أثر مقومات الأمن السيبراني في جودة التدقيق الخارجي في تدقيق شركات التكنولوجيا المالية في الأردن في ضوء معيار التدقيق الدولي رقم 220.

فادي جمال الخروف* **أ.د عماد يوسف أحمد****

تاريخ وصول البحث: 2024/9/9م تاريخ قبول البحث: 2024/11/19م

الملخص

هدف هذا البحث إلى التعرف على أثر مقومات الأمن السيبراني في جودة التدقيق الخارجي في تدقيق شركات التكنولوجيا المالية في الأردن في ضوء معيار التدقيق الدولي رقم 220، من خلال تصميم وتطوير استبانة وتوزيعها على عينة البحث المكونة من (191) محاسبا قانونيا، وباستخدام برنامج التحليل الإحصائي (SPSS)، حيث أظهرت النتائج أنه يوجد أثر ذو دلالة احصائية لمتغير مقومات الأمن السيبراني بأبعاده مجتمعة في جودة التدقيق الخارجي في شركات التكنولوجيا المالية في الأردن، وأن جميع أبعاد المتغير التابع مرتبطة بشكل إيجابي بأبعاد المتغير المستقل وتتأثر بدرجة عالية بمقومات الأمن السيبراني. وقد توصل البحث إلى مجموعة من التوصيات أهمها: استمرار المدققين الخارجيين المزاولين بتدقيق الأنظمة والبرامج وتطبيق المعايير الملزمة وإصدار التقارير حول كفاية أنظمة الأمن السيبراني وإكساب المدققين الخارجيين المزاولين المزيد من المعرفة بالأمن السيبراني وإجراءات الحماية حول الهجمات السيبرانية والاطلاع عليها مما يساهم في رفع جودة التدقيق.

الكلمات المفتاحية: الأمن السيبراني، جودة التدقيق، المدقق الخارجي، معيار التدقيق الدولي رقم 220.

*باحث.

** أستاذ دكتور، قسم المحاسبة، جامعة العلوم الإسلامية العالمية.

The Impact of Cybersecurity Elements on the Quality of External Auditing of Financial Technology Companies in Jordan in Light of International Auditing Standard No. 220

Abstract

This research aims to identify the impact of cybersecurity elements on the quality of external auditing of financial technology companies in Jordan in light of International Auditing Standard No. 220, by designing and developing a questionnaire and distributing it to a research sample consisting of (191) certified accountants, and using the statistical analysis program (SPSS), where the results showed that there is a statistically significant impact of the cybersecurity variable in its combined dimensions on the quality of external auditing with all its dimensions in financial technology companies in Jordan. The results also showed that all dimensions of the dependent variable are positively impacted to the dimensions of the independent variable and are highly affected by the elements of cybersecurity. The research reached a set of recommendations, the most important of which are: Continuing the practice of external auditors to audit systems and programs, applying binding standards, issuing reports on the adequacy of cybersecurity systems, providing practising external auditors with more knowledge of cybersecurity and protection procedures about cyber-attacks and reviewing them, which contributes to raising the quality of auditing.

Keywords: Cybersecurity, Audit Quality, External Auditor, ISA No. 220.

المقدمة:

دفع التطور الاقتصادي والتبادل التجاري على المستوى المحلي والعالمي وانتشار الشركات وحدة المنافسة إلى ضرورة وجود آلية مبتكرة لتنفيذ العمليات المالية اليومية التي تمتاز بضرورة التنفيذ بسرعة عالية جداً وبأعداد كبيرة من الحركات، سواء على مستوى الأفراد أو الشركات والمؤسسات الحكومية، ومن هنا ظهرت شركات التكنولوجيا المالية التي يمكنها تنفيذ تبادل الحركات المالية في ظل أنظمة متخصصة قادرة على تنفيذها بدقة وسرعة عالية بغض النظر عن عدد الحركات ضمن إطار رقابي داخلي وبما يتوافق مع الأنظمة والتعليمات الإلزامية الصادرة عن الجهات المختصة ومراعاة المعايير الدولية للمحاسبة والتدقيق، ونظراً إلى أن هذا النوع من الأنشطة والشركات يرتكز على ربط الأنظمة عبر الشبكات الداخلية وعبر الإنترنت ومخاطرها المتأصلة بسبب طبيعة النشاط، فتكون معرضة إلى مخاطر الهجوم لأغراض إما التخريب أو التعديل أو الحذف والابتزاز أو كشف البيانات والمعلومات السرية أو تدمير أصولها، وهو ما يعرف بالهجوم السيبراني، مما يعرض البيانات المالية إلى التحريف الجوهري وبالتالي التأثير على الأدلة التي يهدف المدقق المستقل إلى جمعها لتشكيل رأيه حول عدالة البيانات المالية. وحيث إن الأمن السيبراني من المواضيع المتجددة والمتطورة بشكل مستمر وبسبب عدم قدرة بعض الأنظمة والبنية التحتية من مواكبة هذا التطور السريع سواء على مستوى الدولة أو على مستوى قطاع شركات التكنولوجيا المالية وكون أن العمليات المالية تتم بشكل آلي داخل أنظمة مغلقة، فقد يكون من الصعب على المدقق المستقل تتبع الحركات وجمع الأدلة بالطريقة التقليدية، ويحتاج قبل ذلك إلى امتلاك المعرفة القانونية والفنية اللازمة على هذه الأنظمة أو الاستعانة بمدقق فني لتكنولوجيا المعلومات، وإجراء بعض الاختبارات للتحقق من سلامة الأنظمة والتنفيذ للعمليات والتحقق من التزام المدقق وأعضاء فريق التدقيق بمعايير التدقيق المعمول بها وآداب السلوك المهني لضمان جودة التدقيق، وبسبب تعرض هذا النوع من الشركات إلى مخاطر سيبرانية بشكل مستمر، فقد دفع الجهات المنظمة للمهنة والمعايير إلى وضع الضوابط والإرشادات والقوانين لمواجهتها والتحسين على جودة التدقيق المطلوبة من المدقق الخارجي بما يكفل تقديم رأي مهني معقول وعادل لأصحاب المصلحة

