مجلة تنمية الرافدين

اسم المقال: دور إجراءات الرقابة الداخلية في مواجهة مخاطر الأمن السيبراني دراسة تحليلية
اسم الكاتب: حسن صالح يوسف، برهان حسين خلف
رابط ثابت: https://political-encyclopedia.org/index.php/library/10215
تاريخ الاسترداد: 2026/11/01 06:39 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة – Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة – Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة تنمية الرافدين كلية الإدارة والاقتصاد / جامعة الموصل ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

Research Paper

The Role of Internal Control Procedures in Confronting Cybersecurity Risks An analytical study

Hassan Saleh Yousif [1], Burhan Hussein Khalaf [2]

[1]Departmentof Accounting, College of Administration and Economics, University of Mosul, Mosul,Iraq.

[2]Department Operations Research and Intelligent Techniques, College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq.

Corresponding author: Burhan Hussein Khalaf
Burhan.h.k@uomosul.edu.iq

DOI: https://doi.org/10.33899/tanra.v44i147.49196

Article History: *Received*: 30/1/2025, *Revised*: 30/4/2025, *Accepted*:11/5/2025, *Published*: 1/9/2025.

Abstract

With the continuous increase in cyber threats and the rising frequency of cyberattacks, it has become imperative for organizations to enhance their regulatory measures in managing and mitigating cybersecurity risks while establishing an effective control system. This study aims to strengthen the role of the audit committee and its effective strategies in addressing cybersecurity risks, including risk assessment, evaluation of policies and procedures, and the use of protective technologies and techniques. A questionnaire was designed to cover both theoretical and practical aspects discussed in the theoretical framework, and a total of 75 questionnaires were distributed among specialists, academics, and professionals in the fields of auditing and cybersecurity. The study utilized the statistical software SPSS and SmartPLS 3.2.3 for data analysis and hypothesis testing. The findings underscore the importance of enhancing the audit committee's efficiency in addressing cyber threats, improving collaboration with IT departments, and leveraging advanced technologies, such as artificial intelligence, to strengthen the cybersecurity culture. The key recommendations of the study include conducting comprehensive and periodic assessments of cybersecurity risks faced by organizations, developing specialized training programs, increasing security awareness, and protecting institutional assets.

Keywords:
Security risks, cybersecurity, internal audit committee

Journal of
TANMIYAT AL-RAFIDAIN
(TANRA)
A scientific, quarterly, international, open access, and peer-reviewed journal

Vol. 44, No. 147
Sep. 2025

© University of Mosul | College of Administration and Economics, *Mosul, Iraq.*

TANRA retain the copyright of published articles, which is released under a "Creative Commons Attribution License for CC-BY-4.0" enabling the unrestricted use, distribution, and reproduction of an article in any medium, provided that the original work is properly cited.

Citation: Yousif, Hassan S. Khalaf, Burhan H., (2025). The Role of Internal Control Procedures in Confronting Cybersecurity Risks An analytical study. *TANMIYAT AL-RAFIDAIN, 44* (147), 267-295. https://doi.org/10.33899/tanra.v44i147.49196

P-ISSN: 1609-591X
e-ISSN: 2664-276X
tanmiyat.uomosul.edu.iq

ورقة بحثية

دور إجراءات الرقابة الداخلية في مواجهة مخاطر الأمن السيبراني دراسة تحليلية

حسن صالح يوسف[1] ، برهان حسين خلف[2]

[1] قسم المحاسبة، كلية الإدارة والاقتصاد، جامعة الموصل، الموصل، العراق.

[2] قسم بحوث العمليات والتقنيات الذكائية، كلية علوم الحاسوب والرياضيات، جامعة الموصل، الموصل، العراق.

المؤلف المراسل: برهان حسين خلف (Burhan.h.k@uomosul.edu.iq)

DOI: https://doi.org/10.33899/tanra.v44i147.49196

تاريخ المقالة: *الاستلام*: 2025/1/30، *التعديل والتنقيح*: 2025/4/30، *القبول*:2025/5/11، *النشر* : 2025/9/1.

المستخلص

في ظل التزايد المستمر للتهديدات السيبرانية، إذ يزداد عدد الهجمات الإلكترونية بشكل مستمر، من هنا أصبح من الضروري للمؤسسات تحسين إجراءاتها الرقابية في إدارة ومواجهة مخاطر الأمن السيبراني وتحقيق نظام رقابي فعال، يهدف البحث إلى تعزيز دور لجنة التدقيق واستراتيجياتها الفعالة في مواجهة مخاطر الأمن السيبراني ،(تقييم المخاطر, تقييم السياسات والإجراءات, التقنيات وأساليب الحماية), إذ تم تصميم استمارة استبيان لتغطية الجوانب النظرية والعملية التي تناولها الإطار النظري ، وتم توزيع (75) استبيانًا على عينة من المتخصصين والأكاديميين والعاملين في مجال التدقيق والأمن السيبراني. واستخدام البرنامج الإحصائي(SPSS) وبرنامج (Smart-PLS 23) لتحليل البيانات واختبار الفرضيات، وتوصل البحث إلى نتيجة وهي أهمية تعزيز كفاءة لجنة التدقيق في التعامل مع التهديدات السيبرانية، وتحسين التعاون مع وحدات تقنية المعلومات والتقنيات الحديثة مثل: الذكاء الاصطناعي، وتعزيز ثقافة الأمن السيبراني، أما أهم توصيات البحث فتمثلت بإجراء تقييم شامل ودوري للمخاطر السيبرانية التي تواجه المؤسسة وتطوير برامج تدريبية متخصصة، وتعزيز الوعي الأمني وحماية الأصول المؤسسية .

الكلمات المفتاحية:

المخاطر الأمنية، الأمن السيبراني ، التدقيق الداخلي

مجلة

تنمية الرافدين

(TANRA): **مجلة علمية، فصلية، دولية، مفتوحة الوصول، محكمة.**

المجلد (44)، العدد (147)، ايلول 2025

© جامعة الموصل |

كلية الإدارة والاقتصاد، *الموصل، العراق.*

تحتفظ (**TANRA**) بحقوق الطبع والنشر للمقالات المنشورة، والتي يتم إصدارها بموجب ترخيص (Creative Commons Attribution)لـ (CC-BY-4.0) الذي يتيح الاستخدام، والتوزيع، والاستنساخ غير المقيد وتوزيع للمقالة في أي وسيط نقل، بشرط اقتباس العمل الأصلي بشكل صحيح.

الاقتباس: خلف، برهان حسين، يوسف، حسن صالح، (2025). دور إجراءات الرقابة الداخلية في مواجهة مخاطر الأمن السيبراني دراسة تحليلية. *تنمية الرافدين*،43 (144)، 267-295.
https://doi.org/10.33899/tanra.v44i147.49196

P-ISSN: 1609-591X
e-ISSN: 2664-276X
tanmiyat.uomosul.edu.iq

1. **المقدمة**

يشهد العصر الحالي تزايدًا مستمرًا في التطور التكنولوجي والأنظمة الرقمية، إذ تعيش المؤسسات اليوم في بيئة رقمية ديناميكية تفرض عليها مواكبة التطور التكنولوجي، ومع هذا التحول الرقمي يتزايد التهديد السيبراني بشكل مستمر. ويصبح الأمان السيبراني أحد التحديات الحيوية التي تواجه المؤسسات، إذ تؤدي لجنة التدقيق دورًا حيويًا في تفعيل الرقابة والتحوط للمخاطر السيبرانية في الشركات، ومع ذلك تتزايد التحديات المتعلقة بالأمن والمخاطر ووفقاً للتقارير عن الأمن السيبراني أكثر من ٢٠٪ من الشركات التي تتعرض لاختراق سيبراني تواجه خسارة كبيرة في الإيرادات، وانخفاض في قاعدة عملائهم، وخسارة فرص الأعمال؛ بتكاليف احتمالية تبلغ حوالي ١٧ مليون دولار، لذا تصنع الشركات أنظمة رقابة داخلية لتقديم تأكيدات معقولة لبلوغ الأهداف المتعلقة والكفاءة التشغيلية والفعالية والتقارير المالية الموثوقة، والامتثال للقانون واللوائح (Farid, 2022,433) .وهذا يتطلب التعامل مع هذه التحديات فهمًا دقيقًا للتهديدات السيبرانية والاستعداد الفعّال للرد عليها. نظراً لما للجنة التدقيق من مكانة مهمة من خلال الأدوار الاستشارية والتوكيدية عن أنشطة الشركات والمؤسسات، والقيام بفحص السياسات الأمنية، وتقييم البرامج الوقائية، وتحليل تأثير التهديدات المحتملة على الأنظمة والبيانات.

المبحث الأول : منهجية البحث

أولاً: مشكلة البحث :

مع تصاعد الاعتماد على التكنولوجيا والتحول الرقمي في مختلف القطاعات، أصبحت المؤسسات عرضة لمخاطر متزايدة ، مثل: الاختراقات، تسريب البيانات، وهجمات الفدية. وعلى الرغم من التطورات التقنية الكبيرة في مجال حماية الأنظمة، إلا أن فعالية مواجهة تلك المخاطر لا تعتمد فقط على الأدوات التقنية، بل تعتمد بشكل كبير على وجود إجراءات رقابة داخلية فعّالة وشاملة، ولكون الرقابة الداخلية تمثل سياسات وإجراءات مصممة لضمان سلامة العمليات وتحقيق أهداف المؤسسة، وتؤدي الرقابة الداخلية دورًا مهماً في التحوط لتلك المخاطر السيبرانية.

وعليه، التساؤل هو مدى فعالية إجراءات الرقابة الداخلية في الحد من مخاطر الأمن السيبراني، يتفرع عن هذا التساؤل الرئيس عدداً من الأسئلة الفرعية:

1. هل لتفعيل دور التدقيق الداخلي تأثير معنوي في مواجهة مخاطر الأمن السيبراني؟
2. إلى أي مدى تسهم السياسات والإجراءات للرقابة في تعزيز الأمن السيبراني؟
3. هل لتحسين الإجراءات الرقابية الداخلية تأثير معنوي في التصدي للمخاطر السيبرانية؟

ثانيا: أهمية البحث

تأتي أهمية البحث من خلال دور لجان التدقيق بوصفها حارساً للشفافية المالية، ومسؤولة عن ضمان التزام الشركات بالمبادئ والممارسات المحاسبية السليمة والحماية أيضًا من أي مخاطر محتملة والحفاظ على نزاهة وموثوقية التقارير المالية للشركة، حيث بدأت لجان التدقيق في إيلاء المزيد من الاهتمام

لممارسات أمن البيانات والخصوصية خروقات البيانات والهجمات الإلكترونية، وإجراء تقييم شامل للمخاطر. تفعيل وبناء أنظمة رقابية كفوءة وفعالة في مواجهة التحديات ومخاطر الاختراق, حيث ذكر في تقرير (Center for Audit Quality, & Deloitte. (2022 بعنوان ممارسات لجنة التدقيق الصادر في شهر مارس 2024 , أُجري استطلاع حول أولويات لجنة التدقيق والتحديات وفعالية اللجنة ، إذ أكد أنّ من أولويات لجنة التدقيق المخاطر السيبرانية والمخاطر المؤسسية , وأشار معظم المستجيبين (69%) إلى أن الأمن السيبراني سيكون من بين المجالات الثلاثة ذات الأولوية القصوى للجنة التدقيق. وتفعيل دور أكبر من خلال دورها التوكيدي والاستشاري ، وتعزيز الجهود المبذولة من قبل لجنة التدقيق الداخلي لتحسين الاستعداد والمواجهة الآنية للتحديات السيبرانية.

ثالثا: أهداف البحث :

1. تعزيز دور لجنة التدقيق الداخلي في ظل الأمن السيبراني.
2. تحسين فعالية الرقابة الحالية والتحوط للمخاطر السيبرانية.
3. تقييم التأثير الفعّال للجنة التدقيق على أنظمة الرقابة وتحقيق الأمان السيبراني.
4. تعزيز الوعي الأمني للجنة التدقيق والتحوط لمخاطر التقنية.

