International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (4), No. (4)
IJFAES
April 2025
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (4)، العدد (4)

تأثير مخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي في ظل التطورات الرقمية الحديثة: دراسة تحليلية لآراء عينة من المدققين الخارجيين والأكاديميين المختصين

جميلة حمران نامس الجبوري
م.د.، كلية الإدارة والاقتصاد، جامعة الحمدانية، العراق
dr.jamela.aljbury@uohamdaniya.edu.iq

المستخلص

يهدف البحث إلى توضيح تأثير مخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي في ظل التطورات الرقمية الحديثة، من خلال إجراء دراسة تحليلية لآراء عينة من المدققين الخارجيين والأكاديميين المختصين، فيما يتعلق بتأثير تلك المخاطر وإجراءات الحماية اللازمة وتأثيرها على كفاءة وفاعلية المدقق الخارجي، وافترضت الدراسة أن هناك علاقة موجبة بين مخاطر الأمن السيبراني وكفاءة وفاعلية المدقق الخارجي في ظل التطورات الرقمية. وتم اختبار فرضية البحث من خلال الدراسة الميدانية التي أجريت على عينة شملت مجموعة مختارة من المدققين الخارجيين والأكاديميين المختصين، وذلك باستخدام المنهج الوصفي التحليلي، باعتماد استمارة الاستبيان وعلى وفق مقياس ليكرت الخماسي لعينة عشوائية، من خلال توزيع (45) استمارة استبيان، حيث تم استرداد (39) منها كاستمارات صالحة للدراسة أي بنسبة استجابة (86.666%)، فقد كانت إجابات المدققين الخارجيين البالغ عددهم (24) استمارة بنسبة (61.54%)، بينما كانت إجابات الأكاديميين المختصين والبالغ عددهم (15) استمارة بنسبة (38.46%)، وفي حين بلغت الاستمارة الغير صالحة للتحليل (6) استمارات مهملة أي بنسبة (13.333%)، وأن نسبة (86.666%) وهو ما يعد نسبة ممتازة ومقبولة لأغراض البحث العلمي. ولأغراض التحليل تم الاعتماد على البرنامج الإحصائي (SPSS) في تحليل إجابات عينة البحث وعرض النتائج وتفسيرها، ومن أهم النتائج التي توصل إليها البحث:

كانت الأوساط الحسابية المرجحة لجميع فقرات تأثير مخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي في ظل التطورات الرقمية الحديثة، حيث بلغ الوسط الحسابي المرجح العام لكل الإجابات (3.213) وانحراف معياري بلغ (0.635) وقيمة (t) الجدولية (2.089)، وهي نسبة مرتفعة وهذا يشير إلى أن هناك تأثير لمخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي في ظل التطورات الرقمية الحديثة، وفقاً لآراء المدققين الخارجيين والأكاديميين المختصين مما انعكس بشكل إيجابي على النتائج.

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (4), No. (4)
IJFAES
April 2025
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (4)، العدد (4)

وقد أوصت الدراسة بضرورة استحداث قسم أو وحدة خاصة بإدارة مخاطر الأمن السيبراني في كل شركة من الشركات، وإجراء تحديثات مستمرة عليه في ضوء التغييرات والمستجدات التقنية والرقمية الحديثة والتدريب المستمر للكوادر المعنية بالأمن السيبراني، وتطوير مهاراتهم وتوجيههم بخطورة وعواقب التهديدات، والمخاطر والأحداث السيبرانية.

الكلمات المفتاحية: الأمن السيبراني، مخاطر الأمن السيبراني، التقنيات الرقمية الحديثة، المدقق الخارجي.

The impact of cybersecurity risks on the efficiency and effectiveness of external auditors in light of modern digital developments: An analytical study of the opinions of a sample of external auditors and specialized academics

Jamila Hamran Namis Al-Jubouri
Assistant Professor, College of Administration and Economics, University of Hamdaniya, Iraq
dr.jamela.aljbury@uohamdaniya.edu.iq

Abstract

The research aims to clarify the impact of cybersecurity risks on the efficiency and effectiveness of the external auditor in light of modern digital developments, by conducting an analytical study of the opinions of a sample of external auditors and specialized academics, regarding the impact of these risks and the necessary protection measures and their impact on the efficiency and effectiveness of the external auditor. The study assumed that there is a positive relationship between cybersecurity risks and the efficiency and effectiveness of the external auditor in light of digital developments.

The research hypothesis was tested through a field study conducted on a sample that included a selected group of external auditors and specialized academics, using the descriptive analytical approach, adopting a questionnaire form and according to the five-point Likert scale for a random sample, through distributing (45) questionnaire

forms, where (39) of them were retrieved as valid forms for the study, i.e. a response rate of (86.666%), as the answers of the external auditors, numbering (24) forms, were (61.54%), while

The answers of the specialized academics, numbering (15) questionnaires, were (38.46%), while the unsuitable questionnaire for analysis was (6) neglected questionnaires, i.e. (13.333%), and the percentage was (86.666%), which is considered an excellent and acceptable percentage for the purposes of scientific research. For the purposes of analysis, the statistical program (SPSS) was relied upon in analyzing the answers of the research sample and presenting and interpreting the results. Among the most important results reached by the research:

The weighted arithmetic means for all paragraphs of the impact of cybersecurity risks on the efficiency and effectiveness of the external auditor in light of modern digital developments, where the general weighted arithmetic mean for all answers reached (3.213) and a standard deviation of (0.635) and the table value (t) was (2.089), This is a high percentage, indicating that cybersecurity risks are having an impact on the efficiency and effectiveness of external auditors in light of recent digital developments, according to the opinions of external auditors and specialized academics, which has had a positive impact on the results.

The study recommended the creation of a dedicated cybersecurity risk management department or unit in each company, ensuring continuous updates to the department in light of recent technological and digital developments, and providing ongoing training for cybersecurity personnel, developing their skills, and educating them about the seriousness and consequences of cyber threats, risks, and incidents.

Keywords: Cybersecurity, Cybersecurity Risks, Modern Digital Technologies, External Auditor.

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (4), No. (4)
IJFAES
April 2025
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (4)، العدد (4)

تمهيد

بسبب الانتشار الواسع لشبكات الإنترنت وتنوع الخدمات التي تقدمها، ازدادت احتمالات تعرض الشركات للمخاطر والهجمات السيبرانية، التي تهدف إلى سرقة المعلومات والبيانات الخاصة بتطبيقاتها ومواقعها الإلكترونية، وأصبحت جميع الشركات معرضة لهذه الهجمات، مما استدعى ضرورة تأمين المعلومات والبيانات من خلال إنشاء أنظمة وتطبيقات تعمل على حمايتها، وهكذا ظهر مفهوم الأمن السيبراني الذي يتضمن كافة العمليات والتطبيقات والممارسات، الهادفة إلى تأمين المواقع الإلكترونية وحفظ المعلومات، وحماية البيانات وموارد الشركات المعتمدة على الإنترنت.

اليوم ومع التقدم التقني الهائل والمستمر في ظل التطورات الرقمية الحديثة، أصبحت مخاطر الأمن السيبراني تشكل مصدر قلق كبير في مجال التدقيق الخارجي، وجزءً أساسيًا من عملية التدقيق الخارجي في ظل العالم الرقمي، وأصبح يلعب المدققون دورًا حاسمًا في الحماية من التهديدات السيبرانية أكثر من أي وقت مضى، من الضروري أن يبقى المدقق الخارجي على اطلاع دائم بالمخاطر والتهديدات السيبرانية، وأن يعمل على تحديد هذه المخاطر عند ممارسة عملية التدقيق، وتقييم تعرض الشركات للمخاطر السيبرانية ومدى فعالية تدابيرها الأمنية، يتطلب ذلك إجراء تقييمات شاملة لتحديد نقاط الضعف والتهديدات المحتملة بدقة، حيث تُمكّن هذه التقييمات المدققين من تقديم توصيات لإجراءات أمنية قوية، مما يساعد الشركات على حماية أصولها وبياناتها الحيوية بشكل فعال، والذي يُعد أحد الجوانب الأساسية للتدقيق الحديث، يجب على المدققين الاستفادة من التقنيات الحديثة وتعزيز ثقافة الوعي بالأمن السيبراني ومخاطره من خلال ذلك، يمكن للمدققين الخارجيين أن يلعبوا دورًا محوريًا في حماية الشركات بشكل مستمر من التهديدات الرقمية الحديثة.

أولاً: مشكلة الدراسة

نتيجة تزايد اعتماد الشركات باختلاف أنواعها على التقنيات الرقمية الحديثة، وتبعه تزايد المخاطر السيبرانية التي تواجهها وأصبح الأمن السيبراني والمخاطر السيبرانية حديث الساعة، حيث احتل الأمن السيبراني في المرتبة الرابعة من بين أبرز 10 مخاطر متوقعة في العامين المقبلين، والتي تصدرت تقرير المخاطر العالمية 2024م الصادر عن منتدى دافوس العالمي من خبراء المخاطر العالميين وصناع السياسات وقادة القطاعات، كما احتلت المخاطر السيبرانية المركز الأول في الاستبيان العالمي لأعلى المخاطر المتوقعة في 2024، والذي أعده المعهد الدولي للمراجعين الداخليين، ووفقاً للعدد 22 من (يوروموسكو) الصادر من المعهد الأوربي

للبحر المتوسط في يوليو 2021، فإنه من ضمن التحديات التي تواجه منطقة الشرق الأوسط وشمال أفريقيا تحديث مؤسساتها العامة ، لمواجهة التهديدات الجديدة في الفضاء السيبراني(القصير،2،2024)، عليه يمكن صياغة مشكلة البحث من خلال طرح التساؤل التالي:

"ما هو تأثير مخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي في ظل التطورات الرقمية الحديثة"

وينبثق من التساؤل الرئيسي الأسئلة الفرعية التالية:

1. ما هو تأثير مخاطر الأمن السيبراني على عملية تخطيط وتنفيذ التدقيق الخارجي.
2. ما هو تأثير مخاطر الأمن السيبراني على تعزيز ثقافة الوعي بالأمن السيبراني لدى المدقق الخارجي.

ثانياً: فرضيات الدراسة

في ضوء مشكلة البحث يمكن صياغة الفرضية للرئيسية للبحث:

"هناك تأثير لمخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي في ظل التطورات الرقمية الحديثة."

وينبثق من التساؤل الرئيسي الأسئلة الفرعية التالية:

1. هناك تأثير لمخاطر الأمن السيبراني على تعزيز ثقافة الوعي بالأمن السيبراني لدى المدقق الخارجي.
2. هناك تأثير لمخاطر الأمن السيبراني على عملية تخطيط وتنفيذ والإجراءات الميدانية لعملية التدقيق من قبل المدقق الخارجي.

ثالثاً: أهداف الدراسة

يمكن بيان الأهداف التي يسعى البحث إلى تحقيقها وفق التالي:

1. بيان مفهوم الأمن السيبراني وأهميته وأهدافه وأنواعه.
2. تحديد مفهوم وعناصر وأبعاد مخاطر الأمن السيبراني.
3. بيان مفهوم التدقيق الخارجي وأهميته في الشركات باختلاف أنواعها وأحجامها.
4. توضيح مفهوم المدقق الخارجي ومؤهلاته العلمية والعملية ودوره في توكيد صحة القوائم لمالية.
5. توضيح تأثير مخاطر الامن السيبراني على كفاءة وفاعلية المدقق الخارجي في ظل التطورات الرقمية الحديثة.

رابعاً: أهمية الدراسة

تتمثل أهمية البحث بالآتي:

1. بيان مفهوم وأهمية الأمن السيبراني بتطبيقاته المختلفة الذي يؤدي إلى تحسين مستوى الأمان والحماية الخاص بأنظمة وبرمجيات الشركات في ظل التطور الرقمي.
2. توضيح ضرورة قيام الشركات بتطبيق أحدث تقنيات وأنظمة الأمان المتاحة في مجال حماية وأمان الشبكات والبيانات والمعلومات في ظل التطورات الرقمية الحديثة.
3. تسليط الضوء على مخاطر التقنيات الحديثة ومنها مخاطر الأمن السيبراني والحاجة إلى اتخاذ كافة التدابير والإجراءات اللازمة لمواجهة هذه المخاطر.
4. مساهمة هذه الدراسة في زيادة وعي وإدراك إدارة الشركة إلى مخاطر الأمن السيبراني.
5. ندرة الدراسات الأكاديمية من وجهة نظر الباحثة حول موضوع تأثير مخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي في ظل التطورات الرقمية الحديثة.
6. تساهم هذه الدراسة في إجراء المزيد من الدراسات المستقبلية.

خامساً: حدود الدراسة

تم تطبيق البحث ميدانياً على عينة شملت العينة المدققين الخارجيين والأكاديميين المختصين وهم الفئة المستهدفة من تطبيق البحث، علماً بأن البحث أنجز في إطاره الميداني للفترة الزمنية الممتدة من (اب 2024 ولغاية كانون الأول 2024).

سادساً: منهج الدراسة

تم الاعتماد في منهجية البحث على:

- **المنهج الوصفي:** حيث اعتمد المنهج الوصفي في تحديد الإطار النظري العام للبحث، وذلك من خلال الاستعانة بالأطاريح والرسائل الجامعية الدوريات والكتب والمجلات العلمية التي تتناول موضوع البحث.

- **المنهج التحليلي:** من خلال إعداد استمارة استبيان، وعلى وفق مقياس ليكرت الخماسي لعينة في تحليل نتائج الدراسة الميدانية، المستندة إلى آراء عينة من المدققين الخارجيين والأكاديميين المختصين، وباستخدام البرنامج الإحصائي (SPSS) إجابات العينة وعرض نتائج البحث وتفسيرها.

سابعاً: خطة الدراسة

تم تقسيم البحث إلى المباحث الآتية:

- المبحث الأول: الإطار المفاهيمي لمخاطر الأمن السيبراني والمدقق الخارجي والدراسات السابقة.
- المبحث الثاني: الجانب التطبيقي للبحث.