مشكلة وأسئلة البحث:

- تم تحديد مشكلة البحث في شركات التكنولوجيا المالية التي تحتاج إلى تدقيق فني مستقل إضافة إلى تدقيق مالي مستقل، من خلال مدققين ذوي خبرة كبيرة في هذا المجال، حيث

إن شركات التكنولوجيا المالية تعتمد بشكل كبير ورئيس على تكنولوجيا المعلومات وعرضة كبيرة للهجمات السيبرانية، ومن هنا تبدأ مشكلة البحث لمحاولة التعرف على أثر مقومات الأمن السيبراني في جودة التدقيق الخارجي وفقاً لمعيار التدقيق الدولي رقم 220، وتكمن مشكلة البحث في الأسئلة التالية:

السؤال الرئيس: هل يوجد أثر لمقومات الأمن السيبراني في جودة التدقيق الخارجي في شركات التكنولوجيا المالية في الأردن؟

السؤال الفرعي الأول: هل يوجد أثر لمقومات الأمن السيبراني في المتطلبات الأخلاقية والاستقلالية في شركات التكنولوجيا المالية في الأردن؟

السؤال الفرعي الثاني: هل يوجد أثر لمقومات الأمن السيبراني في قبول الارتباط الجديد والاستمرار في الارتباط في شركات التكنولوجيا المالية في الأردن؟

السؤال الفرعي الثالث: هل يوجد أثر لمقومات الأمن السيبراني في تنفيذ الارتباط في شركات التكنولوجيا المالية في الأردن؟

الأهمية العلمية للبحث:

تنبع أهمية الدراسة من الناحية النظرية من أهمية جودة التدقيق الخارجي على شركات التكنولوجيا المالية للخروج برأي المدقق الذي يعتبر الركيزة الأساسية حول مدى عدالة البيانات المالية وخلوها من التحريفات الجوهرية، كذلك تناول عنصرا مهماً ذا أثر كبير على شركات التكنولوجيا المالية متمثلة بمقومات الأمن السيبراني التي تعتبر حساسة بسبب طبيعة الأنشطة التشغيلية المالية لهذه الشركات التي تنعكس على البيانات المالية محل تدقيق المدقق الخارجي. كما يتوقع الباحث أن تشكل هذه الدراسة تراكما علميا إضافيا في مجال البحث يمكن تطبيقه على مختلف الشركات والقطاعات.

أهداف البحث:

استناداً إلى الأسئلة المطروحة في المشكلة فإن البحث يهدف إلى قياس أثر ما يلي:

الهدف الرئيس: بيان أثر مقومات الأمن السيبراني في جودة التدقيق الخارجي في شركات تكنولوجيا المعلومات في الأردن.

الهدف الفرعي الاول: بيان أثر مقومات الأمن السيبراني في المتطلبات الأخلاقية والاستقلالية في شركات التكنولوجيا المالية في الأردن.

الهدف الفرعي الثاني: بيان أثر مقومات الأمن السيبراني في قبول الارتباط الجديد والاستمرار في الارتباط في شركات التكنولوجيا المالية في الأردن.

الهدف الفرعي الثالث: بيان أثر مقومات الأمن السيبراني في تنفيذ الارتباط في شركات التكنولوجيا المالية في الأردن.

فرضيات البحث:

Ho1: لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لمقومات الأمن السيبراني بأبعادها مجتمعة (المقومات التكنولوجية، المقومات القانونية، المقومات الاقتصادية) في جودة التدقيق الخارجي بأبعدها (المتطلبات الأخلاقية والاستقلالية، قبول الارتباط الجديد والاستمرار في الارتباط، تنفيذ الارتباط) في شركات التكنولوجيا المالية في الأردن.

الفرضية الفرعية الأولى:Ho1-1 : لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لمقومات الأمن السيبراني في المتطلبات الأخلاقية والاستقلالية في شركات التكنولوجيا المالية في الأردن.

الفرضية الفرعية الثانية: Ho1-2: لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لمقومات الأمن السيبراني في قبول الارتباط الجديد والاستمرار في الارتباط في شركات التكنولوجيا المالية في الأردن.

الفرضية الفرعية الثالثة: Ho1-3: لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لمقومات الأمن السيبراني في تنفيذ الارتباط في شركات التكنولوجيا المالية في الأردن.

