخاطر الأعمال بصورة آنية.
- **معايير المنظمة الدولية للتنميط والتوحيد (ISO):** طورت ISO معيار ISO 27000 ليمكن المنظمات من تنفيذ عمليات ونظم رقابة لدعم مبادئ أمن المعلومات.
- **معايير خاصة بالمعهد الأمريكي للمحاسبين القانونيين (AICPA):** قدم AICPA إطاراً للتقرير عن مخاطر الأمن السيبراني وإدارتها، لمساعدة إدارة الشركات للوصول إلى المعلومات الملائمة والمفيدة عن فعالية برامج إدارة الأمن السيبراني، ويُعد إطار العمل هذا مكوناً رئيسياً في أنظمة الرقابة على مستوى النظام والمنظمة System and Organization Controls (SOC)، حيث قد تختار الإدارة المعايير التي يتم من خلالها تقييم فعالية الضوابط الرقابية لتحقيق أهداف الأمن السيبراني للمؤسسة، وذلك

علي عكس إطار SOC 2 والخاص بتقارير فحص الأمن السيبراني والذى لا يجوز إجراءه إلا باستخدام معايير AICPA لخدمات الثقة.

- **الإطار الخاص بتحسين البنية التحتية للأمن السيبراني (NIST):** تم إصدار أول نسخة من NIST في فبراير 2014 كإطار لتحسين البنية التحتية للأمن السيبراني، وبنى على معايير وارشادات وممارسات لمساعدة المنظمات في الممارسة لتخفيض الأثار المحتملة للمخاطر السيبرانية.

كما أوضحت دراسة Eaton et el. (2019) خمس مراحل لإدارة مخاطر الأمن السيبراني التي ينبغي إجراؤها بشكل مستمر ومتكرر مع استمرار ظهور مخاطر جديدة للأمن السيبراني، وتتمثل هذه المراحل في؛ **تحديد مخاطر** الأمن السيبراني ومدى التعرض لها وأولوياتها، **تصميم وتنفيذ نظم الرقابة** للأمن السيبراني للتخفيف من المخاطر ومدى التعرض، **اختبار الفعالية التشغيلية لنظم رقابة** الأمن السيبراني في التخفيف من المخاطر والتعرض لها، **إعداد تقرير** إدارة مخاطر الأمن السيبراني، و**التوكيد** الموضوعي المستقل عليه.

كما أوضح Eaton et el. (2019) أنه يمكن أن تساهم وظيفة المراجعة الداخلية في نجاح برنامج إدارة مخاطر الأمن السيبراني، حيث يمكن لوظيفة المراجعة الداخلية من خلال دورها الاستشاري مساعدة الإدارة في تنفيذ الثلاثة مراحل الأولي لإدارة مخاطر الأمن السيبراني، كما يمكن أن تساهم من خلال دوريها الاستشاري والتوكيدي في المرحلتين الرابعة والخامسة.

فقد ازداد دور وظيفة المراجعة الداخلية وانتقل من مجرد التحقق من الالتزام بالسياسات، إلى تقديم النصح والتوكيد، وتدريب مديري المراجعة الداخلية (Shamsuddin et al. 2018; Lois et al. 2021)، وتطوير وتحسين نظم الرقابة الداخلية والحوكمة وإدارة مخاطر المؤسسة، وتتولي إدارة المراجعة الداخلية المؤهلة تقديم تقرير موضوعي لمجلس الإدارة والإدارة التنفيذية به رأى مستقل، عن مدى جدوى المؤسسة في تقييم مخاطر الأمن السيبراني والتعامل معها، وبدون هذا التأكد أو الضمان فإن المؤسسة تواجه تهديدات سيبرانية أكثر، وصعوبات تتعلق بأمنها وحماية أصولها، وتتخلف المؤسسة كثيراً عن

مثيلاتها في الصناعة ممن لديهم إدارة مراجعة داخلية توفر مثل هذا التأكيد (Deloitte 2015).

ويخلص الباحث مما سبق إلى أنه أصبح من الضرورة اهتمام الشركات بإدارة مخاطر الأمن السيبراني، من خلال تنفيذ وتشغيل الأساليب الرقابية، وأنشطة إدارة المخاطر الأخرى، لحماية المعلومات والنظم من الأحداث الأمنية التي يمكن أن يتعرضوا لها، واكتشاف الأحداث الأمنية والاستجابة لها والتخفيف منها عندما الأحداث الأمنية لا يتم منعها، وأنه يوجد نوعين من الرقابة الداعمة لإدارة مخاطر الأمن السيبراني وهما؛ الرقابة الداخلية: وهى عملية يتم تنفيذها من قبل مجلس إدارة، والإدارة، والموظفين الآخرين، وتكون مصممة لتقديم توفير معقول عن أن الأهداف تم تحقيقها. والرقابة الأمنية: تمثل الضمانات أو الإجراءات المنصوص عليها في نظام المعلومات لحماية السرية، والسلامة، والإتاحة للنظام ومعلوماته، توفر الرقابة الأمنية الأساليب الإدارية والتقنية للإدارة للاستجابة لمخاطر الأمن السيبراني من خلال الردع، الاكتشاف، المنع. كما خلص الباحث إلى أهمية وظيفة المراجعة الداخلية في إنجاح برنامج إدارة مخاطر الأمن السيبراني، حيث يمكن لإدارة المراجعة الداخلية المؤهلة توفير النصح والاستشارات لمجلس والإدارة التنفيذية لتحسين إدارة المخاطر، والتوكيد الموضوعي المستقل عن مدى جدوى المؤسسة في تقييم مخاطر الأمن السيبراني والتعامل معها.

وعلي الرغم من الدور الهام الذي يمكن أن تلعبه المراجعة الداخلية في نجاح إدارة مخاطر الأمن السيبراني، إلا أن هذا الدور مرهوناً بعديد من العوامل، لعل أهمها من وجهة نظر الباحث **فاعلية المراجعة الداخلية**، متفقاً في ذلك مع عدد من الدراسات (Shamsuddin et al. 2018; Lois et al. 2021; Slapni˘car et al. 2022).

2/6 فعالية وظيفة المراجعة الداخلية، المفهوم والمقاييس

تواجه الشركات في السنوات الأخيرة، زيادة كبيرة في مخاطر الاعمال. تشكل عملية كشف الاحتيال المالي واسع النطاق العديد من التحديات لمجالس الإدارة والإدارة العليا، الأمر الذي أدى بدوره إلى التوجه والتركيز بشكل أقوى نحو حوكمة الشركات (Ta and Doan 2022)، وامتد هذا الاهتمام إلى المراجعة الداخلية باعتبارها المسئولة عن تعزيز

آليات حوكمة الشركات[5]، وأحد أدوات الإدارة العليا لتوفير الاستشارات والتوكيد على عمليات إدارة المخاطر والرقابة والحوكمة، وبذلك أصبحت المراجعة الداخلية مصدراً لإضافة القيمة يحسن فعالية أنظمة إدارة المخاطر والرقابة والحوكمة، ومن ثم امتد اهتمام وظيفة المراجعة الداخلية من التوكيد على الالتزام، والرقابة المالية وحماية الأصول، إلى المشاركة واضافة قيمة للمنظمة(Dellai and Omri 2016; Ta and Doan 2022) .

لقد أكد معهد المراجعين الداخليين (2017) IIA على المدخل الجديد لوظيفة المراجعة الداخلية وعرفها باعتبارها "نشاط توكيدي واستشاري مستقل وموضوعي مصمم لإضافة قيمة للمنظمة لتحسين عملياتها، وهو يساعد المنظمة على تحقيق أهدافها بإيجاد منهج منظم لتقييم وتحسين فعالية عمليات إدارة المخاطر والرقابة والحوكمة". كما قدم IIA تفسيراً للقيمة المضافة، وأوضح أن وظيفة المراجعة الداخلية تضيف قيمة للشركة (وأصحاب المصالح) عندما توفر توكيداً ملائماً موضوعياً، واستشارات موضوعية، وفقاً لمنهج قائم على المخاطر، لأصحاب المصالح (IIA 2020)، ومن ثم يمكن للمراجعة الداخلية من خلال أداء دوريها **الاستشاري Consulting والتوكيدي Assurance** ، تقييم المخاطر، وتحديد أوجه الضعف في هيكل الرقابة الداخلية، وتشكيل ثقافة الشركة والتحسين المستمر للعمليات التشغيلية، بما يدعم الإدارة ومجلس الإدارة في تحقيق أهداف الشركة وأصحاب المصالح.

من خلال الدور الموسع للمراجعة الداخلية، أصبح المراجع الداخلي آلية رقابة أساسية في حوكمة الشركات إلى جانب مراقب الحسابات، ولجنة المراجعة، والإدارة التنفيذية، فيمكن للمراجعة الداخلية القيام بمجموعة واسعة من الأنشطة في شكل خدمات توكيد أو استشارات تساهم في إضافة قيمة للشركة ولأصحاب المصالح بها منها؛ أولاً، يمكنها تقديم توكيد بأن هيكل الرقابة الداخلية مصمم بشكل صحيح ويعمل بفعالية. ثانياً، توفير استشارات لتحسين إدارة المخاطر، ثالثًا، مساعدة لجنة المراجعة ومراقبي الحسابات في تقييم مدى فعالية هيكل الرقابة

[5] أدت الانهيارات والفضائح المالية في مطلع القرن العشرين وما نتج عن ذلك من أزمة مالية عالمية إلى دعم العديد من القوانين والتشريعات والمعايير الدولية (Sarbanes-Oxley Act 2002; OECD 2004; IFAC 2006) مسؤوليات المراجعة الداخلية في تعزيز آليات حوكمة الشركات.

الداخلية. رابعًا، الحد من الاحتيال والاستيلاء غير القانوني على الأصول والتقرير غير الصحيح عن المعلومات المالية (Dellai and Omri 2016; Gros et al. 2017).

كما أشار Carcello et al. (2020) إلى أن إحدى الطرق التي يمكن أن تضيف بها المراجعة الداخلية قيمة للشركة هي تخفيض المخاطر، من خلال تقييم وتحسين فعالية إدارة المخاطر، ولا يقتصر دور المراجعة الداخلية على إدارة المخاطر المتعلقة بالتقرير المالي فقط، بل امتد ليشمل مساندة الإدارة في تقييم مخاطر الأعمال التي يمكن أن تهدد تحقيق أهداف الوحدة، والعمل على إدارتها (Abdelrahim and Al-Malkawi 2022). كما تعتبر وظيفة المراجعة الداخلية أحد الدعائم الرئيسية لتلبية احتياجات مختلف أصحاب المصالح، خاصة المساهمين والإدارة، من خلال إعدادها لتقرير عن مدى فعالية هيكل الرقابة الداخلية، وتوفيرها نظرة أكثر شمولية عن أداء مختلف إدارات وأقسام ومراكز الشركة والمخاطر التي تواجهها، فضلا عن قدرتها على متابعة قرارات مجالس الإدارات (شحاتة 2022).

يعتمد أداء وظيفة المراجعة الداخلية لدورها الحديث على فعاليتها، وعلى الرغم من ذلك، لا يوجد اتفاق بين الدراسات على مفهوم محدد لفعالية المراجعة الداخلية (Badara and Saidin 2013; Lenz and Hahn 2015 ; Dellai and Omri 2016; Lenz et al. 2018; Turetken et al. 2020) فما تزال فعالية المراجعة الداخلية غير مفهومة بشكل مرضٍ، أو بمعني أخر "صندوق أسود a black box" Lenz et al. (2014) ، وفى هذا الصدد أشار Dellai and Omri (2016) إلى أن مفهوم فعالية المراجعة الداخلية مفهوماً صعباً لتعدد توجهاته، ووجود ندرة في دراسته في أدبيات المحاسبة والمراجعة، أيضاً أشار Turetken et al. (2020) إلى عدم وجود اتفاق بين الدراسات بشأن تحديد أو قياس فعالية المراجعة الداخلية.

وفقًا لـــ Dittenhofer (2001); Sarens and De Beelde (2006);Ridley (2008) تشير فعالية المراجعة الداخلية إلى قدرة وظيفة المراجعة الداخلية على تحقيق أهدافها. ويرى كل من Soh and Martinov- Bennie (2011) أن المراجعة الداخلية تعتبر فعالة عندما تتمكن من تلبية توقعات الإدارة العليا ومجلس الإدارة ولجنة المراجعة، وهذا يشمل توفير المعلومات والتحليلات التي تحتاجها الإدارة العليا لاتخاذ قرارات رشيدة حول المخاطر والفرص التي تواجهها المنظمة، وكذلك المساعدة في ضمان أن المنظمة

تلتزم بالقوانين واللوائح المعمول بها. وقد أشار lenz (2013) أن فعالية المراجعة الداخلية تعتبر مفهوم مبني على المخاطر، يساعد المنظمة في تحقيق أهدافها بالتأثير الإيجابي علي جودة حوكمة الشركات. كما حدد Trotman and Duncan (2018) مفهوم فعالية المراجعة على أساس المخرجات، على أنها نتائج وتوصيات المراجعة الداخلية التي تساعد المنظمة على تحقيق أهدافها الاستراتيجية.

وعلى الرغم مما توصل اليه الباحث من تحليل العديد من الدراسات في مجال فعالية المراجعة الداخلية، بأنه لا تزال فعالية المراجعة الداخلية غير مفهومة بشكل مرضٍ، يمكن للباحث المساهمة في تحديد مفهوم لفعالية المراجعة الداخلية يخدم الهدف من البحث، بأنها " **أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي وفقاً للمعايير الدولية للممارسة المهنية للمراجعة وقواعد السلوك المهني، في مجالات إدارة المخاطر والرقابة والحوكمة، مع التأكيد على توافر محركات فعالية المراجعة الداخلية؛ الاستقلال والموضوعية، والمرونة، والكفاءة والتدريب، والعلاقات الجيدة مع مجالس الإدارة، ودعم الإدارة العليا، وتخصيص كافة الموارد اللازمة لأداء أنشطة المراجعة الداخلية، مع ضرورة توفير تقارير دورية داخلية وخارجية، تتضمن نتائج وتوصيات مفيدة تساعد الإدارة، بصفة خاصة، في الوفاء بمسئولياتها، وكذلك مساعدة أصحاب المصالح الأخرين في اتخاذ قرارات رشيدة، وهو ما ينتج عنه خلق قيمة مضافة للشركة**"

وفيما يتعلق بقياس فعالية المراجعة الداخلية، فقد خلص Lenz and Hahn (2015) من خلال تحليل مجموعة متنوعة من الدراسات أهتمت بطرق قياس فعالية المراجعة الداخلية (Soh and Martinov– Bennie 2011; Lenz and Sarens 2012; على سبيل المثال Fazli et al. 2013)، أنه يمكن تمييز اتجاهين لقياس فعالية المراجعة الداخلية في الفكر المحاسبي وهما؛ "جانب العرض supply–side" و"جانب الطلب demand–side".

من منظور "**جانب العرض**" اعتمد قياس فعالية المراجعة الداخلية على التقييم الذاتي للمراجعين الداخليين لفعاليتهم، ومعظم العينات التي اعتمدت عليها هذه الدراسات كانت من المديرين التنفيذين للمراجعة الداخلية، ومن وجهة نظر التقييم الذاتي للمراجعين الداخليين لفعالية وظيفتهم، فإن استقلالية المراجعة الداخلية، وموضوعية المراجع الداخلي، وحجم

وظيفة المراجعة الداخلية، وتوافر الكفاءات والمهارات والتأهيل العلمي اللازم للمراجع الداخلي، علاوة على علاقة وظيفة المراجعة الداخلية مع لجنة المراجعة، ومع مراقب الحسابات، ورغبة مجلس الإدارة ولجنة المراجعة، في العمل مع المراجعة الداخلية وإشراكها باعتبارها شريك استراتيجي في المنظمة، ودعم الإدارة العليا لها، تعد عوامل حاسمة لفعالية المراجعة الداخلية. (Dellai and Omri 2016; Shamsuddin et al. 2018; Abdelrahim and Al-Malkawi 2022; Ta and Doan 2022; Slapniˇcar et al. 2022)

أما من منظور "**جانب الطلب**" اعتمد قياس فعالية المراجعة الداخلية على تقييم العديد من أصحاب المصالح للخدمات التي تقدمها وظيفة المراجعة الداخلية، والأنشطة التي تقوم بها وظيفة المراجعة الداخلية لتلبية هذه التوقعات، لقياس فعاليتها، (Soh and Martinov-Bennie 2011; Roussy and Brivot 2016; Eulerich et al. 2017; Erasmus and Coetzee 2018; Eulerich et al. 2019; Eulerich and Eulerich 2020)، وتكون المراجعة الداخلية فعالة من منظور جانب الطلب، عندما تقابل توقعات الإدارة العليا ولجنة المراجعة باعتبارهما أصحاب المصلحة الرئيسيين للخدمات التي توفرها المراجعة الداخلية، ومدى تنفيذهم لتوصياتها (Erasmus and Coetzee 2018)، كذلك عندما تقابل توقعات مراقبي الحسابات من خلال تقييمات فعالة لهيكل الرقابة الداخلية والافصاح عن جوانب القصور به، كما يمكن الاعتماد على مستوى اعتماد مراقبي الحسابات على وظيفة المراجعة الداخلية كمقياس بديل لفعالية المراجعة الداخلية (Erasmus and Coetzee 2018)، علاوة على ذلك، فإن عدم وجود نقاط ضعف جوهرية تم التقرير عنها في التقارير المطلوبة من قبل الهيئات المنظمة للأسواق المالية عن مشكلات متعلقة بالمراجعة الداخلية أو قصور في هيكل الرقابة الداخلية، أو عدم التزام المراجعين الداخليين بالمعايير الدولية للممارسة المهنية للمراجعة الداخلية، يعد مقياساً ملائماً لفعالية المراجعة الداخلية من جانب الطلب (Eulerich and Eulerich, 2020).