رابعاً : فرضية البحث : من خلال مشكلة البحث وأهميته وأهدافه تم صياغة الفرضيات ، وكما يأتي :

أ. الفرضية الأولى والتي تنص على:((لا يوجد تأثير معنوي إحصائياً لاستراتيجيات تفعيل دور لجنة التدقيق الداخلي في مواجهة مخاطر الأمن السيبراني))

ب. الفرضية الثانية والتي تنص على:((لا يوجد تأثير معنوي إحصائياً لتقييم المخاطر في مواجهة مخاطر الأمن السيبراني))

ج. الفرضية الثالثة والتي تنص على:((لا يوجد تأثير معنوي إحصائياً لتقييم السياسات والإجراءات في مواجهة مخاطر الأمن السيبراني))

د. الفرضية الرابعة والتي تنص على:((لا يوجد تأثير معنوي إحصائياً لتحسين الإجراءات الرقابية في مواجهة مخاطر الأمن السيبراني))

هـ. الفرضية الخامسة والتي تنص على:((لا يوجد تأثير معنوي إحصائياً لاستخدام التقنيات وأساليب الحماية في مواجهة مخاطر الأمن السيبراني))

خامساً: أساليب جمع البيانات:

- الجانب النظري: تم إغناء البحث في الجانب النظري على أهم إسهامات الباحثين والكتاب والأكاديميين التي تم جمعها عن طريق المجلات العلمية العالمية الأجنبية والعربية من خلال أحدث مصادر المجلات الأجنبية والعربية.

- أما الجانب التطبيقي: فقد اعتمد الباحثون على تصميم استمارة الاستبيان لتغطي الجوانب الذي تناوله الإطار النظري والفرضيات ، إذ تم توزيع استبيان عدد(75) على عينة من الأكاديميين والمتخصصين في مجال التدقيق والحسابات والمبرمجين. وتم استخدام البرنامج الإحصائي (SPSS) لاختبار الفرضيات وبرنامج (Smart-PLS 23).

سادساً : الدراسات السابقة:

دراسة (متولي وآخرون,2022) هدفت الدراسة إلى بيان كيفية تسبب جائحة (كوفيد−19) في إثارة العديد من المخاوف بشأن الرقابة الداخلية لشركات التأمين ومواجهة الاحتيال. حيث فرضت الجائحة تحولًا كبيرًا نحو التحول الرقمي، أدى هذا التغيير إلى زيادة مخاطر الهجمات الإلكترونية، أجريت الدراسة على مسؤولي وحدات مخاطر الأمن والمراجعين الداخليين ، وأوصت الدراسةب بعض الحلول التي من شأنها أن تساعد المراجعين الداخليين في التغلب على مخاطر الإنترنت والاحتيال . من خلال شرح المخاطر المتزامنة واقتراح الحلول المحتملة، يتعين على مديري المخاطر والمدققين الداخليين صياغة استراتيجية واضحة للتعامل مع مخاطر الاحتيال والأمن الإلكتروني . وتطرقت دراسة (Lankton, et, al 2021) إلى أن استخدم "الكفاءة والنظريات المؤسسية للتحقيق في تأثير الانتهاكات الأمنية واللجان التقنية على مستوى مجلس الإدارة في الكشف عن أدوار في ميثاق (ITG) مجموعة التقنيات المتكاملة للجنة المراجعة. وتمثلت عينة الدراسة في (١٨٩) شركة. وتشير نتائج الدراسة إلى أن الشركات التي لديها لجنة تكنولوجيا وخرق بيانات من المحتمل أن تكشف أكثر عن أدوار في ميثاق مجموعة التقنيات المتكاملة للجنة المراجعة ، وهذا يشير إلى أن الشركات التي تتعرض لخرق البيانات تدرك مدى ضعفها، ومن خلال الإشراف بالفعل على مستوى مجلس الإدارة يكون من الطبيعي بالنسبة لها زيادة الإشراف من خلال تعيين أدوار للجنة المراجعة في ميثاق التقنيات المتكاملة لهذه اللجنة . وأكدت الدراسة على أن الشركات التي لديها لجان تكنولوجيا وخرق بيانات يكون لديها قدرة أكبر على مواجهة هذه المخاطر ، أما دراسة (Al-Zyoud, Mahmoud, 2021) فهدفت إلى التعرف على أثر التدقيق الداخلي المتمثل بـ (كفاءة التدقيق الداخلي، وحيادية التدقيق الداخلي، والمركز التنظيمي للتدقيق الداخلي، وتخطيط التدقيق الداخلي) في الحد من المخاطر السيبرانية في البنوك التجارية الأردنية. إذ خلصت الدراسة إلى عدم وجود أثر لحيادية التدقيق الداخلي في الحد من المخاطر السيبرانية في البنوك. وأوصت الدراسة بضرورة زيادة مستوى الوعي والمسؤولية اتجاه المخاطر السيبرانية وأثرها على أدائها. وحثت إدارة البنوك على رفع مستوى الوعي بأهمية أثر الحد من المخاطر السيبرانية. وجاء في دراسة (atiyah, 2021, 9) أنّ نجاح مراجعة الأمن السيبراني يتوقف على مساهمات كل من إدارة المنظمة، وإدارة المخاطر، والمراجعة الداخلية. وأكدت الدراسة أن مسؤوليات المراجعة الداخلية في مراجعة الضوابط الرقابية والتحقق من الالتزام بها، ومراجعة إدارة المخاطر، وتحديثات الأمن السيبراني، وردود الأفعال على الانتهاكات السيبرانية. أما دراسة Musaib et al,(2020) فسعت الدراسة إلى فحص ومعرفة ما إذا كانت خبرة لجان المراجعة في مجال تكنولوجيا المعلومات تؤثر

على موثوقية التقارير المالية وحسن توقيتها من عدمه. وتمثلت عينة الدراسة في عدد من الشركات التي تمتلك تكنولوجيا معلومات عالية الجودة ، وأشارت الدراسة إلى خبرة لجان المراجعة في مجال تكنولوجيا المعلومات وتوفير قدر كبير من الثقة على التقارير المالية ، وتوصلت النتائج إلى وجود تقليص في احتمالية نقاط الضعف المادية المتعلقة بتكنولوجيا المعلومات والتي تمثل ٥٥% من جميع نقاط الضعف المبلغ عنها لدى الشركات، وكذلك إعلانات الأرباح في الوقت المناسب في الشركات التي لديها خبرة في مجال تكنولوجيا المعلومات . وسعت دراسة Islam et al , (2018) إلى تحديد العوامل المؤثرة في الأمن السيبراني والتي تكون على علاقة بالتدقيق الداخلية ، ومن خلال استطلاع رأي (97) مراجع داخلي في (166) دولة، وتوصلت الدراسة إلى أن قيام المدققين الداخليين بالتقييم الشامل للمخاطر له تأثير إيجابي كبير في مراجعة الأمن السيبراني، كما أن كفاءة المدققين الداخليين تؤثر أيضا في مراجعة الأمن السيبراني. وأثر فعالية التدقيق الداخلي في إدارة الأمن السيبراني في البنوك .

إن أهم ما يميز هذه الدراسة :

1. عرض استراتيجيات واضحة لتفعيل لجنة التدقيق الداخلي، بدلاً من الاكتفاء بتحليل تأثير التدقيق الداخلي.
2. اعتمدت الدراسات السابقة على عينات مختلفة، مثل : الشركات المتأثرة بالاختراقات الأمنية أو مراجعي البنوك، دون تركيز خاص على المختصين في التدقيق والأمن السيبراني معاً .
3. التركيز على التعاون بين لجنة التدقيق الداخلي ووحدات تقنية المعلومات، ولاسيما فيما يتعلق باستخدام الذكاء الاصطناعي لتعزيز الأمن السيبراني .
4. تقديم عملي يشمل تقييم المخاطر، تقييم السياسات والإجراءات، التقنيات وأساليب الحماية وهو إطار شامل أكثر مما قدمته الدراسات السابقة.
5. استخدام أدوات تحليل متقدمة(SPSS) و (Smart–PLS 23)لاختبار الفرضيات بشكل إحصائي دقيق، مما يمنح الدراسة قوة تحليلية أعلى.
6. شملت الدراسة 75 متخصصًا وأكاديمياً وعاملين في التدقيق والأمن السيبراني، مما يوفر توازناً بين الجانب الأكاديمي والعملي.

المبحث الثاني : الإطار النظري

2–1 مفهوم الأمن السيبراني:

لقد جعل الإنترنت العالم أصغر من نواحي عديدة، لكنه فتح لنا تأثيرات لم تكن من قبل بهذا التنوع والتحدي. ومع نمو الأمن على نحو متسارع، نما عامل القرصنة بشكل أسرع. والأمن السيبراني هو عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية. تهدف الوصول للمعلومات السرية لتدميرها؛

والاستيلاء عليها، وتكون هذه الهجمات السيبرانية عادة على أموال المستخدمين أو مقاطعة عمليات الأعمال العادية(Saeed & Asaad, 2022).

يركز الأمن السيبراني Cyber security على تصميم وتطبيق التقنيات والضوابط والممارسات اللازمة لحماية الأنظمة والبرامج وشبكات الحواسيب والبيانات من التعرض للفيروسات والبرامج الإلكترونية الخبيثة وسد ثغرات نقاط الضعف ،ويعبر مفهوم الأمن السيبراني لأنظمة المحاسبة عن درجة الحماية والتأمين للعمليات المحاسبية من خلال توفير تقنيات وبرمجيات لتأمين الخصوصية ومنع الاختراق السيبراني الداخلي والخارجي للبيانات والأجهزة والبرمجيات ، بما يؤثر على تحقيق أهدافها واستمراريتها، وتزيد هذه المخاطر نتيجة توسع المنشآت في استخدام تكنولوجيا المعلومات، وارتفاع تكاليف معالجة آثار الهجمات الإلكترونية والخسائر المالية، والأضرار بالسمعة. (Othman, 2023)

إن مفهوم الأمن السيبراني يمثل أحد أهم التحديات التي تواجه كافة الدول نتيجة التطور الرقمي والتكنولوجي المتسارع ، الأمر الذي يستدعي تحسين منظومة الأمن السيبراني بما يحقق الحفاظ على سرية المعلومات وحمايتها من أي تهديد ، وتحسين الضوابط والحماية الأمنية واتخاذ التدابير المناسبة والفعالة لمواجهة التهديدات وعمليات القرصنة (Farid, Hanan, 2022).

وأشارت حوادث الأمن السيبراني إلى إخفاقات محتملة فيما يتعلق بالرقابة الداخلية على التقارير المالية، فالمدقق الخارجي مسؤول قانوناً عن اكتشاف أوجه القصور في الرقابة الداخلية، ونظراً للاستخدام المتزايد لتكنولوجيا المعلومات في إعداد التقارير المالية وكذلك للأنشطة التجارية الأخرى، والطبيعة المترابطة المتزايدة لأنظمة تكنولوجيا المعلومات التجارية الحديثة على طول سلسلة القيمة، فإن المدقق مطالب عمليا بتوسيع عمليات التدقيق ليشمل أنظمة أخرى يمكن استغلالها من أجل الوصول غير المصرح به، وذلك بغض النظر عمّا إذا كان النظام مرتبطا بشكل مباشر بالتقارير المالية والمحاسبة، فحتى إذا لم يكن للهجمات الإلكترونية تأثير مباشر على أنظمة المحاسبة في الشركة، فقد يحتاج المدقق إلى بذل جهد إضافي لاكتشاف نقاط ضعف في الضوابط العامة لتكنولوجيا المعلومات(Metwally, Gharib, 2022).

وهناك خمس خطوات يمكن من خلالها الحفاظ على برنامج فعال لإدارة للمخاطر السيبرانية : وتشمل هذه الخطوات ، تحديد المخاطر الإلكترونية ، تصميم وتفعيل هيكل رقابة للأمن السيبراني، واختبار الفعالية التشغيلية لضوابط رقابة الأمن السيبراني، وإعداد التقارير عن إدارة المخاطر السيبرانية والتأكيد من مراقب الحسابات على تقرير إدارة مخاطر الأمنية (Eaton et al،2019) .