الإطار النظري والدراسات السابقة:

الأمن السيبراني:

عرف Kshetri (2013,6) الأمن السيبراني على انه مجموعة الإجراءات اللازمة لإدارة المخاطر وتقديم أفضل حماية ممكنة لأصول الأفراد والشركات بما فيها المستخدمين، وحماية البنية التحتية والأنظمة والبرامج من الهجمات الإلكترونية أو الوصول غير المصرح به (Arnes, 2023, 4)، وهو مجموعة من الوسائل والخطوات التي تمكن من حماية البيانات والمعلومات السرية من غير المصرح لهم والحفاظ على سريتها ولكن بشكل مرن بحيث يتم عرضها للبعض ممن يملكون رخصة الوصول في الوقت المناسب (مؤسسة النقد العربي السعودي Saudi Arabian Monetary Authority May. 2017, 5).

مقومات الأمن السيبراني:

اولاً المقومات التكنولوجية:

أ-تقييم المخاطر والرقابة الداخلية: يجب على إدارة الشركة أن تعمل على تقييم مستوى المخاطر التي قد تتعرض لها الشركة بناء على طبيعة النشاط وحجم العمليات وتصنيفها إما كمخاطر متأصلة أو مخاطر متبقية ووضع نظام رقابي فعال لتخفيض الخطر أو قبوله أو مشاركته أو حتى تجنبه (Romney & Steinbart, 2018, 209)، حيث إن مسؤولية الرقابة الداخلية تقع على عاتق إدارة الشركة بالدرجة الاولى، فالشركة مسؤولة عن تصميم أنظمة رقابة داخلية تمنع من وقوع التحريف الجوهري الذي قد ينشأ عن الغش أو الخطأ المادي، واكتشافه عند حدوثه وتصحيحه بعد وقوع التحريف (ذنيبات، 2015، 173).

ب-المراقبة: تتثمل بمجموعة من الإجراءات التي يتم العمل بها لتوفير درجة معقولة من التأكيد بأن نظام الرقابة الداخلي يحقق أهدافه، وكلما كان نظام الرقابة فعالاً أكثر تَمَّ تقليل درجة المخاطر ومخاطر التحريفات الجوهرية (Romney & Steinbart, 2018, 345).

ج-الاستجابة والتعافي: هي قدرة الشركة من الاستجابة على الهجمات السيبرانية وفي الوقت والسرعة المناسبة، ويشمل ذلك احتواء عملية الاختراق على نطاق ضيق والتواصل بين الأفراد المسؤولين داخل الشركة، وهنا تكمن خبرات الأفراد وقوة الأنظمة الداخلية وتبدأ من الاعتراف بوجود الخلل ثم تقييم طبيعة الهجمة السيبرانية ومصدر ودوافع الهجوم والضرر المتوقع ثم عملية الاحتواء والسيطرة وضمان عدم الانتشار بشكل أوسع والتحرك الفوري لإصلاح الضرر بأسرع وقت ممكن، ثم الإبلاغ لأصحاب المصلحة المعنيين والجهات المختصة، وبعد التعافي واستئناف الأعمال (البنك المركزي الأردني، 2018، 6؛ العامري وآخرون، 2021، 34؛ Romney & Steinbart, 2018, 381).

ثانياً المقومات القانونية:

أ-إطار الأمن السيبراني:

هي مجموعة من التشريعات والأنظمة والتعليمات التي يتم وضعها من قبل المؤسسات أو المنظمات المحلية والدولية بهدف حماية الأفراد والشركات وأصولها من الهجمات السيبرانية (Kshetri, 2013, 4)، وقد يتم التنسيق ما بين الخبراء في القطاع الخاص والأفراد والمؤسسات الحكومية على وضع مجموعة من التشريعات الهادفة إلى الحماية (Didenko, 2020, 162)،

ورغم عدم وجود تعريف موحد أو قانون أو معيار دولي موحد، إلا أن هنالك محاولات للخروج بمعايير دولية لكل قطاع من الصناعة أو بيئة الأعمال، مثل المعيار الدولي ISO/IEC 27001 الخاص بالنهج الشمولي لأمن المعلومات (ISO, the International Organization for Standardization, 26/3/2024) و معيار Financial Industry Regulatory الخاص بحماية المستثمرين في الأسواق المالية من الغش والتلاعب (FINRA, 26/3/2024) ومعيار قابلية نقل التأمين والمساءلة Health Insurance Portability and Accountability Act (HIPAA) (Health and Human Services, 2024) ومعايير أمن بيانات صناعة بطاقات الدفع Payment Card Industry Data Security Standards (PCI-DSS) (Security Standard Council, 2024).

ب-الحوكمة المؤسسية:

هي نظام من خلاله يتم توزيع المهام والمسؤوليات والصلاحيات للأفراد في الشركات بهدف ضمان سير الأعمال بطريقة منظمة ومسؤولة (دائرة مراقبة الشركات، 2017، 2)، وعلاقتهم بأصحاب المصلحة ضمن هيكل تنظيمي معلن ومعمم على كافة المستويات (Ciftci et al., 2019, 91)، مما يحقق التوازن بين أصحاب المصلحة والتركيز على تحقيق المصالح والأهداف العامة لكل قسم دون التعارض مع المصالح والأهداف الرئيسية للشركة ككل (Wheelen & Hunger, 2012, 45).