المبحث الأول: الإطار المفاهيمي لمخاطر الأمن السيبراني والمدقق الخارجي والدراسات السابقة

المحور الأول: الإطار المفاهيمي لمخاطر الأمن السيبراني والمدقق الخارجي:

أولاً: الإطار المفاهيمي لمخاطر الأمن السيبراني:

بعد انتشار التقنيات الرقمية الحديثة وشبكة الإنترنت في بيئة الأعمال، وتزايد استخدامها من قبل الشركات والتأثير على العمل المحاسبي ونظم المعلومات، وارتفاع التعاملات الرقمية في جميع الجوانب الخاصة بعمليات الإنتاج والبيع والعمليات المالية، من خلال استخدامها للتعاملات الإلكترونية على الإنترنت، الذي أدى إلى تعرضها لتحديات وتهديدات مرتبطة باستخدام هذه التقنيات في بيئة الأعمال ومنها مخاطر التلاعب بالأنظمة والشبكات، وإتلاف البيانات وضياع المعلومات المهمة والحساسة، الذي نتج عنه زعزعة الثقة في هذه الشركات وتكبدها لخسائر وتكاليف كبيرة.

الأمر الذي دفع الشركات إلى توفير حماية للمعلومات والبيانات وشبكات الحاسب الآلي، والبنى التحتية المرتبطة بها من أجهزة ومعدات، من أي تدخلات غير مصرح به أو غير مقصود بهدف التسبب بأضرار بأمن أنظمة هذه الشركات، ومن هنا ظهر مفهوم الأمن السيبراني والذي يسعى إلى المحافظة على أمن المعلومات والأجهزة والشبكات، والاهتمام بتوفير وسائل وبرامج لحماية عملياتها وخدماتها، من أي تدخل خارجي لتعطيل والأضرار بأنظمتها التقنية، والذي يُعد الآن ركيزة أساسية لمواجهة التهديدات والمخاطر السيبرانية في كل الشركات والمنشآت، بل وحتى الدول لمواجهة الحروب السيبرانية.

في مجال المخاطر الدولية فقد أورد المنتدى الاقتصادي العالمي في تقريره، أن من أكبر المخاطر الرقمية التي تواجه الشركات في العصر الحديث هي مخاطر الأمن السيبراني، بسبب تزايد المخاوف من الهجمات السيبرانية والأضرار والتحريف المتعمد للمعلومات والبيانات، وتُعد هذه المخاطر الأعلى من ضمن قائمة أعلى خمسة مخاطر محتملة الحدوث. (Pwc. wef, 2020, 11). ويرى (الزهراني، 2020: 11) أن الالتزام بمعايير وإجراءات الحماية المتمثلة والواجب اتخاذها، في سبيل مواجهة المخاطر والتهديدات التي يمكن أن تتعرض لها هذه الأنظمة، والحد من الآثار التي يمكن أن تترتب عليها في أقصى الأحوال، فالأمن السيبراني هو إجراءات الحماية التي يمكن من خلالها المحافظة على أمن الشبكات وأنظمة المعلومات والبيانات وجميع الأجهزة المرتبطة بالإنترنت.

وحدد (بجاد، 2017: 6) مفهوم للأمن السيبراني بأنه "قدرة الدولة لإطلاق مصادر قوتها الاقتصادية والعسكرية، الداخلية والخارجية في جميع المجالات لمواجهة المخاطر ومصادرها، في الداخل والخارج سواء في حالة السلم أو الحرب، مع ضمان استمرار وتأمين انطلاق تلك القوى في الحاضر والمستقبل"، أما (فوزي، 2019: 103) فقد عرف الأمن السيبراني بأنه "مجموعة الإجراءات الأمنية والسياسات والمهمات، المبادئ التوجيهية، وتدريبات، وممارسات، ومقاربات إدارة المخاطر، والتقنيات، التي يمكن استخدامها لتوفير الحماية للبيئة السيبرانية والمؤسسات والمستخدمين"، ويؤكد (المطيري) على ضرورة المحافظة على أمن البنى التحتية الحساسة للدولة من هجمات الروبوتات وغيرها، وسواء كانت الجرائم السيبرانية المرتكبة منفذة من جهات حكومية أو غير حكومية. (المطيري، 2022: 999).

في حين أشار (Althonayan, A. & Andronache, A., 2018: 69)، (C, Arnold & ., S, Ursillo,) 2019، (B ., Hasanefendioglu, 73 :2018) إلى مجموعة من المفاهيم والسياسات والضمانات الأمنية، والمبادئ التوجيهية، والأدوات والأساليب، والإجراءات لإدارة المخاطر، وأفضل الممارسات والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمة والمستخدمين، من التهديدات والهجمات الداخلية والخارجية، وتقليل ومنع الأضرار الناتجة عن الوصول غير المصرح، والتي يمكن أن يؤدي إلى تأثيرات سلبية، وخسائر مالية تعرض المنشاة لمواجهة مشاكل تؤثر في تحقيق أهدافها الاستراتيجية، وفقدان سمعتها وتكبدها لمبالغ مالية.

ويتوقف تحقيق الأمن السيبراني على العوامل الرئيسية التالية: أ-سن التشريعات اللازمة لحماية الأمن السيبراني. ب-تحقيق التنسيق والتعاون بين الجهات المعنية (القطاع الخاص والقطاع العام). ت-توافر

الأدوات التقنية اللازمة لتحقيق الأمن. ث-التنسيق الدولي. ج-قياس الكفاءة بصورة دورية. ح-نشر الوعي بالأمن السيبراني وإذكاؤه. وتُعد المخاطر والتهديدات المحتملة التي تضم الهجمات الإلكترونية، واختراق البرمجيات المشفرة والقرصنة، والفيروسات، والسرقة، والتزوير للبيانات والمعلومات، من المخاطر السيبرانية التي لم يقتصر منفذو هذه الهجمات على الهواة والنشطاء، بل أصبحت تصنف كحروب سيبرانية تديرها دول ومنظمات، ينتج عنه زعزعة الثقة والتسبب بخسائر مالية كبيرة (شحادة، 2022).

توفر تقنية المعلومات والاتصالات إمكانيات ضخمة وغير مسبوقة، لتحسين الإنتاج في جميع القطاعات، وللتواصل عبر القارات، إلا أن مخاطرها تؤثر على أمن النظم والمعلومات والبيانات وسريتها، ويمكن اعتبار المخاطر السيبرانية من المخاطر التشغيلية، التي تضم مخاطر الممتلكات والخصوم، بالإضافة إلى المخاطر الكارثية والتشغيلية التي يغطيها التأمين، ومع ذلك فإن البنية التحتية لهذه التقنيات، تمثل ارتباطًا بين مصالح متعددة وخدمات متنوعة لدول عديدة، مما يجعل المخاطر في المجال السيبراني مخاطر عالمية، لا يمكن لأي جهة أن تضمن سلامتها بعيدًا عن هذه الأخطار، ما دامت سلامة الآخرين معرضة للخطر، Hartmann, C.C., & Carmenate, J. (2021: 9-23)، وهناك جانب آخر للمخاطر هو "الإرهاب السيبراني فهو يُعد تهديد مادي، ومعنوي، أو عدوان، قد تنظمه دول أو مجموعات أو أفراد باستخدام الوسائل والبرامج الإلكترونية، الغرض منه بث الرعب والخوف، والتأثير بشتى أنواع وصور الفساد على الإنسان في معتقداته ودينه وعقله، وقد تشمل التأثير على سمعته وابتزاز أمواله" (السيد، 2021: 49). تؤدي الحوادث والجرائم المرتبطة بالأمن السيبراني إلى أضرار كبيرة، في الشركات وتكبدها خسائر متعددة ترتبط بالقيمة السوقية، فضلاً عن التكاليف المرتبطة بها من غرامات وتكاليف إصلاح الأضرار (Pierangelo Rosati et al., 2020, P.5).

ويتوقع أن ترتفع تكاليف جرائم الأمن السيبراني، والتي تشمل بالإضافة إلى ذلك تكاليف معالجة وإصلاح الأضرار التي تصل إلى 10.5 تريليون دولار سنوياً بحلول عام 2025، خاصة مع ارتفاع مخاطر الأمن السيبراني وتزايد خطورتها، والعواقب المترتبة على حدوثها التي شملت عدد من الهجمات، كانت وكالات حكومية وشركات كبرى من بين ضحاياها، والتي وثقتها التقارير الصادرة عنها، رغم التزايد الكبير في الإنفاق السنوي العالمي الذي تجاوز أكثر من 150 مليار دولار، على برامج وخدمات الأمن السيبراني ومنتجاتها (Zeijlemaker, al, et, 2023)، (Chertoff, 2023).

وعند البحث عن العوامل والأسباب التي تساهم في زيادة وقوع المخاطر السيبرانية، نلاحظ أن بعضها ينتج بسبب أخطاء من الأفراد العاملين بالشركة، بالإضافة إلى المشاكل التقنية، وفيما يلي توضيح لتلك العوامل والأسباب: https://bakkah.com/ar/knowledge-center

1. فقدان البيانات الهامة بسبب حدوث عطل أو توقف في الشبكات.
2. الاستخدام لأجهزة الشركات في أماكن بعيدة أثناء العمل في المنزل أو السفر.
3. القصور في معرفة التحديثات في سياسات الأمن السيبراني أو عدم الاطلاع عليها أو مراجعتها سنوياً.
4. عدم إيلاء الاهتمام بتحديث كلمات المرور بشكل مستمر.
5. إمكانية الدخول إلى الخيارات الإدارية الخاصة من قبل أحد الموظفين الغير مختصين على أنظمة الأمن السيبراني.

أما الحلول العلاجية والاحترازية التي يمكن اتخاذها ضد هجمات الأمن السيبراني فيمكن تحديدها بالآتي:

1. منع الانتهاكات أو تقليل تكلفة عواقبها: إن تطبيق الشركات لاستراتيجيات الأمن السيبراني يساهم في التقليل من العواقب الغير مرغوبة بها الناتجة عن الهجمات السيبرانية، التي قد تؤثر في العمليات التجارية، والوضع المالي لها، كما تؤثر على سمعة الشركة وثقة العملاء بها.
2. ضمان الامتثال للوائح التنظيمية: لضمان حماية البيانات الهامة والحساسة من المخاطر السيبرانية المحتمل حدوثها، على الشركات الامتثال للمتطلبات التنظيمية في المجالات الضرورية والمحددة.
3. الحدّ من التهديدات السيبرانية المتطوّرة: تتبنّى لتدابير الأمن السيبراني وتحديثها باستمرار لمواكبة تقنيات وأدوات الهجوم الرقمي الجديدة والمتطورة، إذ تنشأ أشكال جديدة من الهجمات السيبرانية مع تغيّر التقنيات، بسبب ابتكار استراتيجيات وأدوات جديدة، يستخدمها المجرمون للوصول إلى النظام بدون إذن.

تتعرض الشركات لأشكال متعددة من مخاطر الأمن السيبراني، ومن أشهر هذه الأنواع ما يلي: (https://bakkah.com/ar/knowledge-center)

1. التنصت: تتعرض الأنظمة الإلكترونية للتنصت بهدف سرقة المعلومات الهامة والبيانات، إذ يمكن اختراق كلمات المرور والوصول إلى المعلومات المرسلة، والتنصت على المخاطبات المتبادلة بين المستخدم والمواقع المضيفة.

2. سرقة كلمة المرور: إن سرقة كلمة المرور واختراق المواقع الإلكترونية أسلوب شائع يعتمده المخترقون، بهدف سرقة البيانات الهامة والضرورية للمستخدم، وكلما كانت كلمة المرور سهلة كلما كان اختراقها سهلاً، فقد يحدث الوصول إلى كلمة المرور عبر التنصت أو من خلال التخمين.
3. البرامج الضارة: لا تخلو المخاطر السيبرانية من البرامج الضارة التي يستهدفها المجرمون الإلكترونيون، بغرض سرقة البيانات الهامة للمستخدمين، والتي قد تكون بيانات شخصية، أو مصرفية، وتنشأ البرامج الضارة جراء وجود جزء معين داخل البرنامج المثبت، يكون غير مألوف واطلاقه يلحق أضرار بالأجهزة.
4. عمليات الاحتيال: قد يلجا بعض المجرمون الإلكترونيون إلى أساليب احتيال منها، إرسال رسالة من خلال البريد الإلكتروني تطلب تعبئة البيانات من قبل المستخدم، وكثيرًا ما يقع المستخدمون في هذا الفخ، مما يجعلها من أكثر الوسائل الناجحة في المخاطر السيبرانية.
5. الهجوم عبر المواقع: عند الرغبة في سرقة بيانات المستخدمين، أو إلحاق الضرر بخدمات الموقع، قد يلجا المجرمون الإلكترونيون لاستهداف المواقع غير المشفرة، باستخدام أكواد محددة لتعطيل الموقع، وإرسال الأكواد إلى الموقع من أجل تعطيل وسرقة المعلومات الضرورية.
6. الهندسة الاجتماعية: قد يتم الحصول على كلمة المرور باستخدام الهندسة الاجتماعية، أو مواقع التواصل الاجتماعي لتنفيذ عمليات الاحتيال، للوصول إلى جهاز المستخدم والدخول على بياناته المصرفية وسرقتها.

كما صنفت المخاطر السيبرانية من قبل (Muravskyi, 2021) بأنها:

1. السرية: تمتلك أغلب الشركات بيانات سرية ومعلومات قد يسبب الكشف عنها أضرار على الميزة التنافسية للشركة، وإيراداتها وقيمتها في السوق، إذا تم اختراق السرية من قبل أشخاص غير مصرح لهم، ولذلك يجب تحديد الأشخاص المصرح لهم بالدخول والحصول على المعلومات من قبل الشركة.
2. النزاهة: تتمثل بالمخاطر المرتبطة بالنزاهة والتي تسبب ضرراً، كالتزوير والاحتيال وسرقة المعلومات البيانات.
3. القدرة على الوصول: يُعد تعطل الأنظمة الإلكترونية وعدم إمكانياتها على أداء خدماتها، أحد المخاطر المرتبطة بالأمن السيبراني، المتمثلة بعدم الوصول للمستخدمين المصرح لهم إلى الأنظمة الإلكترونية، متى وأينما يحتاجون إليها.