وفى سياق قياس فعالية المراجعة الداخلية، قد أكد Lenz (2017) على خطورة اعتبار رضا أصحاب المصالح عن خدمات المراجعة الداخلية ومقابلتها لتوقعاتهم، المقياس الرئيسي

لفعالية المراجعة الداخلية لأنه من الناحية العملية يمكن أن تختلف التوقعات بشكل كبير كما أنه في بعض الأحيان قد لا يكون مطلوباً من المراجعة الداخلية تقديم الكثير. علاوة على ذلك، فإن إدارة المرجعة الداخلية تتكيف عادةً مع التوقعات، صعوداً وهبوطاً. وأضاف (Eulerich and Lenz 2019) في هذ الشأن، أنه يمكن أن تختلف توجهات جانبي العرض والطلب للمراجعة الداخلية بشكل كبير. على سبيل المثال، قد تحدد لجنة المراجعة قيمة أنشطة المراجعة الداخلية من خلال منظور الرقابة الداخلية وإدارة المخاطر، بينما قد يكون تركيز المدير التنفيذي للمراجعة الداخلية على تحسين العمليات.

لذلك اعتمد الباحث في هذا البحث على استجابات مجموعتين من الجهات الفاعلة في مجال المراجعة الداخلية والحوكمة من خلال دراسة تجريبية، وهما؛ العاملون بأدوات المراجعة الداخلية، وأعضاء مجلس الإدارة ولجنة المراجعة، في شركات المساهمة المقيدة بالبورصة المصرية، يمثلون على التوالي وجهة نظر "جانب عرض" و"جانب الطلب" بشأن فعالية المراجعة الداخلية (Lenz and Hahn 2015; Roussy et al. 2020).

ويخلص الباحث مما سبق إلى أنه أصبحت المراجعة الداخلية من خلال أدائها المستقل والموضوعي لدوريها التوكيدي والاستشاري مصدراً لإضافة القيمة للمنظمة، يساعد المنظمة على تحقيق أهدافها بإيجاد منهج منظم قائم على المخاطر لتقييم وتحسين فعالية عمليات إدارة المخاطر والرقابة والحوكمة، بما يدعم الإدارة ومجلس الإدارة في تحقيق أهداف الشركة وأصحاب المصالح. يعتمد أداء وظيفة المراجعة الداخلية لدورها الحديث على فعاليتها، وعلى الرغم من ذلك لا يوجد اتفاق بين الدراسات على مفهوم محدد لفعالية المراجعة الداخلية، وقد حاول الباحث المساهمة في تحديد مفهوم لفعالية المراجعة الداخلية يخدم الهدف من البحث، بأنها " أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي وفقاً للمعايير الدولية للممارسة المهنية للمراجعة وقواعد السلوك المهني، في مجالات إدارة المخاطر والرقابة والحوكمة، مع التأكيد على توافر محركات فعالية المراجعة الداخلية؛ الاستقلال والموضوعية، والمرونة، والكفاءة والتدريب، والعلاقات الجيدة مع مجالس الإدارة، ودعم الإدارة العليا، وتخصيص كافة الموارد اللازمة لأداء أنشطة المراجعة الداخلية، مع ضرورة

توفير تقارير دورية داخلية وخارجية، تتضمن نتائج وتوصيات مفيدة تساعد الإدارة، بصفة خاصة، في الوفاء بمسئولياتها، وكذلك مساعدة أصحاب المصالح الأخرين في اتخاذ قرارات رشيدة، وهو ما ينتج عنه خلق قيمة مضافة للشركة"، كما خلص الباحث فيما يتعلق بقياس فعالية المراجعة الداخلية، إلى أنه يمكن تمييز اتجاهين لقياس فعالية المراجعة الداخلية وهما؛ جانب العرض الذى اعتمد في قياس فعالية المراجعة الداخلية على التقييم الذاتي للمراجعين الداخليين لفعاليتهم، وجانب الطلب، الذى اعتمد في قياس فعالية المراجعة الداخلية على تقييم أصحاب المصالح للخدمات التي تقدمها وظيفة المراجعة الداخلية، والأنشطة التي تقوم بها وظيفة المراجعة الداخلية لتلبية هذه التوقعات.

3/6 تحليل الدراسات السابقة واشتقاق فروض البحث

1/3/6 علاقة فعالية المراجعة الداخلية في إدارة مخاطر الأمن السيبراني بقيمتها المضافة واشتقاق الفرض الأول للبحث

تعتبر المراجعة الداخلية أداة إدارية حيوية لتحقيق الرقابة الفعالة في المنظمات (Behrend and Eulerich 2019)، ومع التغيرات المستمرة في الأعمال، وزيادة المخاطر التي تواجهها وتطور أنواعها، امتد اهتمام وظيفة المراجعة الداخلية من التوكيد على الالتزام، والرقابة المالية وحماية الأصول، إلى المشاركة واضافة قيمة للمنظمة من خلال فعالية دوريها الاستشاري والتوكيدي في ثلاثة مجالات رئيسية وهي إدارة المخاطر والرقابة الداخلية وحوكمة الشركات، وكامتداد للدراسات السابقة في مجال فعالية المراجعة الداخلية، يركز البحث الحالي على جانب واحد من فعالية المراجعة الداخلية، **وهو فعالية المراجعة الداخلية في مجال إدارة مخاطر الأمن السيبراني.**

أوصت مبادئ إدارة المخاطر IIA (2013); IIA (2016); COSO (2019); IIA (2020)، وأيدتها العديد من الدراسات (Alina et al. 2017; Kahyaoglu and Çaliyurt, 2018; Jamison et al. 2018; Al-Matari et al. 2020; Slapničar et al. 2022; Hepworth et al. 2022) أنه يمكن الرقابة علي وإدارة المخاطر

السيبرانية بثلاثة خطوط دفاعية[6] the IIA three lines of defense model، **خط الدفاع الأول ضد الهجمات السيبرانية** يتضمن **إدارة تكنولوجيا المعلومات**، والتي تعتبر مخاطر الأمن السيبراني جزء متضمن داخل وظيفتها، وتقوم بوضع قواعد الإشراف والحوكمة والرقابة وعمليات أمن البيانات لإدارة هذه المخاطر. ويتمثل **خط الدفاع الثاني** في **وظيفة أمن المعلومات** التي توفر الخبرة لتنفيذ ومتابعة فعالية نظم الرقابة وإدارة مخاطر الأمن السيبراني[7]، أما **خط الدفاع الثالث** فيتمثل في **وظيفة المراجعة الداخلية** التي توفر فحص مستقل لمقاييس أمن المعلومات، وتلعب دور هام وحيوي في تقييم وتحديد استراتيجيات أمن المعلومات للشركة، وتقدم لمجلس الإدارة وللجان المراجعة/المخاطر النصح والاستشارات بشأن إدارة مخاطر الأمن السيبراني، وكذلك تقدم لهما تأكيد موضوعي مستقل لمدي فعالية استراتيجية وسياسات وإجراءات إدارة مخاطر الأمن السيبراني، ويتضمن ذلك فحص مدى كفاية العمل المقدم من الخط الأول والخط الثاني للحماية من مخاطر الأمن السيبراني، بما يضمن التحسين المستمر.

ويتفق الباحث مع IIA (2020) بأنه تساهم جميع الأدوار داخل خطوط الدفاع الثلاثة التي تعمل معًا بشكل جماعي ضد المخاطر السيبرانية في إضافة القيمة وحمايتها عندما تتماشى مع بعضها البعض ومع المصالح ذات الأولوية لأصحاب المصلحة، يتم تحقيق مواءمة الأنشطة من خلال الاتصال والتنسيق والتعاون مما يضمن إمكانية الاعتماد وتماسك وشفافية المعلومات اللازمة لاتخاذ القرارات على أساس المخاطر.

وبتحليل الدراسات السابقة، أوضحت دراسة Deloitte (2017) أنه نتيجة لزيادة الجرائم السيبرانية، زادت توقعات لجان المراجعة ومجالس إدارة الشركات لأداء المراجعة الداخلية، ودورها في فهم وتقييم قدرات الشركة في إدارة مخاطر الأمن السيبراني، وأشارت الدراسة إلى أن، تهدف المراجعة الداخلية إلى أداء تقييم شامل لمخاطر الأمن السيبراني، بما يوضح

---

[6] لا ينبغي أن يؤخذ الترتيب لخطوط الدفاع ضد هجمات الأمن السيبراني (الأول، الثاني، الثالث) على أنه يشير إلى عمليات متسلسلة. بدلا من ذلك، تعمل جميع الأدوار بشكل متزامن (IIA 2020).

[7] تشمل مسؤولية الإدارة العليا تحقيق الأهداف التنظيمية لأدوار الخط الأول والثاني، حيث توفر لأدوار الخط الأول وظائف الدعم. وتقدم لأدوار الخط الثاني المساعدة في إدارة المخاطر (IIA 2020).

الأهداف والنتائج للجنة المراجعة ومجلس الإدارة، واستخدام النتائج لتطوير خطة للمراجعة الداخلية تواجه مشاكل الأمن السيبراني خلال سنة أو عدد من الفترات، على أن تكون هذه الخطة قابلة للتعديل وفقاً لظهور مخاطر سيبرانية حديثة، أو/و تغيرات في قوتها، ووفقاً لأهمية التهديدات وغيرها من التطورات التنظيمية.

كما هدفت الدراسة إلى تقديم مدخل شامل لتقييم المراجعة الداخلية للأمن السيبراني، بناءً على إطار عمل الأمن السيبراني الذي يتضمن 12 مجالاً داخل ثلاثة أبعاد رئيسية وهي؛ الأمن Secure، الحذر Vigilant، المرونة Resilient، ويستطيع المراجع الداخلي من خلال فهم المجالات داخل أبعاد إطار عمل الأمن السيبراني، معالجة الفجوات فيها، بما يساهم في تخفيف تهديدات مخاطر الأمن السيبراني، وتحديد مستوى نضج إدارة المخاطر بالشركة والعمل على تحسينه للوصول إلى المستوى الأمثل.

وتؤكد الدراسة على أنه تحتاج المراجعة الداخلية لإدارة مخاطر الأمن السيبراني إلى خبراء في المراجعة وإدارة مخاطر الأمن السيبراني، وإشراك الأفراد ذوي الخبرة والمهارة في تكنولوجيا وأمن المعلومات، بما يتطلب توجه الشركات نحو إدارة مراجعة داخلية محترفة في عالم الإنترنت. وخلصت الدراسة إلى أن المراجعة الداخلية لها دور هام في تعزيز الأمن السيبراني، ومساعدة الشركات بشكل مستمر في إدارة التهديدات السيبرانية، وتقديم تقييم موضوعي مستقل للضوابط الموجودة والمطلوبة، ومساعدة لجنة المراجعة ومجلس الإدارة في فهم ومعالجة المخاطر المتنوعة في عالم الرقمنة.

وفي نفس السياق أشارت دراسة Alina et al. (2017) إلى أنه مع تغير المناخ الطبيعي للشركات إلى محاولات التهديدات السيبرانية القوية، تحتاج بيئة الأعمال إلى تكييف أدواتها للتخفيف من مخاطر الأمن السيبراني، والاستجابة له في مراحل مختلفة وهي؛ مرحلة المنع prevention، الكشف detection، التخلص disposal، ومرحلة التحسين improvement. كما تلعب وظيفة المراجعة الداخلية دوراً رئيسياً في تقييم المخاطر والاضطرابات السيبرانية، وتحديد فجوات الرقابة التشغيلية، علي مستوى الأعمال، والعمل مع الإدارة في تطوير والحفاظ على القدرة علي التكييف مع أنواع مختلفة من المخاطر

السيبرانية، وتحسين استمرارية الأعمال وعدم التوقف نتيجة للهجمات السيبرانية، واضافت الدراسة أن أحد الأدوار الهامة لوظيفة المراجعة الداخلية في إدارة مخاطر الأمن السيبراني هو تقديم التأكيدات بشأن الأمن السيبراني، والتخطيط لاستمرار الأعمال، ووضع استراتيجيات التعافي من التهديدات السيبرانية المختلفة، كما أكدت الدراسة علي أن الاتصال الكفء بين وظيفة المراجعة الداخلية والإدارة التنفيذية هام لوضع مستويات مخاطر الأمن السيبراني ضمن مستوى مخاطر الشركة، وبالتالي إمكانية تخفيضها.

كما هدفت دراسة Shamsuddin et al. (2018) التحقق من العوامل المؤثرة على فعالية وظيفة المراجعة الداخلية في إدارة الأمن السيبراني في قطاع البنوك في ماليزيا، واختبرت الدراسة ثلاثة عوامل ترى الدراسة أنها من أكثر العوامل احتمالاً للتأثير في فعالية المراجعة الداخلية في إدارة الأمن السيبراني وهي؛ وعي المراجعين الداخليين بالأمن السيبراني، سياسة البنك حول الأمن السيبراني، المخاطر التنظيمية المرتبطة بالأمن السيبراني،

ومن خلال عينة من 120 مشارك من المراجعين الداخليين من 7 بنوك تجارية في ماليزيا، وباستخدام قائمة استقصاء، ومقابلات شبه مهيكلة مع المراجعين الداخليين في عينة الدراسة، أوضحت نتائج الدراسة وجود علاقة طردية معنوية بين الثلاثة عومل –الوعي، السياسات التنظيمية، إدارة المخاطر التنظيمية المرتبطة بالأمن السيبراني– وفعالية وظيفة المراجعة الداخلية في إدارة الأمن السيبراني.

وقد قامت دراسة Islam et al. (2018) بتحليل دور إدارة المراجعة الداخلية في مراجعة الأمن السيبراني، واضافة رؤى حول خصائص مديري المراجعة الداخلية وخصائص الحوكمة التي من شأنها أن تؤدي لمشاركة فعالة من إدارة المراجعة الداخلية في مراجعة الأمن السيبراني، استخدمت الدراسة استجابات 970 من مديري إدارة المراجعة الداخلية من قاعدة بيانات CBOK, 2015، أشارت نتائج الدراسة إلى وجود علاقة ارتباط منخفضة بين مدى مراجعة الأمن السيبراني ووجود مراجعة داخلية تقليدية، وأن المراجع ذو الخبرة الأكبر سيركز بدرجة أكبر علي مراجعة الأمن السيبراني ضمن المراجعة الداخلية، كما أوضحت نتائج الدراسة وجود ارتباط طردي معنوي بين مدى المراجعة الداخلية الخاصة بأمن المعلومات وكفاءة إدارة المراجعة الداخلية الخاصة بالحوكمة وإدارة المخاطر والرقابة،

كما أن دعم مجلس الإدارة لحوكمة الشركة له أثر إيجابي على مدي مراجعة الأمن السيبراني، بينما لم يتضح معنوية دور لجنة المراجعة في فعالية المراجعة الداخلية للأمن السيبراني، كما اشارت نتائج الداراسة أن التقييم الشامل للمخاطر الذى تقوم به إدارة المراجعة الداخلية له دور إيجابي معنوي في مراجعة الأمن السيبراني. كما أوضحت نتائج الدراسة أنه وعلي غير المتوقع، أن مدير المراجعة الذي لديه شهادة أمن سيبراني CIA مع وجود مهام مراجعة داخلية خاصة بإدارة المخاطر ليس له أثر معنوي علي مراجعة الأمن السيبراني، بينما شهادات أخري مثل شهادة مراجعة النظم الآلية CISA ، وشهادة المحاسب القانوني CPA لها أثار حدية أو مختلطة علي مدى مراجعة الأمن السيبراني.

وفي نفس السياق هدفت دراسة Kahyaoglu and Caliyurt (2018) إلى تحليل مداخل التأكيد على الأمن السيبراني من منظوري المراجعة الداخلية وإدارة المخاطر، وأكدت الدراسة علي دور المراجعة الداخلية في إدارة مخاطر الأمن السيبراني من خلال التأكيد علي أن الأعمال عليها ضوابط رقابية بدرجة كافية، كما لخصت الدراسة حاجة مجلس الإدارة لخدمات المراجعة الداخلية للأمن السيبراني في ثلاثة أسباب وهي؛ تعقد تقارير إدارة تكنولوجيا المعلومات وتركيزها علي المخاطر الفنية دون ربطها بالنواحي المالية أو التشغيلية، كما لا يمكن لموظفي الأمن السيبراني تقديم تأكيد مستقل موضوعي بما يوضح أهمية دور المراجعين الداخليين في توفير تأكيد مستقل بما يوفر أسس للثقة بمدي تحقق أهداف الأمن السيبراني الأربعة – السلامة، الإتاحة، السرية والمساءلة– وأن نظم الرقابة علي أمن المعلومات تعمل وفقاً للوظيفة المتوقعة منها، وأخيرا، نقص الوعي لدي بعض أعضاء مجلس الإدارة بمخاطر الأمن السيبراني.

وأشارت الدراسة إلى أنه يجب على المراجعين الداخليين بناء الثقة داخل المنظمة من خلال تقديم توكيد سيبراني شامل، على أن تكون خطة التوكيد القوية على النحو التالي:

- وضع برنامج مراجعة مستمر قائم علي المخاطر: يجب علي المراجعين الداخليين وضع برنامج للمراجعة الداخلية منظم، شامل، مستمر قائم على أساس المخاطر، يتضمن تحديد لمخاطر المنظمة، وللضوابط الرقابية التي من شأنها التخفيف من هذه المخاطر وأثارها،

وتحديد المتطلبات التشريعية لتسهيل الالتزام، والتقرير لمجلس الإدارة والإدارة التنفيذية بالضوابط الرقابية الموجودة بالفعل، ووضع خطة لتنفيذ الضوابط الرقابية المفقودة علي الأمن السيبراني علي أساس فعاليتها من جانب التكلفة، والتقرير عن الحوكمة والالتزام، واستخدام شركاء خارجيين لتقديم رؤي الصناعة ضمن منظور أوسع للمراجعة الداخلية القائمة علي المخاطر.