ثالثاً المقومات الاقتصادية:

يتم وضع موازنات مالية في شركات وضمن الموازنة السنوية العامة لها لتغطية العديد من النفقات التي قد تتكبدها الشركة لحماية الأفراد والأصول لديها من الهجمات السيبرانية مثل تكاليف البنية التحتية تقليدية Physical Infrastructure، أو بنية تحتية سحابية Cloud Infrastructure (Kim, 2012, 80) والرسوم القانونية والمهنية والتصميم والتدريب والتطوير والرقابة وإدارة النظام والبرامج والصيانة والتدقيق The International Civil Aviation Organization (ICAO, 2024)، بما في ذلك التكاليف المترتبة على حلول الامتثال المرتبطة بحماية البيانات والمعلومات البرامج والأنظمة والافراد، وتكلفة الاسترداد والتعافي (Romney & Steinbart, 2018, 304) وصولاً إلى التدريب والتعليم المستمر (Morgan, 2023).

جودة التدقيق الخارجي:

تتثمل جودة التدقيق في مقدرة المدقق على اكتشاف التحريفات الجوهرية في البيانات المالية التي تعدها الإدارة في حال وُجدت والموضوعية والاستقلالية التي يتمتع بها المدقق، فهي وصف

لمدى نجاح المدقق في جميع مراحل عملية التدقيق سواء قبل وخلال وبعد عملية التدقيق في اكتشاف التحريفات الناشئة عن غش أو خطأ مادي في البيانات المالية، وفي هذا حماية لمصالح المستفيدين من البيانات المالية وبشكل عادل (Dang, 2004, 2)، وتتضمن جودة التدقيق في ظل ما ورد في معيار التدقيق الدولي رقم 220 رقابة الجودة لمراجعة القوائم المالية Quality control for an audit of financial statements، المسؤولين عن رقابة الجودة، المتطلبات الأخلاقية والاستقلالية، قبول الارتباط الجديد والاستمرار في الارتباط، موارد الارتباط البشرية، تنفيذ الارتباط، التفتيش، و التوثيق (Lessambo, 2018, 60؛ Arens et al., 2017, 64).

أ-المتطلبات الأخلاقية والاستقلالية:

يجب على مدقق الحسابات التمتع بها طيلة مهمة الارتباط، التي يجب على الشريك المسؤول في مكتب التدقيق وبشكل مستمر التحقق من توفر هذه المتطلبات لدى فريق التدقيق، وأن يقوم باتخاذ الإجراء المناسب فور ملاحظة اي فقدان لها لدى الفريق أو أي من أعضائه (International Auditing and Assurance Standards Board, 2017, 175). ومن أهم المتطلبات الأخلاقية للمدقق النزاهة، الموضوعية، الكفاءة المهنية والعناية الواجبة، السرية، والسلوك المهني (Arens et al., 2017, 793).

ب-قبول الارتباط الجديد والاستمرار في الارتباط:

يجب على المدقق سواء كان يعمل بشكل منفرد أو على الشريك المسؤول في مكتب التدقيق، أن يقرر قبول الاستمرار مع العميل الحالي لمهمة تدقيق جديدة أو قبول عميل جديد من خلال اتخاذ الإجراءات اللازمة والمناسبة للتحقق من مدى إمكانية قبول الارتباط من رفضه، وفي حال وجد المدقق لاحقاً ان المعلومات التي حصل عليها لم تكن كافية أو مناسبة وتبين له ما يفيد بعدم قبول الارتباط في حال توفرت هذه المعلومات لديه قبل اتخاذ قرار الارتباط، فيجب أن يتم إبلاغ مكتب التدقيق وبشكل فوري ليتم اتخاذ القرار المناسب وبعد الحصول على التشاور الداخلي (International Auditing and Assurance Standards Board, 2017, 176).

ج-تنفيذ الارتباط:

يتم تنفيذ مهمة الارتباط بالتوجيه والإشراف أولاً ومن ثم أداء المهمة والفحص ثم التشاور وفحص جودة الارتباط بمهمة التدقيق، وكما يلي International Auditing and Assurance Standards Board

(2017, 177):

التوجيه والإشراف والأداء: يجب على الشريك المسؤول في مكتب تدقيق الحسابات أن يقوم بالتوجيه والإشراف على فريق التدقيق الخاص بمهمة الارتباط والتحقق من أنه يتم تنفيذ مهمة الارتباط بما يتوافق مع معايير مهنة التدقيق والقوانين والأنظمة والتعليمات الصادرة والمعمول بها بالإضافة إلى السياسات الداخلية لمكتب التدقيق.

الفحص: يجب على الشريك المسؤول أن يقوم بإجراء الفحص حول مدى التوافق والالتزام بالسياسات الداخلية لمكتب التدقيق وحول كفاية الأدلة التي تم الحصول عليها من قبل فريق التدقيق ومناسبتها وكفايتها لتشكيل الرأي حول البيانات المالية والنتائج التي توصل إليها فريق التدقيق.

التشاور: يجب ان يتم إجراء التشاور بين فريق الارتباط أو الفريق داخل مكتب التدقيق حول مهمة الارتباط والمواضيع المعقدة فيها، وأن هذه المشاورات قد تم العمل على تنفيذ نتائجها وذلك لضمان الحصول على رأي مهني من خلال تنفيذ مهمة الارتباط وحتى إصدار الرأي المهني.