2-2 أهمية تدقيق الأمن السيبراني :

على الرغم من أن المخاطر الأمنية التي تواجه المؤسسات قد ازدادت بشكل متسارع، إلا أن هناك نقصاً في البحث الذي استكشف مختلف أنواع أمان أنظمة المعلومات (IS)، ولاسيما فيما يتعلق بطبيعة ونطاق تنفيذيات الأمان للنظام. وهناك أيضًا تفهم محدود لكيفية إدارة المؤسسات للعديد من أبعاد أمان أنظمة المعلومات والمشكلات المحتملة المرتبطة بها، وتعد عمليات تدقيق الأمان السيبراني بُعدًا جديدًا في

ممارسات الأمان، يُعنى بدعم حماية الأصول المعلوماتية الحيوية للشركة. يهدف عملية التدقيق إلى الحصول على أدلة على سياسات الأمان التنظيمية وفعاليتها في حماية سلامة الأصول، وسرية البيانات، وإمكانية الوصول ، وبشكل أساسي، يُستخدم التدقيق لتقييم فعالية قدرة المؤسسة على حماية أصولها. وإدارة أمان أنظمة المعلومات أصبحت أمراً أكثر أهمية للشركات نظراً لتزايد اعتمادها على التكنولوجيا لإجراء الأعمال.(Islam,& Farah,et al,2018) .

لقد تطورت وظيفة التدقيق الداخلي وازدادت أهميتها نتيجة للدور الذي تؤديه داخل المنظمة بوصفها أداة فعالة مهمتها فحص وتقييم كفاءة وفعالية أدوات الرقابة الأخرى، كما يتم الاعتماد عليها بوصفها وظيفة استشارية تعمل على تحسين إدارة المخاطر .(Babiker, I. 2025)

لذا تستخدم شركات تدقيق الحسابات العامة أفراداً حاصلين على شهادة محاسب قانوني معتمد (CPA)، فضلاً عن مؤهلات متنوعة أخرى ذات صلة بتكنولوجيا المعلومات والأمان. ، يُتوقع أن يكون وجود فريق تدقيق داخلي يضم رؤساء تنفيذيين معتمدين (CAEs) حاصلين على شهادة محاسب قانوني معتمد أو شهادة محاسب داخلي معتمد (CIA)، والذين يمتلكون التدريب المناسب في مجال الأمان، مرتبطًا بشكل إيجابي وبشكل كبير مع أداء ممتاز في مجال التدقيق الخاص بالأمان والسيبراني (The Institute of Internal Auditors, 2017).

كما يعد الأمن السيبراني جزءاً مهماً للأفراد والمنظمات والحكومات والمؤسسات التعليمية، إذ أصبح من الضرورة للعائلات حماية أفراد الأسرة من الاحتيال عبر الإنترنت ومن الناحية المالية ضرورة تأمين المعلومات المالية التي يمكن أن تؤثر على الوضع المالي الشخصي، وهناك حاجة حيوية لمستخدمي الإنترنت لفهم كيفية حماية أنفسهم من الاحتيال عبر الإنترنت وسرقة الهوية ، ويؤدي التعلم المناسب عن السلوك عبر الإنترنت وحماية النظام إلى تقليل نقاط الضعف وجعل بيئة الإنترنت أكثر أماناً .(Al-Barzanji, Al-Saqqa, 2023)

تؤدي وظيفة التدقيق الداخلي الحديثة (Internal Audit Function (IAF دورا حيوياً في تحسين عمليات المنشآت، سواء الهادفة أو غير الهادفة لتحقيق الأرباح، فضلا عن اعتبارها بمثابة أحد الركائز الأساسية لحوكمة الشركات، جنبا إلى جنب مع لجنة المراجعة والإدارة، وكونها متطلبا ضروريا لتقييم مختلف الجوانب الرقابية بهذه المنشآت بما يمكنها من تحسين عملياتها وإدارة مخاطرها، ومن ثم إضفاء المصداقية والشفافية على ما توصله قوائمها المالية من معلومات (Shehata, 2020).

أما المخاطر السيبرانية فقد عرفتها الاستراتيجية الوطنية للأمن السيبراني في العراق بأنها احتمال وجود تهديد وهشاشة داخل الفضاء الإلكتروني للبلد يضر بأمن نظم المعلومات وهياكل البنى التحتية المعلوماتية الأساسية من خلال التهديدات السيبرانية والثغرات الموجود في الفضاءات السحابية (Iraqi Cybersecurity Strategy, 2020).

وأشارت دراسة (Steinbart et al. 2012) إلى أن مستوى معرفة مدققي تكنولوجيا المعلومات، وموقفهم تجاه التعاون مع متخصصي الأمان، والدعم من الإدارة العليا، والباحثين على العلاقة بين محترفي أمان المعلومات ومدققي الأمان الداخليين، حيث وجدوا، ووجود علاقة جيدة وتنسيق فعال بينهم يعزز فعالية أمان المعلومات مرتبطة إيجابيًا بالكشف عن حوادث الأمان.

والطرائق التي يقوم بها المدققون الداخليون لضمانات السيبرانية هي من خلال استفادتهم من استقلاليتهم، أنّ العديد من الموظفين الذين يعملون في مجالات تكنولوجيا المعلومات والأمان، قد يجدون صعوبة في تقديم الضمانات المستقلة والموضوعية التي يتطلع إليها أعضاء مجلس الإدارة في مجال السيبرانية. بالمقابل، يحتفظ المدققون الداخليون باستقلاليتهم، حيث يستمدون قيمة وموثوقية الخدمات التي يقدمونها من المبادئ الأساسية هو معترف بها في الأطُر والمعايير العالمية، التي وضعها معهد المدققين الداخليين (Nikola Simic,2022) .

2-3 تفعيل الدور الرقابي للتدقيق في مواجهة المخاطر الأمن السيبراني.

لقد زاد اهتمام الشركات في السنوات الأخيرة، بالدور الذي يمكن تؤديه وظيفة التدقيق الداخلي بوصفها أحد 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 من خلال قدرتها على توفير استشارات وتأكيدات مستقلة وموضوعية حول كفاية وفعالية إدارة المخاطر ودراسة وتحليل فعالية التدقيق الداخلي في مجال إدارة مخاطر بما يعزز التحسين المستمر. (Hanan, 2024).

وتلعب وظيفة التدقيق دورا مهما في إدارة مخاطر الأمن السيبراني على اعتبار أنها من المخاطر الناشئة، وهي الخطر الذي يؤدي الى خسائر مالية فادحة، فضلا عن مخاطر السمعة والمخاطر التشغيلية، من خلال بناء إدارة فاعلة لمخاطر الأمن السيبراني ، ويتم ذلك من خدمات التوكيد وخدمات الاستشارية في مجالات تكنولوجيا المعلومة، إذ تؤدي خدمات التوكيد المقدمة من قبل مدقق الحسابات بوصفها خدمات أخرى دورا في توكيد فاعلية البرنامج المعتمد في إدارة مخاطر الأمن السيبراني في الوحدة الاقتصادية فضلا عن الإفصاح الطوعي أو الإلزامي عن مخاطر الأمن السيبراني، حيث بين المعهد الأمريكي للمحاسبين القانونيين AICPA وتقرير لجنة تبادل الأوراق المالية في البورصة ، فإن مخاطر السيبرانية تشكل أحد المخاطر المستحدثة في البيئة العالمية والمحلية (Ibtihaj et al., 2022).

ذكرت دراسة (Almaleeh2019) أن التغيرات المتسارعة في بيئة الأعمال والممارسة المهنية للمحاسبة، تطلب مواكبة وظيفة التدقيق الداخلي لتلك التغيرات من خلال قدرتها على القيام بدوريها الاستشاري الذى يستهدف تقديم المشورة والنصح والإرشاد لمجالس إدارات الشركات ، والتوكيدي الذي يستهدف تحسين جودة ومحتوى المعلومات المفصح عنها بالتقارير الداخلية لخدمة متخذي القرارات بصفة عامة، ومجلس الإدارة بصفة خاصة.

وهناك عدة إجراءات ووسائل يتطلب اتخاذها واستخدامها ضمن الرقابة الداخلية لمواجهة مخاطر الأمن السيبراني ومن بين هذه الإجراءات (Mansour, 2021).

أ- تحديد المخاطر الأمنية السيبرانية التي تواجه المؤسسة وتحديد الأصول الحيوية التي يجب حمايتها.

ب- يجب وضع سياسات وإجراءات الأمن السيبراني وتحديثها بشكل دوري لتوفير الحماية اللازمة للأصول الحيوية.

ت- تدريب الموظفين على كيفية التعامل مع المخاطر الأمنية السيبرانية وتوعيتهم بأهمية الأمن السيبراني.

ث- تنفيذ التدقيق الأمني السيبراني بشكل دوري لتحديد الثغرات الأمنية وتصحيحها.

ج- استخدام التقنيات الحديثة مثل: الذكاء الاصطناعي، وتحليل البيانات لتحسين الأمن السيبراني.

ح- التعاون مع الجهات الحكومية المختصة في مجال الأمن السيبراني لتحسين الأمن السيبراني وتبادل المعلومات الأمنية.

تعد وظيفة التدقيق الداخلية أحد الركائز الأساسية لتلبية احتياجات مختلف أصحاب المصالح ، ولا سيما المساهمين والإدارة، إذ تعمل المراجعة الداخلية على إعداد تقرير عن مدى فعالية هيكل الرقابة الداخلية (Shehata, 2022)).وتعمل جودة المراجعة الداخلية على تمكين إدارات المنشآت من تصميم خطوط دفاع قوية لمواجهة مخاطر لطبيعة واحتياج البيئة التكنولوجية ونوعية وكثافة المخاطر من السيبراني ، وتتمثل في الآتي: (Ameerhum, 2020)

- تقييم النضج السيبراني: يتمثل في تحديد الفجوات في الواقع الحالي للأمن وفهم محددات وأبعاد نقاط الضعف المطلوب التركيز عليها .
- مراجعة التكنولوجيا الجديدة : حيث تقدم منصات التكنولوجيا الناشئة والتي تضم (السحابة والشبكات الاجتماعية والجوال والبيانات الضخمة وأنظمة الذكاء الاصطناعي وغيرها) ومراجعة عنصر الأمان قبل وبعد تنفيذ التكنولوجيا الجديدة.
- مراجعة التكنولوجيا العميقة : قيام المراجعة الداخلية بتقييم المخاطر الأمنية المتعلقة بأنظمة التكنولوجيا المتطورة مع التأكيد على الفهم الشامل للمخاطر الأمنية.

4-2 أهم الجهود المحلية والدولية للتصدي لتحديات المخاطر السيبرانية

إن التقدم والتطور التكنولوجي في العديد من المجالات مثل : الخدمات المصرفية عبر الإنترنت والتسوق. أدى إلى أن يكون المجال الرقمي عاملًا مهمًا في العالم، وأثبتت تكنولوجيا المعلومات والاتصالات أنها عامل حيوي للغاية في الإنتاجية والنمو والابتكار، وشهد العالم تقدمًا تكنولوجيًا كبيرًا، وأثر هذا التطور أيضًا على ممارسات المحاسبة (Ojeka, et al. 2017)

لجنة التدقيق وتعد آلية لحوكمة الشركات، كما أن فعاليتها في عمليات التقارير المالية تعد مصدر قلق للرقابيين والمستثمرين. وتمثل القضايا الكبيرة المتعلقة بالاحتيال، مثل: حالات إنرون وورلد كوم في السنوات السابقة، مصدراً لفقدان الثقة من قبل المستثمرين في التقارير المالية وأنشطة الشركات وعلى مر السنوات الأخيرة، تم توجيه انتقادات كبيرة للجنة التدقيق بسبب عدم كفايتها في ضمان استقلال المدققين الخارجيين لإصدار تقارير مالية فعّالة ، نتيجةً لتلك الانتقادات، زادت الرقابة على أنشطة اللجنة. وفقًا للكود الخاص بحوكمة الشركات للبنوك في نيجيريا، يُطلب من أعضاء لجنة التدقيق أن يكون لديهم معرفة مالية ومحاسبية وأن يكونوا ذوي درجة عالية من الاستقلال. (Ojeka, et al. 2017)

قدم المعهد الأمريكي للمحاسبين القانونيين AICPA في أبريل 2017 إطارا لإعداد تقرير إدارة مخاطر الأمن السيبراني (ضوابط النظام والمنظمة) لإرشاد الشركات ودعمها في الإفصاح الاختياري عن مخاطر الأمن السيبراني، وذلك من خلال تمكين الشركات من تبني نهج لإدارة مخاطر الأمن السيبراني، والتقرير عنها وتوصيل تلك الأنشطة ونتائجها إلى أصحاب المصالح. ولدعم الإطار تم إصدار مجموعتين من المعايير لوصف أهداف عمليات وضوابط الأمن السيبراني الفعالة التي يجب على الشركات تصميمها وتنفيذها للحصول على برنامج قوي وفعال لإدارة مخاطر الأمن السيبراني.