- إطار عمل للتأكيد على الأمن السيبراني: يجب أن يستخدم المراجعين الداخليين استخدام أطر ومعايير لتجنب عدم الاتساق في التقارير الموجهة لمجلس الإدارة، وضمان التوافق مع الإدارة لتوفير المراجع الداخلي التوكيد على الأمن السيبراني، مع ضرورة تعاون المراجع الداخلي مع موظف أمن المعلومات.
- التنفيذ ضمن دورة توكيد مستمرة: يجب علي المراجع الداخلي تطوير عمليات مراجعة داخلية وفقاً لمدخل قائم على مخاطر الأمن السيبراني، مع الحفاظ على العلاقة خارج أوقات المراجعة لفهم أفضل لقضايا الأمن السيبراني ونقاط الضعف فيه داخل المنظمة، وبهذا يصبح المراجعون الداخليون من خلال توفير التوكيد على الأمن السيبراني "مستشارين إلكترونيين موثوقينtrusted cyber advisors "، وبهذا تكون وظيفة المراجعة الداخلية ذات قيمة مضافة لجميع أصحاب المصلحة.

وخلصت الدراسة إلى أنه يحتاج المراجع الداخلي حتى يصبح مستشار موثوق للأمن السيبراني، ينبغي عليه؛ تحديد قدرات مدير إدارة المراجعة الداخلية والمراجعين الداخليين ومهاراتهم في تكنولوجيا المعلومات والأمن السيبراني، والاستفادة من الاسناد لهذه الخدمات، وتحديد كيفية تعامل المنظمة مع الأمن السيبراني ضمن خطة المراجعة الداخلية المبنية على أساس المخاطر. كما ينبغي علي المراجع الداخلي التأهيل العلمي والتدريب في مجال الأمن السيبراني وإدارة مخاطره، للتعرف على مخاطر الأمن السيبراني بشكل استباقي، ووجود شراكة مع مدير فريق الأمن السيبراني للشركة، وتوفير توكيد علي سلامة إجراءات الأمن السيبراني للمنظمة، وعلى الاستجابة للحوادث السيبرانية وخطط التعافي منها واستمرارية الأعمال، والتقرير عن النتائج إلى الإدارة ومجلس الإدارة ولجنة المراجعة، وعلي المراجعين

الداخليين توفير فحص مستقل لاستراتيجية الأمن السيبراني قبل تطوير السياسات والإجراءات، وأن يكون المراجعون الداخليون جزء من فرق تنفيذ مشروع تكنولوجيا المعلومات للتأكد من معالجة المخاطر السيبرانية ودمجها، بدلاً من إضافتها للمخاطر ذات الصلة بالعمليات.

وهدفت دراسة Stafford et al. (2018) إلى التحقق من دور وظيفة المراجعة الداخلية في إدارة مخاطر الأمن السيبراني من منظور التهديدات الداخلية، المتمثلة في عدم التزام الموظفين ذوي المعرفة بسياسات الأمن السيبراني، مما يؤثر بصورة سلبية دون قصد على أمن معلومات الشركة من خلال ممارسات الحوسبة غير الأمنة، واتخاذ خطوات غير مصرح بها بدعوى زيادة كفاءة وسرعة انجاز المهام.

واعتمدت الدراسة على دراستي حالة لرضا الموظفين عن الأمن السيبراني، أو تجاهل عناصر الأمن السيبراني وعدم الالتزام بها، وإجراء تحليل وصفي لأنواع المراجعة الداخلية التي تحل المشاكل الأمنية نتيجة الرضا أو عدم الالتزام بالأمن السيبراني[8]، مع مقابلات مع المراجعين الداخليين.

وأشارت الدراسة إلى أهمية دور المراجعة الداخلية في التخفيف من التهديدات الداخلية للأمن السيبراني[9]، من خلال تحديد واكتشاف المستخدم الضار للأمن السيبراني، وتحديد جوانب عدم الالتزام بسياسات أمن المعلومات، والتوجيه الاستشاري والنصح لضرورة الالتزام بسياسات الأمن السيبراني وعدم حذف أو تجاهل النواحي الأمنية المقدمة من مزودي الخدمة، كما تقوم إدارة المراجعة الداخلية بإجراء برامج لتثقيف وتدريب للمستخدمين غير الملتزمين، والتحفيز للالتزام بمتطلبات أمن المعلومات، مع وضع وتنفيذ برامج للكشف والوقاية والتصحيح لتقييم نظم المعلومات بصورة مستمرة، كما تتضح أهمية المراجع الداخلي في التحقق من الالتزام بضوابط الرقابة على أمن المعلومات المقدمة من مزود الخدمة والتي قد يتم الغاءها بدعوى الموظفين أن ذلك لصالح كفاءة العمل.

---

[8] أوضحت نتائج الدراسة عدم التزام المستخدمين بسياسات أمن المعلومات أهمها استخدامهم لحاسبتهم الشخصية في العمل بما يعتبر تهديد للأمن السيبراني، بما يتطلب وجود محفزات لدعم الالتزام بسياسات أمن المعلومات.

[9] يعمل مزودي الخدمات الالكترونية للشركات على تأمين الأجهزة والبرامج، وتوجه المستخدمين للالتزام بأمن المعلومات، من المشاكل التي تواجه الشركات هي حذف الموظفين ذوي المعرفة للأساليب الأمنية بهدف سرعة انجاز الأعمال، مما يضر دون قصد بالأمن السيبراني للشركة، ويمثل تهديد داخلي للأمن السيبراني(2018) Stafford et al. .

كما طورت دراسة Slapni˘car et al. (2022) مؤشراً لفعالية المراجعة الداخلية للأمن السيبراني يعتمد على معايير الأداء المهني للمراجعة الداخلية، والتي تتطلب من كل عملية مراجعة أن تشمل ثلاثة أبعاد وهي، التخطيط، الأداء، والتقرير، وذلك بهدف تحليل فعالية المراجعة الداخلية للأمن السيبراني، وافترضت الدراسة أن فعالية مراجعة الأمن السيبراني ترتبط إيجاباً مع إدارة المخاطر السيبرانية، وسلباً مع احتمال حدوث هجوم سيبراني ناجح.

استخدمت الدراسة قائمة استقصاء على عينة مكونة من 183 مراجع داخلي ومدير إدارة مراجعة في عدد من الدول والصناعات. وأظهرت نتائج الدراسة أن المراجعة الداخلية للأمن السيبراني مرتفعة نسبياً بمتوسط 58%، وتوجد اختلافات المراجعة الداخلية للأمن السيبراني بين الدول والصناعات، كما أشارت نتائج الدراسة إلى وجود علاقة قوية بين التخطيط والأداء ونضج إدارة مخاطر الأمن السيبراني- كمقياس بديل عن تنفيذ المؤسسات بشكل منهجي لإدارة مخاطر الأمن السيبراني-، وعدم وجود ارتباط قوي بين التقرير عن فعالية إدارة مخاطر الأمن السيبراني لمجلس الإدارة ونضج إدارة مخاطر الأمن السيبراني، وبالرغم من أن المراجعة الداخلية للأمن السيبراني ترتبط طردياً مع نضج إدارة المخاطر، الا أن انها لا تخفض من احتمال حدوث هجمات سيبرانية.

واستهدفت دراسة شحاتة (2022) إجراء تحليل انتقادي للمصادر العلمية ذات الصلة بالدور الفعال للمراجع الداخلي في إدارة مخاطر الأمن السيبراني في الشركات المقيدة في البورصة المصرية، وقد أشارت الدراسة إلى إمكانية بلورة الدورين الاستشاري والتوكيدي للمراجع الخارجي في مجال إدارة مخاطر الأمن السيبراني للشركة، من خلال تقديم مدير إدارة المراجعة الداخلية بتقديم النصح لمجلس الإدارة بصدد تحديد وتوصيف وقياس مخاطر الأمن السيبراني المحيطة ببيئة عمل الشركة التكنولوجية وكيفية مواجهتها وتفادي أثارها على تحقيق الشركة لأهدافها المرجوة وذلك فيما يتعلق بالدور الاستشاري، أما فيما يتعلق بالدور التوكيدي فيرتكز علي تقديم تقرير باستنتاج Conclusion بشأن مدى صدق التقارير المعدة من قبل المسئولين عن إدارة مخاطر الأمن السيبراني بالشركة. وقد خلصت الدراسة لوجود مجموعة من متطلبات دعم الدور الفاعل للمراجع الداخلي في إدارة مخاطر الأمن السيبراني أهمها؛ ارتقاء إدارات الشركات بثقافة النظر للمراجعة الداخلية كوظيفة مضيفة للقيمة، انشاء تنظيم مهني للمراجعة

الداخلية الحديثة، تطوير نظام التعليم المحاسبي من خلال إعادة النظر في برامج التعليم المحاسبي الرقمي وكذلك برامج التعليم المهني المستمر، وأخيراً، تنظيم وتفعيل الإفصاح عن جودة وظيفة المراجعة الداخلية.

كما استهدفت دراسة محروس وصالح (2022) تطوير أداء المراجعة الداخلية في منظمات الأعمال المصرية لمواجهة مخاطر الأمن السيبراني، وذلك عن طريق استخدام المنهجية الرشيقة Agile Approach[10] كأحد مناهج التطوير اعلىيثة للمراجعة الداخلية، وتوصلت الدراسة إلى وجود اتفاق بين أراء فئات المستقصي منهم بشأن التزايد المستمر لمخاطر الأمن السيبراني وتأثيراته علي مستوى منظمات الأعمال وعلى المستوى القومي، وعدم وجود اختلافات معنوية بين فئات المستقصي منهم بشأن قصور أداء المراجعة الداخلية التقليدية في مواجهة مخاطر الأمن السيبراني وأسباب هذا القصور، واتفاقهم على إمكانية تطوير أداء المراجعة الداخلية من خلال استخدام المنهجية الرشيقة في مواجهة مخاطر الأمن السيبراني.

وفي نفس السياق، من خلال دراسة ميدانية على عينة مكونة من 135 مشارك من مسئولي المراجعة الداخلية، مسئولي تكنولوجيا المعلومات، مسئولي إدارة المخاطر، والمستثمرين في شركات الاتصالات المقيدة في البورصة المصرية، توصلت دراسة أميرهم (2022) إلى وجود علاقة إيجابية ذات دلالة إحصائية بين كل من المقدرة المهنية لفريق المراجعة الداخلية، مشاركة وظيفة المراجعة الداخلية في إدارة المخاطر المؤسسية، جودة تنفيذ المهام، وحجم قسم المراجعة الداخلية ودعم الإدارة والحد من مخاطر الأمن السيبراني، مما كان له أثر إيجابي معنوي علي ترشيد قرارات المستثمرين.

وبناءً علي تحليل الدراسات السابقة لفاعلية المراجعة الداخلية في إدارة مخاطر الأمن السيبراني، خلص الباحث إلى أهمية دور المراجعة الداخلية وانعكاسها علي إدارة مخاطر الأمن السيبراني، الا أن هذا الدور مرهوناً بفاعلية المراجعة الداخلية في تحقيق أهداف المنظمة، وتحقيق قيمة مضافة لها، ولصعوبة قياس فعالية المراجعة الداخلية، اتجهت معظم الدراسات (Dellai et al. 2016; Abdelrahim and Al-Malkawi 2022; Ta and Doan 2022) لقياسها من خلال العوامل التي تتوافر فيها ومن شأنها تحقيق أهدافها، وفي

[10] تعني المنهجية الرشيقة Agile Approach القدرة على التحرك بسرعة وسهولة، والقدرة على التفكير بطريقة ذكية، للتعامل مع الاحتياجات المتغيرة لأصحاب المصالح (محروس وصالح 2022).

مجال فعالية المراجعة الداخلية في إدارة مخاطر الأمن السيبراني، يعد من أهم العوامل المؤثرة علي فعالية المراجعة الداخلية[11]، التأهيل العلمي والتدريب المستمر في مجال الأمن السيبراني وتكنولوجيا المعلومات(Islam et al. 2018)، الوعي بالأمن السيبراني والتهديدات الداخلية والخارجية له (Shamsuddin et al. 2018; Stafford et al. 2018)، الدور الاستشاري للمراجع الداخلي في نواحي إدارة مخاطر الأمن السيبراني، والدور التوكيدي له علي أعمال إدارة مخاطر الأمن السيبراني، الاعتماد علي برنامج مراجعة داخلية شامل لمراجعة إدارة مخاطر الأمن السيبراني Kahyaoglu and Caliyurt (2018)، كما وجد البعض Slapničar et al. (2022) أن فعالية المراجعة الداخلية تتحقق عند الالتزام بمعايير الممارسة المهنية للمراجعة الداخلية، والتي تتطلب من كل عملية مراجعة أن تشمل التخطيط، التنفيذ، التقرير.

ومع اختلاف منظور الدراسات لفاعلية المراجعة الداخلية، الا أن هناك اتفاق على دور فعالية المراجعة الداخلية في إدارة مخاطر الأمن السيبراني، وتخفيض نقاط الضعف في الأمن السيبراني للشركة، مما يخفض من التهديدات السيبرانية الناجحة. وبناءً على ذلك يمكن صياغة فرض البحث الأول على النحو التالي:

H_1: تؤثر فعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني إيجاباً ومعنوياً على قيمتها المضافة في الشركات المقيدة بالبورصة المصرية.

[11] علي افتراض توافر العوامل المؤثرة على فعالية المراجعة الداخلية التقليدية مثل الاستقلال، التأهيل العلمي كمراجع حسابات داخلي، العلاقة مع لجنة المراجعة.

2/3/6 تحليل أثر التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات علي العلاقة بين فعالية المراجعة الداخلية في إدارة مخاطر الأمن السيبراني وقيمتها المضافة واشتقاق الفرض الثاني للبحث

وفقاً للـــ COBIT5 (2012) ,ISACA تعتبر الرقابة على مخاطر أمن المعلومات والمراجعة المستقلة لها، جزء هام من حوكمة تكنولوجيا المعلومات، ولا تقع مسئولية إدارة مخاطر أمن المعلومات على إدارة تكنولوجيا المعلومات فقط، بل يجب أن تتضمن وظائف أخرى أهمها وظيفة المراجعة الداخلية (ISACA 2011)، وتلعب وظيفتي المراجعة الداخلية وأمن المعلومات دوراً هاماً في الوقاية والكشف والتخفيف من مخاطر الأمن السيبراني (CIS 2019) تتضمن الرقابة الفعالة على أمن المعلومات اجراء عمليات الفحص بصورة مستمرة، سواء الفحص الذاتي الذى عادة ما تقوم به إدارة أمن المعلومات نفسها، أو الفحص المستقل من قبل وظيفة المراجعة الداخلية، التي توفر التقييم والتوكيد المستقل علي فعالية نظم رقابة المعلومات، وينبغي علي المؤسسة استخدام نتائج عمليات الفحص لتحسين تصميم وفعالية تشغيل أمن المعلومات، لذلك فإن أمن المعلومات يشترك مع وظيفة المراجعة الداخلية في تحقيق هدف عالي الأهمية يتمثل في تعظيم فعالية جهود المنظمة في حماية أحد أهم أصولها "معلومات الشركة" (Steinbart et al. 2013)، لذلك أوصى COBIT5, ITGI (2012) إدارة أمن المعلومات بتكوين لجنة لإدارة مخاطر أمن المعلومات تضم اللجنة ممثلين عن المراجعة الداخلية كأعضاء دائمين لتقديم الاستشارات للجنة بشأن مخاطر الامتثال، وأشارت دراسة Steinbart et al. (2018) إلى عدد من الأدلة علي أن التعاون بين إدارة المراجعة الداخلية وإدارة تكنولوجيا المعلومات تحسن من جودة إدارة المخاطر وقبول توصيات المراجعة الداخلية منها؛ نقل المعرفة والتعليم بين القسمين سواء الاستشارات المقدمة من إدارة المراجعة الداخلية لتحسين عمل الضوابط الأمنية، أو فهم المراجع الداخلي لضوابط تكنولوجيا المعلومات من قبل موظفي تكنولوجيا المعلومات، الاشتراك في نفس الأهداف والسعي علي تحقيقها، تخفيض التعارض الموجود بين الوظيفتين وتحسين العلاقة بينهما بما يساعد علي تحديد مشكلات أمن المعلومات وعلاجها، كما أن التعاون بين الإدارتين يساعد على كشف الانحرافات وايقافها قبل التسبب في أضرار مادية جوهرية للشركة، وتخفيض نقاط الضعف التي يمكن استغلالها لتنفيذ هجمات ناجحة، وتمكن علاقة التعاون بينهما من معالجة الثغرات الأمنية وبالتالي فرص أقل

لنجاح الهجمات السيبرانية، أو علي الأقل الكشف عن الهجمات السيبرانية في الوقت المناسب ووقف استمرار الخسائر المادية إذ حدثت. كما أشارت دراسة Jamison et al. (2018) إلى أهمية العلاقة بين وظيفتي المراجعة الداخلية وتكنولوجيا المعلومات لفاعلية الأمن السيبراني، والتي من الممكن أن توفر أساساً قوياً لمعالجة المخاطر السيبرانية، الأمر الذي يتطلب المزيد من التنسيق والتعاون بينهما للوصول لمزيد من الفهم والوضوح للمخاطر السيبرانية من خلال التقييمات المشتركة، التي ربما تجرى تقليدياً فقط من خلال المراجعة الداخلية. كما قدمت IIA Global Knowledge Brief (2022) عدد من فوائد العلاقة القوية بين مديري المراجعة الداخلية ونظرائهم في مجال أمن المعلومات[12]، منها؛ فهم ومواءمة ملف تعريف المخاطر السيبرانية للمنظمة[13] بدءاً من تحديد نقاط الضعف، والفرص في الممارسات المصممة لإدارة مخاطر الأمن السيبراني، وحتى اختبار نضج الأمن السيبراني واحتمال الاختراقات، بما يساعد على تحديد المخاطر السيبرانية والحد منها والقضاء عليها إن أمكن. ويوفر فهم المراجعة الداخلية لملف المخاطر السيبرانية الأساس لبناء خطة مراجعة، ويمكنها من تحسين ما تضيفه من قيمة في هذا المجال. كما يمكن للعلاقة الجيدة بين الوظيفتين أن تعزز المرونة وسرعة الاستجابة للحوادث السيبرانية أو التغيرات في العوامل التي تؤثر على الأمن السيبراني، فهي تساعد في توفير تقارير متسقة وموحدة إلى المديرين التنفيذين ومجلس الإدارة حول مخاطر الأمن السيبراني، الاحتياجات، والأولويات، تمكن العلاقة الجيدة بين مديري المراجعة الداخلية وأمن المعلومات من فهم أدوار كل منهما، بما يحسن من استقلالية المراجعة الداخلية، حيث لكل منهما فهماً وتقديراً أعمق للأدوار والأساليب والواجبات. وأخيراً يمكن لهذه العلاقة القوية بين الوظيفتين أن

---

[12] قدمت IIA Global Knowledge Brief (2022) عدد من فوائد العلاقة القوية بين مديري المراجعة الداخلية ونظرائهم في مجال أمن المعلومات بهدف لفت انتباه IIA لإدراج عامل العلاقة السليمة بين وظيفتي المراجعة الداخلية وأمن المعلومات، ضمن إرشاداته الموجهة للمنظمات، لمساعدتهم عند فحص وتحديد أولويات التوكيد بشأن عمليات الأمن السيبراني، ومساعدة المراجعين الداخليين على تحديد عمليات الأمن السيبراني، وتحديد مكوناتها، والنظر في إرشادات الرقابة ذات الصلة في أطر الرقابة علي تكنولوجيا المعلومات، وفهم أساليب مراجعة عمليات الأمن السيبراني.