فحص رقابة جودة التدقيق: تشمل جودة التدقيق جميع المهام والمتطلبات الأخلاقية والاستقلالية والسلوك المهني واختيار فريق التدقيق المناسب لمهمة الارتباط والالتزام بالمعايير الصادرة من الجهات التنظيمية والقوانين والتعليمات من الجهات المختصة المعمول بها والسياسات الداخلية لمكتب التدقيق، وعمليات التشاور ومناقشة الإصدار الجوهرية والهامة والتوثيق، وتعيين مسؤول لفحص الرقابة على جودة عملية الارتباط، وعدم إصدار تأريخ تقرير المدقق حول البيانات المالية قبل التحقق من أن فحص رقابة جودة الارتباط قد تمت بالفعل وبشكل صحيح وأن البيانات المالية قد تم فحصها مع فحص استنتاجات فريق مهمة التدقيق والعمل على تقويمها إن كان يلزم.

الدراسات السابقة:

أجرى علي (2023) دراسة هدفت هذه الدراسة إلى التوصل لمنهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل، وبالتالي التعرف على أثر مخاطر الأمن السيبراني على نطاق ومسؤوليات المدقق الخارجي، ومن أهم النتائج التي توصلت إليها الدراسة، وجود علاقة بين مخاطر وتهديدات الأمن السيبراني على المراجعة الداخلية وبالتالي على المراجع الخارجي، وأن تقييم مخاطر الأمن السيبراني لدى الشركات يعتمد على المدقق الخارجي،

ومن أهم توصيات الدراسة، ضرورة تضمين مخاطر الأمن السيبراني في تقييمات المدقق لمخاطر تكنولوجيا المعلومات في شركة العميل.

وقام فريد (2022) بعمل دراسة هدفت هذه الدراسة إلى إيضاح الدور المقترح لمراجع الحسابات في إضفاء الثقة على تقرير إدارة مخاطر الأمن السيبراني، التعرف على الكيفية التي تتم بها إدارة مخاطر الأمن السيبراني والاعتبارات الخاصة بالأمن السيبراني عند تقييم المخاطر في مرحلة التخطيط لعملية التدقيق وكيفية الاستجابة لها، ومن أهم النتائج التي توصلت إليها الدراسة، أنه يجب على مدقق الحسابات الخارجي أن يتوفر له الفهم الكافي حول كامل التأثير لمخاطر تكنولوجيا المعلومات بشكل شامل وكيفية الاستجابة لها، وأن يتم عمل تدقيق فني مستقل فيما يتعلق بإدارة الأمن السيبراني من قبل العميل، وأوصت الدراسة، بضرورة إدارة مخاطر الأمن السيبراني من قبل الشركات التي اعتمدت إلى التحول الرقمي في أعمالها.

أجرى العلوان (2022) دراسة هدفت هذه الدراسة إلى تحديد أدوار الأمن السيبراني المعتمد على الذكاء الاصطناعي المشتق من أمن المعلومات المتعلق بمرحلة الحماية الوقائية ومرحلة الاكتشاف ومرحلة المعالجة (التصحيح) بعد الاكتشاف، كما هدفت إلى التعرف على أهم تحديات الأمن السيبراني ذي الاعتماد على الأمن السيبراني، ومن أهم النتائج التي توصلت إليها الدراسة، هو التأكيد على تحديات الأمن السيبراني المعتمد على الذكاء الاصطناعي في حماية المنظمات وعدم كفاية الأنظمة التقليدية في مواجهة الهجمات السيبرانية غير التقليدية والمتطورة المستمرة، ومن أهم التوصيات بأن تعزز المنظمات الأمن السيبراني المعتمد على الذكاء الاصطناعي لحماية أمن المعلومات ضمن خطط شاملة غير مجزئة.

وقاموا كل من قوجيل وطيبة (2022) بعمل دراسة هدفت هذه الدراسة إلى التعرف على أبرز المخاطر المتولدة من استخدام التكنولوجيا المالية بمختلف تقنياتها في القطاع المصرفي ومدى الترابط بين كل من التكنولوجيا المالية والنشاط المالي وكيفية توفير إجراءات التجنب والوقاية من تلك المخاطر، ومن أهم النتائج التي توصلت إليها الدراسة، أن مخاطر تكنولوجيا المعلومات تختلف عن المخاطر المتعارف عليها في التشغيل التقليدي للعمليات المالية متمثلة بتهديدات الخطر السيبراني أو مخاطر الإنترنت، مما يدفع إلى إيجاد طرق حماية دائمة ومستمرة، مع التوصية بضرورة إيجاد تحالف دولي لإدارة المخاطر المرتبطة بالتقنيات المالية وسن القوانين والإرشادات والأنظمة لمواجهة مخاطر التكنولوجيا المالية.

وأجرى بكاي (2022) دراسة هدفت هذه الدراسة إلى تحقيق فهم أعلى بمدى تأثيرات عوامل العولمة الرقمية وتكنولوجيا ومن ثم تقييم تجارب مختلفة من أقاليم متنوعة عالمية في استخدامات تكنولوجيا المعلومات في مهنة التدقيق الخارجي، ومن أهم النتائج التي توصلت إليها الدراسة، وجود علاقة بين تكنولوجيا المعلومات وبين مهنة التدقيق، بحيث تتأثر جودة التدقيق بتكنولوجيا المعلومات بشكل إيجابي أو سلبي وهذا يعتمد على الأساليب الحديثة التي يتم تطبيقها التي يجب تطويرها وبشكل مستمر لمواكبة التطور التكنولوجي، ومن أهم التوصيات، وضع البرامج التوعوية لرفع مستوى المعرفة بالتقنيات الرقمية في أعمال التدقيق ومراجعة التشريعات القانونية المتعلقة بكل من الافصاح الرقمي وما يخص أدلة الاثبات الرقمية.