2-5 <u>مدخل مفاهيمي عن لجنة التدقيق الداخلي :</u>

تعد لجان التدقيق (Audit Committee) من المفاهيم الحديثة التي تحظى باهتمام العديد من الدول مثل : الولايات المتحدة الأمريكية، وكندا، والمملكة المتحدة، وأستراليا وغيرها من الدول، كما توصي العديد من المنظمات المهنية بتكوينها نظراً للدور الذي تقوم به في مراقبة عمليات التقرير المالي والإفصاح لحملة الأسهم والتأكد من مصداقيتها، وكذلك في تدعيم استقلال عملية التدقيق، الأمر الذي حدّ ببعض الدول إلى إصدار التشريعات الملزمة لوجودها داخل شركات المساهمة ، ومن جهة أخرى ، فإنّ لجنة التدقيق تسهم في دعم كفاءة الرقابة الداخلية التي تعتبر العمود الفقري للشركات الكبرى ، وذلك من خدمة حماية الموجودات التي يقدمها للشركة والحفاظ على المعلومات المتنوعة من التلاعب ، لاسيما الحفاظ على تحقيق الخطط المستقبلية المرسومة, وتعد العلاقة التكاملية بين التدقيق الداخلي ولجنة التدقيق من الأدوات الرقابية التي تعملان سوية بوصفهما أداة رقابية تعمل على رفع وتحسين أنظمة الرقابة الداخلية وتقوي دعامة هيكل الرقابة الداخلية، لأجل الحد من الاحتيال المحاسبي وتخفيض المخاطر وإداراتها بشكل ملائم. وهي لجنة منتخبة من مجلس الإدارة لأعضاء غير تنفيذيين لهم الخبرة المالية والمحاسبية ، تهدف إلى الأشراف على السياسات المحاسبية والتقارير والالتزام بالتعليمات وحماية المساهمين من حالات الاحتيال في القوائم المالية ، وزيادة فاعلية الرقابة الداخلية .(Badolato, Donelson, & Ege, 2014)

عرفت الهيئة الكندية للمحاسبين القانويين (1992) the canadien institue of chartered accountants (CICA لجان التدقيق بأنها " لجان مكونة من مديري الشركة الذين ترتكز مسؤولياتهم في تدقيق القوائم المالية السنوية قبل تسليمها إلى مجلس الإدارة، وتعد لجان التدقيق حلقة وصل بين المدققين

ومجلس الإدارة وتتلخص نشاطاتها في نطاق ونتائج التدقيق، وكذلك الرقابة الداخلية للشركة وجميع المعلومات المالية المعدة. (Abdullah, 2015)

إنّ لجان التدقيق لابد من أن تمتلك المؤهلات والخبرات الكافية في اتخاذ القرارات المالية ودعم التقارير المالية وتحقيق إفصاح عن كافة العمليات الجارية بصورة أكثر شفافية واستقلالية ودعم قواعد الحوكمة وإدارة المخاطر الحالية والمستقبلية ، لذا من مهمات لجان التدقيق التي تساعد بها مجلس الإدارة والمدقق الداخلي والمدقق الخارجي بناء أنظمة رقابية فعالة..

2-6 دور لجنة التدقيق في دعم التدقيق الداخلي:

يعد المدقق الخارجي عاملاً مهماً يمنح الطمأنينة للمساهمين حول التأكد من صدق تمثيل القوائم المالية للبيانات المالية وخلوها من الأخطاء الجوهرية على المدقق الخارجي أن يهتم بتطبيق قواعد وآداب السلوك الاخلاقي والمهني وتنفيذ أعمال التدقيق والتخطيط لكي يعطي رأياً فنياً محايداً ومستقلاً ، والتأكد من أن البيانات المالية خالية من الأخطاء الجوهرية, ولكي يقوم المدقق الخارجي بأداء مهامه بكل استقلالية وحيادية، فقد أعطت الكثير من المؤسسات الاقتصادية أهمية على أن يكون من مهام لجنة التدقيق مساعدة المدقق الخارجي في أداء مهامه من دون ضغط أو تدخل من إدارة المؤسسة.

وفيما يأتي أهم المهام التي تقدمها لجنة التدقيق في مساعدة التدقيق الخارجي (Abd alSadah, 2023) تقوم لجنة التدقيق بتعيين وترشيح المدقق الخارجي وتحديد أتعابه.

1. دعم استقلالية المدقق الخارجي وتعزيزها في أداء مهامه وتوفير كافة المعلومات التي يحتاج إليها.
2. إيجاد الحلول المناسبة في حالة وجود خلافات بين المدقق الخارجي والإدارة.
3. العمل على التنسيق بين المدقق الخارجي والداخلي.

نظراً لأهمية وظيفة التدقيق الداخلي في الحد من التلاعب واكتشاف الأخطاء ، فقد أعطت العديد من الهيئات أهمية بالغة بضرورة قيام لجان التدقيق بمتابعة سير خطط التدقيق الداخلي واختيار الأشخاص المناسبين للقيام بعملية التدقيق وتحديد الأخطاء ومعالجتها ، وعلى المدققين الداخليين أن يتمتعوا باستقلالية لكي يؤدوا دورهم بشكل فاعل. لذلك ، فإنّ وجود لجنة تدقيق في المؤسسة من شأنها دعم وتعزيز استقلالية التدقيق الداخلي. (Al-Sous, 2012).

2-7 الإشراف الرقابي على الأمن السيبراني

اتسع دور لجنة المراجعة في السنوات الأخيرة إلى ما هو أبعد من المجالات التقليدية، مثل :الإشراف على التقارير المالية وضوابطها المتصلة، وكذلك الإشراف على المراجع الخارجي، لتشمل المخاطر الناشئة، تتحمل العديد من لجان المراجعة مسؤولية الإشراف على مجالات ناشئة مثل :الأمان السيبراني ، والمسؤولية الاجتماعية والبيئية (ESG).

تتضمن قاعدة الكشف عن مخاطر للأمان السيبراني الصادرة من هيئة الأوراق المالية والبورصات "SEC" متطلبات جديدة تتعلق بكشف مجلس الإدارة والإشراف على مخاطر الأمان السيبراني.

وتعزيز جزءاً من دورهم الرقابي، قد يقوم مجلس الإدارة بتقييم مدى قوة برنامج إدارة مخاطر الأمان السيبراني. وصف لعملية الإشراف تتطلب القاعدة وصفاً شاملاً للعملية المتبعة من قبل المجلس أو اللجنة المختارة للبقاء على اطلاع حيال مخاطر الأمان السيبراني. ويشمل ذلك الأساليب والآليات المستخدمة لمراقبة وتقييم والاستجابة لتطورات التهديدات السيبرانية في عام 2023، تم ملاحظة زيادة في الكشف حول مسؤولية لجنة المراجعة تجاه هذه المجالات. ارتفعت نسبة شركات التي كشفت عن أن لجنة المراجعة مسؤولة عن الإشراف على مخاطر الأمان السيبراني من 54% في عام 2022 إلى 59% في عام 2023. بالمثل، ارتفعت نسبة الشركات التي كشفت عن أن لجنة المراجعة مسؤولة عن الإشراف على ESG من 18% في عام 2022 إلى 29% في عام 2023. تتطلب هذه المسؤوليات الجديدة توسيع مهارات أعضاء لجنة المراجعة. ومن الملاحظ أنه تمت رؤية تغييرات في تكوين لجنة المراجعة، سواء من حيث الأعضاء والخبرة، والمسؤوليات. على سبيل المثال، يكشف أكثر من نصف الشركات أن مجلس الإدارة يتضمن خبيرًا في الأمان السيبراني (51%) وخبيرًا في ESG أو الاستدامة (54%).

يجب أن يسهم التدقيق الداخلي بفاعلية في الحفاظ على أمن الخدمات والعمليات الإلكترونية ولاسيما بعد تكرار الانتهاكات والخسائر المالية الكبيرة لفتت حوادث اختراق أنظمة المعلومات التجارية المتزايدة انتباه الشركات إلى الأساليب اللازمة للحد من هذه الحوادث وآثارها . (Lois, Drogalas, 2021). أشار تقرير لشركة .Center for Audit Quality, & Deloitte. (2022) إلى أنه أصدرت هيئة الأوراق المالية والبورصات قاعدة نهائية تتطلب إفصاحات محسنة وموحدة حول مخاطر الأمن السيبراني والاستراتيجيات والحوكمة والحوادث من قبل المسجلين. تستجيب القاعدة للمخاوف المتزايدة بشأن وصول المستثمرين المستمر إلى معلومات الأمن السيبراني بسبب : التكنولوجيا الرقمية ، الذكاء الاصطناعي ، وإعدادات العمل الهجينة ، واستخدام العملات المشفرة ، وارتفاع الأرباح غير المشروعة من التهديدات السيبرانية ، مما يؤدي إلى تضخيم مخاطر وتكاليف الأمن السيبراني بشكل عام. وقد حددت نظرة عامة على حكم الإفصاح عن الأمن السيبراني للجنة الأوراق المالية والبورصات ، مع أربع خطوات يمكنك اتخاذها للمساعدة في إعداد قواعد الأمن السيبراني الخاصة بهيئة الأوراق المالية والبورصات للشركات العامة والامتثال لها.

وفيما يأتي أربع خطوات عملية يمكنك اتخاذها للتحضير لقواعد الأمن السيبراني للجنة الأوراق المالية والبورصات للشركات العامة والامتثال لها :

- إجراء تقييم : حماية سمعة المنظمة والحماية من المخاطر السيبرانية مع الامتثال لقواعد هيئة الأوراق المالية والبورصات:
  - تطوير أساسي يطور بدوره قدرات الاستجابة مع تطور التهديدات.
  - تحديد المخاطر المحتملة ومعالجة القضايا على الفور.
  - تقديم دليل على أنك تتخذ خطوات للامتثال.

- فهم نضج الاستجابة للحوادث والتصعيد وعمليات الإبلاغ.
- تطوير قدرات الاستجابة للحوادث السيبرانية والإبلاغ عنها:
  - حماية مصالح المنظمة والحفاظ على الثقة وتعزيز المرونة الإلكترونية .
  - تحديد معايير الأهمية النسبية وتضمينها في عمليات الحوادث .
  - الاستمرار في الوفاء بالتزامات الإفصاح مع تطور الحوادث.
  - التعلم من الحوادث السابقة وتحسين المرونة.
  - الحفاظ على ثقة المستثمرين وحماية قيمة المساهمين.
- تطبيق عمليات التنسيق بين أصحاب المصلحة لإحداث قدرات واسعة للإفصاح:
  - تسهيل الكشف المناسب في الوقت المناسب .
  - الجمع بين التوجيه القانوني والخبرة في مجال الأمن السيبراني .
  - تطوير المساءلة عن الامتثال والإفصاح.
  - تقديم إفصاحات متسقة بشفافية.
- تعزيز إطار حوكمة الأمن السيبراني وتزويد المساهمين بالثقة ، بأن الإنترنت يمثل أولوية تنظيمية قصوى:
  - تعزيز الحوكمة من خلال تثقيف مجلس الإدارة والإدارة.
  - تعزيز ثقافة المسؤولية والمساءلة.
  - تنفيذ نماذج التشغيل لإدارة المخاطر .
  - تحديد لجنة مجلس الإدارة أو اللجنة الفرعية المسؤولة عن الإشراف على الأمن السيبراني .