في حين يمكن استعرض أهم مخاطر اختراقات الأمن السيبراني والتي تتمثل بالآتي: (Van Wyk, 2021) (Conteh & Schmick, 2021) (&Fonseca, Alic ,2021)

- مخاطر انتهاك الخصوصية: مع التزايد في مخاطر الابتزاز وسرقة للبيانات الشخصية، بسبب صعوبة المحافظة على الخصوصية الشخصية في العالم الرقمي، فإن مخاطر الانتهاك تعتبر أحد حالات الاختراق للأمن السيبراني.
- مخاطر تأمين البيانات والمعلومات: من ميزات التقنية الرقمية قدرتها على جمع وتخزين كميات هائلة من المعلومات ولبيانات، والتي قد تكون معلومات خاصة مرتبطة بالشركات والأفراد، ويكون الحفاظ على أمان هذه البيانات مهم جداً، قد يسبب الاختراق الحصول على كميات ضخمة من المعلومات الخاصة، إلى الخصوم والشركات المنافسة وجهات أخرى.
- مخاطر انتهاك حقوق الملكية الفكرية: نسخ الوسائط والبيانات الرقمية، أو إعادة إنتاجها أصبح سهل الحدوث في عصر الرقمنة، بسبب صعوبة تطبيق قوانين حقوق وتأخر التشريعات القانونية في الجانب الرقمي، وبالتالي فإن حماية الملكية الفكرية والأدبية والمؤلفات للأفراد والشركات في العالم الرقمي، تمثل نقلة رقمية حديثة لتوفير الحماية من مخاطر الانتهاك.
- مخاطر عدم الكشف عن الهوية: إخفاء هويات المستخدمين أحد المجالات الواسعة التي توفرها التقنية الرقمية، وتشير الكثير من الدراسات إلى فرض عقوبات متشددة على مخاطر عدم كشف الهوية.

ثانياً: الإطار المفاهيمي للتدقيق الخارجي والمدقق الخارجي:

مع تطور معالم الحياة الإنسانية في مختلف المجالات والنواحي الاقتصادية والاجتماعية والمالية والقانونية، ظهر التدقيق الخارجي كأحد أشكال الرقابة وحظي باهتمام واسع وكبير كل شركة من الشركات، بغض النظر عن نوعها وحجمها والتي تهدف إلى توفير الحماية لأموال الشركة ومساعدتها في اتخاذ القرارات المختلفة، وتتم عملية التدقيق الخارجي من خلال التعاقد مع شركة محاسبية مستقلة مختصة ومحايدة للقيام بعملية الفحص والتدقيق المطلوبة (https://hbrarabic.com).

ونتيجة للتطورات الرقمية الحديثة وما أحدثته من تغييرات كبيرة في كافة المجالات، ومنها ما أحدثته من تأثير على التدقيق الخارجي، حيث كان هناك سعي متواصل من قبل المنظمات الهيئات المهنية المختصة في مجال التقنيات الرقمية الحديثة، للقيام بوضع برامج لإدارة الأمن السيبراني والمخاطرة المرتبطة به، وفقاً

للمعايير والقواعد المهنية المناسبة باعتبار مخاطر الأمن السيبراني (مخاطر أعمال)، فهي ذات أهمية لا تقل عن المخاطر المالية والتشغيلية ومخاطر السمعة، كما أدى إلى قيام الجهات المهنية المختصة بمهنة المحاسبة والتدقيق والباحثين في مجال الفكر المحاسبي والمالي الأخذ بموضوع الأمن السيبراني، منطلقين بذلك من منهج إمكانية وجود تأثير لمخاطر الأمن السيبراني على الشركات والمؤسسات بياناتها ومعلوماتها تقاريرها المالية، ووالذي ينعكس على أعمال المدقق الخارجي، حيث تم إصدار دليل الأمن السيبراني من قبل المعهد الأمريكي للمحاسبين المعتمدين، وذلك استجابة للضرورات التطبيقية وحاجة مهنة التدقيق، ويجب على المدقق الانتباه بشكل خاص إلى الانتهاكات والحوادث السيبرانية وهذا ما أكد عليه مركز جودة المراجعة، ويمكن أن يكون للمدقق الخارجي دوراً مهماً في الحد أو منع أو التخفيف من آثار هذه الانتهاكات والحوادث من خلال العمل على توفير ضمانات إضافية خاصة بموضوع ضوابط التقنيات الرقمية الحديثة، وقد قام (AICPA, 2016) بإصدار إطار عمل لإعداد التقارير الخاصة بإبلاغ إدارة الشركة ومجلس الإدارة بمخاطر الأمن السيبراني (علي، 2023: 4). ولقد عقدت الجهات المهنية المختصة بمهنة المحاسبة والتدقيق عدة ندوات ولقاءات لمناقشة موضوع الأمن السيبراني والمشاكل الناتجة عنه، والتحديات التي تواجه الشركات والأسواق المالية، وآثارها المحتملة على البيانات والمعلومات وإعداد التقارير المالية والحلول اللازمة لمعالجة تلك القضايا والتحديات (PCAOB. 2014: 2013) (IFAC. 2019) (CAQ. 2014: 2016: 2017): وتوصلت تلك المناقشات والندوات إلى أن تهديدات الأمن السيبراني هي من أكبر المخاطر التي تواجه الشركات والأسواق المالية والتي تنعكس على أداء الشركات وإعداد تقاريرها المالية ومهنة التدقيق. وعليه تُعد مخاطر الأمن السيبراني خطراً لا يمكن تجاهله وذات أهمية كبيرة.

وأشارت الدراسات (Roskot et al 2021) (Singh, 2019) (Smith, 2024) إلى مخاطر الأمن السيبراني وأن تلك المخاطر لها تأثير على أداء الشركات حيث تؤدي إلى انخفاض المبيعات أو الأرباح، أو الإضرار بسمعة الشركة، ويُعد هذا من أخطر نتائج التهديدات واختراقات الأمن السيبراني، حيث ينعكس ذلك إلى فقدان ثقة العملاء بالشركة، وبالتالي، خسارة الأرباح وهذا يفقد الشركة قدرتها على الاستمرار، وعلى الرغم من ذلك، لا تهتم الشركات اهتمام كافي بمخاطر الأمن السيبراني، وأن نقص المعرفة لدى الشركات بمخاطر الأمن السيبراني، يُعد من الأسباب الرئيسية لحدوث الخروقات الخاصة بجرائم لأمن السيبراني، وفي الوقت الحاضر ومع ارتفاع معدل التغير السريع لاختراقات الأمن السيبراني، إن مخاطر الأمن السيبراني أصبحت تمثل تهديد كبير لغرض استمرار الشركات في نشاطها، ويترتب على ذلك تحمل الشركات لتكاليف عالية وذلك في حالة تعرضها للاختراق (Elnagar al et 2024)، وأكدت دراسة (K. Hamm, 2019) بأن المدقق الخارجي يركز على عملية إعداد

التقارير المالية عند استخدام تقنية المعلومات والضوابط التقنية المتعلقة بتلك التقارير مثال ذلك الضوابط المتعلقة بموثوقية البيانات والتقارير المالية الأساسية، وعند القيام بعملية التدقيق الشامل حيث يقوم المدقق بتقييم نظام الرقابة الداخلية على التقارير المالية بشكل منفصل، وعندما تكون الشركات كبيرة الحجم، وأكثر قيمة، وضمن قطاع صناعات قليل القدرة على المنافسة وتمتلك المزيد من الأصول غير الملموسة وأقل عرضة للقيود المالية، تكون عندئذ الشركات أكثر عرضة للهجمات السيبرانية (Kamiya et al ,2021) (Harris et al.2023).

وكما هو معلوم بأن المدقق الخارجي يكون مسؤول عن تحديد مصداقية وعدالة القوائم المالية وخاصة المعتمدة من جهات خارجية، حيث يكون مستقل تماماً عن إدارة الشركة، في حين المدقق الداخلي يكون مرتبط بإدارة الشركة ويخدم توجهاتهم ويقدم لها البيانات والمعلومات اللازمة https://www.a-h-g.net/ar/news، وأشارت هيئة خبراء المحاسبين المعتمدين الفرنسية إلى مهنة التدقيق الخارجي بأنها "عملية إبداء الرأي المهني من قبل شخص مهني مؤهل ومستقل، حول انتظام الحسابات الختامية لشركة معينة وخلال فترة زمنية معينة" (رفاعة، 2017:15)، ويرى (مسعد والخطيب، 2009 :61) بأن المدقق الخارجي شخص مهني مستقل من خارج الشركة محل المراجعة والتدقيق، يتم تكليفه للقيام بعملية التدقيق بواسطة الملاك، وأن يتمتع بالاستقلالية الكاملة في ممارسة مهامه لتحقيق الهدف الرئيسي في إبداء الرأي الفني المحايد في سلامة وصدق تمثيل القوائم المالية التي تم إعدادها من الإدارة عن نتيجة الأعمال والمركز المالي للشركة محل التدقيق فضلاً عن تدقيق القوائم المالية للشركة، يمكنه القيام بمهام تدقيق الالتزام والتدقيق التشغيلي لنفس الشركة، كما يمكنه القيام بمزاولة عملية التدقيق كفرد أو من خلال عضويته في شركة ويزاول مهنته هذه بترخيص معتمد وفقاً لقوانين لمزاولة المهنة، ويطلق على المدقق الخارجي أسماء منها: (محاسب معتمد، محاسب قانوني، مراجع حسابات، مراقب حسابات، محافظ حسابات)، في حين أن (سواد، 2009: 122) حدده بأنه "شخص أو مجموعة الأشخاص الذين يقومون بمهنة المراجعة شريطة أن تتوفر فيهم، جميع ما تطلبه قواعد المراجعة المتعارف عليها والمتعلقة بالشخص المراجع القواعد العامة للمراجعة، التأهيل العلمي والمهني، الاستقلالية، والعناية المهنية".

وهناك مجموعة من الصفات التي يجب أن يتحلى بها المدقق الخارجي وهي كالآتي (مسعد والخطيب، 2009: 61) (العبيدي وعويد، 2021: 76):

1. الحفاظ على أسرار العميل الذي يدقق أعماله وألا يتم الإفصاح عن أية معلومات يطلع عليها خلال تأدية عمله.
2. أن يكون المدقق عملي ومواكب لكل ما هو جديد في القوانين والتشريعات.
3. أن يكون مهنياً وكفأً يمتلك المؤهلات الأكاديمية والمهنية، التي تؤهله بأن يكون قادراً على التعامل مع الأدلة بشكل موضوعي ودقيق.
4. أن يتمتع بالحرية غير تابع لأي جهة كانت مستقل بقراراته، وأن يهتم بمصلحة عمله على مصالحه الشخصية.
5. أن يكون صبوراً، حيث أن طبيعة عمله روتينية مما يؤدي إلى الملل.
6. أن يقوم بتأدية عمله في مجال اختصاصه، وتقديم المشورة عندما يطلب منه إذا كانت مرتبطة بعمله.
7. أن يكون قادراً على التعبير عن رأيه بكل دقة ووضوح واستقلالية، ولبقاً في التعامل مع الآخرين.
8. أن يكون أمين وواقعي عند التعامل مع عميله، ولا يقبل عمل لأي عميل أو جهة معينة إلا بعد أن يتفهم طبيعة نشاط العميل وأن يقتنع بصحته.

في حين أن هناك العديد من الحقوق والواجبات المترتبة على المدقق الخارجي وتتمثل بالآتي (محمود وآخرون، 2011: 113):

1. يحق له الاطلاع وطلب البيانات والإيضاحات اللازمة لعملية التدقيق.
2. يحق للمدقق الحصول على صورة من الإخطارات المرسلة للمساهمين.
3. يحق له دعوة الجمعية العامة للمساهمين لمناقشة كافة التفاصيل الخاصة بعملية التدقيق وبيان المعوقات والانحرافات.
4. تحديد وقت إجراء الجرد لكافة الأصول الخاضعة للجرد في الشركة.

ويتوجب عليه أداء الواجبات المترتبة على عاتقه ويمكن بيانها وفق التالي:

1. حضور اجتماع الهيئة العامة لمساهمي الشركة.

2. القيام بمراجعة أصول وخصوم الشركة.
3. مراقبة سير أعمال الشركة ومراجعة حساباتها.
4. فحص الأنظمة المالية والإدارية للشركة.
5. إعداد تقرير التدقيق.
6. الالتزام بأصول وقواعد المهنة.

كما ينبغي على المدقق الخارجي الالتزام والامتثال للمعايير المهنية المختصة والتي تتمثل بالآتي: (فايز، 2015: 206)

1. يمتثل المدقق لكافة معايير التدقيق الدولية ذات العلاقة بالتدقيق، ويكون معيار معين مرتبطاً بعملية التدقيق عندما يكون نافذ المفعول وتكون الظروف التي يتناولها المعيار قائمة.
2. حصول المدقق على فهم حول كامل نص معيار تدقيق دولي معين بما في ذلك التطبيق والمادة التوضيحية الأخرى، وذلك في سبيل فهم أهدافه وتطبيق متطلباته بالشكل الملائم.
3. ينبغي أن يعرض المدقق امتثاله لمعايير التدقيق الدولية في تقرير التدقيق، إلا في حال امتثاله لمتطلبات هذا المعيار وكافة المعايير ذات العلاقة بالتدقيق.

ولكي يقوم المدقق بتنفيذ عملية التدقيق والمهام الموكلة اليه يجب القيام بجمع المعلومات التي تمكنه من التعرف على طبيعة الشركة ونظمها الإدارية والمالية والقانونية وذلك من خلال الآتي: (أبو سرعة، 2010: 77): https://www.a-h-g.net/ar/news

- الاطلاع على التقارير المالية للشركة ولعدد كافي من السنوات، ومقارنتها مع الشركات المماثلة والتي لها نفس الظروف ونفس النشاط، وإجراء دراسة لعدد من محاضر مجلس الإدارة والجمعية العامة للمساهمين.
- دراسة تقارير المدقق الداخلي وتحليلها والتعرف على هيكل إدارة التدقيق الداخلي ومسؤوليته، ودراسة الهيكل التنظيمي للشركة، وتحليل خطوط الاتصال والسلطات والمسؤوليات.

- دراسة أوراق العمل الخاصة بتدقيق السنوات الماضية، وإجراء تحليل للسياسات الإدارية للشركة، وذلك من خلال الدليل الخاص بالسياسات والقوانين والأنظمة الداخلية في الشركة.
- إجراء زيارات متعددة للشركة محل التدقيق والمراجعة، وذلك لغرض التعرف والوقوف على مختلف الظروف والأحوال التي تعمل في ظلها، كالظروف المالية، والاقتصادية، والاجتماعية، والقواعد والسياسات المحاسبية الخاصة بالشركة.
- الاتصال المباشر ببعض المسؤولين والموظفين في الشركة، وذلك للاستفسار عن أي ملاحظات أو أمور تبدو غامضة للمدقق الخارجي.
- القيام بالتدقيق النظام المالي المطبق ونظام الرقابة الداخلية المعتمد للشركة، وتدقيق المستندات المؤيدة للقيود المحاسبية والمطالبات المالية، وتدقيق اكتمال الشروط المالية والقانونية ومطابقتها للمعايير المحاسبية.
- إجراء تدقيق للقوائم المالية والحسابات الختامية في ضوء الموازنة السنوية والنظام المالي المطبق، والقيام بإعداد التقارير الخاصة بنتائج التدقيق وفحص الدفاتر والسجلات المالية، وتحليلها وتقديم الاقتراحات والتوصيات اللازمة.