[13] ملف تعريف المخاطر السيبرانية للمنظمة the organization's cyber risk profile هو تحليل كمي لأنواع التهديدات السيبرانية التي تواجهها المنظمة، يحدد هذا التحليل الأصول والمخاطر السيبرانية، سياسات الفحص والممارسات المصممة لإدارة تلك المخاطر، بما يتيح الفهم لأى نقاط ضعف تكون موجودة (IIA Global Knowledge Brief 2022).

تدعم المدخل الشامل للتعاون على مستوى إدارات المنظمة فيما يتعلق بقضايا الأمن السيبراني.

وعلى خلاف ما سبق، لم تتوصل دراسة Lois et al. (2021) في سياق اختبار العوامل التي تؤثر في الأمن السيبراني وترتبط بصورة ملائمة بالمراجعة الداخلية بالتطبيق على المراجعين الداخليين في الشركات المدرجة في بورصة أثينا، إلى وجود علاقة معنوية بين القيمة المضافة من فعالية المراجعة الداخلية في إدارة مخاطر الأمن السيبراني والتعاون بين المراجعين الداخليين وموظفي إدارة تكنولوجيا المعلومات.

وبناءً على ما سبق واتساقاً مع معظم الدراسات السابقة، يتوقع الباحث أن جودة العلاقة بين وظيفتي المراجعة الداخلية وأمن المعلومات يمكن أن تحسن من فعالية المراجعة الداخلية في إدارة مخاطر الأمن السيبراني من خلال نقل معرفة أمن المعلومات للمراجعة الداخلية، وبناءً على ذلك يمكن صياغة فرض البحث الثاني على النحو التالي:

H_2: يختلف التأثير الإيجابي المعنوي لفعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني على قيمتها المضافة باختلاف مستوى التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات في الشركات المقيدة في البورصة المصرية.

3/3/6 تحليل أثر دعم الإدارة العليا لوظيفة المراجعة الداخلية علي العلاقة بين فعالية المراجعة الداخلية في إدارة مخاطر الأمن السيبراني وقيمتها المضافة واشتقاق الفرض الثالث للبحث

تعتبر الإدارة العليا مسئولة عن الإشراف على تكنولوجيا المعلومات على مستوى الشركة، وعلى السياسات والاستراتيجيات التي تتضمن تقييم وتخفيض الاختراقات الأمنية (Haislip et al. 2017)، وأدت زيادة المخاطر السيبرانية الى زيادة أهمية دور الإدارة العليا في القيام بمعالجة مخاطر الامن السيبراني (Islam et al. 2018). وكما تم مناقشته، فإن مراجعة الأمن السيبراني وإدارة مخاطره جزء من عمل إدارة المراجعة الداخلية، لذلك من المحتمل أكثر أن دعم الإدارة العليا لوظيفة المراجعة الداخلية واهتمامها بقضايا الأمن السيبراني يكون له تأثير إيجابي على إجراءات المراجعة الداخلية فيما يتعلق بإدارة مخاطر الأمن السيبراني. وفي هذا الشأن، أشارت دراسة Islam et al. (2018) أن فعالية إدارة المخاطر ترتبط إيجاباً مع وجود

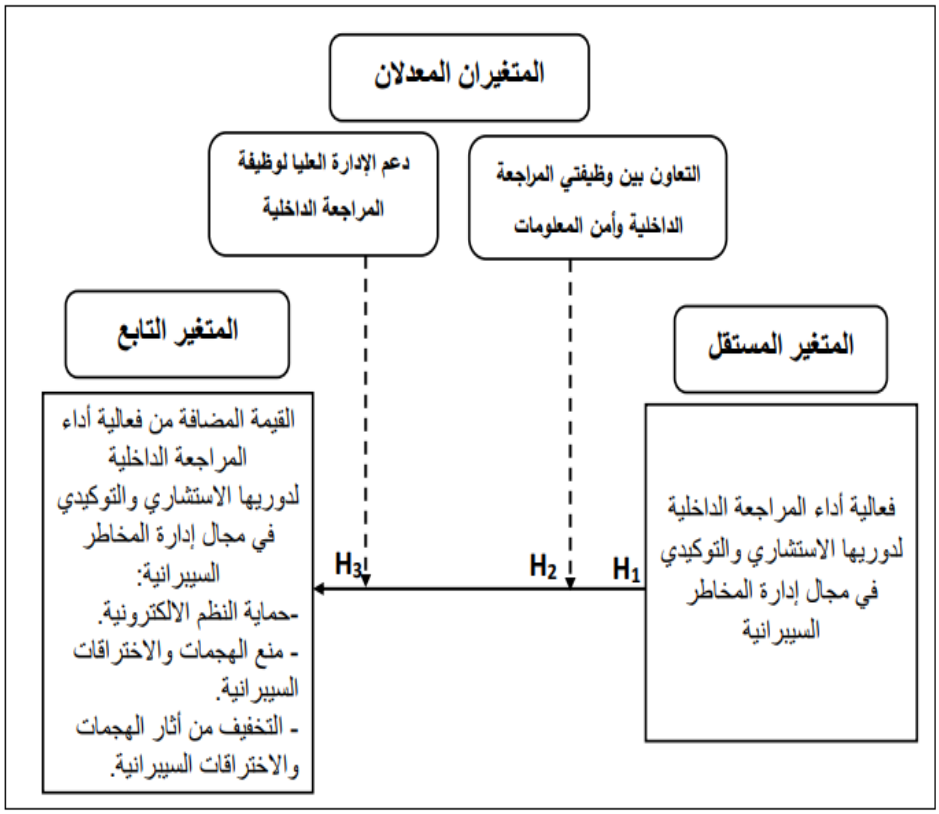
مدير مستقل لإدارة المخاطر تابع تنظيمياً لمجلس الإدارة. وفي نفس السياق أكدت دراسة Ta and Doan (2022) على أنه يعد دعم الإدارة العليا لوظيفة المراجعة الداخلية من العوامل الهامة لتحسين فعالية المراجعة الداخلية، فهو عنصر أساسي في قبول وتقدير دور إدارة المراجعة الداخلية من قبل الإدارات الأخرى داخل الشركة، مما يسهل قيام المراجعين الداخليين بمهامهم ومسئولياتهم المتعلقة بالإشراف ومراقبة عناصر هيكل الرقابة الداخلية، وإدارة المخاطر وحوكمة الشركات، بما يتسق مع عدد من الدراسات التي اهتمت بتحديد العوامل المؤثرة علي فعالية المراجعة الداخلية Mihret et al. (2010); Octavia; (2013); Dellai et al. (2016); Hussein and Hilal (2021) التي توصلت إلى أن دعم الإدارة العليا لوظيفة المراجعة الداخلية من أهم العوامل المؤثرة علي فعاليتها، وأن الميل الإيجابي للإدارة تجاه المراجعة الداخلية وتنفيذ الاقتراحات والتوصيات المقدمة منها، يلعب دور هام في عملية تخطيط المراجعة الداخلية وفعالية عملياتها وإجراءاتها (Octavia 2013; Dellai et al. 2016) ، من خلال التدريب والتطوير للمراجعين الداخليين وبناء قدرات وكفاءات قادرة علي منع الاحتيال وكشفه والتحقيق فيه والإبلاغ عنه (Alazzabi et al. 2023) وتخصيص الموارد الكافية والمشاركة في خطط المراجعة (Hussein and Hilal 2021) .

مما سبق يتوقع الباحث، إن الموقف الداعم للإدارة العليا لوظيفة المراجعة الداخلية، من حيث الوضع التنظيمي وتبعيتها مباشرة لمجلس الإدارة، ومن خلال تخصيص الموارد المناسبة لها، ووضع ميزانية مناسبة لتنفيذ عملياتها، وتنفيذ برامج التدريب والتطوير للمراجعين الداخليين، المشاركة في خطط المراجعة، والموافقة علي وتنفيذ توصياتها، تعزيز الاعتراف والقبول والتقدير الكافي لها من الإدارة العليا ومن ثم من الإدارات المختلفة داخل الشركة، من شأنه أن يؤثر إيجاباً ومعنوياً علي العلاقة بين فعالية المراجعة الداخلية وإدارة مخاطر الأمن السيبراني مقارنة بالشركات التي ينخفض لديها دعم الإدارة العليا لوظيفة المراجعة الداخلية، وبناءً على ذلك يمكن صياغة فرض البحث الثالث على النحو التالي:

H_3: يختلف التأثير الإيجابي المعنوي لفعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني على قيمتها المضافة باختلاف

مستوى دعم الإدارة العليا لوظيفة المراجعة الداخلية في الشركات المقيدة في البورصة المصرية.

وبناءً على فروض البحث يمكن عرض نموذج الدراسة على النحو التالي:



4/6 منهجية البحث

تحقيقاً لهدف البحث، فقد تم اختبار فروض البحث في بيئة الممارسة المهنية المصرية اعتماداً على المدخل التجريبي قياساً على(Cadotte and Fogarty 2021) وبناءً عليه تم تحديد أهداف الدراسة التجريبية، ومجتمع وعينة الدراسة، ووصف وإجراءات الحالة التجريبية والتصميم التجريبي، وتوصيف وقياس متغيرات الدراسة، على النحو التالي:

1/4/6 أهداف الدراسة التجريبية

تهدف الدراسة التجريبية إلى اختبار فروض البحث في بيئة الممارسة المهنية المصرية، والتوصل إلى دليل تجريبي بشأن القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني، والأثر المعدل للتعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات ودعم الإدارة العليا على هذه القيمة المضافة، وعلي الرغم من أن معظم الدراسات ذات الصلة بموضوع الدراسة انتهجت المدخل الميداني من خلال قوائم استقصاء (Shamsuddin et al. 2018; Islam et al. 2018; Lois et al. 2021; Slapni˘car et al. 2022)، أو المنهج النظري التحليلي (Kahyaoglu and Caliyurt 2018; Eaton et al. 2019; شحاتة 2022)، أو استخدمت دراسة الحالة باستخدام المقابلات الشخصية (Stafford et al. 2018) إلا أن الباحث استخدم المنهج التجريبي (Cadotte and Fogarty 2021) كمحاولة لسد فجوة الدراسات السابقة، ولما للمدخل التجريبي من مزايا أهمها إمكانية التحكم والرقابة على متغيرات الدراسة.

2/4/6 مجتمع وعينة الدراسة

يتكون مجتمع الدراسة من المهتمين بوظيفة المراجعة الداخلية في شركات المساهمة المقيدة بالبورصة المصرية، فمن جانب العرض، العاملون بأدوات المراجعة الداخلية، ومن جانب الطلب كل من مجلس الإدارة ولجنة المراجعة، قياساً على (Lenz and Hahn 2015; Roussy et al. 2020)، وتتكون عينة الدراسة (2480) مشاهدة من (62)[14] مشارك تتضمن 33 مراجع داخلي، 19 من أعضاء لجان المراجعة، 10 من أعضاء مجالس الإدارة.

[14] أرسل الباحث الحالات التجريبية لمفردات العينة عن طريق منصات التواصل الاجتماعي بنموذج google form ، وبالتواصل الفعلي عن طريق التوصيل اليدوي، استلم الباحث 73 استجابة، استبعد منهم (4) استجابات لم يتمكنوا من الرد بشكل صحيح على سؤال اختبار إدراكهم للحالة الافتراضية (تحديد مستوى فعالية المراجعة الداخلية وذلك بناء على معلومات الحالة الافتراضية المقدمة لهم)، كما استبعد عدد (7) استجابات لم يستكملوا الإجابة على أسئلة الحالة التجريبية.

3/4/6 وصف وإجراءات الحالة التجريبية والتصميم التجريبي:

1/3/4/6 وصف وإجراءات الحالة التجريبية

لإجراء الدراسة التجريبية اعتمد الباحث على؛ تصميم حالة افتراضية لمؤسسة تعمل في مجال الاتصالات[15]، تندرج ضمن قطاع الاتصالات و اعلام وتكنولوجيا المعلومات في البورصة المصرية، وعرضها على المشاركين بشكل عشوائي، وأعد الباحث تجربتين، تضمنا ثمان حالات تجريبية تستوعب المعالجات المختلفة للمتغير المستقل مع المتغيرين المعدلين للعلاقة محل الدراسة؛ التجربة الأولى تمثل مستوى أداء مرتفع لوظيفة المراجعة الداخلية في إدارة مخاطر الأمن السيبراني، وللحصول علي معالجات مختلفة تم إضافة مؤشرات للتجربة مرة تشير إلى تعاون مرتفع وأخرى منخفض بين وظيفتي المراجعة الداخلية وأمن المعلومات (الحالتين التجريبيتين الأولي والثانية). أما الحالتين التجريبيتين الثالثة والرابعة تم اضافة مؤشرات تشير مرة إلى دعم مرتفع وأخرى منخفض للإدارة العليا لوظيفة المراجعة الداخلية.

وفيما يتعلق بالتجربة الثانية تمثل مستوى أداء منخفض لوظيفة المراجعة الداخلية في إدارة مخاطر الأمن السيبراني، ثم تم إضافة مؤشرات للحالة التجريبية مرة تشير إلى تعاون مرتفع وأخرى منخفض بين وظيفتي المراجعة الداخلية وأمن المعلومات (الحالتين التجريبيتين الخامسة والسادسة). أما للحالات التجريبية السابعة والثامنة تم اضافة مؤشرات تشير مرة إلى دعم مرتفع وأخرى منخفض للإدارة العليا لوظيفة المراجعة الداخلية.

يطلب من المشاركين في عينة الدراسة الإجابة على بعض الأسئلة التي تهدف لقياس القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني، إضافة إلى مجموعة من الأسئلة– تم إدراجها في بداية الحالة التجريبية– تهدف إلى قياس بعض الخصائص الديموغرافية لمفردات العينة، مثل؛ المركز الوظيفي، مستوى الخبرة، التأهيل العلمي، الحصول على دورات أو شهادات في مجال تكنولوجيا المعلومات و/ أو الأمن السيبراني.

[15] من أكثر المؤسسات المعرضة لهجمات سيبرانية المؤسسات المالية، والاتصالات، وتكنولوجيا المعلومات.

2/3/4/6 التصميم التجريبي:

استخدم الباحث لقياس أثر فعالية وظيفة المراجعة الداخلية في إدارة مخاطر الأمن السيبراني وتأثير التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات، والدور الداعم للإدارة العليا لوظيفة المراجعة الداخلية على فعالية المراجعة الداخلية في إدارة مخاطر الأمن السيبراني تصميماً تجريبياً (2×2×2) بين المجموعات وذلك على النحو المبين في الجدول التالي:

جدول (1) التصميم التجريبي 2×2×2

محددات جودة إدارة مخاطر الأمن السيبراني / مستوى فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني	التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات		دعم الإدارة العليا لوظيفة المراجعة الداخلية	
	مرتفع	منخفض	مرتفع	منخفض
مرتفع	(1) أ- حماية النظم الالكترونية. ب- منع الهجمات والاختراقات السيبرانية. ج- التخفيف من أثار الهجمات والاختراقات السيبرانية.	(2) أ- حماية النظم الالكترونية. ب- منع الهجمات والاختراقات السيبرانية. ج- التخفيف من أثار الهجمات والاختراقات السيبرانية.	(3) أ- حماية النظم الالكترونية. ب- منع الهجمات والاختراقات السيبرانية. ج- التخفيف من أثار الهجمات والاختراقات السيبرانية.	(4) أ- حماية النظم الالكترونية. ب- منع الهجمات والاختراقات السيبرانية. ج- التخفيف من أثار الهجمات والاختراقات السيبرانية.
منخفض	(5) أ- حماية النظم الالكترونية ب- منع الهجمات والاختراقات السيبرانية ج- التخفيف من أثار الهجمات والاختراقات السيبرانية	(6) أ- حماية النظم الالكترونية. ب- منع الهجمات والاختراقات السيبرانية. ج- التخفيف من أثار الهجمات والاختراقات السيبرانية.	(7) أ- حماية النظم الالكترونية. ب- منع الهجمات والاختراقات السيبرانية. ج- التخفيف من أثار الهجمات والاختراقات السيبرانية.	(8) أ- حماية النظم الالكترونية. ب- منع الهجمات والاختراقات السيبرانية. ج- التخفيف من أثار الهجمات والاختراقات السيبرانية.