كما قام دراسة الشهري (2021) بدراسة هدفت هذه الدراسة إلى التعرف على مدى التزام مدققي الحسابات في مكاتب التدقيق الكويتية بتطبيق معيار جودة التدقيق الدولي رقم 220 فيما يتعلق بكل من (المتطلبات المهنية و الأخلاقية، قبول العملاء الجدد والاستمرار مع العملاء الحاليين، توزيع المهام، التنفيذ و التوجيه، التفتيش، والتوثيق)، ومن أهم النتائج التي توصلت إليها الدراسة، التزام مدققي الحسابات العاملين في مكاتب وشركات التدقيق في الكويت بتطبيق معيار التدقيق الدولي رقم 220 بالأبعاد التي أشار إليها المعيار، مع التوصية بضرورة اعتماد مكاتب وشركات التدقيق في الكويت مدونة السلوك الأخلاقي والإجراءات التأديبية بما يتوافق مع معيار التدقيق الدولي 220.

أجرى Usman et al (2024) دراسة هدفت هذه الدراسة إلى تعزيز مراجعة دور المدقق الداخلي في عمليات تقييم المخاطر المتعلقة بالأمن السيبراني في المؤسسات القائمة على التمويل التي تقدم خدمات أعمالها من خلال إطار إنشاء إطار نظري يساعد على تحقيق ذلك، ومن أهم النتائج التي توصلت إليها الدراسة، أن الدراسات المتعلقة بخصائص المدققين الداخليين وتقييم مخاطر الأمن السيبراني تعتبر قليلة وغير قوية في أغلب الدول النامية والقطاع الأكاديمي، وأن هنالك ارتباطا إيجابيا بين خصائص المدقق الداخلي وبين تقييم مخاطر الأمن السيبراني.

قاموا Saputra and Paranoan (2024) بدراسة هدفت هذه الدراسة إلى تقديم الأدلة الأخطاربية الخاصة بتحليل تأثيرات الأمن السيبراني والرقمنة وتصورات البيانات على الجودة المرتبطة بعمليات التدقيق البيئي الداخلي، ومن أهم النتائج التي توصلت إليها الدراسة، أن هنالك علاقة إيجابية بين كل من الأمن السيبراني والرقمنة وتصورات البيانات على جودة عمليات التدقيق الداخلي، حيث إن المدقق الداخلي يسعى كأحد مهامه إلى التحقق من الامتثال للأنظمة

والقوانين، فهم يحتاجون إلى تتبع البيانات لأغراض تقييم الامتثال، ولكن هذا يحتاج إلى بنية تحتية قوية متوافقة مع هذه الأنظمة لحماية البيانات من مخاطر الأمن السيبراني وتوفير بيانات ومعلومات وقرارات موثوقة من خلال الرجوع إلى المعايير الخاصة بالأمن السيبراني.

كما قاموا Alsakini et al. (2024) بدراسة هدفت هذه الدراسة إلى التعرف على مدى تأثير الأمن السيبراني على جودة البيانات المالية، ومن أهم النتائج التي توصلت إليها الدراسة، أن عمليات الاختراقات السيبرانية المتمثلة بالكشف عن المعلومات وسرقات كلمات المرور المشفرة واختراقات قواعد البيانات كان لها تأثير إيجابي وجوهري على البيانات المحاسبية وأن هنالك تأثيرا جوهريا أيضًا لاختراقات الأمن السيبراني على جودة التقارير المالية، وأن الاستجابة السريعة للهجمات السيبرانية يكون لها تأثير كبير في التخفيف من التأثير على البيانات المحاسبية والتقارير المالية وسمعة البنك، كما أوصت الدراسة بضرورة تحول استراتيجية البنوك من الحماية إلى المقاومة وتطوير الاستجابة السريعة وتحسين المعرفة لدى العاملين في المؤسسة حول أحدث تهديدات الأمن السيبراني والعمل على تحديث البرامج المحاسبية والأنظمة الحاسوبية بما يتوافق مع حجم المؤسسة المالية.

وقاموا Kurniawan and Mulyawan (2023) بعمل دراسة هدفت هذه الدراسة إلى فحص العلاقة بين كل من قدرات المعرفة الرقمية لدى المدققين في ظل النمو المستمر لتكنولوجيا المعلومات وتدقيق المخاطر، جهود التدقيق، أداء التدقيق، والعلاقة بين كل من مخاطر التدقيق في ظل نمو تكنولوجيا المعلومات وبين جهود التدقيق وبين أداء التدقيق من جهة أخرى، ومن أهم نتائج الدراسة، أن العلاقة بين المتغيرات إيجابية وأن المدققين أصبحوا أكثر ارتباطاً بتكنولوجيا المعلومات مما يدفعهم إلى التعاون مع فريق تكنولوجيا المعلومات لتقديم معلومات أكثر موثوقية والتكييف مع مخاطر تكنولوجيا المعلومات، ومن أهم النتائج التي توصلت إليها الدراسة، أن الشركات غالباً لا تفصح عن الهجمات السيبرانية طوعاً بعد تعرضها للهجوم، ومن أهم التوصيات، بأن يتم بناء تفادي الافصاح الاختياري من قبل الشركات من خلال التشريعات اللازمة لربط معلومات الهجمات السيبرانية مع مواقع أمنية متاحة للجمهور.