ويجب على المدقق الخارجي أن يكون على إلمام بكل مقومات مهنة المراجعة والتدقيق وتقنية المعلومات، كاستخدام البرامج الجاهزة، والتدقيق عن بعد، وتبنى عملاء ممن دقق حساباتهم لأدوات تقنية المعلومات (Maffei et al, 2021)، ساعد التقدم التقني وتطوره السريع الذي شهدته جميع المجالات العلمية والمهنية، وذلك للتحول من النمط التقليدي إلى الطرق التقنية الحديثة، إلى حاجة المدققين الخارجيين ولضمان تطبيق ذلك بدرجة عالية من الكفاءة والفاعلية والدقة، التوجه نحو إجراء التدريب المستمر، وزيادة المعرفة نحو تطبيق أدوات التقنية الحديثة، فضلاً عن تطوير معايير التدقيق الخاصة بذلك، بالإضافة إلى تطوير الجودة الخاصة بالأحكام المهنية، واستخدام الوسائل الخاصة بدعم القرارات في جمع الأدلة وتنفيذها، وهو ما سيتم بيانه وفق الآتي (عبدالحليم وآخرون، 2024: 11-12) (سعاد وكهينه، 2022، 48) (عبدالحفيظ ومرزوق، 2020، 9):

1. التأهيل العلمي والعملي المستمر للمدقق الخارجي: لغرض ضمان تحقيق المدقق الخارجي لدرجة عالية من الكفاءة المهنية، يجب أن يكون لديه القدرة على تطوير مهاراته، وزيادة مستوى المعرفة العلمية والعملية، وذلك لمواكبة التغيرات والتطورات التقنية الحديثة في مهنة التدقيق، لذلك ينبغي تفعيل وتطبيق برنامج شامل للتدريب المستمر داخل مكاتب المحاسبة والتدقيق.

2. التوجه نحو ممارسة التدقيق المستمر: فقد ساعد التقدم السريع في مجال تقنية المعلومات، وظهور الشبكة الدولية للمعلومات وتبادل البيانات الإلكترونية، إلى التحول الملموس من الأسلوب التقليدي إلى الأسلوب الإلكتروني، حيث استطاعت الشركات من الحصول على دفعة قوية لإطلاق مواقعها الإلكترونية على شبكة الإنترنت، وذلك لتحقيق مزايا اقتصادية وتنافسية، وهذا أدى إلى ظهور كميات كبيرة من البيانات الكمية والوصفية، ومحتوى متعدد الوسائط مثل: الصور، ومقاطع الفيديو، هذا التحول الكبير انعكس على المعلومات المحاسبية، حيث تحولت من النمط الورقي إلى النمط الإلكتروني، ونتيجة لذلك تطلب الأمر القيام بتحسين المداخل التقنية الحديثة لتدقيق الحسابات، ومن بين هذه المداخل: مدخل التدقيق المستمر حيث يمكن للمدققين الخارجيين الانتهاء من عمليات التدقيق بكفاءة عالية، وتقديم تقارير مستمرة حول جميع تعاملات الشركة وتحديثاتها، ولضمان اتخاذ القرارات المناسبة في الوقت المناسب.
3. تطوير معايير التدقيق لمواكبة التطورات الرقمية الحديثة: لا تزال هناك ضرورة لتطوير معايير التدقيق، وذلك لضمان تحقيق الاستفادة القصوى من أدوات تحليل البيانات، ومواكبة التطورات الرقمية والتقنية الحديثة، وتعزيز إجراءات عملية التدقيق.
4. تطوير جودة أحكام المدققين الخارجيين المهنية: حتى يتم تطوير جودة أحكام المدققين الخارجيين المهنية، هناك تحديات تواجه بيئة ممارسة عملية التدقيق الخارجي، عليه يجب تطوير الوضع المهني بحيث يكون هناك توافق، بين دستور مهنة المحاسبة والتدقيق مع التطورات الرقمية والتقنية الحديثة التي يشهدها العالم الحالي.
5. استخدام وسائل دعم القرار في جمع الأدلة وتنفيذها: نتيجة التطورات الرقمية والتقنية الحديثة ظهرت بعض التقنيات التي تتضمن تحليل البيانات في ظل زيادة حجم البيانات والتي تساعد عند إجراء عملية التدقيق ومن أبرزها: أ-تقنية تعلم الآلة learning Machine (ML) للتعرف على الأنماط والتمثيل المرئي للبيانات، ب-تقنية التنقيب في البيانات mining Data (DM) حيث يمكن تطبيقها في عملية التدقيق من خلال، استخدام الشبكات العصبية، وشجرة القرارات، في الكشف عن البيانات المضللة في القوائم المالية)، ت-تقنية سلاسل الكتل Computing Cloud (حيث أنها تعد وسيلة حيوية تقوم بتوفير مساحات تخزينية للبيانات الكبيرة، يمكن الاستفادة منها كبنية تحتية لتنفيذ عملية التدقيق بكفاءة وفاعلية).

وفقاً للدراسات التالية: (فرج، 129،2022) (Haapamaki& Sihvonen, 2019) (No & Vasarhelyi, 2017) (Aldorisio,2020) (Rosati,2019) يشتمل نموذج توكيد المدقق الخارجي على مزاعم الإدارة عن إدارة مخاطر الأمن السيبراني على ثلاثة عناصر أساسية تتمثل في:

أ. **طبيعة توقيت التقرير:** بما أن تهديدات ومخاطر الأمن السيبراني مرتبطة بفترة زمنية وتعتمد على متغيرات متعددة منها: الخصائص التنظيمية، طبيعة العمليات المعرضة للخطر خلال فترة معينة، يجب أن يكون تقرير المدقق الخارجي معبراً عن استنتاجه للفترة الزمنية الممتدة على طول فترة تكليفه بعملية التدقيق وإتمامها.

ب. **طبيعة استنتاج المدقق:** كما هو معروف فإن تقارير التدقيق التقليدية ترتكز على إبداء الرأي حول عدالة (عادلة /غير عادلة) التقارير المالية، ومدى تعبيرها عن المركز المالي ونتائج الأعمال، وهذا ما لا ينطبق على حالة التوكيد على إدارة مخاطر الأمن السيبراني، حيث أنها عملية مستمرة متغيرة، لا تأخذ حكماً واحداً على طول الوقت، وإنما من الأفضل وجود تدقيق فوري مستمر لحالة درجة الأمن السيبراني، والتعبير عن تلك الحالة في أوقات مستمرة ومتتالية.

ت. **الأهمية النسبية**: حيث تنص معايير التدقيق المقبولة قبولاً عاماً على مفهوم الأهمية النسبية للعناصر، والذي يفسر عادة كنسبة من: الدخل، أو من إجمالي الأصول، وهذا الأمر لا يصلح تطبيقه مع التوكيد على إدارة مخاطر الأمن السيبراني، فهناك عناصر لا يمكن قياسها نقداً مثل: (الاستدامة، سلاسل التوريد، العلامات التجارية، إدراك المخاطر)، وبالتالي لا يمكن أن يصلح مفهوم الأهمية النسبية في هذه الحالات.

ومن الطرق المستخدمة لتدقيق الأمن السيبراني في الشركات الآتي (محمود وآخرون، 2025: 840):

- تدقيق السياسات الخاصة بأمن البيانات عند البدء بعملية التدقيق من حيث (السرية والسلامة والإتاحة).
- يتم تصنيف البيانات وتحديد مستويات الأمان الخاصة بها، والالتزام بحمايتها، وتفاصيل هيكل الشبكة.
- العمل على جمع سياسات الأمن السيبراني ومتطلباتها في وثيقة واحدة، وذلك للحصول على فهم شامل للممارسات الخاصة بأمن تقنية المعلومات لتحديد نقاط الضعف الموجودة بها.
- إجراء تدقيق لمعايير مخاطر الأمن السيبراني للشركة (معايير الوصف).
- القيام بإنشاء قائمة بأفراد المسئولين عن الأمن السيبراني من حيث مسئولياتهم وواجباتهم.

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (4), No. (4)
IJFAES
April 2025
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (4)، العدد (4)

المحور الثاني: الدراسات السابقة

ت	اسم الباحث والسنة	هدف الدراسة	أهم نتائج الدراسة
-1	دراسة محمود (2025)	دراسة أثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارات المستثمرين، وتحقيقاً لأهداف الدراسة، ومن أجل اختبار الفروض اعتمدت الدراسة على الدراسة التجريبية، وتمثل مجتمع الدراسة في المستثمرين وشكلت عينة الدراسة (75) مفردة صحيحة.	توصلت الدراسة: إلى أهمية توكيد المراجع الخارجي عن مخاطر الأمن السيبراني، وإلى أهمية الإفصاح عن مخاطر الأمن السيبراني في الشركة، وأهمية قيام الإدارة بالتقييم الذاتي لنظام إدارة مخاطر الأمن السيبراني، لتحديد ما إذا كان هناك أوجه ضعف جوهرية في هذا النظام واتخاذ ما يلزم من إجراءات للتغلب على أوجه الضعف في برنامج إدارة مخاطر الأمن السيبراني، كما وتوصلت نتائج الدراسة التجريبية: إلى وجود إلى وجود تأثير لتوكيد المراجع الخارجي، عن مخاطر الأمن السيبراني معنوياً على قرارات المستثمرين.
-2	دراسة عثمان (2023)	هدفت الدراسة إلى اختبار أثر توكيد المراجع الخارجي على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين في الأسهم، وكذلك اختبار أثر مستوى الخبرة والتأهيل العلمي للمستثمر كمتغيرات وسيطة على العلاقة محل الدراسة، وتم إجراء دراسة تجريبية باستخدام عينة من 100 من المستثمرين في بيئة الأعمال المصرية عن عامين، 2019، 2020.	وتوصلت الدراسة: إلى وجود علاقة معنوية إيجابية بين التوكيد المهني للمراجع الخارجي على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني ورغبة وقرارات المستثمرين بالأسهم، حيث أصبح الإفصاح عن مخاطر الأمن السيبراني التي تواجهها الشركات، ومعرفة كيف تدير الشركات أعمالها على الشبكات، وما تواجهه من مخاطر أمنية قد تؤدي إلى خسائر مالية ضخمة، وفقد السمعة والإضرار بالقدرة التنافسية للشركة ذا أهمية متزايدة، للمستثمرين والحكومات والمستهلكين والبائعين وأصحاب المصلحة الآخرين، لإصدار قرارات وأحكام سليمة والتأثير على سعر السهم، وقيمة المساهمين في الأجل الطويل، وضرورة التوكيد على إفصاحات وإدارة مخاطر الأمن السيبراني، بما يعمل على تعزيز سلامة وموثوقية التقارير المالية ومستوى الشفافية وتقليل مستوى عدم تماثل المعلومات، بين المديرين وأصحاب المصلحة بشكل عام وعلى قرارات وأحكام المستثمرين بشكل خاص، وزيادة الثقة والرغبة في الاستثمار في أسهم الشركات.
-3	دراسة على (2023)	استهدفت الدراسة: التوصل لمنهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل بالبيئة المصرية، وعلى ذلك تناولت الدراسة النظرية انعكاسات مخاطر الأمن السيبراني على أعمال المراجع الخارجي وخطوات المنهج المقترح، واعتمدت منهجية الدراسة التطبيقية على شركات المساهمة المقيدة في البورصة المصرية، والعاملة في القطاعات والنشطة المرتبطة	توصلت الدراسة: إلى أن تقييم مخاطر الأمن السيبراني يعتمد على عمليات الدراسة ل (20) شركة المراجعة التي تدرس، وتقيم مجموعة من الضوابط المحددة مسبقاً في مجموعة متنوعة من الموضوعات المتعلقة بالأمن السيبراني، كما أوضحت نتائج التحليل الإحصائي وجود تأثير طردي معنوي، لمخاطر هجمات الأمن السيبراني بمنشأة العميل على أعمال المراجع الخارجي، ووجود ارتباط طردي معنوي بين إدارة الإفصاح عن مخاطر الأمن السيبراني والمنهج الإجرائي المقترح لأعمال المراجع الخارجي.