وفقاً لوصف الحالة التجريبية والتصميم التجريبي تظهر الـ 8 معالجات التجريبية على النحو التالي:

المعالجة رقم (1): مستوى فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية "مرتفع"، وتعاون "مرتفع" بين وظيفتي المراجعة الداخلية وأمن المعلومات، وإدراك أفراد العينة – المهتمين بوظيفة المراجعة الداخلية في شركات المساهمة المقيدة بالبورصة المصرية– للقيمة المضافة من فعالية أداء IA لدوريها في مجال إدارة المخاطر السيبرانية.

المعالجة رقم (2): مستوى فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية "مرتفع"، وتعاون "منخفض" بين وظيفتي المراجعة الداخلية وأمن المعلومات، وإدراك أفراد العينة – المهتمين بوظيفة المراجعة الداخلية في شركات المساهمة المقيدة بالبورصة المصرية– للقيمة المضافة من فعالية أداء IA لدوريها في مجال إدارة المخاطر السيبرانية.

المعالجة رقم (3): مستوى فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية "مرتفع"، ودعم "مرتفع" من الإدارة العليا لوظيفة المراجعة الداخلية، وإدراك أفراد العينة – المهتمين بوظيفة المراجعة الداخلية في شركات المساهمة المقيدة بالبورصة المصرية– للقيمة المضافة من فعالية أداء IA لدوريها في مجال إدارة المخاطر السيبرانية.

المعالجة رقم (4): مستوى فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية "مرتفع"، ودعم "منخفض" من الإدارة العليا لوظيفة المراجعة الداخلية، وإدراك أفراد العينة – المهتمين بوظيفة المراجعة الداخلية في شركات المساهمة المقيدة بالبورصة المصرية– للقيمة المضافة من فعالية أداء IA لدوريها في مجال إدارة المخاطر السيبرانية.

المعالجة رقم (5): مستوى فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية "منخفض"، وتعاون "مرتفع" بين وظيفتي المراجعة الداخلية وأمن المعلومات، وإدراك أفراد العينة – المهتمين بوظيفة المراجعة الداخلية في شركات المساهمة المقيدة بالبورصة المصرية– للقيمة المضافة من فعالية أداء IA لدوريها في مجال إدارة المخاطر السيبرانية.

المعالجة رقم (6): مستوى فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية " منخفض"، وتعاون "منخفض" بين وظيفتي المراجعة الداخلية وأمن المعلومات، وإدراك أفراد العينة – المهتمين بوظيفة المراجعة الداخلية في شركات المساهمة المقيدة بالبورصة المصرية– للقيمة المضافة من فعالية أداء IA لدوريها في مجال إدارة المخاطر السيبرانية.

المعالجة رقم (7): مستوى فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية " منخفض"، ودعم "مرتفع" من الإدارة العليا لوظيفة المراجعة الداخلية، وإدراك أفراد العينة – المهتمين بوظيفة المراجعة الداخلية في شركات المساهمة المقيدة بالبورصة المصرية– للقيمة المضافة من فعالية أداء IA لدوريها في مجال إدارة المخاطر السيبرانية.

المعالجة رقم (8): مستوى فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية " منخفض"، ودعم "منخفض" من الإدارة العليا لوظيفة المراجعة الداخلية، وإدراك أفراد العينة – المهتمين بوظيفة المراجعة الداخلية في شركات المساهمة المقيدة بالبورصة المصرية– للقيمة المضافة من فعالية أداء IA لدوريها في مجال إدارة المخاطر السيبرانية.

ولاختبار فروض البحث، تم إجراء مجموعة من المقارنات بين نتائج المعالجات لاختبار القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني، وتأثير اختلاف التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات ودعم الإدارة العليا لوظيفة المراجعة الداخلية على هذه القيمة المضافة، كالتالي: **المقارنة الأولى:** مقارنة بين حالتي مستوى مرتفع/ مقابل منخفض لفعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية، قبل التعرض للتلاعبات في مستوى المتغيرين المعدلين للعلاقة محل الدراسة، وذلك لاختبار الفرض الأول للبحث (H_1).

المقارنة الثانية: مقارنة بين [(1) × (5)] × [(2) × (6)]، وذلك لاختبار مدى اختلاف أثر فعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني على قيمتها المضافة باختلاف مستوى التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات، من ثم اختبار الفرض الثاني للبحث (H_2).

المقارنة الثالثة: مقارنة بين [(3) × (7)] × [(4) × (8)]، وذلك لاختبار مدى اختلاف أثر فعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني على قيمتها المضافة باختلاف دعم الإدارة العليا لوظيفة المراجعة الداخلية، ومن ثم اختبار الفرض الثالث للبحث (H_3).

4/4/6 توصيف وقياس المتغيرات:

في ضوء فروض البحث، تضمنت متغيرات الدراسة متغير مستقل واحد، وهو فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني، ومتغير تابع، وهو القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني، بالإضافة إلى متغيرين معدلين وهما؛ مستوى التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات، ودعم الإدارة العليا لوظيفة المراجعة الداخلية. وتم توصيف هذه المتغيرات وقياسها على النحو التالي:

1/4/4/6- المتغير المستقل: فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني

يقصد به، عملية مراجعة داخلية تتم وفقاً لمعايير الممارسة المهنية للمراجعة الداخلية، تم معالجة هذا المتغير على مستويين، من خلال تعرض المشاركين في الدراسة لتجربتين تتضمن كل منهما مجموعة من المعالجات التجريبية، حيث تعرض المشاركين في التجربة الأولى لمستوى مرتفع من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني، بينما تعرض المشاركين في التجربة الثانية، لمستوى منخفض من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني، قياساً على (Slapniˇcar et al. 2022)

2/4/4/6- المتغير التابع: القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها في مجال إدارة المخاطر السيبرانية

يقصد به، عملية تنفيذ وتشغيل الأساليب الرقابية، وأنشطة إدارة المخاطر الأخرى، لحماية المعلومات والنظم من الأحداث الأمنية التي يمكن أن يتعرضوا لها، واكتشاف الأحداث الأمنية والاستجابة لها والتخفيف منها عندما الأحداث الأمنية لا يتم منعها (AICPA 2017)، تم قياس هذا المتغير قياساً على (Steinbart et al. 2015; Lois et al. 2021; Slapni˘car et al. 2022) بردود أفراد العينة على مقياس من صفر حتى 10 بشأن:

1- حماية الأصول المعلوماتية والنظم والحاسبات والبرامج الجاهزة.

2- منع الهجمات والاختراقات السيبرانية.

3- التخفيف من الأثار المالية والنوعية للهجمات والاختراقات السيبرانية التي لا يتم منعها.

3/4/4/6- المتغيران المعدلان:

- **مستوى التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات**

يقصد به، العلاقة الجيدة والتنسيق بين وظيفتي المراجعة الداخلية وتكنولوجيا المعلومات في مجال إدارة مخاطر الأمن السيبراني للوصول لمزيد من الفهم والوضوح للمخاطر السيبرانية التي تعرضت لها أو من المحتمل أن تتعرض لها (Jamison et al. (2018، وتم قياسه من خلال تعرض المشاركين في الدراسة لحالات الدراسة التجريبية، حيث تعرض المشاركين في التجربة في الحالتين التجريبيتين الأولى والخامسة لمؤشرات تشير إلى تعاون مرتفع بين وظيفتي المراجعة الداخلية وأمن المعلومات، بينما في الحالتين التجريبيتين الثانية والسادسة تعرض المشاركين في التجربة لمؤشرات تدل على تعاون منخفض بينهما.

- **دعم الإدارة العليا لوظيفة المراجعة الداخلية**

يقصد به، إن الموقف الداعم للإدارة العليا لوظيفة المراجعة الداخلية، وتعزيز الاعتراف والقبول والتقدير من الإدارات المختلفة داخل الشركة (Ta and Doan 2022)، وتم قياس هذا المتغير من خلال تعرض المشاركين في الدراسة للحالات التجريبية، حيث تعرض المشاركين في التجربة في الحالتين التجريبيتين الثالثة والسابعة لمؤشرات تشير إلى دعم

مرتفع من الإدارة العليا لوظيفة المراجعة الداخلية ، بينما في الحالتين التجريبيتين الرابعة والثامنة تعرض المشاركين في التجربة لمؤشرات تدل على دعم منخفض من الإدارة العليا لها.

5/6 نتائج الدراسة التجريبية

1/5/6 الإحصاءات الوصفية

1/1/5/6 الإحصاءات الوصفية لعينة الدراسة

جدول (2) الإحصاء الوصفي لعينة الدراسة

Variable		Frequency	Percent	Cumulative
Gender	Male	45	72.6	72.6
	Female	17	27.4	100.0
		62	100.0	
Background	Internal Auditor	33	53.2	53.2
	Audit committee member	19	30.6	83.9
	Member of the Board of Directors	10	16.1	100.0
		62	100.0	
Qualification	Bachelor's	27	43.5	43.5
	Diploma	11	17.7	61.3
	Master's	18	29.0	90.3
	Ph.D.	6	9.7	100.0
		62	100.0	
Certification	Yes	18	27.4	27.4
	NO	44	72.6	100.0
		62	100.0	
Experience	Less than 5 years	13	21.0	21.0
	From 5 years to less than 10	15	24.2	45.2
	From 10 years to less than 15	9	14.5	59.7
	From 15 years to less than 20	11	17.7	77.4
	From 20 years and over	14	22.6	100.0
		62	100.0	

توضح الإحصاءات الوصفية (جدول 2)، أنه بلغ عدد المشاركين في التجربة 62 مشارك، يتضمن 33 مراجع داخلي، 19 من أعضاء لجان المراجعة، 10 من أعضاء مجالس الإدارة، وأن النسبة الأكبر كانت من الذكور بنسبة مشاركة 72.6%، وأن نسبة 29% حاصلين على ماجستير في المحاسبة، كما أن 27.4% من المشاركين حاصلين على شهادات مهنية متضمنة شهادات في الأمن السيبراني، وفى تكنولوجيا المعلومات، كما أن 54.8% من العينة لديهم خبرة في مجال تخصصهم من 10 سنوات لأكثر من 20 سنة.

2/1/5/6 نتائج اختبارات الثبات (الاعتمادية) Reliability Tests

يوضح (جدول 3) نتيجة معامل كرونباخ ألفا Cronbach's Alpha (0.671)، وهي تمثل نسبة مقبولة للصدق والثبات (Taber 2018)، مما يعني صدق وثبات الأسئلة الخاصة بالحالات الافتراضية التجريبية، وإمكانية الاعتماد عليها وتعميم نتائج العينة على مجتمع الدراسة.

جدول (3) نتائج اختبارات الثبات (الاعتمادية)

Cronbach's Alpha	N of Items
.671	40

3/1/5/6 نتائج اختبارات الاعتدالية Tests of Normality

ولتحديد طبيعة الأساليب الإحصائية التي سيتم الاعتماد عليها في اختبار فروض البحث (أساليب معلميه أو لامعلميه)، قام الباحث بإجراء اختبار الاعتدالية من خلال اختباري Kolomogorov–Smirnov و Shapiro– Wilk، للتحقق من ما إذا كان المجتمع الذي سحبت منه العينة موزعاً توزيعاً طبيعياً أم لا، وأظهرت نتائج الاختبار عدم صحة الفرض القائل أن البيانات مسحوبة من مجتمع يتبع التوزيع الطبيعي (قيمة P–value أقل من 5% لكل الأسئلة على مستوى حالات الدراسة)[16]، وعليه سوف يعتمد الباحث على الأساليب الإحصائية اللامعلمية لاختبار فروض البحث.

2/5/6 نتائج اختبارات فروض الدراسة

يهدف هذا القسم إلى عرض نتائج فروض الدراسة باستخدام الاختبارات اللامعلميه، وتحليل الحساسية الذي يتناول اختبار مدى حساسية نتائج اختبارات فرضي البحث لاختلاف عينة الدراسة من خلال تحديد ما إذا كان هناك فروق معنوية ذات دلالة إحصائية بين مجموعتي، جانب العرض ممثلة في عينة المراجعين الداخليين، وجانب الطلب ممثلة في عينة أعضاء لجنة المراجعة ومجلس الإدارة، فيما يتعلق بإدراكهم للقيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن

[16] يمكن الرجوع للباحث للحصول على النتائج التفصيلية للاختبارين.

السيبراني. والتحليل الإضافي الذي يتناول اختبار مدى وجود اختلاف بين مستوى أهمية أداء وظيفة المراجعة الداخلية لدورها الاستشاري مقارنة بدورها التوكيدي، في حالة فعالية أدائها للدورين (التجربة الأولي) فيما يتعلق بقيمتها المضافة في مجال إدارة مخاطر الأمن السيبراني.

أولاً: التحليل الأساسي

لاختبار فروض البحث وللتحقق من القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني اعتمد الباحث على اجراء تجربتين، تعكس التجربة الأولى مستوى مرتفع لفعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية بينما تعكس التجربة الثانية مستوى منخفض لهذه الفعالية، مع مجموعة من المعالجات تشير إلي التعاون أو/عدم التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات، ودعم أو/عدم دعم الإدارة العليا لوظيفة المراجعة الداخلية

ولاختبار الفرض الأول (H_1) بأن "تؤثر فعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني إيجاباً ومعنوياً على قيمتها المضافة في الشركات المقيدة بالبورصة المصرية". استخدم الباحث اختبار ولكوكسن Wilcoxon Signed–Ranks Test للتحقق من مدى وجود اختلاف في القيمة المضافة من فعالية أداء IA لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية مقاسة بـــ (حماية النظم الالكترونية، التخفيف من أثار الهجمات والاختراقات السيبرانية، منع الهجمات والاختراقات السيبرانية) مقارنة بين حالتي مستوى مرتفع لفعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية/ مستوى منخفض لهذه الفعالية.

أظهرت النتائج الإحصائية (جدول 4) وجود اختلاف ذو دلالة إحصائية بين متوسط إجابات المشاركين عن الحالتين التجريبيتين (مستوى مرتفع لفعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية/ مستوى منخفض لهذه

الفعالية) فيما يتعلق بالقيمة المضافة من فعالية المراجعة الداخلية في مجال إدارة مخاطر الأمن السيبراني مقاسة بـــــ؛ حماية النظم الالكترونية (Z= −6.766; P− Value= .000) ، **التخفيف من أثار الهجمات والاختراقات السيبرانية** (Z= −6.849; P− Value= .000)**، منع الهجمات والاختراقات السيبرانية** (Z= −6.866; P− Value= .000). وأن اتجاه المشاركين في التجربة إلى تحديد حماية أعلى للنظم الإلكترونية، وقدرة أعلى على التخفيف من و/ منع الهجمات والاختراقات السيبرانية في ظل مستوى مرتفع لفعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية مقارنة بالمستوى المنخفض لهذه الفعالية، حيث ظهرت الرتب الموجبة ل High IA EFF – Low IA EFF/ Protecting; Reducing; Preventing أكبر من الرتب السالبة، وكذلك ظهر الوسط الحسابي لردود المشاركين في الحالة التجريبية مستوى مرتفع لفعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية للمقاييس البديلة للمتغير التابع حماية النظم الالكترونية، **التخفيف من أثار و/منع الهجمات والاختراقات السيبرانية** (6.61; 6.29; 6.26) على التوالي، في مقابل(2.50; 2.19; 1.26) على التوالي، للمستوى المنخفض.

كما ظهر الانحراف المعياري لردود المشاركين في الحالة التجريبية مستوى مرتفع لفعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية للمقاييس البديلة للمتغير التابع أقل منه في الحالة المقابلة، مما يشير إلى دقة أراء واتساق إدراك المشاركين في حالة مستوى المرتفع لفعالية المراجعة الداخلية للقيمة المضافة من هذه الفاعلية بشأن حماية النظم الالكترونية، التخفيف من أثار الهجمات والاختراقات السيبرانية، ومنع الهجمات والاختراقات السيبرانية. وتدعم هذه النتائج مجتمعة **قبول الفرض الأول للبحث (H_1).**

وتتفق هذه النتيجة مع ما توصلت إليه كل من دراسة Kahyaoglu and Caliyurt (2018); شحاتة (2022); Slapniˇcar et al. (2022) من التأثير الإيجابي لفعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني على قيمتها المضافة.