قاموا Ngo and Tick (2021) بعمل دراسة هدفت هذه الدراسة إلى التعرف على العلاقة بين مخاطر الأمن السيبراني وجودة التدقيق الخارجي الذي يتم بذله بشكل إضافي وخاص من قبل المدقق الخارجي للشركات التي واجهت هجمات أمن سيبرانية من خلال فرض رسوم تدقيق أعلى

من المعتاد لمواجهة خطر عدم القدرة على اكتشاف المخاطر المتعلقة بالأمن السيبراني والمؤثرة على البيانات المالية، ومن أهم النتائج التي توصلت إليها الدراسة، أن هنالك زيادة ضغط مستمرة على المدقق الخارجي بسبب تزايد مخاطر وحدة الهجمات السيبرانية وأثرها على البيانات المالية، ووجود علاقة إيجابية بين رسوم التدقيق والهجوم السيبراني، مما يعني زيادة جودة التدقيق الخارجي بسبب مخاطر الهجوم السيبراني، كما أوصت الدراسة بضرورة إجراء المزيد من الدراسات على فترات زمنية أطول وبمعلومات أكثر شمولية.

وقاموا (Almasria et al. (2021 بعمل دراسة هدفت هذه الدراسة إلى فحص دور نظم المعلومات المحاسبية في تحسين جودة إجراءات التدقيق الخارجي الذي يعتمد على نظم المعلومات المحاسبية للحصول على المعلومات المحاسبية محل التدقيق، ومن أهم النتائج التي توصلت إليها الدراسة، أن هنالك تأثيرا هاما لنظم المعلومات المحاسبية في تحسين بعض جوانب جودة التدقيق الخارجي، وأن هنالك وعيا من قبل المدقق الخارجي بأهمية الدور الذي تلعبه نظم المعلومات المحاسبية في تحسين جودة إجراءات التدقيق رغم البطء من قبل المدققين لا سيما الفرديين في الاستجابة للنمو السريع في تكنولوجيا المعلومات، ومن أهم توصيات الدراسة ضرورة قيام الهيئات التنظيمية في الأردن من إنشاء ورش عمل دورية وبشكل منتظم لرفع الوعي حول دور تكنلوجيا المعلومات ودوره في تحسين جودة التدقيق الخارجي.

كما قاموا (Serag and Al Aqiliy (2020 بدراسة هدفت هذه الدراسة إلى التعرف على محددات التطبيق لتحليلات البيانات الضخمة في التدقيق الخارجي، إضافة إلى التعرف على توجه المدققين المحتملين في استخدام تكنولوجيا المعلومات في تحليل البيانات الضخمة ليس من باب تنفيذ التعليمات التنظيمية فحسب، وإنما في تقديم ميزة إضافية للعملاء والمتعلقة بالكفاءة، الفعالية، خفض التكلفة، والجودة، ومن أهم النتائج التي توصلت إليها الدراسة، أن هنالك مجموعة من التحديات التي تقيد استخدام تقنيات تحليل البيانات الضخمة مثل حجم شركة التدقيق، البنية التحتية لنظم المعلومات، وعمليات المراجعة طويلة الأجل.

وقاموا (Rosati et al. (2020 بدراسة هدفت هذه الدراسة إلى التعرف على علاقة حوادث الأمن السيبراني في جودة التدقيق، ومن أهم النتائج التي توصلت إليها الدراسة، أن حوادث الأمن السيبراني لا تؤثر بشكل كبير على جودة التدقيق، وأن شركات التدقيق لديها قدرة كبيرة للتعامل مع التقارير المالية التي يتم تدقيها حتى في ظل عدم وجود التشريعات التنظيمية الكافية، ولكن هذه النتيجة قد لا يكون من المناسب تعميمها لا سيما أن الدراسة على لتدقيق الأربع الكبار

الذين يمتازون بجودة تدقيق على كل الاحوال، وبهذا توصي الدراسة بأن يتم عمل دراسات على الشركات الأخرى غير الأربع الكبار.

منهجية الدراسة (الطريقة والإجراءات):

نوع الدراسة وطبيعتها:

تصنف هذه الدراسة من حيث الطبيعة بأنها دراسة تطبيقية، ومن حيث الغرض فهي إيضاحية؛ كونها تهدف إلى بيان أثر مقومات الأمن السيبراني في جودة التدقيق الخارجي في شركات التكنولوجيا المالية في الأردن، ومن حيث التخطيط فهي غير مخططة؛ كونها تُجرى ضمن حدود بيئة مجتمع الدراسة دون التدخل المُباشر فيها، أما من حيث الزمن فهي مقطعية، كونها تحدث لمرة واحدة.

منهج الدراسة:

استخدم الباحث المنهج الوصفي التحليلي؛ والذي يعتبر من أهم المناهج العلمية التي تتناسب مع هذا النوع من الدراسات، لقدرته على إبراز كافة تفاصيل وعناصر مواضيعها، ووصفها وتحليلها بشكل تفصيلي وشامل، وجمع الحقائق والمعلومات منها، مما يسهم في إغناء المعرفة بها، وتعزيز الفهم بمواضيعها.

مجتمع وعينة الدراسة:

تكون مجتمع الدراسة من المدققين الخارجيين المزاولين لمهنة التدقيق في الأردن، وقد أشارت الإحصائيات الصادرة عن جميعة المحاسبين القانونيين الأردنيين بتاريخ 19 كانون ثاني من عام 2024 المتوفرة على الموقع الإلكتروني (https://jacpa.org.jo/) إلى وجود (412) مدقق خارجي مزاول لمهنة التدقيق في الأردن.