		بالتقنيات الحديثة في نظم المعلومات والتكنولوجيا.	
-4	دراسة فرج (2022)	استهدفت الدراسة: إلى اختبار العلاقة بين توكيد مراقب الحسابات على مزاعم الإدارة، عن إدارة مخاطر الأمن الإلكتروني (الأمن السيبراني) وقرار الاستثمار بالأسهم، وكذلك اختبار أثر تأهيل وخبرة المستثمرين على العلاقة محل الاختبار.	توصلت الدراسة: إلى وجود تأثير لتوكيد مراقب الحسابات على مزاعم الإدارة، عن إدارة مخاطر الأمن الإلكتروني إيجاباً الشركات المقيدة، ومعنوياً على قرار الاستثمار بأسهم بالبورصة المصرية، وتم استخدام متغيرات معدلة تمثلت في مستوى التأهيل العلمي للمستثمر، ومستوى خبرة المستثمر، وخلصت الدراسة إلى عدم وجود تأثير معنوي لمتغيري التأهيل والخبرة، كل على حدة على قرار الاستثمار بالأسهم، وكذلك عدم وجود تأثير معنوي لمتغيري التأهيل والخبرة معاً على قرار الاستثمار بالأسهم.
-5	دراسة Li,B,et.Al, (2022)	استهدفت الدراسة: قياس مدى استجابة المراجعون لمخاطر الأمن السيبراني من خلال الاستثمار بشكل أكبر في رأس المال البشري للأمن السيبراني، كما حققت الدراسة في دور المراجعين في مساعدة عملائهم غير المخترقين، في زيادة الوعي بالأمن السيبراني والاستثمار في موظفي الأمن السيبراني.	توصلت الدراسة: إلى أن طلب مكاتب المراجعة على موظفي الأمن السيبراني قد ارتفع بعد أن واجهت شركات، عملائهم الأحداث اختراق بياناتها الإلكترونية، كما ظهرت هذه التأثيرات فقط للمراجعين الموجودين في الولايات، التي تعرضت فقط بشكل متقطع لخروقات البيانات.
-6	Antunes,M,et al(2022)	استهدفت الدراسة: نظام معلومات عام لمراجعة الأمن السيبراني تلعب دوراً رئيسياً، وأشارت الدراسة إلى أن إدارة الأمن السيبراني في المؤسسات الحديثة، وأن هناك عدد كبير من المعايير والطرق والأدوات لتنفيذ إطار عمل الأمن السيبراني، فعلى الصعيد العالمي يتم تنفيذ هذه المعايير من خلال أدوات مخصصة لجمع، وتحليل المزيد من مراجعة الأمن السيبراني الذي يتم تنفيذه في المؤسسة، حيث أن الهدف العام للمراجعة يتمثل في تقييم مخاطر الأمن السيبراني والتخفيف من حدتها.	وتوصلت الدراسة: إلى أن تقييم مخاطر الأمن السيبراني التي تدرس وتقيم مجموعة من الضوابط المحددة مسبقاً، يعتمد على عمليات المراجعة في مجموعة متنوعة من الموضوعات المتعلقة بالأمن السيبراني، وأنه يتم تطبيق قائمة مرجعية بالإجراءات لكل عنصر رقابة، ويقترح مجموعة من الإجراءات التصحيحية من أجل التخفيف من العيوب، وزيادة مستوى الامتثال للمعايير المستخدمة.
-7	دراسة-Al Matari,O.M.,et al (2021)	استهدفت الدراسة: تكوين إطار مقترح لإجراء دراسة مقارنة لأدوات مراجعة الأمن السيبراني وأطر المراجعة المتعارف عليها، وتمثل الهدف الرئيسي للدراسة في تنفيذ أداة متكاملة للأمن السيبراني لمراجعة نظم المعلومات والأمن	توصلت الدراسة: إلى أن مستويات المراجعة تزيد من احتمالية اكتشاف نقاط ضعف الرقابة الداخلية، وتوفر المزيد من الضوابط والتوازنات للمنظمات من خلال، مواءمة هذا الإطار المتكامل مع التقنيات والوظائف الحديثة، والقضايا ذات الصلة بالأمن السيبراني.

		السيبراني بهدف جعل عملية مراجعة الأمن السيبراني أسهل وأكثر شمول، حيث يمكن للأداة المتكاملة أيضاً قياس مقدار الوقت، والجهد الموفر لتحقيق العمليات اليومية.	
-8	دراسة (2019) Frank.M.L.,et al	استهدفت الدراسة: قياس تأثير الإفصاح عن هجوم سيبراني سابق، على فعالية الإفصاح عن إدارة مخاطر الأمن السيبراني، والتأكيد المستقل على تصورات المستثمرين حول جاذبية الاستثمار.	انتهت الدراسة إلى أن غياب تقرير التأكيد المستقل حول إدارة مخاطر الأمن السيبراني، يكون أكثر فاعلية عندما لا تفصح الشركة عن هجوم إلكتروني سابق، نظراً لأن المستثمرين غير المحترفين أقل عرضة للتشكيك في موثوقية تقارير الإدارة حول الأمن السيبراني، ومع ذلك فإن إصدار تقرير تأكيد مستقل مع تقرير الإدارة حول إدارة مخاطر الأمن السيبراني، يوفر فائدة إضافية أكبر للشركات التي أفصحت مقابل التي لم تفصح عن هجوم إلكتروني سابق، حيث أن هذه الشركات تستفيد أكثر من خلال تعزيز موثوقية التأكيد المستقل، وانتهت الدراسة إلى أنه يمكن تعزيز جاذبية الاستثمار في الشركة، من خلال إصدار تقرير تأكيد مستقل عن مخاطر الأمن السيبراني.

المبحث الثالث: الجانب التطبيقي

يتناول هذا المبحث بيان الطريقة والإجراءات التي تم اتباعها في تنفيذ البحث ميدانياً للوصول إلى أهدافه، والعينة التي طبقت عليها الدراسة (المدققين الخارجيين والأكاديميين المختصين)، ووصف الخصائص الديموغرافية لأفراد العينة، وأهم الأساليب الإحصائية المستخدمة لتحليل البيانات حيث تم استخدام المعالجات الإحصائية من خلال برنامج التحليل الإحصائي (SPSS)، معادلة ألفا كرونباخ: للتحقق من ثبات أداة الدراسة وتطبيقها، المتوسطات الحسابية والانحرافات المعيارية.

اختبار فرضية الدراسة الميدانية وتحليل نتائجها

مجتمع وعينة الدراسة:

تكون مجتمع الدراسة من (المدققين الخارجيين والأكاديميين المختصين) والبالغ عددهم (45)، حيث تم توزيع جميع استمارات الاستبيان على عينة الدراسة، فقد استرد منها (39) استمارة جميعها صالحة للتحليل، أي بنسبة استجابة (86.666%) حيث كانت إجابات المدققين الخارجيين البالغ عددهم (24) استمارة بنسبة (61.54%)، بينما كانت إجابات الأكاديميين المختصين والبالغ عددهم (15) استمارة بنسبة (38.46%)، في حين بلغت الاستمارة الغير صالحة للتحليل (6) استمارات مهملة أي بنسبة (13.333%)،

وتُعد نسبة الاستجابة لآراء المشاركين البالغة (86.666%) نسبة جيدة لاستقصاء بياناتها واستخدامها كأساس في تحليل الدراسة، وبلغت فترة توزيع الاستمارات واستلامها خلال مدة (65) يوم واعتبارًا من الخميس 2 /1/ 2025 ولغاية يوم الأربعاء 2/26 /2025.

أداة الدراسة:

لقد تضمن هذا المبحث قياس العلاقة بين متغيرات البحث، وهما المتغير المستقل مخاطر الأمن السيبراني والمتغير التابع كفاءة وفاعلية المدقق الخارجي، حيث استخدمت الباحثة استمارة الاستبيان كأداة رئيسية للدراسة، لملائمتها لهذا النوع من الدراسات التطبيقية، للحصول على بيانات من عينة الدراسة والتي تسهم في قياس تأثير مخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي في ظل التطورات الرقمية الحديثة، عن طريق استخدام برنامج (SPSS) للتأكد من وجود العلاقة بينهما من عدمه، حيث اشتملت الاستبانة على قسمين:

القسم الأول: المتغيرات الديموغرافية: ويهدف إلى معرفة الخصائص الديموغرافية للمجيبين (عينة الدراسة) على أسئلة الدراسة منها: (الجنس، التخصص العلمي، المؤهل العلمي، سنوات الخبرة).

القسم الثاني: يتضمن محاور الدراسة والذي يضم:

- **المحور الأول:** مخاطر الأمن السيبراني ويتضمن (10) أسئلة.
- **المحور الثاني:** كفاءة وفاعلية المدقق الخارجي ويتضمن (10) أسئلة.
- **المحور الثالث:** تأثير مخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي ويتضمن (14) أسئلة.

تم اعتماد مقياس ليكرت الخماسي وهو عبارة عن مقياس مئوي مكون من خمس درجات يهدف إلى تحديد موافقة أفراد العينة، على كل فقرة من فقرات أداة الدراسة مقسمة على ثلاث مستويات، حيث تم احتساب درجة القطع من خلال حاصل الفرق بين أعلى مقياس (5) درجات، وأقل قيمة والممثلة بـ(1) درجة، ومن ثم تحويلها إلى بيانات كمية يمكن قياسها إحصائياً، ومن ثم إعطاءها الأوزان النسبية المبينة في الجدول رقم (1) أدناه:

جدول رقم (1): درجات مقياس ليكرت الخماسي (المصدر: من إعداد الباحثة)

التصنيف	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
الدرجة	5	4	3	2	1
الوزن النسبي	%100	%80	%60	%40	%20

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (4), No. (4)
IJFAES
April 2025
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (4)، العدد (4)

ولحساب المدى كالآتي: الحد الأعلى للفئة-الحد الأدنى للفئة = 5-1 = 4 كما تم حساب طول الفئة من خلال تقسيم المدى على عدد الفئات (الخيارات) فيكون: 4/5=0,80؛ حيث تكون الفئة الأولى لقيم المتوسط الحسابي من 1 إلى 1+0.80 وهكذا بالنسبة لبقية المتوسطات الحسابية، ويعتمد الجدول رقم (2) في تفسير قيم المتوسطات ودرجات الموافقة في آراء عينة الدراسة.

جدول رقم (2): المتوسطات الحسابية باستخدام مقياس ليكرت الخماسي

ت	درجة المقياس	الاتجاه / المتوسط الحسابي	درجة الاتجاه	نوع الاتجاه
1	1	من 1 والغاية 1.70	منخفض جداً	سلبي
2	2	من 1.70 ولغاية 2.50	منخفض	سلبي
3	3	من 2.50 ولغاية 3.30	متوسط	غير متأكد
4	4	من 3.30 ولغاية 4.10	مرتفع	إيجابي
5	5	من 4.10 ولغاية 5	مرتفع جداً	إيجابي

ثبات أداة الدراسة (معادلة ألفا كرونباخ):

قامت الباحثة باختبار ثبات وصدق فقرات الاستبانة وذلك عن طريق استخدام معامل الثبات ألفا كرونباخ (Alpha s'Cronbach)، وكانت قيم الاختبار لمتغيرات الدراسة جميعها، وللاستبانة بشكل عام أعلى من (60%) مما يعني القدرة على الوثوق فيما تسفر عنه الدراسة من نتائج، أي أن النتائج قابلة للتعميم على مجتمع الدراسة، ويوضح الجدول رقم (3) أدناه معامل الثبات والصدق لكل محور من محاور البحث الثلاثة.

جدول رقم (3): معامل ثبات وصدق أداة الدراسة (الفا كرونباخ) (المصدر: من إعداد الباحثة بالاعتماد على بيانات برنامج التحليل الإحصائي SPSS)

المحور	البيان	عدد الفقرات	قيمة معامل الفا كرونباخ	الدرجة الصدق
الأول	مخاطر الأمن السيبراني.	10	0.861	0.927
الثاني	كفاءة وفاعلية المدقق الخارجي.	10	0.708	0.841
الثالث	تأثير مخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي في ظل التطورات الرقمية الحديثة.	14	0.832	0.912
	الإجمالي	34	0.824	0.907

من خلال الجدول رقم (3) يتضح أن القيم الخاصة بمعامل الثبات بالنسبة لجميع محاور الاستبانة تجاوزت (70%) وهي نسبة مقبولة، وقد تراوحت قيم معامل الثبات بين (0.861)، (0.708) للمحور الأول والثالث على التوالي، فيما جاءت القيمة الإجمالية للمعامل ذاته والتي قدرت ب (0.824)، وهي قيمة مرتفعة حيث تقترب من الواحد الصحيح، وهذا يدل على صدق الاستبانة وتمثيلها لمجتمع الدراسة.

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (4), No. (4)
IJFAES
April 2025
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (4)، العدد (4)

- معاملات ارتباط بيرسون لكل محور من محاور الاستبانة:

تم إيجاد معاملات الارتباط بين معدل كل محور والمعدل الكلي للفقرات وكما هي موضحة في الجدول رقم (4) الآتي:

جدول رقم (4): معاملات ارتباط بيرسون لكل محور من محاور الاستبانة ودرجتها الكلية (المصدر: من إعداد الباحثة)

المحور	البيان	عدد الفقرات	قيم معامل الارتباط بيرسون	مستوى الدلالة
الأول	مخاطر الأمن السيبراني	10	0.704**	0.000
الثاني	كفاءة وفاعلية المدقق الخارجي	10	0.660**	0.000
الثالث	تأثير مخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي	14	0.650**	0.000

**الارتباط دال عند مستوى 0،01

يتضح من الجدول رقم (4) أن قيم معاملات ارتباط بيرسون بين معدل كل محور من محاور الاستبانة والمعدل الكلي لها تراوحت بين (0,650) كحد أدنى و(0,704) كحد أقصى، وجميعها موجبة ودالة عند مستوى دلالة (0,01) وبالتالي فإن المحاور الثلاث المكونة للاستبانة متسقة داخلياً مع الاستبانة ككل، وبالنتيجة الإجابات التي تم الحصول عليها من أسئلة الاستبانة تعطي المعلومات التي وضعت من أجلها.

التحليل الوصفي لعينة البحث

القسم الأول: المعلومات الديموغرافية:

وقد جاء توصيف خصائص أفراد عينة الدراسة (المعلومات الديموغرافية)، من حيث (الجنس، المؤهل العلمي، التخصص العلمي وسنوات الخبرة)، وكما يوضحه الجدول رقم (5) التالي:

الجدول رقم (5): وصف خصائص عينة الدراسة (المصدر: من إعداد الباحثة بالاعتماد على بيانات برنامج التحليل الإحصائي SPSS)

ت	المتغير	التفاصيل	العدد	النسبة المئوية%	المجموع
1	الجنس	ذكر	22	56.4	%100
		أنثى	17	43.6	
2	المؤهل العلمي	بكالوريوس	9	23.08	
		ماجستير	12	30.77	
		دكتوراه	18	46.15	%100
3	التخصص العلمي	مدقق خارجي	24	61.54	
		أستاذ أكاديمي	15	38.46	%100
4	سنوات الخبرة	من 5-10 سنوات	9	23.07	

	17.95	7	من 10 -15 سنة		
	51.28	20	من 15 – 20 سنة		
%100	7.69	3	20 سنة فأكثر		

يتضح من خلال الجدول رقم (5) الآتي:

1. أن أغلب أفراد عينة الدراسة هم من الذكور، حيث شكلت نسبتهم (56.4 %) في حين شكلت نسبة الإناث البالغة (43.6%).
2. تتوزع عينة الدراسة بين مختلف المؤهلات العلمية حيث تم اختيار العينة من الأفراد الحاصلين على البكالوريوس والماجستير والدكتوراه، وتبين أن من يحملون درجة البكالوريوس بنسبة (23.08%) وهي النسبة الأقل، وفي حين يلي ذلك من يحملون درجة الماجستير ونسبتهم (30.77%) من عينة الدراسة، يليها النسبة الأعلى وهم من يحملون درجة الدكتوراه ونسبتهم (46.15%).
3. يتضح من خلال متغير التخصص العلمي أن إجابات المدققين الخارجيين كانت الأعلى حيث بلغت نسبتهم (61.54)، في حين كانت إجابات الأساتذة الأكاديميين أقل نسبة فقد بلغت (38.46).
4. أما ما يخص سنوات الخبرة فتبين أن النسبة الأقل كانت للسنوات (20 فأكثر) حيث بلغت نسبتهم (7.69%) من عينة الدراسة، أما النسبة الأعلى لسنوات الخبرة لعينة الدراسة فكانت من ذوي الخبرة من (15 -20)سنة حيث بلغت نسبتهم (51.28%).