جدول (4): نتيجة اختبار Wilcoxon Signed-Ranks لفعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني على قيمتها المضافة

Ranks

		N	Mean Rank	Sum of Ranks
high IA EFF/Protecting – Low IA EFF/Protecting	Negative Ranks	4	4.38	17.50
	Positive Ranks	58	33.37	1935.50
	Ties	0		
	Total	62		
high IA EFF/Reducing – Low IA EFF/Reducing	Negative Ranks	0	.00	.00
	Positive Ranks	61	31.00	1891.00
	Ties	1		
	Total	62		
high IA EFF/Preventing Low IA EFF/Preventing	Negative Ranks	0	.00	.00
	Positive Ranks	61	31.00	1891.00
	Ties	1		
	Total	62		

Descriptive Statistics

	Mean	Std. Deviation
Low IA EFF/Protecting	2.50	1.871
Low IA EFF /Reducing	2.19	1.265
Low IA EFF /Preventing	1.26	1.588
high IA EFF /Protecting	6.61	.732
high IA EFF /Reducing	6.29	.755
high IA EFF /Preventing	6.26	.651

Test Statistics

	High IA EFF -Low IA EFF/ Protecting	High IA EFF -Low IA EFF/ Reducing	High IA EFF -Low IA EFF/ Preventing
Z	-6.766	-6.849	-6.866
Asymp. Sig. (2-tailed)	.000	.000	.000

ولاختبار الفرض الثاني (H_2) بأن " يختلف التأثير المعنوي لفعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني على قيمتها المضافة باختلاف مستوى التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات في الشركات المقيدة في البورصة المصرية". قام الباحث بمقارنة معنوية الفروق بين متوسط إجابات المجموعتين الأولى والخامسة "مستوى فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية "مرتفع" مقابل "منخفض"/ مع تعاون "مرتفع" بين وظيفتي المراجعة الداخلية وأمن المعلومات"، مع معنوية الفروق

للمجموعتين الثانية والسادسة "مستوى فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية "مرتفع" مقابل "منخفض"/ مع تعاون "منخفض" بين وظيفتي المراجعة الداخلية وأمن المعلومات" فيما يتعلق بإدراك أفراد العينة – المهتمين بوظيفة المراجعة الداخلية في شركات المساهمة المقيدة بالبورصة المصرية– للقيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها في مجال إدارة المخاطر السيبرانية مقاسة بثلاثة مقاييس؛ حماية النظم الالكترونية، التخفيف من أثار و/منع الهجمات والاختراقات السيبرانية. ويوضح الجدول (5)، إحصائية (Z)، ومستوى الدلالة (P–Value)، وتشير النتائج إلى وجود اختلاف ذو دلالة معنوية بين متوسط إجابات المجموعتين الأولى والخامسة (حالتي مستوى فعالية أداء المراجعة الداخلية "مرتفع" مقابل "منخفض/ مع مستوى تعاون **"مرتفع"** بين وظيفتي المراجعة الداخلية وأمن المعلومات) فيما يتعلق بالقيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها في مجال إدارة المخاطر السيبرانية مقاسة بـــ حماية النظم الالكترونية، التخفيف من أثار الهجمات والاختراقات السيبرانية، منع الهجمات والاختراقات السيبرانية حيث أن (Z= −6.923, P–Value= .000)، (Z= −6.962, P–Value= .000)، (Z= −6.938, P–Value= .000) ، لكل منهم على التوالي، وكذلك بالنسبة لمتوسط إجابات المجموعتين الثانية والسادسة (حالتي مستوى فعالية أداء المراجعة الداخلية "مرتفع" مقابل "منخفض/ مع مستوى تعاون **"منخفض"** بين وظيفتي المراجعة الداخلية وأمن المعلومات) حيث اشارت النتائج الإحصائية إلى أن (Z= −7.067, P–Value= .000)، (Z= −6.933, P–Value= .000)، (Z= −7.062, P–Value= .000) لكل من حماية النظم الالكترونية، التخفيف من أثار الهجمات والاختراقات السيبرانية، منع الهجمات والاختراقات السيبرانية على التوالي. وتشير هذه النتائج الإحصائية إلى عدم تأثير التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات على العلاقة محل الدراسة وأن الأثر الإيجابي لفعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني على قيمتها المضافة لن يختلف باختلاف مستوى التعاون بين

وظيفتي المراجعة الداخلية وأمن المعلومات في الشركات المقيدة بالبورصة المصرية. ومن ثم يمكن الباحث **رفض الفرض الثاني للبحث (H_2)**.

وتتفق هذه النتيجة مع ما توصلت إليه دراسة Lois et al. (2021) من عدم وجود تأثير "للتعاون" بين المراجع الداخلي وموظفي تكنولوجيا المعلومات على إدارة مخاطر الأمن السيبراني، بينما تختلف مع ما توصل إليه كل من Steinbart et al. (2018); Jamison et al. (2018) في أن التعاون يؤدي إلى تبادل المعرفة وكشف المزيد من الانتهاكات السيبرانية قبل أن تتسبب في خسائر مالية أو غيرها من خسائر الأعمال.

ويمكن للباحث تفسير هذه النتيجة التي جاءت بخلاف توقعه، إلى احتمال اقتناع المهتمين بالمراجعة الداخلية في جانبي العرض والطلب أن "التعاون" مع قسم محدد يهدد استقلال المراجع الداخلي، ويضعف ما تقدمه المراجعة الداخلية من فحص موضوعي ومحايد لعمليات الأمن السيبراني، كما أن قيام المراجع الداخلي بدوره في إدارة مخاطر الأمن السيبراني يتطلب معرفة أكبر بنظم وتكنولوجيا المعلومات من خلال حصوله على شهادات متخصصة وتدريب في مجال تكنولوجيا المعلومات والأمن السيبراني، ولا يمكن تعويض ذلك من خلال التعاون الجيد مع موظفي أمن المعلومات.

جدول (5): نتائج اختبار Wilcoxon Signed-Ranks للأثر التفاعلي لفعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني والتعاون بين ووظيفتي المراجعة الداخلية وأمن المعلومات على القيمة المضافة من هذه الفعالية

تعاون منخفض بين وظيفتي المراجعة الداخلية وأمن المعلومات				تعاون مرتفع بين وظيفتي المراجعة الداخلية وأمن المعلومات			
	Case 2 - Case 6 Protecting	Case 2 - Case 6 Reducing	Case 2 - Case 6 Preventing		Case 1 - Case 5 Protecting	Case 1 - Case 5 Reducing	Case 1 - Case 5 Preventing
Z	-7.067	-6.933	-7.062	Z	-6.923	-6.962	-6.938
Asymp. Sig. (2-tailed)	.000	.000	.000	Asymp. Sig. (2-tailed)	.000	.000	.000

ولاختبار الفرض الثاني (H_3) بأن "يختلف التأثير المعنوي لفعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني على قيمتها

المضافة باختلاف مستوى دعم الإدارة العليا لوظيفة المراجعة الداخلية في الشركات المقيدة في البورصة المصرية." قام الباحث بمقارنة معنوية الفروق بين متوسط إجابات المجموعتين الثالثة والسابعة "مستوى فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية "مرتفع" مقابل "منخفض"/ مع دعم "مرتفع" من الإدارة العليا لوظيفة المراجعة"، مع معنوية الفروق للمجموعتين الرابعة والثامنة "مستوى فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية "مرتفع" مقابل "منخفض"/ مع دعم "منخفض" من الإدارة العليا لوظيفة المراجعة"، فيما يتعلق بإدراك أفراد العينة – المهتمين بوظيفة المراجعة الداخلية في شركات المساهمة المقيدة بالبورصة المصرية– للقيمة المضافة من فعالية أداء المراجعة لدوريها في مجال إدارة المخاطر السيبرانية مقاسة بثلاثة مقاييس؛ حماية النظم الالكترونية، التخفيف من أثار و/منع الهجمات والاختراقات السيبرانية.

ويوضح الجدول (6)، إحصائية (Z)، ومستوى الدلالة (P–Value)، وتشير النتائج إلى وجود اختلاف ذو دلالة معنوية بين متوسط إجابات المجموعتين الثالثة والسابعة (حالتي مستوى فعالية أداء المراجعة الداخلية "مرتفع" مقابل "منخفض/ مع **دعم "مرتفع"** من الإدارة العليا لوظيفة المراجعة) فيما يتعلق بالقيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها في مجال إدارة المخاطر السيبرانية مقاسة بـــ حماية النظم الالكترونية، التخفيف من أثار الهجمات والاختراقات السيبرانية، منع الهجمات والاختراقات السيبرانية حيث أن (Z= – 7.003, P–Value= .000)، (Z= −7.192, P–Value= .000)، (Z= −7.016, P–Value= .000) ، لكل منهم على التوالي، في حين لم يتحقق بالنسبة لحالتي الدعم المنخفض للإدارة العليا لوظيفة المراجعة الداخلية، فقد أظهرت النتائج الاحصائية عدم وجود اختلاف ذو دلالة معنوية بين متوسط إجابات المجموعتين الرابعة والثامنة (حالتي مستوى فعالية أداء المراجعة الداخلية "مرتفع" مقابل "منخفض/ مع دعم "منخفض" من الإدارة العليا لوظيفة المراجعة الداخلية) ، حيث ظهرت (Z= −1.814, P–Value= .070)، (Z= −.468, P–Value= .640)، (Z= −1.229, P–Value= .219) لكل من الأسئلة

التي تقيس المتغير التابع المتعلقة بحماية النظم الالكترونية، التخفيف من أثار الهجمات والاختراقات السيبرانية، منع الهجمات والاختراقات السيبرانية على التوالي. ويشير ذلك إلى تأثير دعم الإدارة العليا لوظيفة المراجعة الداخلية على العلاقة محل الدراسة وأن الأثر الإيجابي لفعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني على قيمتها المضافة يختلف باختلاف مستوى دعم الإدارة العليا لوظيفة المراجعة الداخلية في الشركات المقيدة بالبورصة المصرية. ومن ثم يمكن الباحث **قبول الفرض الثالث للبحث(H_3)**.

جدول (6): نتائج اختبار Wilcoxon Signed-Ranks للأثر التفاعلي لفعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني ودعم الإدارة العليا لوظيفة المراجعة الداخلية على القيمة المضافة من هذه الفعالية

دعم "مرتفع" من الإدارة العليا لوظيفة المراجعة الداخلية				دعم "منخفض" من الإدارة العليا لوظيفة المراجعة الداخلية			
	Case 3 - Case 7 Protecting	Case 3 - Case 7 Reducing	Case 3 - Case 7 Preventing		Case 4 - Case 8 Protecting	Case 4 - Case 8 Reducing	Case 4 - Case 8 Preventing
Z	-7.003	-7.192	-7.016	Z	-1.814	-.468	-1.229
Asymp. Sig. (2-tailed)	.000	.000	.000	Asymp. Sig. (2-tailed)	.070	.640	.219

وتتفق هذه النتيجة مع ما توصل إليه كل Mihret et al. (2010); Octavia; (2013); Dellai et al. (2016) أن دعم الإدارة العليا لوظيفة المراجعة الداخلية من أهم العوامل المؤثرة علي فعاليتها، وأيضاً تتفق مع دراسة Islam et al. (2018) التي توصلت إلى وجود أثر إيجابي لتدخل مجلس الإدارة في سياسات الحوكمة ضمن عمل المراجعة الداخلية على مراجعة الأمن السيبراني، إلا أن هذه العلاقة الإيجابية تحققت فقط في الولايات المتحدة من ضمن عدد من دول العينة، كما تتفق مع دراسة Ta and Doan (2022) التي وجدت أن دعم الإدارة العليا لوظيفة المراجعة الداخلية عنصر أساسي في قبول وتقدير دورها من

قبل الإدارات الأخرى داخل الشركة، مما يسهل قيام المراجعين الداخليين بمهامهم ومسئولياتهم المتعلقة بالإشراف ومراقبة عناصر هيكل الرقابة الداخلية، وإدارة المخاطر وحوكمة الشركات.

ثانياً: تحليل الحساسية

يستهدف الباحث من تحليل الحساسية اختبار مدي حساسية نتائج اختبارات الفرض الأول للبحث[17] لاختلاف منظور المهتمين بوظيفة المراجعة الداخلية لفعاليتها ومن ثم ما تقدمه من قيمة مضافة، بحيث يتحقق الباحث من ما إذا كانت الاستنتاجات التي تم التوصل إليها فيما يتعلق بالأثر الإيجابي لفعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني على قيمتها المضافة مدفوعاً بمنظور المهتمين بوظيفة المراجعة الداخلية، ما إذا كان من العاملين بأدوات المراجعة الداخلية (منظور جانب العرض)، أو من أعضاء كل من مجلس الإدارة ولجنة المراجعة (منظور جانب الطلب)، لذلك قام الباحث باختبار كيف يختلف ادراك عينة الدراسة من المهتمين بوظيفة المراجعة الداخلية باختلاف جانبي العرض والطلب بالاتساق مع (Lenz and Hahn 2015; Roussy et al. 2020)، وبالنسبة للفرض الأول يتوقع الباحث أن تؤثر فعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني إيجاباً ومعنوياً على قيمتها المضافة، وقام الباحث بالمقارنات الثنائية بين مستويي فعالية المراجعة الداخلية المرتفعة والمنخفضة باستخدام اختبار Wilcoxon Signed-Ranks (جدول 7)، حيث تكون استنتاجات الباحث ذات متانة في حالة ما إذا كانت فعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني تؤثر إيجاباً ومعنوياً علي إدراك كل من جانبي العرض والطلب كل علي حدا فيما يتعلق بالقيمة المضافة لهذه الفعالية مقاسة بثلاثة مقاييس بديلة وهى؛ حماية النظم الالكترونية، التخفيف من أثار الهجمات والاختراقات السيبرانية، منع الهجمات والاختراقات السيبرانية.

[17] حيث يختبر الفرض الأول العلاقة الرئيسية للبحث.

جدول (٧): نتيجة اختبار Wilcoxon Signed–Ranks لفعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني على قيمتها المضافة وفقاً لمنظور جانبي العرض والطلب

جدول (٧/أ): منظور جانب العرض
حالة فعالية المراجعة الداخلية مقابل حالة عدم فعالية المراجعة الداخلية

Ranks

		N	Mean Rank	Sum of Ranks
high IA EFF/Protecting – Low IA EFF/Protecting	Negative Ranks	4	4.38	17.50
	Positive Ranks	29	18.74	543.50
	Ties	0		
	Total	33		
high IA EFF/Reducing – Low IA EFF/Reducing	Negative Ranks	0	.00	.00
	Positive Ranks	32	16.50	528.00
	Ties	1		
	Total	33		
high IA EFF/Preventing Low IA EFF/Preventing	Negative Ranks	0	.00	.00
	Positive Ranks	32	16.50	528.00
	Ties	1		
	Total	33		

Descriptive Statistics

	Mean	Std. Deviation
Low IA EFF/Protecting	3.61	1.749
Low IA EFF /Reducing	2.64	1.558
Low IA EFF /Preventing	2.06	1.784
high IA EFF /Protecting	6.73	.719
high IA EFF /Reducing	6.24	.663
high IA EFF /Preventing	6.27	.761

Test Statistics

	High IA EFF -Low IA EFF/ Protecting	High IA EFF -Low IA EFF/ Reducing	High IA EFF -Low IA EFF/ Preventing
Z	-4.737	-4.971	-4.968
Asymp. Sig. (2-tailed)	.000	.000	.000

جدول (7/ب): منظور جانب الطلب
حالة فعالية المراجعة الداخلية مقابل حالة عدم فعالية المراجعة الداخلية

Ranks

		N	Mean Rank	Sum of Ranks
high IA EFF/Protecting – Low IA EFF/Protecting	Negative Ranks	0	.00	.00
	Positive Ranks	29	15.00	435.00
	Ties	0		
	Total	29		
high IA EFF/Reducing – Low IA EFF/Reducing	Negative Ranks	0	.00	.00
	Positive Ranks	29	15.00	435.00
	Ties	0		
	Total	29		
high IA EFF/Preventing Low IA EFF/Preventing	Negative Ranks	0	.00	.00
	Positive Ranks	29	15.00	435.00
	Ties	0		
	Total	29		

Descriptive Statistics

	Mean	Std. Deviation
Low IA EFF/Protecting	1.24	1.023
Low IA EFF /Reducing	1.69	.471
Low IA EFF /Preventing	.34	.484
high IA EFF /Protecting	6.48	.738
high IA EFF /Reducing	6.34	.857
high IA EFF /Preventing	6.24	.511

Test Statistics

	High IA EFF -Low IA EFF/ Protecting	High IA EFF -Low IA EFF/ Reducing	High IA EFF -Low IA EFF/ Preventing
Z	-4.761	-4.757	-4.852
Asymp. Sig. (2-tailed)	.000	.000	.000

وقد أظهرت نتائج التحليل الإحصائي (جدول 7)، وجود اختلاف معنوي بين متوسط إدراك المشاركين للقيمة المضافة من فعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني لكل من منظور العرض والطلب كل على حدا، حيث من منظور جانب العرض (جدول 7/أ) ظهر متوسط حماية النظم الالكترونية ،(Z=−4.737, P− Value = .000) التخفيف من أثار الهجمات والاختراقات السيبرانية (Z=−4.971, P− Value = .000) و منع الهجمات والاختراقات السيبرانية (Z=−4.968, P− Value = .000)، بين عينتي العاملين بأدوات المراجعة الداخلية (منظور جانب العرض)، وكذلك بين عينتي أعضاء كل من مجلس الإدارة ولجنة المراجعة (منظور جانب الطلب) جدول (7/ب) حيث أن حماية النظم الالكترونية،(Z=−4.761, P− Value = .000) التخفيف من أثار الهجمات والاختراقات السيبرانية (Z=−4.757, P− Value = .000) ومنع الهجمات والاختراقات السيبرانية (Z=−4.852, P− Value = .000)، في حالة الفعالية المرتفعة مقابل الفعالية المنخفضة.

كما ظهر اتجاه المشاركين في التجربة إلى تحديد حماية أعلى للنظم الإلكترونية، وقدرة أعلى على التخفيف من و/ منع الهجمات والاختراقات السيبرانية في ظل مستوى مرتفع لفعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة المخاطر السيبرانية مقارنة بالمستوى المنخفض لهذه الفعالية، حيث ظهرت الرتب الموجبة لـــ High IA EFF – Low IA EFF/ Protecting; Reducing; Preventing أكبر من الرتب السالبة بين عينتي جانب العرض، وكذلك بين عينتي جانب الطلب.

وتتفق هذه النتائج مع نتائج التحليل الأساسي (جدول 4)، مما يدعم النتائج الرئيسية للدراسة، وجودة وإمكانية الاعتماد على تصميم نموذج البحث واختبار الفرض الرئيسي للبحث في ظل التحليل الأساسي.