المبحث الثالث : الجانب التطبيقي

تم تنفيذ الدراسة التحليلية على مجتمع بحثي مكوّن من عينة تضم المدققين الداخليين والخارجيين، فضلاً عن الأكاديميين والمتخصصين في مجال الأمن السيبراني. وقد تم تصميم استبيان شامل يغطي الجوانب النظرية والعملية التي تناولها الإطار النظري للدراسة، بهدف جمع البيانات اللازمة للتحليل. تم توزيع 75 استبيانًا على المشاركين، كما تم الاعتماد على البرنامج الإحصائي SPSS لتحليل البيانات واختبار الفرضيات، فضلاً عن استخدام برنامج Smart-PLS 23 لتعزيز دقة التحليل واستخلاص النتائج المتعلقة بمدى فاعلية استراتيجيات التدقيق الداخلي في مواجهة المخاطر السيبرانية.

الجدول (1). معلومات تتعلق بالمستجيبين

المؤهل العلمي	التكرار	النسبة %
دبلوم	1	1.3
بكالوريوس	43	57.3
دبلوم عالٍ	10	13.3
ماجستير	14	18.7

دكتوراه	7	9.3
المجموع	75	100.0
التخصص	**التكرار**	**النسبة %**
مدقق داخلي	31	41.3
تكنولوجيا المعلومات	3	4.0
إدارة المخاطر	5	6.7
محاسب	6	8.0
أخرى	30	40.0
المجموع	75	100.0
سنوات الخبرة	**التكرار**	**النسبة %**
أقل من 6 سنوات	18	24.0
من 6 إلى 10 سنوات	15	20.0
من 11 إلى 15 سنة	31	41.3
16 سنة فأكثر	11	14.7
المجموع	**75**	**100.0**

المصدر : من إعداد الباحثين بالاعتماد على برنامج SPSS

تشير النتائج في الجدول إلى ما يمكن تلخيصه في الآتي:

أ- **المؤهل العلمي:** أظهرت النتائج أن أعلى نسبة كانت لشهادة (البكالوريوس) بنسبة (57.3%)، في حين إنّ أقل نسبة كانت ممن يحملون شهادة الدبلوم بنسبة (1.3%). **وهذا يدل على أن غالبية المبحوثين يحملون شهادة البكالوريوس في تخصص التدقيق وهم على دراية كافية في الإجابة على أسئلة الاستبيان .**

ب- **التخصص:** أظهرت النتائج أن أعلى نسبة كانت لتخصص (التدقيق الداخلي) بنسبة (41.3%)، في حين كانت أقل نسبة ممن تخصص تكنولوجيا المعلومات بنسبة (4.0%).

ت- **سنوات الخبرة:** وبخصوص عدد سنوات الخبرة ، فإنّ فئة من لديهم خدمة (من 11 إلى 15 سنة) هي الأعلى نسبة، إذ بلغت (41.3%)، والفئة (16 سنة فأكثر) بأقل نسبة وتساوي (14.7%).

3-1 التحليل الوصفي لفقرات أبعاد الاستبانة

سيتم استخراج كل من المتوسطات الحسابية والانحرافات المعيارية وشدة الاستجابة لجميع فقرات أبعاد الاستبانة.

3-1-1 تحليل فقرات وأبعاد متغير استراتيجيات تفعيل دور لجنة التدقيق الداخلي

تم حساب التكرارات والنسب والمتوسطات الحسابية والانحرافات المعيارية ومؤشر شدة الاستجابة لفقرات أبعاد متغير (استراتيجيات تفعيل دور لجنة التدقيق الداخلي)، على النحو الآتي:

1. تقييم المخاطر:

الجدول (2). المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد تقييم المخاطر

الفقرات	مقياس الاستجابة					المتوسط الحسابي	المعيار ف الانحرا	شدة الاستجا بة %
	أتفق بدرجة عالية جداً(5)	أتفق (4)	محايد (3)	لا أتفق (2)	لا أتفق إطلاقاً (1)			

			%	ت	%	ت	%	ت	%	ت	%	ت	
76.3	1.216	3.813	1.3	1	25.3	19	0.0	0	37.3	28	36.0	27	X1_1
76.5	1.155	3.827	2.7	2	20.0	15	0.0	0	46.7	35	30.7	23	X1_2
77.1	1.171	3.853	5.3	4	14.7	11	0.0	0	49.3	37	30.7	23	X1_3
72.5	1.260	3.627	4.0	3	26.7	20	0.0	0	41.3	31	28.0	21	X1_4
78.7	1.143	3.933	4.0	3	14.7	11	0.0	0	46.7	35	34.7	26	X1_5
76.2%	1.189	3.811	3.5%		20.3%		0.0%		44.3%		32.0%		البعد
			23.8%						76.3%				

المصدر : من إعداد الباحثين بالاعتماد على برنامج SPSS

يتبين من الجدول أن بعد تقييم المخاطر تمثل بالفقرات (X1_1 إلى X1_5) وبنسبة (76.3%) من المبحوثين نحو الاتفاق (أتفق بدرجة عالية جداً، أتفق) على إجمالي هذا البعد، ونسبة عدم الاتفاق (لا أتفق، لا أتفق اطلاقاً) بلغتى(23.8%) ويعزز ذلك المتوسط الحسابي (3.811) وبانحراف المعياري (1.189) وشدة استجابة (76.2%)، وقد جاءت في المرتبة الأولى من حيث شدة الاستجابة الفقرة التي تنص على ((تتوفر دورات تدريبية مستمرة لموظفي التدقيق الداخلي تتعلق بتحليل المخاطر))، وجاءت في المرتبة الأخيرة الفقرة التي تنص على ((تتوفر تقارير ومتابعات دورية حول تقييم المخاطر)).

2. تقييم السياسات والإجراءات:

الجدول (3). المتوسطات الحسابية والانحرافات المعيارية لفقرات بعد تقييم السياسات والإجراءات

الفقرات	مقياس الاستجابة										المتوسط الحسابي	الانحراف المعياري	% شدة الاستجابة
	أتفق بدرجة عالية جداً(5)		أتفق (4)		محايد (3)		لا أتفق (2)		لا أتفق اطلاقاً (1)				
	ت	%	ت	%	ت	%	ت	%	ت	%			
X2_1	33	44.0	27	36.0	0	0.0	11	14.7	4	5.3	3.987	1.236	79.7
X2_2	27	36.0	27	36.0	0	0.0	16	21.3	5	6.7	3.733	1.329	74.7
X2_3	21	28.0	38	50.7	0	0.0	13	17.3	3	4.0	3.813	1.147	76.3
X2_4	24	32.0	36	48.0	0	0.0	13	17.3	2	2.7	3.893	1.122	77.9
X2_5	23	30.7	38	50.7	0	0.0	12	16.0	2	2.7	3.907	1.093	78.1
البعد	34.1%		44.3%		0.0%		17.3%		4.3%		3.867	1.185	77.3%
	78.4%						21.6%						

المصدر : من إعداد الباحث بالاعتماد على برنامج SPSS

يتبين من الجدول أعلاه أن بعد تقييم السياسات والإجراءات تمثل بالفقرات (X2_1 إلى X2_5) وبنسبة (78.4%) من المبحوثين نحو الاتفاق (أتفق بدرجة عالية جداً، أتفق) على إجمالي هذا البعد ونسبة عدم الاتفاق (لا أتفق، لا أتفق اطلاقاً) بنسبة قدرها (21.6%) ويعزز ذلك المتوسط الحسابي (3.867) وبانحراف المعياري (1.185) وشدة استجابة (77.3%)، وقد جاءت في المرتبة الأولى من حيث شدة

الاستجابة الفقرة التي تنص على (تقوم لجنة التدقيق الداخلي بتقييم فعالية السياسات والإجراءات)، وجاءت في المرتبة الأخيرة الفقرة التي تنص على (تتوفر إجراءات تنفيذية للتعامل مع الحوادث).

3. تحسين الإجراءات الرقابية:

الجدول (4). المتوسطات الحسابية والانحرافات المعيارية لفقرات بعد تحسين الإجراءات الرقابية

الفقرات	مقياس الاستجابة										المتوسط الحسابي	الانحراف المعياري	شدة الاستجابة %
	أتفق بدرجة عالية جداً(5)		أتفق (4)		محايد (3)		لا أتفق (2)		لا أتفق اطلاقاً (1)				
	ت	%	ت	%	ت	%	ت	%	ت	%			
X3_1	32	42.7	29	38.7	0	0.0	10	13.3	4	5.3	4.000	1.208	80.0
X3_2	19	25.3	42	56.0	0	0.0	11	14.7	3	4.0	3.840	1.091	76.8
X3_3	24	32.0	32	42.7	0	0.0	14	18.7	5	6.7	3.747	1.274	74.9
X3_4	27	36.0	37	49.3	0	0.0	7	9.3	4	5.3	4.013	1.109	80.3
X3_5	27	36.0	38	50.7	0	0.0	9	12.0	1	1.3	4.080	0.983	81.6
البعد	34.4%		47.5%		0.0%		13.6%		4.5%		3.936	1.133	78.7%
	81.9%						18.1%						

المصدر : من إعداد الباحثين بالاعتماد على برنامج SPSS

يوضح الجدول أنّ بُعد تحسين الإجراءات الرقابية تمثل بالفقرات (X3_1 إلى X3_5) وبنسبة (81.9%) من المبحوثين نحو الاتفاق (أتفق بدرجة عالية جداً، أتفق) على إجمالي هذا البعد ونسبة عدم الاتفاق (لا أتفق، لا أتفق اطلاقاً) بنسبة قدرها (18.1%) ويعزز ذلك المتوسط الحسابي (3.936) وبانحراف المعياري (1.133) وشدة استجابة (78.7%)، وقد جاءت في المرتبة الأولى من حيث شدة الاستجابة، وهي الفقرة التي تنص على ((تقوم لجنة التدقيق الداخلي بتقييم دوري لفعالية الإجراءات الرقابية))، وجاءت في المرتبة الأخيرة الفقرة التي تنص على ((يوجد إطار عمل محدد لتنفيذ الإجراءات الرقابية)).

4. التقنيات وأساليب الحماية:

الجدول (5). المتوسطات الحسابية والانحرافات المعيارية لفقرات بعد التقنيات وأساليب الحماية

الفقرات	مقياس الاستجابة										المتوسط الحسابي	الانحراف المعياري	شدة الاستجابة %
	أتفق بدرجة عالية جداً(5)		أتفق (4)		محايد (3)		لا أتفق (2)		لا أتفق اطلاقاً (1)				
	ت	%	ت	%	ت	%	ت	%	ت	%			
X4_1	30	40.0	32	42.7	0	0.0	7	9.3	6	8.0	3.973	1.230	79.5
X4_2	25	33.3	30	40.0	0	0.0	16	21.3	4	5.3	3.747	1.274	74.9
X4_3	32	42.7	26	34.7	0	0.0	10	13.3	7	9.3	3.880	1.345	77.6
X4_4	29	38.7	33	44.0	0	0.0	7	9.3	6	8.0	3.960	1.224	79.2
X4_5	25	33.3	33	44.0	0	0.0	11	14.7	6	8.0	3.800	1.273	76.0
البعد	37.6%		41.1%		0.0%		13.6%		7.7%		3.872	1.269	77.4%
	78.7%						21.3%						

المصدر : من إعداد الباحث بالاعتماد على برنامج SPSS

يظهر من الجدول أن بعد التقنيات وأساليب الحماية تمثل بالفقرات (X4_1 إلى X4_5) وبنسبة (78.7%) من المبحوثين نحو الاتفاق (أتفق بدرجة عالية جداً، أتفق) على إجمالي هذا البعد ونسبة عدم الاتفاق (لا أتفق، لا أتفق اطلاقاً) بنسبة قدرها (21.3%) ويعزز ذلك المتوسط الحسابي (3.872) وبانحراف المعياري (1.269) وشدة استجابة (77.4%)، وقد جاءت في المرتبة الأولى من حيث شدة الاستجابة الفقرة التي تنص على ((تتوفر برامج تدريب للموظفين تعنى باستخدام التقنيات وأساليب الحماية))، وجاءت في المرتبة الأخيرة الفقرة التي تنص على ((استخدام أنظمة كشف التسلل (IDS) وأنظمة منع التسلل (IPS))).