القسم الثاني: تحليل البيانات واختبار الفرضيات

في هذا الجزء من تحليل الدراسة تناولت الباحثة تحليل وتفسير استجابات أفراد العينة، المتعلقة بتوضيح تأثير استخدام تقنية الحوسبة السحابية في تحسين جودة التدقيق الداخلي من خلال ثلاث محاور: حيث يرتبط المحور الأول بتقنية الحوسبة السحابية، والمحور الثاني يتعلق بجودة التدقيق الداخلي، أما المحور الثالث فتناول تأثير استخدام تقنية الحوسبة السحابية في تحسين جودة التدقيق الداخلي.

وتسعى الباحثة في هذا الجزء إلى اختبار فرضيات الدراسة، حيث تم استخدام الوسط الحسابي والانحراف المعياري لكل محور من المحاور الثلاث أعلاه، للتعرف على مدى وجود تأثير لاستخدام تقنية الحوسبة السحابية في تحسين جودة التدقيق الداخلي، وكما موضح في الجداول رقم (4-5-6)، وكذلك إجراء تحليل

معاملات الارتباط لتلك المحاور من خلال، استخدام معامل الارتباط بيرسون وتحليل الانحدار الخطي لفرضيات البحث وكما موضح في أدناه:

المحور الأول: مخاطر الأمن السيبراني:

يبين الجدول رقم (6) الوسط الحسابي والانحراف المعياري والنسبة المئوية لإجابات أفراد العينة عن متغيرات الدراسة لمخاطر الأمن السيبراني ووفق الآتي:

الجدول رقم (6): المتوسط الحسابي والانحراف المعياري لمحور مخاطر الأمن السيبراني (المصدر: من إعداد الباحثة بالاعتماد على بيانات برنامج التحليل الإحصائي SPSS)

	فقرات الدراسة	عدد العينة	الانحراف المعياري	المتوسط الحسابي	الترتيب	النسبة المئوية%
1	تعد مخاطر الأمن السيبراني جزءً هاماً لا يتجزأ من مخاطر العالم الرقمي الحديث، والتي ظهرت بعد الثورة الرقمية التي سادت في دول العالم المعاصرة.	39	0.664	4.080	4	%81.6
2	تحدث مخاطر الأمن السيبراني نتيجة فقدان أو ضرر أنظمة المعلومات والاتصالات في الشركات التي تتعرض للهجمات السيبرانية.	39	0.903	3.640	10	%72.8
3	أن عدم الاهتمام بخصوصية البيانات قد تؤدي إلى تداعيات مالية وقانونية وهذا يُعد جانباً مهماً من مخاطر الأمن السيبراني في الشركات.	39	0.833	3.870	9	%77.4
4	يُعد اتخاذ وتنفيذ تدابير الأمن السيبراني الفعالة من الأمور المهمة والضرورية اللازمة لحماية المعلومات الحساسة ومنع حدوث خروقات البيانات، وذلك من خلال تحديد مخاطر الأمن السيبراني المحتملة والقيام بتحديث البرامج والأجهزة وتدريب الموظفين المختصين واتخاذ كافة إجراءات الحماية.	39	0.643	4.460	1	%89.2
5	لإدارة مخاطر الأمن السيبراني يجب اعتماد نهج استباقي واتخاذ التدابير الوقائية، وذلك للحفاظ على البيانات والمعلومات من تلك المخاطر.	39	0.946	4.000	6	%80
6	لمنع أو اكتشاف المخاطر السيبرانية وتقييم المخاطر بطريقة شاملة، يتطلب تحديد وتحليل وتقييم المخاطر السيبرانية التي تواجه الشركة، وذلك لضمان كفاية الإجراءات الوقائية المتخذة.	39	0.584	4.360	2	%87.2
7	قيام الشركة بدمج مخاطر الأمن السيبراني في الخطة الاستراتيجية، وتحديد المخاطر التي تواجهها والتي تؤثر على تحقيقها لأهدافها والرقابة عليها، واتخاذ القرارات اللازمة بشأنها.	39	0.778	3.970	7	%79.4
8	عند وجود احتمال لمحاولات إتلاف أو تعطيل عمليات شبكة الكمبيوتر، ونظام المعلومات الضعيفة التحصين عند ذلك تحدث التهديدات السيبرانية.	39	0.777	4.030	5	%80.6
9	ترتبط مخاطر الأمن السيبراني بتعدد أهداف الهجمات الإلكترونية ومنها: الابتزاز، والسرقة، وتدمير الأصول المالية، وسرقة الملكية الفكرية أو المعلومات الحساسة، والتي تخص الشركات الأخرى أو شركاءها الآخرين أو عملائها.	39	0.793	3.950	8	%79
10	إن فهم المدقق لكيفية تحديد الشركة لمخاطر الأمن السيبراني والرقابة عليها يتطلب ذلك التوسع ليشمل البيئة السيبرانية، والتركيز على الجوانب التكنولوجيا حيث كلما زادت مخاطر هجمات الأمن السيبراني، كلما انعكس ذلك على نطاق ومسئوليات أعمال المدقق الخارجي.	39	0.838	4.330	3	%86.6
	المجموع	39	0.522	4.069		%81.38

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (4), No. (4)
IJFAES
April 2025
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (4)، العدد (4)

وفيما يلي توضيح لآراء عينة البحث حول المحور الأول مخاطر الأمن السيبراني كما في الجدول رقم (6):

يلاحظ أن أعلى متوسط حسابي جاء من خلال الفقرة رقم (4) حيث بلغ المتوسط الحسابي (4.460)، وبانحراف معياري (0.643)، وبنسبة بلغت (89.2%)، بمعنى أنه "يُعد تنفيذ تدابير الأمن السيبراني الفعالة أمراً ضرورياً لحماية المعلومات الحساسة ومنع حدوث خروقات البيانات من خلال تحديد المخاطر السيبرانية المحتملة وتحديث البرامج والأجهزة وتدريب الموظفين المختصين واتخاذ كافة إجراءات الحماية"، في حين بلغ أقل متوسط حسابي للفقرة (2) نسبة (0 3.64) وبانحراف معياري بلغ (0.903)، وبنسبة (72.8%)، بمعنى أنه "تحدث مخاطر الأمن السيبراني نتيجة فقدان أو ضرر أنظمة المعلومات والاتصالات في الشركات التي تتعرض للهجمات السيبرانية".

المحور الثاني: المدقق الخارجي:

يبين الجدول رقم (7) الوسط الحسابي والانحراف المعياري والنسبة المئوية لإجابات أفراد العينة عن المحور الثاني: المدقق الخارجي وكما موضحة في الجدول أدناه:

الجدول رقم (7): الوسط الحسابي والانحراف المعياري لمحور المدقق الخارجي (المصدر: من إعداد الباحثة بالاعتماد على بيانات برنامج التحليل الإحصائي SPSS)

	فقرات الدراسة	عدد العينة	الانحراف المعياري	المتوسط الحسابي	الترتيب	النسبة المئوية%
1	امتلاك المدقق الخارجي المعرفة العلمية والرقمية في مجال الأمن السيبراني والمخاطر الناتجة عنه يساعد على تحقيق درجة عالية من الدقة عند القيام بالتأكد من توفر الإجراءات اللازمة لمنع الهجمات الإلكترونية والانتهاكات.	39	1.188	3.560	8	%71.2
2	القيام بتضمين مخاطر الأمن السيبراني كجزء من تقييم المدقق لمخاطر تكنولوجيا المعلومات في الشركة عينة الدراسة عند قيامه بتخطيط عملية التدقيق وتنفيذها وكذلك إجراءات العمل الميداني الواجب القيام فيه.	39	1.056	3.790	7	%75.8
3	يعد الاستقلال الذهني للمدقق الخارجي عنصراً ضرورياً وحيوياً عند القيام بتدقيق البيانات والأنظمة الإلكترونية المطبقة في الشركة عينة الدراسة وتحديد مخاطر الأمن السيبراني ونتائجه على مستقبلها.	39	1.181	3.360	10	%67.2
4	الالتزام بالمعايير المهنية المتعارف عليها من قبل المدقق الخارجي يساهم في تحسين عملية التأكيد اللازمة لحماية البيانات ومواجهة التهديدات والمخاطر الناتجة عن الأمن السيبراني والمساعدة في إدارة ومواجهة تلك المخاطر.	39	1.075	4.050	5	%81
5	مشاركة المدقق الخارجي في الدورات التأهيلية الرقمية الخاصة بالأمن السيبراني والمخاطر الناتجة عنه وأثرها على نظام حماية البيانات يحقق كفاءة وفاعلية كبيرة بعملية التدقيق لتلك البيانات والأنظمة.	39	0.900	4.040	3	%80.8

6	يجب أن يمتلك المدقق الخارجي الوعي والدراية والثقافة التقنية الخاصة بالأمن السيبراني والمخاطر والتهديدات التي قد تتعرض لها الشركة محل الفحص والتدقيق، وأنها قد وضعت إجراءات لحماية بياناتها ومعلوماتها وبنيتها التحتية من مخاطر الأمن السيبراني.	39	0.756	4.510	1	%90.2
7	لتعزيز إجراءات الحماية اللازمة ضرورة قيام المدقق الخارجي بالتأكد من توافر ضوابط الأمن السيبراني متكاملة ومترابطة وبشكل فعال وأن تكون متوافقة ومتناسقة مع المعايير التنظيمية التي تعزز إجراءات الحماية.	39	0.863	4.310	2	%86.2
8	القيام بتحليل البيانات والأنظمة والتقارير المالية من قبل المدقق الخارجي والتحقق من مدى صحتها عند تطبيق الأمن السيبراني والتحقق من عمليات الاختراق المحتملة، وتحديد تلك المخاطر والتأكد من توافر كافة وسائل الحماية اللازمة.	39	0.996	3.540	9	%70.8
9	ضرورة قيام المدقق الخارجي بالاستجابة لمخاطر الأمن السيبراني من خلال التأكد من وجود كوادر مؤهلة علمياً ورقمياً من موظفين وعاملين متخصصين في مجال الأمن السيبراني لتطبيقه ومواجهة كافة التهديدات والاختراقات والمخاطر الناتجة عنه.	39	1.036	4.080	4	%81.6
10	القيام بإجراء التقييمات الشاملة لمخاطر الأمن السيبراني من قبل المدقق الخارجي والتي تحدد بدقة نقاط الضعف والتهديدات المحتملة وذلك لمواجهة المسؤوليات الملقاة على عاتقه في ضمان سلامة التقارير المالية للشركة عينة الدراسة وعدالتها.	39	0.873	3.970	9	%79.4
	المجموع	39	0.526	3.926		%60.52

وفيما يلي توضيح لآراء عينة البحث حول المحور المدقق الخارجي كما هي في الجدول رقم (7):

ويلاحظ أن أعلى متوسط حسابي جاء من خلال الفقرة رقم (6) حيث بلغ المتوسط الحسابي (4.510)، وبانحراف معياري (0.756) وبنسبة (90.2%) بمعنى أنه "يجب أن يمتلك المدقق الخارجي الوعي والدراية والثقافة التقنية الخاصة بالأمن السيبراني والمخاطر والتهديدات التي قد تتعرض لها الشركة محل الفحص والتدقيق ، وأنها قد وضعت إجراءات لحماية بياناتها ومعلوماتها وبنيتها التحتية من مخاطر الأمن السيبراني"، في حين بلغ أقل متوسط حسابي للفقرة (3) نسبة(3.360) وبانحراف معياري بلغ (1.181)، وبنسبة (67.2%) بمعنى أنه "يعد الاستقلال الذهني للمدقق الخارجي عنصراً ضرورياً وحيوياً عند القيام بتدقيق البيانات والأنظمة الإلكترونية المطبقة في الشركة عينة الدراسة وتحديد مخاطر الأمن السيبراني ونتائجه على مستقبلها".

المحور الثالث: تأثير مخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي

يبين الجدول رقم (8) الوسط الحسابي والانحراف المعياري والنسبة المئوية لإجابات أفراد العينة عن متغيرات الدراسة تأثير مخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي وكما في الجدول التالي:

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (4), No. (4)
IJFAES
April 2025
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (4)، العدد (4)

الجدول رقم (8): المتوسط الحسابي والانحراف المعياري لمحور تأثير مخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي
(المصدر: من إعداد الباحثة بالاعتماد على بيانات برنامج التحليل الإحصائي SPSS)