ثالثاً: التحليل الإضافي

يهدف التحليل الإضافي إلى اختبار ما إذا كان مستوى التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات، ودعم الإدارة العليا لوظيفة المراجعة الداخلية، كمتغيرين مستقلين

يؤثر على القيمة المضافة من فعالية المراجعة الداخلية في مجال إدارة مخاطر الأمن السيبراني في حالة التعرض لمستوى فعالية مرتفع لأداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في هذا المجال، ولتحقيق هذا الهدف، قام الباحث بتحليل التجربة الأولى (حالة التعرض لمستوى فعالية مرتفع لأداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني)، ولاختبار أثر التعاون كمتغير مستقل، قام الباحث بمقارنة ردود المشاركين في الحالة التجريبية الأولى (تعاون مرتفع) وردود المشاركين في الحالة التجريبية الثانية (تعاون منخفض)، أما لاختبار أثر دعم الإدارة العليا كمتغير مستقل، قام الباحث بمقارنة ردود المشاركين في الحالة التجريبية الثالثة (دعم مرتفع) ردود المشاركين في الحالة التجريبية الرابعة (دعم منخفض)، ويوضح الجدول (8)، (9) نتيجة اختبار Wilcoxon Signed–Ranks للمقارنتين، على النحو التالي:

جدول (8): نتيجة اختبار Wilcoxon Signed–Ranks لأثر التعاون بين وظيفتي المراجعة الداخلية وأمن المعلومات على القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني في حالة مستوى فعالية مرتفع لهذا الأداء

Ranks

		N	Mean Rank	Sum of Ranks
High - Low cooperation /Protecting	Negative Ranks	1	4.50	4.50
	Positive Ranks	61	31.94	1948.50
	Ties	0		
	Total	62		
High - Low cooperation /Reducing	Negative Ranks	1	4.00	4.00
	Positive Ranks	60	31.45	1887.00
	Ties	1		
	Total	62		
High- Low cooperation /Preventing	Negative Ranks	2	7.00	14.00
	Positive Ranks	57	30.81	1756.00
	Ties	3		
	Total	62		

Descriptive Statistics

	Mean	Std. Deviation
Low cooperation/Protecting	6.29	.710
Low cooperation /Reducing	6.05	.931
Low cooperation /Preventing	5.77	.913
high cooperation /Protecting	8.82	.497
high cooperation /Reducing	8.58	.588
high cooperation /Preventing	7.81	.765

Test Statistics

	High - Low cooperation /Protecting	High - Low cooperation /Reducing	High- Low cooperation /Preventing
Z	-7.042	-6.869	-6.673
Asymp. Sig. (2-tailed)	.000	.000	.000

جدول (9): نتيجة اختبار Wilcoxon Signed-Ranks لأثر دعم الإدارة العليا لوظيفة المراجعة الداخلية على القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني في حالة مستوى فعالية مرتفع لهذا الأداء

Ranks

		N	Mean Rank	Sum of Ranks
High - Low Support /Protecting	Negative Ranks	0	.00	.00
	Positive Ranks	62	31.50	1953.00
	Ties	0		
	Total	62		
High - Low Support /Reducing	Negative Ranks	0	.00	.00
	Positive Ranks	62	31.50	1953.00
	Ties	0		
	Total	62		
High- Low Support /Preventing	Negative Ranks	0	.00	.00
	Positive Ranks	62	31.50	1953.00
	Ties	0		
	Total	62		

Descriptive Statistics

	Mean	Std. Deviation
Low Support /Protecting	1.37	.683
Low Support /Reducing	1.26	.723
Low Support /Preventing	1.06	.569
high Support /Protecting	8.94	.400
high Support /Reducing	9.00	.256
high Support /Preventing	7.81	.623

Test Statistics

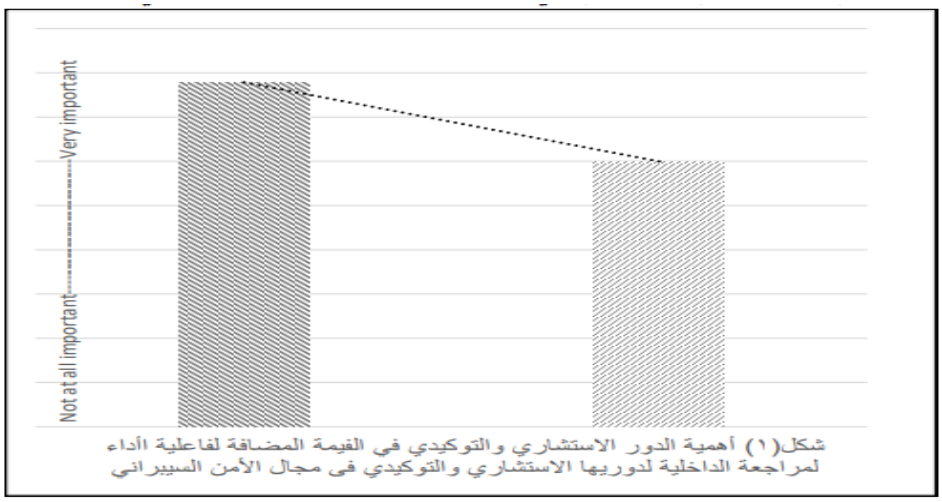
	High - Low Support /Protecting	High - Low Support /Reducing	High- Low Support /Preventing
Z	-7.029	-7.219	-7.035
Asymp. Sig. (2-tailed)	.000	.000	.000

ويتضح من النتائج الإحصائية (جدول 8) وجود تأثير معنوي إيجابي لمتغير التعاون والعلاقة الجيدة بين المراجعين الداخليين وموظفي أمن المعلومات على القيمة المضافة من فعالية أداء المراجعة الداخلية في مجال إدارة مخاطر الأمن السيبراني من خلال حماية النظم الالكترونية، التخفيف من أثار الهجمات والاختراقات السيبرانية، ومنع الهجمات والاختراقات السيبرانية، كما يتضح من النتائج الإحصائية (جدول 9) وجود تأثير معنوي إيجابي لمتغير دعم الإدارة العليا لوظيفة المراجعة الداخلية على القيمة المضافة من فعالية أداء المراجعة الداخلية في مجال إدارة مخاطر الأمن السيبراني للثلاث مقاييس البديلة لهذه القيمة المضافة. مما يشير أن لمتغيري "التعاون"، و"الدعم" أثرا معنوياً إيجابياً على إدراك المهتمين بوظيفة المراجعة الداخلية جانبي العرض والطلب معاً على القيمة المضافة التي توفرها فعالية أداء المراجعة الداخلية في مجال حماية النظم الالكترونية وتخفيف من أثار الهجمات والاختراقات السيبرانية حالة حدوثها وإمكانية منعها قبل وقوع أثارها.

ومن الجدير بالذكر، أنه بالرغم من الأثر المعنوي الإيجابي للمتغيرين "التعاون" و"الدعم"، حيث وجود اختلافات معنوية ذات دلالة إحصائية بين مقارنة حالتي "التعاون المرتفع مقابل المنخفض"، وكذلك بين مقارنة حالتي "الدعم المرتفع مقابل المنخفض" في ظل مستوى فعالية مرتفع، إلا أنه ظهر الوسط الحسابي حالة دعم الإدارة العليا المنخفض أقل بدرجة ملحوظة من متوسط المقياس (5 درجات)، حيث ظهر الوسط الحسابي لردود المشاركين لمقاييس المتغير التابع "الحماية، التخفيف والمنع" (1.37،1.26، 1.06 على التوالي) مقارنة بحالة الدعم المرتفع الذى ظهر أعلى بدرجة كبيرة من متوسط المقياس حيث كان للثلاث مقاييس (8.94،9.00،7.81على التوالي). في المقابل ظهر الوسط الحسابي حالتي التعاون المنخفض والمرتفع أعلى من متوسط المقياس حيث ظهر متوسط الردود مقاييس المتغير التابع الحماية، التخفيف والمنع في حالة التعاون المنخفض (6.29،6.05، 5.77 على التوالي) وظهر في حالة التعاون المرتفع (8.82،8.58، 7.81على التوالي)، وتشير هذه النتيجة إلى أهمية متغير دعم الإدارة كمتغير حاسم وحرج في تحقيق القيمة المضافة من فعالية المراجعة الداخلية في مجال إدارة مخاطر الأمن السيبراني، فمع انخفاض الدعم انخفض إدراك المشاركين في التجربة للقيمة المضافة من فعالية أداء المراجعة الداخلية في حماية النظم الالكترونية، والتخفيف من أثار الهجمات والاختراقات السيبرانية، ومنع الهجمات والاختراقات السيبرانية، إلى منخفض جداً وبمعنى أدق إلى ما يقترب من عدم تأثير لهذه الفعالية على قيمتها المضافة في مجال إدارة مخاطر الأمن السيبراني.

كما قام الباحث بتحليل إضافي لتحديد مدى أهمية الدورين الاستشاري والتوكيدي كل على حدا في تعزيز القيمة المضافة من فعالية أداء المراجعة الداخلية في مجال إدارة مخاطر الأمن السيبراني في ظل مستوى فعالية مرتفع.

يوضح شكل (1) الأهمية النسبية لكل من الدور الاستشاري والتوكيدي في المضافة من فعالية أداء المراجعة الداخلية في مجال إدارة مخاطر الأمن السيبراني لجميع المشاركين الذين استلموا حالات مستوى مرتفع لفعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني.



شكل(١) أهمية الدور الاستشاري والتوكيدي في القيمة المضافة لفاعلية أداء لمراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال الأمن السيبراني

كما أظهرت النتائج الإحصائية (جدول 10) اختلافات معنوية ذات دلالة إحصائية بين الدورين الاستشاري والتوكيدي مع اتجاه إعطاء المشاركين في التجربة لأهمية أكبر للدور التوكيدي كعنصر مضيف للقيمة في مجال إدارة مخاطر الأمن السيبراني مقارنة بالدور الاستشاري في حالات التعاون المرتفع، والمنخفض، والدعم المنخفض حيث ظهرت (p-value=.000) في الثلاث حالات مع انخفاض متوسط أهمية الدور الاستشاري بدرجة كبيرة في حالتي التعاون المنخفض، والدعم المنخفض حيث ظهر الوسط الحسابي للأهمية (4.40 ;2.73 على التوالي) وهو أقل من متوسط المقياس، إلا أنه زال ذلك الاختلاف المعنوي بين الدورين (Z=-1.613; P-Value=.107)، فقط في حالة الدعم المرتفع للإدارة العليا لوظيفة المراجعة الداخلية، مما يشير إلى النصح والاستشارات التي تقدمها المراجعة الداخلية للإدارة العليا وللإدارات المختلفة بالمنظمة في نطاق الدور الاستشاري تزداد أهميتها وتحتل نفس أهمية الدور التوكيدي إحصائياً في تعزيز القيمة المضافة من فعالية أداء المراجعة الداخلية في مجال إدارة مخاطر الأمن السيبراني عند وجود دعم مرتفع من الإدارة العليا لوظيفة المراجعة الداخلية.

جدول (10): نتيجة اختبار Wilcoxon Signed-Ranks لأهمية الدور الاستشاري مقارنة بالتوكيدي التعاون بين على القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني في حالة مستوى فعالية مرتفع لهذا الأداء

Ranks

		N	Mean Rank	Sum of Ranks
Assurance Role – Consulting Role/ High cooperation	Negative Ranks	0	.00	.00
	Positive Ranks	46	23.50	1081.00
	Ties	16		
	Total	62		
Assurance Role – Consulting Role/ High Support	Negative Ranks	2	3.50	7.00
	Positive Ranks	6	4.83	29.00
	Ties	54		
	Total	62		
Assurance Role – Consulting Role/ low cooperation	Negative Ranks	0	.00	.00
	Positive Ranks	62	31.50	1953.00
	Ties	0		
	Total	62		
Assurance Role – Consulting Role/ Low Support	Negative Ranks	2	6.00	12.00
	Positive Ranks	53	28.83	1528.00
	Ties	7		
	Total	62		

Descriptive Statistics

	Mean	Std. Deviation
High cooperation/ Consulting Role	8.18	.385
High Support/ Consulting Role	8.68	.566
low cooperation/ Consulting Role	4.40	1.108
low Support/ Consulting Role	2.73	1.230
High cooperation/Assurance Role	8.92	.275
High Support/ Assurance Role	8.77	.459
low cooperation/Assurance Role	8.42	.759
low Support/ Assurance Role	5.03	.923

Test Statistics

	Assurance Role – Consulting Role/ High cooperation	Assurance Role – Consulting Role/ High Support	Assurance Role – Consulting Role/ low cooperation	Assurance Role – Consulting Role/ Low Support
Z	-6.782	-1.613	-6.884	-6.397
Asymp. Sig. (2-tailed)	.000	.107	.000	.000

6/6 الخلاصة والتوصيات وأهم مجالات البحث المستقبلية المقترحة

استهدف هذا البحث إجراء دراسة انتقادية للمراجع العلمية ذات الصلة بالقيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني واختبار هذه العلاقة، إضافة إلى دراسة الأثر المعدل لكل من التعاون بين

وظيفتي المراجعة الداخلية وأمن المعلومات، ودعم الإدارة العليا لوظيفة المراجعة الداخلية على العلاقة محل الدراسة، وذلك من خلال تصميم تجريبي على عينة من المهتمين بوظيفة المراجعة الداخلية في شركات المساهمة المقيدة بالبورصة المصرية.

تنظر المنظمات المهنية إلى أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في إدارة المخاطر والرقابة الداخلية، وحوكمة الشركات بأنه عامل هام وداعم للقيمة المضافة الناتجة من هذا الأداء، ومن ثم فإن أداء المراجعة لدوريها الاستشاري والتوكيدي في ظل التحول الرقمي الذي غلب على واقع الأعمال في الفترة الأخيرة وزيادة استخدام تكنولوجيا المعلومات، وما صاحبه من مخاطر أمن سيبراني يمكن أن يوثر إيجاباً على قيمتها المضافة في إدارة مخاطر الأمن السيبراني، ومع ذلك، فإن هذا هذا الأثر مرهوناً بفعالية أداء المراجعة الداخلية لدويها الاستشاري والتوكيدي في هذا المجال، كما قد يؤثر علي هذا الأثر العلاقة الجيدة والتنسيق بين وظيفتي المراجعة الداخلية وتكنولوجيا المعلومات في مجال إدارة مخاطر الأمن السيبراني، والموقف الداعم للإدارة العليا لوظيفة المراجعة الداخلية، وتعزيزها الاعتراف والقبول والتقدير من الإدارات المختلفة داخل الشركة لوظيفة المراجعة الداخلية.

وأظهرت نتائج الدراسة التجريبية أن فعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني تؤثر إيجاباً ومعنوياً على قيمتها المضافة في مجال إدارة مخطر الأمن السيبراني، من حيث التأثير الإيجابي على حماية النظم الالكترونية، التخفيف من أثار الهجمات والاختراقات السيبرانية، منع الهجمات والاختراقات السيبرانية، مما يشير إلى أن فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي مراجعة مخاطر الأمن السيبراني له أثر هام في ما توفره من قيمة مضافة للشركة في مجال إدارة مخاطر الأمن السيبراني.

كما اتضح عدم وجود تأثير "للتعاون" بين المراجع الداخلي وموظفي تكنولوجيا المعلومات على إدارة مخاطر الأمن السيبراني وأن الأثر الإيجابي لفعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني على قيمتها المضافة لا يختلف باختلاف "التعاون"، بينما اتضح وجود تأثير معنوي لدعم الإدارة العليا لوظيفة

المراجعة الداخلية على العلاقة محل الدراسة وأن الأثر الإيجابي لفعالية أداء وظيفة المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني على قيمتها المضافة يختلف باختلاف مستوى دعم الإدارة العليا لوظيفة المراجعة الداخلية.

وأخيراً، أظهرت النتائج الإحصائية للتحليل الإضافي أن فعالية أداء المراجعة الداخلية المرتفعة للدور التوكيدي في مراجعة الأمن السيبراني تساهم في تحسين إدارة مخاطر الأمن السيبراني، بدرجة أكبر من الدور الاستشاري، ومع ذلك، اختفى ذلك الاختلاف المعنوي بين الدورين الاستشاري والتوكيدي مع وجود دعم مرتفع من الإدارة العليا لوظيفة المراجعة الداخلية، وساهم كل من الدورين الاستشاري والتوكيدي بشكل متساوي احصائياً في تحسين إدارة مخاطر الأمن السيبراني.

وفي ضوء أهداف البحث ومشكلته وحدوده، وما انتهي إليه من نتائج في شقيه النظري والتجريبي، يوصي الباحث بما يلي:

- اهتمام المنظمات المهنية ومجالس إدارات الشركات بتوفير مناخ ملائم يعزز فعالية المراجعة الداخلية للقيام بدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني ويتضمن ذلك، توفير القوانين واللوائح المتعلقة بالأمن السيبراني لمساعدة المراجع الداخلي على مراجعة الامتثال لها، توفير التدريب للمراجع الداخلي في مجالات تكنولوجيا المعلومات والأمن السيبراني، ارتقاء النظر لوظيفة المراجعة الداخلية كنشاط مضيف للقيمة، واضفاء الطابع المهني عليها.
- الاهتمام بدعم الإدارة العليا لوظيفة المراجعة الداخلية وتوفير الاستقلال التنظيمي لها، بما له من أهمية في تفعيل الدورين التوكيدي والاستشاري لها بصفة عامة، وفي مجال إدارة مخاطر الأمن السيبراني بصفة خاصة، الأمر الذي ينعكس على تخفيض مستوى فجوة التوقعات في المراجعة الداخلية، ويمكن المراجعين الداخليين من تحسين الأداء لأدوارهم، واضافة قيمة للشركة.
- تحديد مجلس إدارة الشركة بعد أخذ توصية لجنة المراجعة لأحد أطر عمل الأمن السيبراني بما يضمن توفير المعايير والمبادئ التوجيهية والممارسات التي يمكن أن يستند إليها المراجع الداخلي عند وضع خطة لمراجعة الأمن السيبراني.