3-1-2 تحليل فقرات متغير مواجهة مخاطر الأمن السيبراني وأبعاده

تم حساب التكرارات والنسب والمتوسطات الحسابية والانحرافات المعيارية ومؤشر شدة الاستجابة لفقرات أبعاد متغير (مواجهة مخاطر الأمن السيبراني)، على النحو الآتي:

1. تسريب المعلومات:

الجدول (6). المتوسطات الحسابية والانحرافات المعيارية لفقرات بعد تسريب المعلومات

الفقرات	مقياس الاستجابة										المتوسط الحسابي	الانحراف المعياري	شدة الاستجابة %
	أتفق بدرجة عالية جداً(5)		أتفق (4)		محايد (3)		لا أتفق (2)		لا أتفق إطلاقاً (1)				
	ت	%	ت	%	ت	%	ت	%	ت	%			
Y1_1	30	40.0	37	49.3	0	0.0	5	6.7	3	4.0	4.147	1.009	82.9
Y1_2	29	38.7	30	40.0	0	0.0	13	17.3	3	4.0	3.920	1.205	78.4
Y1_3	29	38.7	33	44.0	0	0.0	11	14.7	2	2.7	4.013	1.109	80.3
Y1_4	29	38.7	30	40.0	0	0.0	12	16.0	4	5.3	3.907	1.232	78.1
البعد	39.0%		43.3%		0.0%		13.7%		4.0%		3.997	1.139	79.9%
	82.3%				17.7%								

المصدر : من إعداد الباحثين بالاعتماد على برنامج SPSS

يوضح الجدول أن بعد تسريب المعلومات تمثل بالفقرات (Y1_1 إلى Y1_4) وبنسبة (82.3%) من المبحوثين نحو الاتفاق (أتفق بدرجة عالية جداً، أتفق) على إجمالي هذا البعد ونسبة عدم الاتفاق (لا أتفق، لا أتفق اطلاقاً) بلغت (17.7%) ويعزز ذلك المتوسط الحسابي (3.997) وبانحراف المعياري (1.139) وشدة استجابة (79.9%)، وقد جاءت في المرتبة الأولى من حيث شدة الاستجابة الفقرة التي تنص على ((تتوفر برامج تدريب تعمل في تعزيز الوعي بمخاطر تسريب البيانات)).

2. البرمجيات الخبيثة:

الجدول (7). المتوسطات الحسابية والانحرافات المعيارية لفقرات بعد البرمجيات الخبيثة

الفقرات	مقياس الاستجابة										المتوسط الحسابي	الانحراف المعياري	شدة الاستجابة %
	أتفق بدرجة عالية جداً(5)		أتفق (4)		محايد (3)		لا أتفق (2)		لا أتفق اطلاقاً (1)				
	ت	%	ت	%	ت	%	ت	%	ت	%			

Y2_1	30	40.0	29	38.7	0	0.0	11	14.7	5	6.7	3.907	1.265	78.1
Y2_2	23	30.7	41	54.7	0	0.0	7	9.3	4	5.3	3.960	1.084	79.2
Y2_3	29	38.7	34	45.3	0	0.0	7	9.3	5	6.7	4.000	1.174	80.0
Y2_4	28	37.3	36	48.0	0	0.0	7	9.3	4	5.3	4.027	1.115	80.5
البعد	36.7%		46.7%		0.0%		10.7%		6.0%		3.973	1.159	79.5%
	83.4%						16.7%						

المصدر : من إعداد الباحثين بالاعتماد على برنامج SPSS

يتبين من الجدول أعلاه أن بعد البرمجيات الخبيثة تمثل بالفقرات (Y2_1 إلى Y2_5) وبنسبة (83.4%) من المبحوثين نحو الاتفاق (أتفق بدرجة عالية جداً، أتفق) على إجمالي هذا البعد ونسبة عدم الاتفاق (لا أتفق، لا أتفق اطلاقاً) قدرها (16.7%) ويعزز ذلك المتوسط الحسابي (3.973) وبانحراف المعياري (1.159) وشدة استجابة (79.5%)، وقد جاءت في المرتبة الأولى من حيث شدة الاستجابة الفقرة التي تنص على ((هناك تعاون وثيق لفريق تكنولوجيا المعلومات في مواجهة مخاطر البرمجيات الخبيثة))، وجاءت في المرتبة الأخيرة الفقرة التي تنص على ((هناك تدريبًا منتظمًا حول تهديدات البرمجيات الخبيثة)).

3. القرصنة والهجمات:

الجدول (8). المتوسطات الحسابية والانحرافات المعيارية لفقرات بعد القرصنة والهجمات

الفقرات	مقياس الاستجابة										المتوسط الحسابي	الانحراف المعياري	شدة الاستجابة %
	أتفق بدرجة عالية جداً(5)		أتفق (4)		محايد (3)		لا أتفق (2)		لا أتفق اطلاقاً (1)				
	ت	%	ت	%	ت	%	ت	%	ت	%			
Y3_1	31	41.3	34	45.3	0	0.0	9	12.0	1	1.3	4.133	1.004	82.7
Y3_2	24	32.0	32	42.7	0	0.0	14	18.7	5	6.7	3.747	1.274	74.9
Y3_3	21	28.0	40	53.3	0	0.0	11	14.7	3	4.0	3.867	1.107	77.3
Y3_4	32	42.7	28	37.3	0	0.0	11	14.7	4	5.3	3.973	1.230	79.5
البعد	36.0%		44.7%		0.0%		15.0%		4.3%		3.930	1.154	78.6%
	80.7%						19.3%						

المصدر : من إعداد الباحثين بالاعتماد على برنامج SPSS

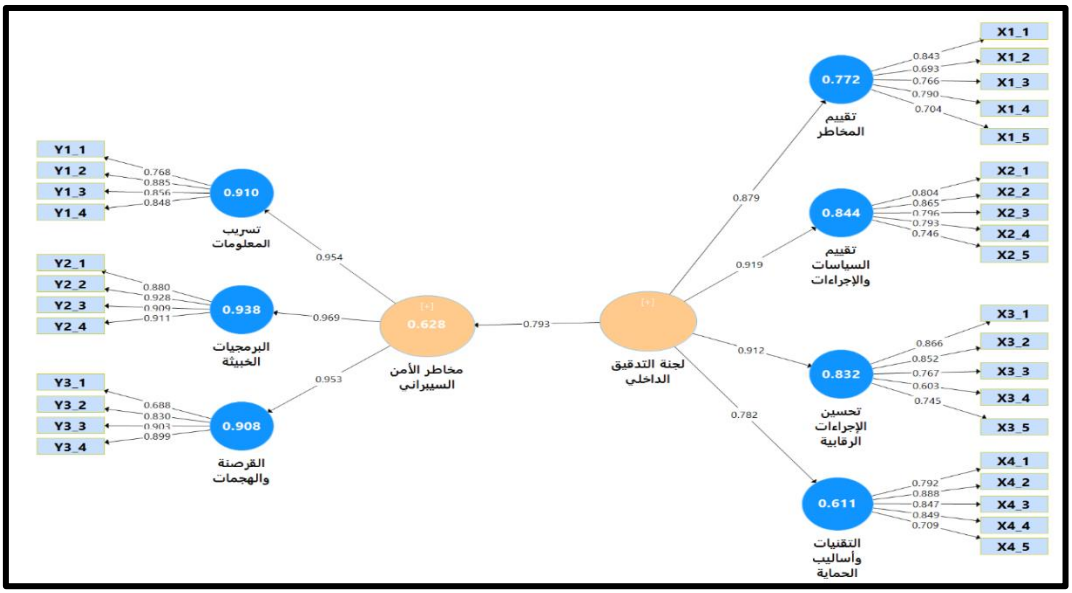
يتبين من الجدول أن بعد القرصنة والهجمات تمثل بالفقرات (Y3_1 إلى Y3_4) وبنسبة (80.7%) من المبحوثين نحو الاتفاق (أتفق بدرجة عالية جداً، أتفق) على إجمالي هذا البعد ونسبة عدم الاتفاق (لا أتفق، لا أتفق اطلاقاً) بلغت (19.3%) ويعزز ذلك المتوسط الحسابي (3.930) وبانحراف المعياري (1.154) وشدة استجابة (78.6%)، وقد جاءت في المرتبة الأولى من حيث شدة الاستجابة الفقرة التي تنص على ((الأدوات التكنولوجية المستخدمة في مؤسستك فعالة للكشف عن محاولات القرصنة والهجمات الإلكترونية))، وجاءت في المرتبة الأخيرة الفقرة التي تنص على ((يتم إجراء اختبارات اختراق دورية لاكتشاف نقاط الضعف في أنظمة مؤسستك تجاه القرصنة والهجمات الإلكترونية)).

ولغرض التأكد من فرضيات البحث والتحقق من صحتها قمنا بوضع نماذج (PLS-SEM) لإثبات أو نفي هذه الفرضية باستخدام برنامج Smart-PLS 3، وكما يأتي:

1. اختبار الفرضية الأولى سيتم اختبار الفرضية الأولى التي تنص على:

((لا يوجد تأثير معنوي إحصائياً لاستراتيجيات تفعيل دور لجنة التدقيق الداخلي في مواجهة مخاطر الأمن السيبراني))

والشكل (1) يعرض رسم الأنموذج الخاصة بهذه الفرضية، كما يظهر الجدول (9) نتائج تحليل الانحدار الخاصة بالأنموذج ، والتي تشير إلى رفض الفرضية الأولى.



الشكل (1). تأثير استراتيجيات تفعيل دور لجنة التدقيق الداخلي في مواجهة مخاطر الأمن السيبراني

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart-PLS 23.

الجدول (9). تأثيراستراتيجيات تفعيل دور لجنة التدقيق الداخلي في مواجهة مخاطر الأمن السيبراني

المتغير المعتمد: مواجهة مخاطر الأمن السيبراني				
المتغير المستقل	**معامل التأثير**	**قيم t**	**Sig**	**معامل التحديد**
تفعيل دور لجنة التدقيق الداخلي	0.793	8.657	<0.001	0.628

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart-PLS 23.

ونلاحظ من الجدول (9) أنّ معامل التأثير في هذا التحليل يشير إلى قوة واتجاه العلاقة بين المتغير المستقل والمتغير التابع ، ومعامل التأثير = 0.793: يعني أن هناك تأثيرًا إيجابيًا قويًا بين المتغيرين، أي أن تفعيل دور لجنة التدقيق الداخلي يسهم بشكل إيجابي في مواجهة مخاطر الأمن السيبراني. وبذلك نرفض

الفرضية الأولى؛ لأن قيمة Sig أقل من مستوى المعنوية (0.05)، مما يعني بأن هناك تأثيراً معنوياً إحصائياً لاستراتيجيات تفعيل دور لجنة التدقيق الداخلي في مواجهة مخاطر الأمن السيبراني، أي أنه:

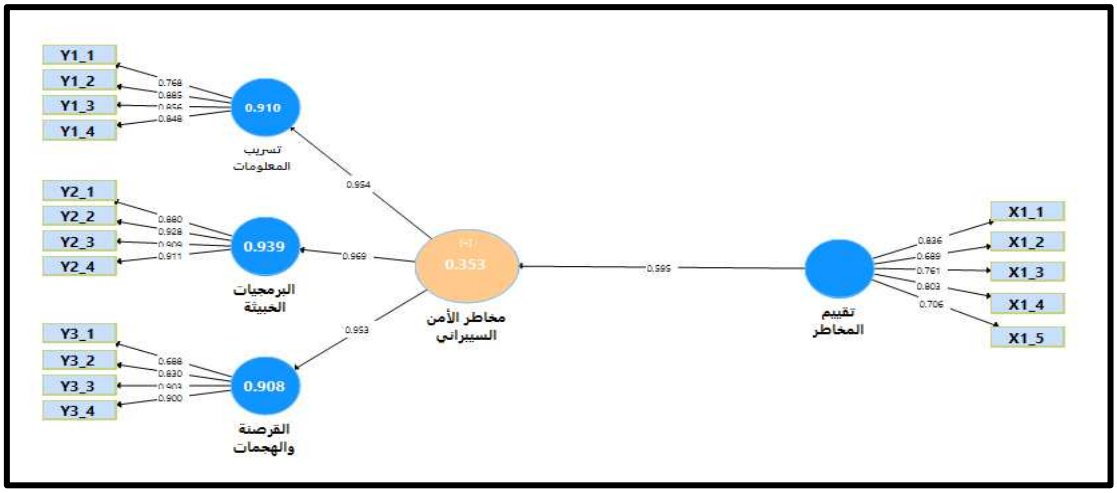
((*يوجد تأثير معنوي إحصائياً لاستراتيجيات تفعيل دور لجنة التدقيق الداخلي في مواجهة مخاطر الأمن السيبراني*))

وتشير قيمة معامل التحديد إلى أن هذا التأثير يفسر حوالي 63%.