	فقرات الدراسة	عدد العينة	الانحراف المعياري	المتوسط الحسابي	الترتيب	النسبة المئوية%
1	للاستفادة من التطورات الرقمية والتى تعد أمراً حيوياً فى تعزيز جوانب الأمن السيبرانى فى عملية التدقيق، مما يتطلب القيام باتخاذ كافة الوسائل والإجراءات التى تعزز الأخذ بمخاطر الأمن السيبرانى لدى المدقق الخارجى.	3961	1.115	3.380	5	%67.6
2	تعد مخاطر الأمن السيبرانى فى العالم الرقمى اليوم جزءً أساسيًا من عملية التدقيق الخارجى، وضرورة بقاء المدقق الخارجى على اطلاع دائم بالمخاطر والتهديدات السيبرانية، وأن يعمل على تحديد واتخاذ كافة الإجراءات التدقيقية عند ممارسة عملية التدقيق الخاصة بهذه المخاطر.	3961	1.395	2.720	10	%54.4
3	لغرض القيام بإجراء تقييم شامل لمخاطر الأمن السيبرانى فى ظل التطورات الرقمية الحديثة وبشكل أكثر كفاءة وفاعلية للمدقق الخارجى والذي يوفر رؤية عميقة وشاملة لتلك المخاطر والتهديدات الخاصة بالأمن السيبرانى.	3961	1.080	2.690	11	%53.8
4	لضمان اتباع نهج شامل لعملية التدقيق فى العصر الرقمى الحديث على المدقق الخارجى التعاون بشكل وثيق ودقيق مع متخصصى تكنولوجيا المعلومات وذلك لاكتساب فهم عميق للبنية التحتية التكنولوجية وتقييم المخاطر المرتبطة بها بشكل أكثر فعالية.	3961	1.144	2.820	9	%56.4
5	ضرورة قيام المدقق الخارجى بالامتثال للوائح الخاصة بحماية البيانات والمعلومات الحساسة من الوصول، والكشف غير المصرح به، من التدابير الأساسية للحماية من مخاطر الأمن السيبرانى، التشفير، وضوابط الوصول، والتخزين الآمن للبيانات، وهذا يساعد فى تحديد أهداف التدقيق والمدقق بشكل أكثر وضوح ودقة وبما يحقق درجة أكبر من الكفاءة والفاعلية.	3961	0.644	4.490	1	%89.8
6	مساهمة المدقق الخارجى فى تحسين وتعزيز عملية تأكيد الحماية للبيانات ومواجهة التهديدات والمخاطر الخاصة بالأمن السيبرانى من خلال الالتزام بالمعايير المهنية المطلوبة لإتمام عملية التدقيق.	3961	1.217	3.310	7	%66.2
7	القيام بتنفيذ عملية التدقيق لأنظمة الحماية الخاصة بمخاطر الأمن السيبرانى يتطلب تكييف خطة التدقيق وإجراءاتها وفريق التدقيق للتطورات الرقمية الحديثة من خلال دمج التقنيات الحديثة للوصول إلى النتائج المطلوبة بشكل كفوء وفعال.	3961	1.173	2.173	12	%43.46
8	بناءً على المخاطر المصاحبة لاستخدام الأمن السيبراني، المساعدة فى توفير السياسات والمعايير اللازمة لتقييم وتصحيح نقاط الضعف.	3961	0.995	2.560	13	51.2%
9	المساهمة فى إنشاء سياسات ومعايير أمان واضحة لمواجهة مخاطر الأمن السيبرانى، والتى تساعد فى تحسين إدارة الخصوصية وأمن المعلومات والبيانات والأنظمة الإلكترونية المطبقة.	3961	1.315	2.460	14	%49.2
10	الاطلاع على تفاصيل تقييم مخاطر الأمن السيبراني والتقرير الخاص بها، من حيث توفير الموارد والوقت لتعزيز الأمن، وتحديد التهديدات المحتملة بشكل مستمر، وتجنب مشكل التوقف للتطبيقات، والإجراءات المتخذة لمواجهة تهديدات جديدة.	3961	1.272	3.410	4	%68.2

11	مساعدة متخذي القرارات في الشركة لفهم المعلومات التي يتم حمايتها من المخاطر السيبرانية، وتتمثل بالتنصت، سرقة كلمة المرور، الهجوم غير المتوقع، عمليات الاحتيال، البرامج الضارة، الهندسة الاجتماعية وغيرها من المخاطر، وإجراءات الحماية اللازمة تم تطبيقها لمواجهة هذه المخاطر.	3939	1.174	2.870	8	%57.4
12	ضرورة قيام المدقق الخارجي بتدقيق الضوابط الوقائية الخاصة بتطبيق التشفير، مكافحة الفيروسات، المراقبة الأمنية المستمرة، الإجراءات الاستقصائية لاكتشاف أوقات حدوث هجوم السيبراني أو التهديدات الأمنية..... وغيرها من الإجراءات الوقائية.	3939	0.701	04.33	2	%86.6
13	لضمان صحة ودقة البيانات الواردة في التقارير قيام المدقق بالاطلاع على توثيق جميع المخاطر في سجل المخاطر ويجب القيام بالتحديث بشكل منتظم لغرض التأكد الدائم من هناك حساب محدث لمخاطر الأمن السيبراني والذي يساعد الإدارة في اتخاذ القرارات الخاصة بالإجراءات والسياسات والضوابط المتعلقة بتلك المخاطر.	3939	1.203	3.360	6	%67.2
14	لغرض التقليل من المخاطر السيبرانية والمخاطر الأخرى المرتبطة بمخاطر التحول الرقمي، وذلك من خلال: تدقيق ضوابط الوصول إلى البيانات، لغرض ضمان تنفيذ ضوابط وصول صارمة، وأن الموظفين المصرح لهم فقط يمكنهم التعامل مع بيانات التدقيق الحساسة والقيام بتحليلها والحفاظ عليها من حيث دقتها اكتمالها وموثوقيته.	39	1.196	03.87	3	%77.4
	المجموع	39	0.635	3.213		%64.26

وفيما يلي توضيح لآراء عينة البحث حول المحور تأثير مخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي كما هي في الجدول رقم (9):

يلاحظ أن أعلى متوسط حسابي جاء من خلال الفقرة رقم (5)، حيث بلغ المتوسط الحسابي (4.490)، وبانحراف معياري (0.644)، وبنسبة (89.8%) بمعنى أنه "ضرورة قيام المدقق الخارجي بالامتثال للوائح الخاصة بحماية البيانات والمعلومات الحساسة من الوصول، والكشف غير المصرح به، من التدابير الأساسية للحماية من مخاطر الأمن السيبراني، التشفير، وضوابط الوصول، والتخزين الآمن للبيانات، وهذا يساعد في تحديد أهداف التدقيق والمدقق بشكل أكثر وضوح ودقة وبما يحقق درجة أكبر من الكفاءة والفاعلية، في حين بلغ أقل متوسط حسابي للفقرة (9) نسبة (2.490) وبانحراف معياري بلغ (1.315)، وبنسبة (49.2)، بمعنى "أن المساهمة في إنشاء سياسات ومعايير أمان واضحة لمواجهة مخاطر الأمن السيبراني والتي تساعد في تحسين إدارة الخصوصية وأمن المعلومات والبيانات والأنظمة الإلكترونية المطبقة".

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (4), No. (4)
IJFAES
April 2025
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (4)، العدد (4)

جدول رقم (10): المتوسط الحسابي العام والانحراف المعياري لجميع محاور الدراسة (المصدر: من إعداد الباحثة بالاعتماد على بيانات برنامج التحليل الإحصائي SPSS)

محاور الدراسة	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية%
المحور الأول: مخاطر الأمن السيبراني.	0694.	0.522	38.18%
المحور الثاني: المدقق الخارجي.	926.3	526.0	5260.%
المحور الثالث: تأثير مخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي في ظل التطورات الرقمية الحديثة.	.2133	635.0	%64.26

1. كان إجمالي الأوساط الحسابية المرجحة لجميع فقرات المحور الأول: مخاطر الأمن السيبراني حيث بلغ الوسط الحسابي المرجح العام لكل الإجابات (4.069) وانحراف معياري بلغ (0.522)، وبنسبة مئوية بلغت (81.38%)، وهي نسبة مرتفعة وهذا يشير إلى ان مخاطر كبيرة للأمن السيبراني يجب الاهتمام بها وأخذها في الاعتبار مما انعكس بشكل إيجابي على النتائج.
2. كان إجمالي الأوساط الحسابية المرجحة لجميع فقرات المحور الثاني: المدقق الخارجي حيث بلغ الوسط الحسابي المرجح العام لكل الإجابات (3.213) وانحراف معياري بلغ (0.635)، وبنسبة مئوية بلغت (64.26%)، وهي نسبة مرتفعة وهذا يشير إلى أن كفاءة وفاعلية المدقق الخارجي مما انعكس بشكل إيجابي على النتائج.
3. كانت الأوساط الحسابية المرجحة لجميع فقرات المحور الثالث: تأثير مخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي حيث بلغ الوسط الحسابي المرجح العام لكل الإجابات (3.026) وانحراف معياري بلغ (0.526)، وبنسبة مئوية بلغت (60.52%)، وهي نسبة مرتفعة، وهذا يشير إلى أن وجود تأثير لمخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي في ظل التطورات الرقمية الحديثة مما انعكس بشكل إيجابي على النتائج.

اختبار فرضيات الدراسة

لغرض القيام باختبار فرضيات الدراسة فقد تمت الاستعانة باختبار (t) للعينة الواحد، لاختبار الفروض المعنوية بين المتوسطات الحسابية للعينة باستخدام قيمة معيارية حددت ب (3) وهي تمثل متوسط درجات سلم ليكرت الخماسي.

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (4), No. (4)
IJFAES
April 2025
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (4)، العدد (4)

1. اختبار الفرضية الفرعية الأولى: هناك تأثير لمخاطر الأمن السيبراني على تعزيز ثقافة الوعي بالأمن السيبراني لدى المدقق الخارجي:

جدول رقم (11): نتائج اختبار المتوسط الحسابي والانحراف المعياري للفرضية الفرعية الأولى (المصدر: من إعداد الباحثة بالاعتماد على بيانات برنامج التحليل الإحصائي SPSS)

إجمالي المتوسط الحسابي	إجمالي الانحراف المعياري	قيمة تي الجدولية	القيمة الاحتمالية
4.069	0.522	12.786	0.000

من خلال النتائج الموضحة في الجدول أعلاه، المتوسط الحسابي الإجمالي لآراء أفراء العينة حول هناك تأثير لمخاطر الأمن السيبراني على تعزيز ثقافة الوعي بالأمن السيبراني لدى المدقق الخارجي أعلى من القيمة الفرضية (3) إذ بلغ (4.069)، وبانحراف معياري بلغ (0.522) وبلغت قيمة (t) (12.786) وهي ذات دلالة إحصائية عند مستوى أقل من (0.05)، مما يعني أن ردود أفراد العينة في هذا المحور جاءت إيجابية بدرجة كبيرة، وبالتالي يتم رفض الفرضية الصفرية التي تقوم على أنه "لا يوجد تأثير لمخاطر الأمن السيبراني على تعزيز ثقافة الوعي بالأمن السيبراني لدى المدقق الخارجي، وتقبل الفرضية البديلة.

2. اختبار الفرضية الفرعية الثانية: هناك تأثير لمخاطر الأمن السيبراني على عملية تخطيط وتنفيذ والإجراءات الميدانية لعملية التدقيق من قبل المدقق الخارجي:

جدول رقم (12): نتائج اختبار المتوسط الحسابي والانحراف المعياري للفرضية الفرعية الثانية (المصدر: من إعداد الباحثة بالاعتماد على بيانات برنامج التحليل الإحصائي SPSS)

إجمالي المتوسط الحسابي	إجمالي الانحراف المعياري	قيمة t الجدولية	القيمة الاحتمالية
926.3	526.0	10.989	0.000

من خلال النتائج الموضحة في الجدول أعلاه، المتوسط الحسابي الإجمالي لآراء أفراء العينة حول تأثير لمخاطر الأمن السيبراني على عملية تخطيط وتنفيذ والإجراءات الميدانية لعملية التدقيق من قبل المدقق الخارجي أعلى من القيمة الفرضية (3) إذ بلغ (3.926)، وبانحراف معياري بلغ (0.526) وبلغت قيمة (t) (10.989) وهي ذات دلالة إحصائية عند مستوى أقل من (0.05)، مما يعني أن ردود أفراد العينة في هذا المحور جاءت إيجابية بدرجة كبيرة، وبالتالي يتم رفض الفرضية الصفرية التي تقوم على أنه "لا يوجد تأثير لمخاطر الأمن السيبراني على عملية تخطيط وتنفيذ والإجراءات الميدانية لعملية التدقيق من قبل المدقق الخارجي، وتقبل الفرضية البديلة.

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (4), No. (4)
IJFAES
April 2025
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (4)، العدد (4)

3. اختبار الفرضية الرئيسية للدراسة: هناك تأثير لمخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي في ظل التطورات الرقمية الحديثة":

جدول رقم (13): نتائج اختبار المتوسط الحسابي والانحراف المعياري للفرضية الرئيسية للدراسة (المصدر: من إعداد الباحثة بالاعتماد على بيانات برنامج التحليل الإحصائي SPSS)

إجمالي المتوسط الحسابي	إجمالي الانحراف المعياري	قيمة تي الجدولية	القيمة الاحتمالية
3.213	0.635	2.089	0.043

من خلال النتائج الموضحة في الجدول أعلاه، المتوسط الحسابي الإجمالي لآراء أفراء العينة حول هناك تأثير لمخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي في ظل التطورات الرقمية الحديثة" أعلى من القيمة الفرضية (3) إذ بلغ (3.213)، وبانحراف معياري بلغ (0.635) وبلغت قيمة (t) (2.089) وهي ذات دلالة إحصائية عند مستوى أقل من (0.05)، مما يعني أن ردود أفراد العينة في هذا المحور جاءت إيجابية بدرجة كبيرة، وبالتالي يتم رفض الفرضية الصفرية التي تقوم على أنه "لا يوجد تأثير لمخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي في ظل التطورات الرقمية الحديثة"، وتقبل الفرضية البديلة.

الاستنتاجات والتوصيات

أولاً: الاستنتاجات:

1. مجموعة من المفاهيم والسياسات والضمانات الأمنية، والمبادئ التوجيهية، والأدوات والأساليب، والاجراءات لإدارة المخاطر، وأفضل الممارسات والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمة والمستخدمين، من التهديدات والهجمات الداخلية والخارجية وتقليل ومنع الأضرار الناتجة عن الوصول غير المصرح، والتي يمكن أن تؤدي إلى تأثيرات سلبية وخسائر مالية تعرض المنشاة لمواجهة مشاكل تؤثر في تحقيق أهدافها الاستراتيجية وفقدان سمعتها وتكبدها لمبالغ مالية.
2. أن من أكبر المخاطر الرقمية التي تواجه الشركات في العصر الحديث هي مخاطر الأمن السيبراني بسبب تزايد المخاوف من الهجمات السيبرانية والأضرار والتحريف المتعمد للمعلومات والبيانات وتعد هذه المخاطر الأعلى من ضمن قائمة أعلى خمسة مخاطر محتملة الحدوث.
3. كانت الأوساط الحسابية المرجحة لجميع فقرات مخاطر الأمن السيبراني حيث بلغ الوسط الحسابي المرجح العام لكل الإجابات (4.069) وانحراف معياري بلغ (0.522) وقيمة (t) الجدولية (12.786)،

وهي نسبة مرتفعة وهذا يشير إلى أن هناك تأثير لمخاطر الأمن السيبراني على تعزيز ثقافة الوعي بالأمن السيبراني لدى المدقق الخارجي. مما انعكس بشكل إيجابي على النتائج.