- ضرورة العمل بشكل تكاملي بين إدارة المراجعة الداخلية وقسمي إدارة المخاطر وأمن المعلومات، بما يوفر رؤية شاملة للمراجع الداخلي عن مخاطر الأمن السيبراني، ومن الجانب الأخر يمكن قسمي إدارة المخاطر وأمن المعلومات من تلقى النصح والاستشارة من جانب المراجع الداخلي.
- تطوير نظام التعليم المحاسبي، لأخذ كافة المستجدات في بيئة الأعمال، لا سيما التحول الرقمي للأعمال، والتطورات المتسارعة في تكنولوجيا المعلومات، فلم يعد التعليم المحاسبي التقليدي يلبي طموحات الطلاب، كما أنه لا يفي باحتياجات سوق العمل.
- زيادة اهتمام البحث الأكاديمي في مصر بمجال المراجعة الداخلية في ظل تبني الشركات لأدوات التحول الرقمي، والتعرض لمخاطر الأمن السيبراني، خاصة أن مجال المراجعة الداخلية به ندرة في الأبحاث الأكاديمية المصرية.

وبشأن مجالات البحث المقترحة، يعتقد الباحث بأهمية البحث مستقبلًا في بعض المجالات ذات الصلة، والتي من أهمها ما يلي:

- أثر فعالية لجنة المراجعة على العلاقة بين المراجعة الداخلية للأمن السيبراني ونضج إدارة مخاطر الأمن السيبراني – دراسة تطبيقية
- إطار مقترح لإسناد وظيفة المراجعة الداخلية بدوريها الاستشاري والتوكيد في مجال إدارة مخاطر الأمن السيبراني – دراسة تجريبية في البنوك المصرية.
- العوامل المحددة لفعالية أداء المراجعة الداخلية في إدارة مخاطر الأمن السيبراني – دراسة تحليلية وتجريبية
- دور حوكمة تكنولوجيا المعلومات في تفعيل الدورين الاستشاري والتوكيدي للمراجعة الداخلية في مراجعة نظم أمن المعلومات.
- أثر استخدام المراجعة الداخلية لأدوات تحليل البيانات الضخمة على قرار اعتماد مراقب الحسابات عليها– دراسة تجريبية.
- إطار إجرائي مقترح لتفعيل أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال التحقق من المنصة السحابية.

مراجع البحث

المراجع العربية:

- أميرهم، جيهان عادل ناجى. (2022). أثر جودة المراجعة الداخلية في الحد من مخاطر الامن السيبراني وانعكاساته على ترشيد قرارات المستثمرين (دارسة ميدانية) *مجلة البحوث المالية والتجارية*، كلية التجارة – جامعة بورسعيد 23(3): 325-377.
- المجلس الأعلى للأمن السيبراني. 2017. *الاستراتيجية الوطنية للأمن السيبراني* 2017– 2021، رئاسة مجلس الوزراء، جمهورية مصر العربية: ص 1– 10
- دستور جمهورية مصر العربية .2014. *المادة 31.*
- شحاتة، شحاتة السيد. 2022. نحو دور فاعل للمراجع الداخلي في إدارة مخاطر الأمن السيبراني في الشركات المقيدة بالبورصة المصرية. *المجلة العلمية للدراسات والبحوث المالية والإدارية*، كلية التجارة – جامعة مدينة السادات 13(2): ص 26–37.
- علي، عبد الوهاب نصر. 2022. مهنة المحاسبة في مواجهة تداعيات التحول الرقمي في مصر: قصور الممارسة وحتمية التطوير. *المجلة العلمية للدراسات والبحوث المالية والإدارية*، كلية التجارة – جامعة مدينة السادات 13(2): ص 15–25.
- محروس، رمضان عارف رمضان، و أبو الحمد مصطفى صالح. 2022. استخدام المنهجية الرشيقة في تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني. *مجلة البحوث المالية والتجارية*، كلية التجارة – جامعة بورسعيد 23(3): ص 432–491.

المراجع الأجنبية:

- Abdelrahim, A., and H. A. N. Al-Malkawi. 2022. The influential factors of internal audit effectiveness: A conceptual model. *International Journal of Financial Studies 10*(3): 71.
- Alazzabi, W. Y. E., H., Mustafa, and A. I. Karage. 2023. Risk management, top management support, internal audit activities and fraud mitigation. *Journal of Financial Crime 30*(2): 569-582.
- Alina, C. M., S. E. Cerasela, and G. Gabriela. 2017. Internal audit role in cybersecurity. *Ovidius University Annals, Series Economic Sciences 17*(2): 510513.
- Al-Matari, O. M., I. M. Helal, S. A. Mazen, and S. Elhennawy. 2021. Integrated framework for cybersecurity auditing. *Information Security Journal: A Global Perspective 30*(4): 189-204.
- American Institute of Certified Public Accountants (AICPA). 2017. Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program. New York, NY: AICPA Assurance Services Executive Committee
- Annarelli, A., F. Nonino, and G. Palombi. 2020. Understanding the management of cyber resilient systems. *Computers & industrial engineering 149*: 106829.
- Badara, M. A. S., and S. Z. Saidin. 2013. The journey so far on internal audit effectiveness: A calling for expansion. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, *3*(3), 340-351.
- Behrend, J., and M. Eulerich. 2019. The evolution of internal audit research: a bibliometric analysis of published documents (1926–2016). *Accounting History Review 29*(1): 103-139.
- Betti, N., and G. Sarens. (2021). Understanding the internal audit function in a digitalised business environment. *Journal of Accounting & Organizational Change 17*(2): 197-216.
- Cadotte R., and T.J. Fogarty. 2021. Internal Auditor Responses to Cyberthreats: An Experiment. *Internal Auditing* 36 (6): 25-36.
- Carcello, J. V., M. Eulerich, A. Masli, and D. A. Wood. (2020). Are internal audits associated with reductions in perceived risk?. *Auditing: A Journal of Practice & Theory 39*(3): 55-73.

- Center for Internet Security (CIS). 2019. CIS controls. Version 7.1. *Available at: https://learn.cisecurity.org/cis-controls-download*
- Committee of Sponsoring Organizations of the Tredway Commission (COSO). 2004. Enterprise Risk Management—Integrated Framework. Washington, DC: COSO.
- Committee of Sponsoring Organizations of the Tredway Commission (COSO). 2017. Enterprise Risk Management: Integrating with Strategy and Performance. Washington, DC: COSO.
- Committee of Sponsoring Organizations of the Tredway Commission (COSO). 2019. Enterprise wide management (ERM) for Cybersecurity. Washington, DC: COSO.
- Dellai, H., and M. A. B. Omri. 2016. Factors affecting the internal audit effectiveness in Tunisian organizations. *Research Journal of Finance and Accounting 7*(16): 208-221.
- Deloitte. 2015. Global risk management survey, ninth edition. Available at: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/financial-services/ru-global-risk-management-survey-9th-edition.pdf
- Deloitte. 2017. Cybersecurity and the role of internal audit. An urgent call to action.
- Dittenhofer, M. 2001. Internal auditing effectiveness: an expansion of present methods. *Managerial auditing journal 16*(8): 443-450.
- Drašček, M., S. Slapničar, T. Vuko, and M. Čular. 2022. How Effective Is Your Cybersecurity Audit?. *ISACA Journal 3*: 1-6.
- Eaton, T. V., J. H. Grenier, and D. Layman. 2019. Accounting and cybersecurity risk management. *Current Issues in Auditing 13*(2): C1-C9.
- Erasmus, L., and P. Coetzee. 2018. Drivers of stakeholders' view of internal audit effectiveness: Management versus audit committee. *Managerial Auditing Journal 33*(1): 90-114.
- Eulerich, M., J. Henseler, and A. G. Köhler. 2017. The internal audit dilemma–the impact of executive directors versus audit committees on internal auditing work. *Managerial Auditing Journal 32*(9): 854-878.

- Eulerich, M., J. Kremin, and D. A. Wood. 2019. Factors that influence the perceived use of the internal audit function's work by executive management and audit committee. *Advances in accounting 45*:100410.
- Eulerich, M., and R. Lenz. 2019. Internal Auditing's Organization and Relationship to other Governance Functions. *Corporate Ownership & Control 16*(4): 84-102
- Eulerich, A. K., and M. Eulerich. 2020. What is the value of internal auditing?–A literature review on qualitative and quantitative perspectives. *A Literature Review on Qualitative and Quantitative Perspectives. Maandblad Voor Accountancy en Bedrijfseconomie 94*: 83-92.
- Gros, M., S. Koch, and C. Wallek. 2017. Internal audit function quality and financial reporting: results of a survey on German listed companies. *Journal of Management & Governance 21*: 291-329.
- Haislip, J., J. Lim, and R. Pinsker. 2017. Do the Roles of the CEO and CFO Differ When It Comes to Data Security Breaches? 23rd Americas Conference on Information Systems, Boston, MA, August 10–12.
- Hartmann, C. C., and J. Carmenate. 2021. Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches: Implications for practice, policy, and research. *Current Issues in Auditing 15*(2): A9-A23.
- Hepworth, L. R., C. Greenman, D. Esplin, and R. Johnston. 2022. Cybersecurity and Data Privacy: The Rising Expectations Within Internal Audit. *Journal of Forensic and Investigative Accounting 14*(3): 454- 465.
- Hussein, W. N., and A. M. Hilal. 2021. The Impact of Senior Management on Internal Audit Activities and its Reflection in Mitigating Financial Fraud–Field Study. *Journal of Positive Sciences (JPS) 8: 1-10.*

- ISACA. 2011. COBIT 5 Framework. *Rolling Meadows, IL: ISACA.*
- ISACA. 2012. *Securing Mobile Devices Using COBIT 5 for Information Security*. ISA*CA.*
- IT Governance Institute (ITGI). 2012. COBIT5: A Business Framework for the Governance and Management of Enterprise It. Rolling Meadows, IL: IT Governance Institute
- Institute of Internal Auditors (IIA), T. (2009). The role of internal auditing in enterprise-wide risk management. *IIA Position Paper, Institute of Internal Auditors* 1-8.
- Institute of Internal Auditors (IIA). (2013). The three lines of defense in effective risk management and control, ***Available at: https://www.theiia.org/***
- Institute of Internal Auditors (IIA). 2016. International Standards for the Professional Practice of Internal Auditing. Lake Mary, FL: IIA.
- Institute of Internal Auditing (IIA) .2017. International Standards for the Professional Practice of Internal Auditing. ***Available at: https://www.theiia.org/***
- Institute of Internal Auditors (IIA). (2020). The IIA's Three Lines Model—An Update of the Three Lines of Defense. Institute of Internal Auditors, Altamonte Springs.
- Institute of Internal Auditors. Global Knowledge Brief (IIA). (2022). Cybersecurity in 2022 Part 2 - Critical Partners — Internal Audit and the CIS. ***Available at: https://www.theiia.org/en/content/articles/global-knowledge-brief/2022/june/Cybersecurity-Part-2-Critical-Partners-Internal-Audit-and-the-CISO/***
- Islam, M. S., N. Farah, and T. S. Stafford. 2018. Factors associated with security/cybersecurity audit by internal audit function: An international study. Managerial Auditing Journal 33 (4): 377–409.

- Jamison, J., L. Morris, and C. Wilkinson. 2018. The future of cyber security in internal audit. ***Available at:*** *https://www.crowe.com/-/media/Crowe/LLP/folio-pdf/The-Future-of-Cybersecurity-in-IA-RISK-18000-002A-update.pdf*
- Janvrin, D. J., and T. Wang. 2022. Linking cybersecurity and accounting: An event, impact, response framework. *Accounting Horizons 36*(4): 67-112.
- Jiang, W., J. Legoria, K. J. Reichelt, and S. Walton. 2022. Firm use of cybersecurity risk disclosures. *Journal of Information Systems 36*(1): 151-180.
- Kahyaoglu, S. B., and K. Caliyurt. 2018. Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal 33*(4): 360-376.
- Kelton, A. S., and R. R. Pennington. 2020. Do voluntary disclosures mitigate the cybersecurity breach contagion effect? *Journal of Information Systems 34*(3): 133-157.
- Lankton, N., J. B. Price, and M. Karim. 2021. Cybersecurity breaches and the role of information technology governance in audit committee charters. *Journal of Information Systems 35*(1): 101-119.
- Lee, I. 2021. Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons 64*(5): 659-671.
- Lenz, R. 2013. Insights into the effectiveness of internal audit: a multi-method and multi-perspective study. *Available at: SSRN 2541580*.
- Lenz, R., G. Sarens, and K. D'Silva. 2014. Probing the discriminatory power of characteristics of internal audit functions: Sorting the wheat from the chaff. *International Journal of Auditing 18*(2): 126-138.
- Lenz, R., and U. Hahn. 2015. A synthesis of empirical internal audit effectiveness literature pointing to new research opportunities. *Managerial Auditing Journal* 30 (1): 5–33.
- Lenz, R. 2017. Time is ripe to revolutionize the audit. *EDPACS*: *56*(4), 19-22.

- Lenz, R., G. Sarens, and K. K. Jeppesen. 2018. In Search of a Measure of Effectiveness for Internal Audit Functions: An Institutional Perspective. *EDPACS* 58 (2): 1–36.
- Li, H., W. G. No, and J. E. Boritz. 2020. Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory 39*(1): 151-171.
- Lois, P., G. Drogalas, A. Karagiorgos, A. Thrassou, and D. Vrontis. 2021. Internal auditing and cyber security: audit role and procedural contribution. *International Journal of Managerial and Financial Accounting 13*(1): 25-47.
- Mihret, D. G., K., James, and J. M. Mula. (2010). Antecedents and organizational performance implications of internal audit effectiveness: some propositions and research agenda. *Pacific Accounting Review* 22(3): 224-252.
- National Association of Corporate Directors (NACD) .2020. Director's Handbook on Cyber-Risk Oversight. ***Available at:*** *Governance Resources | NACD (nacdonline.org)*
- Octavia, E. 2013. The effects of implementation on internal audit and good corporate governance in corporate performance. *Journal Of Global Business and Economics* 6(1): 77-87.
- Pacheco-Paredes, A., and C. M. Wheatley. 2022. Do Auditors Consider Cybersecurity Insurance in Pricing Audits?. ***Available at:*** *SSRN 4171153*.
- Public Company Accounting Oversight Board (PCAOB). 2020. Strategic plan 2020–2024. *available at: https://pcaobus.org/about/strategic-plan-budget/the-pcaob-2020-2024-strategic-plan*
- Roussy, M., and M. Brivot. 2016. Internal audit quality: a polysemous notion?. *Accounting, Auditing & Accountability Journal 29*(5): 714-738.

- Roussy, M., O. Barbe, and S. Raimbault. 2020. Internal audit: from effectiveness to organizational significance. *Managerial Auditing Journal 35*(2): 322-342.
- Ridley, J. 2008. *Cutting edge internal auditing*. West Sussex: John Wiley and Sons.
- Sarens, G., and I. De Beelde. 2006. The relationship between internal audit and senior management: A qualitative analysis of expectations and perceptions. *International Journal of Auditing 10*(3): 219-241.
- Saudi Arabian Monetary Authority. 2017. Cyber security framework. *Saudi Arabian Monetary Authority: Riyadh, Saudi Arabia*.
- Shamsuddin, A., M. A. Adam, S. A. Adnan, S. N. I. Madzlan, and Y. M. Yasin. 2018. the effectiveness of internal audit functions in managing cyber security in Malaysia's banking institutions. *International Journal of Industrial Management 4*: 61-69.
- Slapničar, S., T. Vuko, M. Čular, and M. Drašček. 2022. Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems 44*:100548.
- Soh, D. S., and N. Martinov-Bennie. (2011). The internal audit function: Perceptions of internal audit roles, effectiveness and evaluation. *Managerial auditing journal 26*(7): 605-622.
- Stafford, T., G. Deitz, and Y. Li. 2018. The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal 33*(4): 410-424.
- Steinbart, P. J., R. L. Raschke, G. Gal, and W. N. Dilla. 2013. Information security professionals' perceptions about the relationship between the information security and internal audit functions. Journal of Information Systems 27 (2): 65–86.

- Steinbart, P.J. Raschke, R. Gal, G., and Dilla, W. (2015), "The influence of internal audit on information security effectiveness: perceptions of internal auditors", *available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2685943*
- Steinbart, P. J., R. L. Raschke, G. Gal, and W. N. Dilla. 2018. The influence of a good relationship between the internal audit and information security functions on information security outcomes. Accounting, Organizations and Society 71: 15–29.
- Stine, K., S. Quinn, G. Witte, and R. K. Gardner. 2020. Integrating cybersecurity and enterprise risk management (ERM). *National Institute of Standards and Technology, 10*.
- Ta, T. T., and T. N. Doan. 2022. Factors affecting internal audit effectiveness: empirical evidence from Vietnam. *International journal of financial studies 10*(2): 1–14.
- Taber, K. S. 2018. The Use of Cronbach's Alpha when developing and reporting research instruments in science education. *Research in Science Education* 48(6): 1273–1296.
- Trotman, A. J., and K. R. Duncan. 2018. Internal audit quality: Insights from audit committee members, senior management, and internal auditors. *Auditing: A Journal of Practice & Theory 37*(4): 235-259.
- Turetken, O., S. Jethefer, and B. Ozkan. 2020. Internal audit effectiveness: operationalization and influencing factors. *Managerial Auditing Journal 35*(2): 238-271.
- Walton, S., P. R. Wheeler, Y. Zhang, and X. Zhao. 2021. An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems 35*(1): 155-186.