2. اختبار الفرضية الثانية سيتم اختبار الفرضية الثانية التي تنص على:

((لا يوجد تأثير معنوي إحصائياً لتقييم المخاطر في مواجهة مخاطر الأمن السيبراني))

والشكل (2) يعرض رسم الأنموذج الخاص بهذه الفرضية، كما يظهر الجدول (10) نتائج تحليل الانحدار الخاصة بالأنموذج والتي تشير إلى رفض الفرضية الثانية.



الشكل (2). تأثير تقييم المخاطر في مواجهة مخاطر الأمن السيبراني

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart-PLS 23.

الجدول (10). تأثير تقييم المخاطر في مواجهة مخاطر الأمن السيبراني

المتغير المعتمد: مواجهة مخاطر الأمن السيبراني				
المتغير المستقل	**معامل التأثير**	**قيم t**	**Sig**	**معامل التحديد**
تقييم المخاطر	0.595	4.573	<0.001	0.353

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart-PLS 23.

ونلاحظ من الجدول (10) أننا نرفض الفرضية الثانية؛ وذلك لأن قيمة Sig أقل من مستوى المعنوية (0.05)، مما يعني بأن هناك تأثيراً معنوياً إحصائياً لتقييم المخاطر في مواجهة مخاطر الأمن السيبراني، أي أنه:

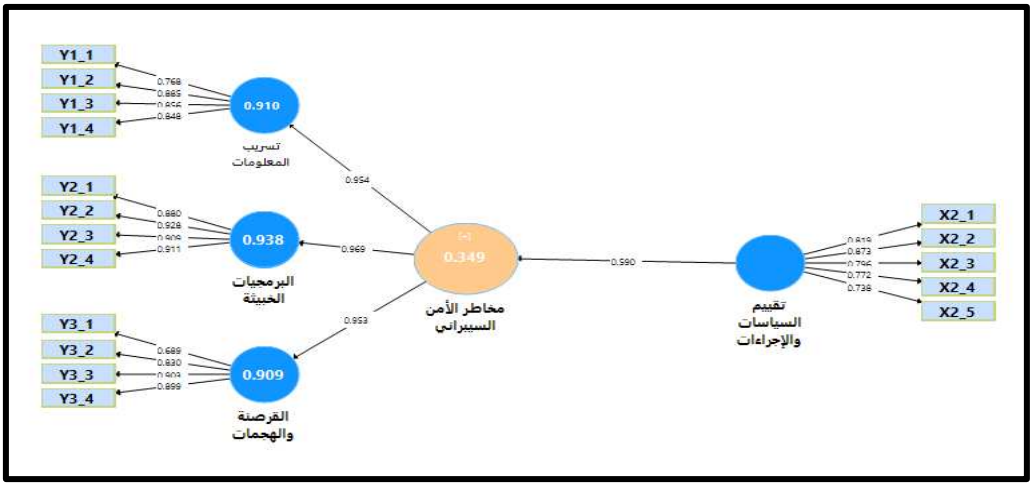
((*يوجد تأثير معنوي إحصائياً لتقييم المخاطر في مواجهة مخاطر الأمن السيبراني*))

وتشير قيمة معامل التحديد إلى أن هذا التأثير يفسر حوالي 35%.

3. اختبار الفرضية الثالثة سيتم اختبار الفرضية الثالثة التي تنص على:

((لا يوجد تأثير معنوي إحصائياً لتقييم السياسات والإجراءات في مواجهة مخاطر الأمن السيبراني))

والشكل (3) يعرض رسم الأنموذج الخاص بهذه الفرضية، كما يظهر الجدول (11) نتائج تحليل الانحدار الخاصة بالأنموذج والتي تشير إلى رفض الفرضية الثالثة.



الشكل (3). تأثير تقييم السياسات والإجراءات في مواجهة مخاطر الأمن السيبراني

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart-PLS 23.

الجدول (11). تأثير تقييم السياسات والإجراءات في مواجهة مخاطر الأمن السيبراني

المتغير المعتمد: مواجهة مخاطر الأمن السيبراني				
المتغير المستقل	**معامل التأثير**	**قيم t**	**Sig**	**معامل التحديد**
تقييم السياسات والإجراءات	0.590	3.644	<0.001	0.349

المصدر: إعداد الباحث بالاعتماد على برنامج Smart-PLS 23.

ونلاحظ من الجدول (11) أننا نرفض الفرضية الثالثة؛ وذلك لأن قيمة Sig أقل من مستوى المعنوية (0.05)، مما يعني بأن هناك تأثيراً معنوياً إحصائياً لتقييم السياسات والإجراءات في مواجهة مخاطر الأمن السيبراني، أي أنه:

((*يوجد تأثير معنوي إحصائياً لتقييم السياسات والإجراءات في مواجهة مخاطر الأمن السيبراني*))

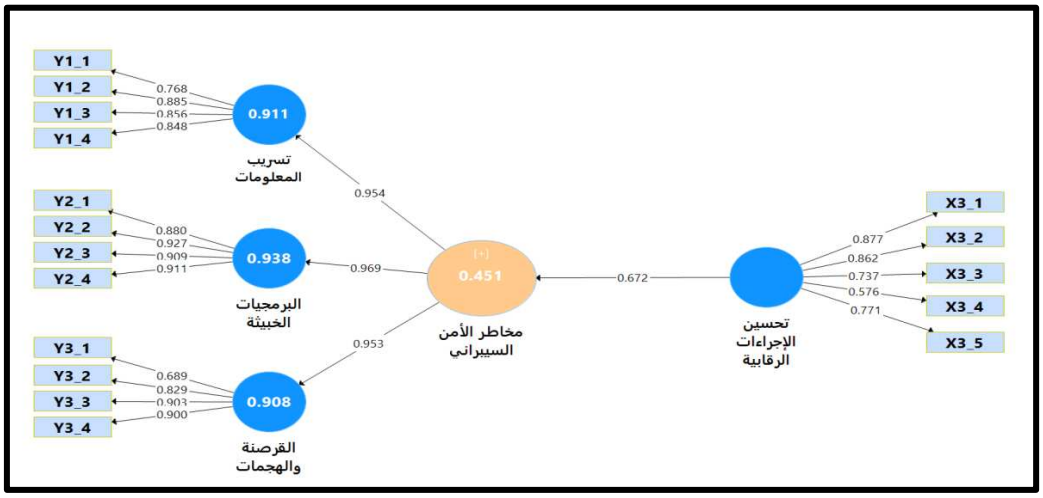
وتشير قيمة معامل التحديد إلى أن هذا التأثير يفسر حوالي 35%.

4. اختبار الفرضية الرابعة

سيتم اختبار الفرضية الرابعة التي تنص على:

((لا يوجد تأثير معنوي إحصائياً لتحسين الإجراءات الرقابية في مواجهة مخاطر الأمن السيبراني))

والشكل (4) يعرض رسم الأنموذج الخاص بهذه الفرضية، كما يظهر الجدول (12) نتائج تحليل الانحدار الخاصة بالأنموذج والتي تشير إلى رفض الفرضية الرابعة.



الشكل (4). تأثير تحسين الإجراءات الرقابية في مواجهة مخاطر الأمن السيبراني

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart-PLS 23.

الجدول (12). تأثير تحسين الإجراءات الرقابية في مواجهة مخاطر الأمن السيبراني

المتغير المعتمد: مواجهة مخاطر الأمن السيبراني				
المتغير المستقل	**معامل التأثير**	**قيم t**	**Sig**	**معامل التحديد**
تحسين الإجراءات الرقابية	0.672	5.913	<0.001	0.451

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart-PLS 23.

ونلاحظ من الجدول (12) أننا نرفض الفرضية الرابعة؛ لأن قيمة Sig أقل من مستوى المعنوية (0.05)، مما يعني بأن هناك تأثيراً معنوياً إحصائياً لتحسين الإجراءات الرقابية في مواجهة مخاطر الأمن السيبراني، أي أنه:

((*يوجد تأثير معنوي إحصائياً لتحسين الإجراءات الرقابية في مواجهة مخاطر الأمن السيبراني*))

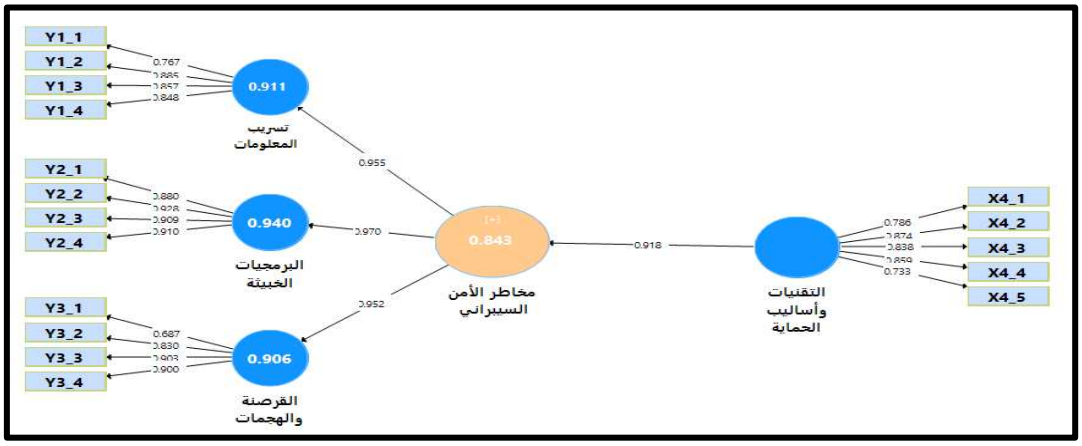
وتشير قيمة معامل التحديد إلى أن هذا التأثير يفسر حوالي 45%.

5. اختبار الفرضية الخامسة

سيتم اختبار الفرضية الخامسة التي تنص على:

((لا يوجد تأثير معنوي إحصائياً للتقنيات وأساليب الحماية في مواجهة مخاطر الأمن السيبراني)).

والشكل (5) يعرض رسم الأنموذج الخاص بهذه الفرضية، كما يظهر الجدول (13) نتائج تحليل الانحدار الخاصة بالأنموذج والتي تشير إلى رفض الفرضية الخامسة.



الشكل (5). تأثير التقنيات وأساليب الحماية في مواجهة مخاطر الأمن السيبراني

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart-PLS 23.

الجدول (13). تأثير التقنيات وأساليب الحماية في مواجهة مخاطر الأمن السيبراني

المتغير المعتمد: مواجهة مخاطر الأمن السيبراني				
المتغير المستقل	**معامل التأثير**	**قيم t**	**Sig**	**معامل التحديد**
التقنيات وأساليب الحماية	0.918	29.051	<0.001	0.843

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart-PLS 23.

ونلاحظ من الجدول (13) أننا نرفض الفرضية الخامسة؛ وذلك لأن قيمة Sig أقل من مستوى المعنوية (0.05)، مما يعني بأن هناك تأثيراً معنوياً إحصائياً للتقنيات وأساليب الحماية في مواجهة مخاطر الأمن السيبراني، أي أنه: ((*يوجد تأثير معنوي إحصائياً للتقنيات وأساليب الحماية في مواجهة مخاطر الأمن السيبراني*)) وتشير قيمة معامل التحديد إلى أن هذا التأثير يفسر أكثر من 84%.