4. كانت الأوساط الحسابية المرجحة لجميع فقرات المدقق الخارجي حيث بلغ الوسط الحسابي المرجح العام لكل الإجابات (3.926) وانحراف معياري بلغ (0.526) وقيمة (t) الجدولية (10.989)، وهي نسبة مرتفعة وهذا يشير إلى أن هناك تأثير لمخاطر الأمن السيبراني على عملية تخطيط وتنفيذ والإجراءات الميدانية لعملية التدقيق من قبل المدقق الخارجي، مما انعكس بشكل إيجابي على النتائج.

5. كانت الأوساط الحسابية المرجحة لجميع فقرات هناك تأثير لمخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي في ظل التطورات الرقمية الحديثة". حيث بلغ الوسط الحسابي المرجح العام لكل الإجابات (3.213) وانحراف معياري بلغ (0.635) وقيمة (t) الجدولية (2.089)، وهي نسبة مرتفعة وهذا يشير إلى أن هناك تأثير لمخاطر الأمن السيبراني على كفاءة وفاعلية المدقق الخارجي، وفقاً لآراء المدققين الخارجيين والأكاديميين المختصين مما انعكس بشكل إيجابي على النتائج.

ثانياً: التوصيات:

1. ضرورة قيام إدارة الشركة بالتنسيق والتعاون مع الهيئات والمنظمات المهنية المختصة بتقنية المعلومات بصياغة وإصدار الإرشادات والمعايير التي تنظم عملية إعداد وعرض تقرير مخاطر الأمن السيبراني وذلك لتلبية كافة احتياجاتها كافة.

2. ضرورة قيام الهيئات الرقابية المختصة بحث وتوجيه وزيادة وعي الشركات بأهمية مخاطر الأمن السيبراني على القوائم والتقارير المالية السنوية وإجراء المزيد من الإفصاحات عنها وفرض عقوبات صارمة على الشركات في حالة عدم الالتزام بتلك الإفصاحات في حالة تعرضها لأية اختراقات أو انتهاكات واتخاذ الإجراءات التنظيمية اللازمة لمواجهة تلك الاختراقات.

3. يجب على الجهات المهنية المختصة بإصدار معايير المحاسبة والتدقيق بتوفير كافة الإرشادات اللازمة عن محتوى تقارير مخاطر الأمن السيبراني ومسؤولية المدقق الخارجي عند قيامه بتدقيق تلك التقارير الخاصة بالإفصاح عن مخاطر الأمن السيبراني.

4. استحداث قسم أو وحدة خاص بإدارة مخاطر الأمن السيبراني في كل شركة من الشركات وإجراء تحديثات مستمرة عليه في ضوء التغييرات والمستجدات التقنية والرقمية والتدريب المستمر للكوادر المعنية

بالأمن السيبراني وتطوير مهاراتهم وتوجيههم بخطورة وعواقب التهديدات والمخاطر والأحداث السيبرانية.

5. إجراء المزيد من الدراسات المستقبلية حول مخاطر الأمن السيبراني وتأثيراته على القوائم والتقارير المالية في الشركات فضلاً عن تأثيراته على كفاءة وفاعلية المدقق الخارجي في ظل التطور المستمر للتقنيات الرقمية الحديثة.

قائمة المصادر

1. أبو سرعة، عبدالسلام عبدالله سعيد، (2010)، التكامل بين المراجعة الداخلية والمراجعة الخارجية، رسالة ماجستير، كلية العلوم الاقتصادية وعلوم التسيير، جامعة الجزائر 3. الجزائر.
2. خالد سامي السيد، الأمن القومي الإلكتروني وجرائم المعلومات، دار النهضة العربية، الطبعة الأولى، 2021.
3. رفاعة، تامر مزيد، (2017)، أصول تدقيق الحسابات وتطبيقاته على دوائر العمليات في المنشأة، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان، الأردن.
4. سعاد، شدري معمر، وكهينه، رشام، (2022)، أثر كفاءة المدقق الخارجي على تحسين جودة التدقيق بالاعتماد على أعمال التدقيق الداخلي – دراسة ميدانية من وجهة نظر محافظي الحسابات والخبراء المحاسبين، مجلة الاستراتيجية والتنمية، المجلد 12، العدد 01، ص 44-63.
5. سواد، زاهر توفيق، (2009)، مراجعة الحسابات والتدقيق، دار الرأية للنشر والتوزيع، عمان، الأردن.
6. شحادة، مها (2022)، تأثير أبعاد التحول الرقمي في النضج الرقمي للمصارف الإسلامية: بحث تطبيقي في البنوك الإسلامية الأردنية، مجلة الجامعة القاسمية للاقتصاد الإسلامي، المجلد، 2 العدد 1.
7. عبد الحفيظ، قزيز، ومرزوق، سقراوي، (2020)، دور التدقيق الخارجي في تحقيق موثوقية المعلومات المحاسبية – دراسة ميدانية، بحث مشترك لاستكمال متطلبات الماجستير، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرباح ورقلة، الجزائر.

8. عبد الرحمن بجاد، دور الأمن السيبراني في تعزيز الأمن الإنساني، رسالة ماجستير في العلوم الاستراتيجية، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية قسم الأمن الإنساني، السعودية، عام 2017، ص 6.

9. عبدالحليم، أحمد حامد محمود، وعثمان، محمد ناجي، وابراهيم، ياسر جمعة زيدان، (2024)، البيانات الضخمة وإجراءات المراجعة الخارجية (التحديات – الفرص) "دراسة ميدانية"، المجلة العلمية للدراسات والبحوث المالية والإدارية -المجلد السادس عشر – العدد الرابع.

10. عبدالقادر، محمد فتحي، (2020)، أثر استخدام البيانات الضخمة على جودة المراجعة الخارجية: دراسة نظرية، مجلة الدراسات التجارية المعاصرة، المجلد السادس، العدد العاشر، الجزء الثاني.

11. عبدالله يحيي سعيد الزهراني، استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة، دراسة مقارنة، رسالة قدمت لنيل درجة الماجستير في العلوم الاستراتيجية، جامعة نايف العربية، للعلوم الأمنية، كلية العلوم الاستراتيجية قسم الدراسات الاستراتيجية، السعودية، عام 2727، ص .11.

12. العبيدي، علي قاسم حسن، وعويد، علي كريم، (2021)، جودة أداء المدقق الخارجي في ظل معايير التدقيق الدولية ومتغيرات البيئة الخارجية، مجلة الريادة للمال والأعمال، المجلد الثاني، العدد(3).

13. عثمان، محمد أحمد عبد العزيز، (2023)، أثر توكيد مراقب الحسابات على الإفصاح عن عمليات إدارة مخاطر الأمن السيبراني على رغبة وقرارات المستثمرين بالأسهم–دراسة تجريبية، مجلة الإسكندرية للبحوث المحاسبية، المجلد السابع، العدد الثاني، ص 167.

14. علي، هبة جمال هاشم، (2023)، منهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل: دليل تطبيقي، المجلة العلمية للدراسات والبحوث المالية والتجارية جامعة دمياط. المجلد الرابع -العدد الثاني – الجزء الثاني.

15. فايز، سايح، (2015)، أهمية تبني معايير المراجعة الدولية في ظل الإصلاح المحاسبي، أطروحة دكتوراه، كلية العلوم الاقتصادية، جامعة البليدة، الجزائر.

16. فرج، هاني خليل فرج. (2022). أثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكتروني على قرار الاستثمار بالأسهم -دراسة تجريبية، مجلة المحاسبة والمراجعة لاتحاد الجامعات العربية. المجلد، 11، العدد 2.

17. فوزي، إسلام، (2019)، الأمن السيبراني: الأبعاد الاجتماعية والقانونية -تحليل سوسيولوجي، المجلة الاجتماعية القومية، المجلد 56، العدد 2، جامعة دمنهور.

18. فيروز، عزوز، (2023)، التدقيق الخارجي كآلية لتحسين جودة المعلومات المحاسبية، رسالة ماجستير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة ابن خلدون، تيارات، الجزائر.

19. القصير، ابتسام محمود، (2024)، حوكمة تقنية المعلومات للحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية في المؤسسات الليبية العامة، مجلة البحوث الأكاديمية العلوم الإدارية والمالية، العدد، 28 المجلد، 2.

20. مجلة البحوث الفقهية والقانونية، العدد 38.

21. محمود، يارا محمود يونس، وحافظ، سماح طارق، والجوهري، ابراهيم السيد، (2025)، أثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارات المستثمرين: دراسة تجريبية، بحث مستل من أطروحة دكتوراه، المجلة العلمية للدراسات والبحوث المالية والتجارية كلية التجارة، جامعة دمياط، المجلد السادس، العدد الأول، الجزء الثاني، يناير 2025.

22. مسعد، محمد فضل، والخطيب، خالد ارغب، (2009)، دراسة متعمقة في تدقيق الحسابات، دار كنوز المعرفة العلمية للنشر والتوزيع، عمان، الأردن.

23. المطيري، خالد ظاهر (2022)، دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي.

24. Alic, D. (2021). The role of data protection and cybersecurity regulations in artificial intelligence global governance: a comparative analysis of the European Union, the United States, and China Regulatory Framework. Search in.

25. Alidarous, M. (2024). Driving Venture Capital Interest: The Influence of the Big 4 Audit Firms on IPOs. Journal of Risk and Financial Management, 17(7), 292.

26. Al-Matari, O. M., Helal, I. M., Mazen, S. A., & Elhennawy, S. (2021). Integrated framework for cybersecurity auditing. Information Security Journal: A Global Perspective, 30(4), 189-204.

27. Althonayan, A., & Andronache, A. (2018, September). Shifting from information security towards a cybersecurity paradigm. In Proceedings of the 2018 10th International Conference on Information Management and Engineering (pp. 68-79).

28. American Institute of Certified Public Accountants (AICPA (2018b), "SOC for cyber security: a backgrounder.

29. Andreadis, L., Kalotychou, E., Louca, C., Lundblad, C. T., & Makridis, C. (2022). Cyberattacks, Media Coverage and Municipal Finance. Media Coverage and Municipal Finance (October 14, 2022).

30. Antunes, M., Maximiano, M., & Gomes, R. (2022). A Client-Centered Information Security and Cybersecurity Auditing Framework. Applied Sciences, 12(9), 4102.

31. Coffie, W., & Bedi, I. (2019). The effects of IFRS adoption and firm size on audit fees in financial institutions in Ghana. Accounting Research Journal, 32(3), 436-453.

32. Conteh, N. Y., & Schmick, P. J. (2021). Cybersecurity risks, vulnerabilities, and countermeasures to prevent social engineering attacks. In Ethical hacking techniques and countermeasures for cybercrime prevention (pp. 19-31). IGI Global.

33. Elnagar, S. M. A., Ahmed, A. S. A. A., & Basiouny, M. M. M. (2024). The Impact of Cybersecurity Risk Disclosure on the Quality of Financial Reporting and Market Value. Evidence from Egyptian Stock Market. Educational Administration: Theory and Practice, 30(5), 2504-2516.

34. Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2019). How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. Journal of Information Systems, 33(3), 183-200.

35. Haapamaki, E. and J. Sihvonen.2019. Cybersecurity in accounting research. Managerial Auditing Journal, Vol. 34, No. 7: 808-834.

36. Haapamäki, E. and J. Sihvonen.2019. Cybersecurity in accounting research. Managerial Auditing Journal, Vol. 34, No. 7: 808-834.

37. Hamm, K. (2019). Keynote Address Cybersecurity: Where Are We, and What More Can Be Done?. The CPA Journal, 89(8), 34-39.

38. Harris, D., Kuzey, C. Naaman, C. & Sahyoun, N. (2023). Cybersecurity Risk Disclosure Quality: Does it affect the Cost of Debt? Journal of Forensic and Investigative Accounting. 15(2):1-21.

39. Hartmann, C. C., & Carmenate, J. (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.

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

41. Li, B., Li, Y., Pittman, J., & Wang, W. (2022). Auditors' Response to Cybersecurity Risk: Human Capital Investment and Cross-Client Influence. Available at SSRN 4192802.

42. Mendhurwar, S., & Mishra, R. (2021). Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. Enterprise Information Systems, 15(4), 565-584.

43. Muravskyi, Volodymyr (2021), Accounting and Cybersecurity: Monograph Kindle Publishing, KDP, Seattle. USA.

44. No, W. G., & Vasarhelyi, M. A. (2017). Cybersecurity and continuous assurance. Journal of Emerging Technologies in Accounting, 14(1), 1-12.

45. Pei, R., Jin, Z., and Yang, Z. (2020). Cyber-attacks Measurement for Public Companies: An Empirical Analysis. (https://papers.ssrn.com).

46. Price water housecoopers. (PwC). (2020). Managing the impact ofCOVID-19 on cyber security.

47. Public Company Accounting Oversight Board – PCAOB (2013). Considerations for Audits of Internal Control over Financial Reporting: Public Company Accounting Oversight Board (PCAOB).

48. Rosati, P., Gogolin, F., & Lynn, T. (2019). Audit Firm Assessments of Cyber-Security Risk: Evidence from Audit Fees and SEC Comment Letters. The International Journal of Accounting, 54(3).

49. Rosati, P.2019. Audit Firm Assessments of Cyber-Security Risk: Evidence from Audit Fees and SEC Comment Letters. The International Journal of Accounting, Vol. 54, No. 3:1-56.

50. Roskot, M., Wanasika, I., & Kroupova, Z. (2021). Cybercrime in Europe: surprising results of an expensive lapse. Journal of Business Strategy, 42(2), 91-9.

51. Singh, H. (2024). Is corporate reputation associated with voluntary cybersecurity risk reporting?. Meditari Accountancy Research.

52. Singh, H. (2024). Is corporate reputation associated with voluntary cybersecurity risk reporting?. Meditari Accountancy Research.

53. Smith, T., Jones, A., Johnson, L., & Smith, L. (2019). Examination of cybercrime and its effects on corporate stock value. Journal of Information, Communication and Ethics in Society, 17(1), 42-60.

54. Smith, T., Jones, A., Johnson, L., & Smith, L. (2019). Examination of cybercrime and its effects on corporate stock value. Journal of Information, Communication and Ethics in Society, 17(1), 42-60.

55. Van Zyl, W., & Uliana, E. (2022). Fixing diluted earnings per share: Recognizing the dilutive effects of employee stock options. Accounting & Finance, 62(2), 2993-3019.

56. Vekez, N. 2019. Three Studies on Cybersecurity Disclosure and Assurance, A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy. University of Central Florida.

57. https://bakkah.com/ar/knowledge-center.

58. https://hbrarabic.com.

59. https://www.a-h-g.net/ar/news.