النتائج والتوصيات

توصل البحث إلى النتائج الآتية :

1. أظهرت الدراسة أن التدقيق الداخلي يؤدي دورًا حيويًا في تعزيز الرقابة والتصدي لمخاطر الأمن السيبراني من خلال تطوير سياسات وإجراءات مراقبة دقيقة.
2. أهمية تعزيز كفاءة لجنة التدقيق وتحسين التعاون مع وحدات تقنية المعلومات .
3. مواكبة التطورات السريعة في بيئة التهديدات السيبرانية وتطوير مهارات المحاسبين والمدققين من خلال وضع خطط وبرامج تدريبية .
4. التعاون محدود مع وحدات تقنية المعلومات يحد من القدرة على استجابة فعالة وسريعة للمخاطر السيبرانية.

5. غياب تشريعات واضحة أو سياسات داخلية قوية تعيق دور لجنة التدقيق الداخلي في التصدي لمخاطر الأمن السيبراني.
6. أظهرت الدراسة أهمية تبني تقنيات حديثة، مثل :الذكاء الاصطناعي، لتحليل البيانات ورصد المخاطر السيبرانية، مما يعزز دور لجنة التدقيق في هذا المجال.
7. ثقافة الأمن السيبراني في المؤسسة تتطلب زيادة وعي الموظفين، مما يقلل عبء العمل على لجنة التدقيق الداخلي.

وبناءً على الاستنتاجات يوصي الباحثان بالآتي :

1. إعداد دليل سياسات وإجراءات موحد يحدد دور لجنة التدقيق الداخلي في إدارة المخاطر السيبرانية، بما يضمن خطوات واضحة للتعامل مع الحوادث.
2. ضرورة توفير دورات تدريبية متخصصة في مجال الأمن السيبراني في المؤسسات لتمكين المدققين من تقييم المخاطر السيبرانية بشكل أفضل.
3. توصي الدراسة بتنفيذ تمارين محاكاة للهجمات السيبرانية لقياس مدى استعداد المؤسسة ولجنة التدقيق الداخلي للتعامل مع هذه التهديدات.
4. توصي الدراسة بإجراء تقييم شامل ودوري للمخاطر السيبرانية التي تواجه المؤسسة، وتحديث الإجراءات بناءً على النتائج.
5. توصية المؤسسات بتبني تقنيات الذكاء الاصطناعي والتحليلات الرقمية لمراقبة الأنظمة واكتشاف الأنشطة المشبوهة بشكل استباقي.
6. تنفيذ برامج توعوية لجميع موظفي المؤسسة لتعزيز ثقافة الأمن السيبراني ،وتقليل السلوكيات التي قد تعرض المؤسسة للمخاطر.
7. تخصيص ميزانيات كافية لتعزيز قدرات لجنة التدقيق الداخلي في مواجهة المخاطر السيبرانية، بما يشمل التدريب، والأدوات، والموارد التقنية.

- **الإقرار بالشكر (Acknowledgements):**

  نشكر جامعة الموصل وكافة الاساتذه على تشجيعها لإتمام هذه الدراسة .كما نشكر زملاءنا والاساتذه المحاسبين والمدققين على الاجابة على الاسئلة، مما ساعدنا في إنجاز هذا البحث

- **التمويل (Funding):** عدم تلقي أي تمويل أو دعم مالي .
- **أفصاحات المؤلفين (Author Disclosures):** لا يوجد أي تضارب في المصالح يؤثر على هذا العمل

References

- **Arabic References**

البرزنجي ، سهى.، السقا ، زياد يحيى . (2023). متطلبات التدقيق الداخلي لتعزيز الأمن السيبراني في الوحدات الاقتصادية في ضوء إرشادات معهد المدققين الداخليين IIA، *مجلة تكريت للعلوم الإدارية والاقتصادية*, 19(63), 94–112. https://doi.org/10.25130/tjaes.19.63.2.5

الرشيدي، طارق وعباس ،داليا .(2019) .أثر الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية على أسعار الأسهم وأحجام التداول .*مجلة المحاسبة والمراجعة، كلية التجارة* ، جامعة طنطا، العدد الثاني ، القاهرة،. (8) 2، 439–487.
https://doi.org/10.21608/naus.2019.92313

شحاته، السيد شحاته.(2020) .إطار مقترح لإسناد وظيفة المراجعة الداخلية بدوريها الاستشاري والتوكيدي فى مجال إدارة المخاطر فى الوحدات الصغيرة ومتوسطة الحجم. *المجلة العلمية التجارة والتمويل*، ، 40، عدد خاص (مؤتمر الكلية ،الجزء الأول) 109–128.
https://doi.org/110.21608/CAF.2020.154090

الصوص, آياد سعيد محمود.(2012). *مدى فاعلية دور لجان المراجعة في دعم اليات التدقيق الداخلي و الخارجي : دراسة تطبيقية على البنوك العاملة في فلسطين*، رسالة ماجستير، الجامعة الإسلامية – غزة.

عبدالمنعم، يوسف طه.(2021) .التحول الرقمي على مهنة المحاسبة والمراجعة فى ظل فيروس كورونا باستخدام برمجيات تخطيط موارد المؤسسات. بحث غ منشور تقدم للمؤتمر الرابع لقسم المحاسبة ، كلية التجارة، جامعة الإسكندرية.

عثمان ,خالد محمد .(2023). أثر العلاقة المشتركة بين تعقيد عمليات البنك والإفصاح عن إجراءات إدارة مخاطر الأمن السيبراني على الأداء المالي– دراسة تطبيقية. *مجلة البحوث المحاسبية*, المجلد 4(10) ،الجزء الثانى، ديسمبر 2023، 1107–1183.
https://doi.org/10.21608/abj.2023.334101

عطية، أحمد محمد (2021).التحول الرقمي في مصر هل يُلقي بمسئوليات جديدة على المراجع؟ .*مجلة البحوث التجارية* كلية التجارة ، جامعة الزقازيق. (34) 1 ، 51–65.
https://search.mandumah.com/Record/1151274

فريد ،حنان .(2022). الدور المقترح لمراجع الحسابات في إضفاء الثقة عن تقرير إدارة المخاطر الأمن السيبراني وأثره في دلالة القوائم المالية دراسة تجريبية ، *المجلة العلمية للدراسات التجارية والبيئية* ، (52) 4، 412–488. https://doi.org/10.21608/jces.2022.285187

متولي، مصطفى زكي، غريب، حسين عبد العال.(2022).قياس تأثير الإفصاح عن مخاطر الأمن السيبراني على أتعاب المراجعة الخارجية. *مجلة العلوم التجارية* ، 4 ،245–328.

يعقوب، ابتهاج إسماعيل وآخرون .(2022). مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية في سوق الأوراق المالية وفق المتطلبات الدولية .*مجلة الدراسات المالية والمحاسبية والإدارية*.(9)1، 1404-1430.

يوسف, و حنان محمد إسماعيل. (2024). القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني–دراسة انتقادية وتجريبية. *مجلة البحوث المحاسبية*, *11*(1), 525-594.

https://doi.org/10.21608/abj.2024.340155

مستشارية الأمن الوطني. (2020). استراتيجية الأمن السيبراني العراقية.

https://www.itu.int/en/ITU-

- **Arabic References are presented in Roman script (translated)**

Al-Barzanji, S., & Al-Saqqa, Z. Y. (2023). Internal Audit Requirements to Enhance Cybersecurity in Economic Units in Light of the IIA Guidelines. Tikrit Journal for Administrative and Economic Sciences, 19(63), 94–112 https://doi.org/10.25130/tjaes.19.63.2.5

Al-Rashidi, T., & Abbas, D. (2019). The Impact of Cybersecurity Risk Disclosure in Financial Reports on Stock Prices and Trading Volumes. Journal of Accounting and Auditing, 8(2), 439–487. https://doi.org/10.21608/naus.2019.92313

Atiya, A. M. (2021). Digital Transformation in Egypt: Does It Impose New Responsibilities on the Auditor? Journal of Commercial Research, 43(1), 51–65. https://search.mandumah.com/Record/1151274

Amirhom, J. A. N. (2022). The impact of internal audit quality on reducing cybersecurity risks and its reflections on guiding investors' decisions (A field study). *Journal of Financial and Commercial Research*, 23(3), 325–377 DOI: 10.21608/jsst.2022.153499.1452.

Farid, H. (2022). The Proposed Role of the Auditor in Adding Confidence to the Cybersecurity Risk Management Report and Its Impact on the Significance of Financial Statements: An Experimental Study. Scientific Journal for Commercial and Environmental Studies, 4(52), 412–488.

Iraqi Cybersecurity Strategy. (2020). National Security Advisory.

Metwally, M. Z., & Gharib, H. A. (2022). Measuring the Impact of Cybersecurity Risk Disclosure on External Audit Fees. Journal of Commercial Sciences, 4, 245–328 .https://doi.org/10.21608/sjar.2022.283706

Saeed, V. A., & Asaad, R. R. (2022). Cyber security threats, vulnerability, challenges with proposed solution. Applied Computing Journal, 2(4), 227–244. https://doi.org/10.52098/acj.202260

Osman, K. M. (2023). The Joint Relationship Between Bank Operations Complexity and Disclosure of Cybersecurity Risk Management Procedures on Financial Performance: An Applied Study. Journal of Accounting Research, 10(4), 1107–1183. https://doi.org/10.21608/abj.2023.334101

Shahata, S. S. (2020). A Proposed Framework for Assigning the Internal Audit Function in Its Advisory and Assurance Roles in Risk Management in Small and Medium-Sized Units. Scientific Journal of Commerce and Finance, 40(Special Issue), 109–128. https://doi.org/110.21608/CAF.2020.154090

Youssef, H. M. I. (2024). The Add Value of the Effectiveness of Internal Audit Performance in Its Advisory and Assurance Roles in Cybersecurity Risk Management: A Critical and Experimental Study. Journal of Accounting Research, 11(1), 525–594. https://doi.org/10.21608/abj.2024.340155

Mleih, N. (2021). The impact of digital transformation on audit quality: An exploratory study by the Delphi methodology. *Scientific Journal of Business Research* , 42(3), 9–36.

- **English References**

Ojeka, S. A., Ben-Caleb, E., & Ekpe, E. O. I. (2017). Cyber security in the nigerian banking sector: an appraisal of audit committee effectiveness. *International Review of Management and Marketing*, *7*(2), 340-346.
https://dergipark.org.tr/en/download/article-file/367549

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems*, *13*(3), 228-243.
https://doi.org/10.1016/j.accinf.2012.06.007

Babiker, I. (2025). The role of internal audit in enhancing cyber security from the auditors' point of view. *Journal of Cybersecurity Research*, 4(1), 127–146.
https://doi.org/10.21608/jcese.2024.321691.1079

Badolato, P. G., Donelson, D. C., & Ege, M. (2014). Audit committee financial expertise and earnings management: The role of status. *Journal of accounting and economics*, *58*(2-3), 208-230. https://doi.org/10.1016/j.jacceco.2014.08.006

Center for Audit Quality, & Deloitte. (2022). Audit committee practices report: Common threads across audit committees. https://www.thecaq.org/wp-content/uploads/2022/01/caq-deloitte-audit-committee-practices-report_2022-01.pdf

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. Current *Issues in Auditing*, 13(2), C1–C9. https://doi.org/10.2308/ciia-52419

Islam, M. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal*, *33*(4), 377-409. https://doi.org/10.1108/MAJ-07-2017-1595

International Institute of Internal Auditors (IIA). (2017). International standards for the professional practice of internal auditing. https://iianigeria.org/ippf-standards-2017

Lankton, N., Price, J. B., & Karim, M. (2021). Cybersecurity breaches and the role of information technology governance in audit committee charters. *Journal of Information Systems*, 35(1), 101–119. https://doi.org/10.2308/isys-18-071

Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D. (2021). Internal auditing and cyber security: Audit role and procedural contribution. *International Journal of Managerial and Financial Accounting*, 13(1), 25–47. https://doi.org/10.1504/IJMFA.2021.116207

Abdulsaleh, A. (2014). Towards an effective audit committee role in corporate governance in Libyan banks: composition criteria and membership requirements. *European Journal of Business and Management*, *6*(38), 157-166. https://core.ac.uk/reader/234626130