واستخدم الباحث أسلوب العينة العشوائية البسيطة لاختيار أفراد عينة الدراسة، وتم تحديد عددهم من خلال جداول (Sekaran & Bougie, 2016) الإحصائية التي بلغت (199) مدققاً مزاولاً وذلك عند نسبة هامش خطأ (5%) ومستوى ثقة (95%).

وحدة (التحليل) المعاينة:

تكونت وحدة (التحليل) المعاينة من المدققين الخارجيين المزاولين في الأردن، وعددهم (199) مدققاً. وتمت عملية توزيع الاستبانات على المدققين إلكترونياً من خلال إرسال رابط الاستبانة إلى جميعة المحاسبين القانونيين الأردنيين، الذين أبدوا استعداداً بنشرها على المدققين الخارجيين

المزاولين في الأردن، واستعادتها إلكترونياً، حيث تم استرداد (191) استبانة كانت جميعها صالحة لتطبيق التحليل، وبنسبة استرداد (96.0%) من مجموع الاستبانات الموزعة.

طرق جمع البيانات:

اتجه الباحث في إعداد الإطار العملي للدراسة إلى استخدام الاستبانة التي تم تصميمها بالاعتماد على مصادر البيانات والمعلومات الثانوية بما يتناسب مع مواضيع الدراسة والمتغيرات الممثلة في أنموذج الدراسة.

أداة الدراسة:

تعتبر أداة الدراسة الوسيلة التي استخدمتها الدراسة الحالية لجمع البيانات اللازمة عن متغيرات الدراسة، المتمثلة بمقومات الأمن السيبراني وجودة التدقيق الخارجي. وقد تمثلت هذه الأداة في الاستبانة التي تم توجيهها إلى المدققين الخارجيين المزاولين في الأردن؛ بهدف جمع المعلومات العامة عن هؤلاء المدققين واستخلاص الحقائق عن المتغيرات في بيئة الدراسة من خلال إبداء الآراء حول الفقرات المخصصة لقياسها. ولذا، تم تقسيم الاستبانة إلى (3) أجزاء، وعلى النحو الآتي:

الجزء الأول: الخصائص الشخصية والوظيفية، يهدف هذا الجزء من الاستبانة إلى جمع المعلومات العامة عن أفراد وحدة (التحليل) والمعاينة والمتمثلة في المدققين الخارجيين المزاولين في الأردن، حيث طرحت الاستبانة (3) أسئلة شخصية ووظيفية تتعلق بهم وتمثلت في العمر والمؤهل العلمي وعدد سنوات الخبرة.

الجزء الثاني: مقومات الأمن السيبراني، يهدف هذا الجزء من الاستبانة إلى جمع الحقائق والمعلومات عن مقومات الأمن السيبراني، من خلال إبداء درجة الموافقة على الفقرات التي تمت صياغتها بما يتناسب مع المتغيرات الفرعية المستخدمة لقياسه، التي تمثلت في (3) متغيرات وهي: المقومات التكنولوجية، والمقومات القانونية، والمقومات الاقتصادية.

الجزء الثالث: جودة التدقيق الخارجي، يهدف هذا الجزء من الاستبانة إلى جمع الحقائق والمعلومات عن جودة التدقيق الخارجي حسب المعيار الدولي للتدقيق رقم 220، من خلال إبداء درجة الموافقة على الفقرات التي تمت صياغتها بما يتناسب مع المتغيرات الفرعية المستخدمة لقياسه، التي تمثلت في (3) متغيرات وهي: المتطلبات الأخلاقية والاستقلالية، وقبول الارتباط الجديد والاستمرار في الارتباط مع العميل، وتنفيذ الارتباط.

الجدول (1): مستويات الثبات وما يقابلها من قيم لمعاملات كرونباخ ألفا

مستوى الثبات	ثبات منخفض	ثبات متوسط	ثبات مرتفع
قيم معاملات كرونباخ ألفا	أقل من 0.40	0.40 – أقل من 0.70	0.70 – 1.0

والجدول الآتي يعرض نتائج قيم معاملات كرونباخ ألفا لأداة الدراسة الحالية، حيث ظهرت النتائج كما يأتي:

الجدول (2): نتائج اختبار الثبات لأداة الدراسة

الرقم	المتغيرات الرئيسة والفرعية	قيم معاملات كرونباخ ألفا
1	المقومات التكنولوجية	0.861
2	المقومات القانونية	0.910
3	المقومات الاقتصادية	0.822
مقومات الأمن السيبراني		**0.927**
1	المتطلبات الأخلاقية والاستقلالية	0.862
2	قبول الارتباط الجديد والاستمرار في الارتباط مع العميل	0.855
3	تنفيذ الارتباط	0.931
جودة التدقيق الخارجي		**0.920**

يتضح من نتائج معاملات كرونباخ ألفا (وهي مقياس يقوم على الارتباط بين العناصر المختلفة ضمن الاختبار الواحد لقياس الاتساق الداخلي لإجابات المستجوبين (Knapp,1991)) في الجدول (2) ارتفاع مستوى الثبات في أداة الدراسة، حيث تراوحت القيم لجميع المتغيرات الرئيسة والفرعية في الدراسة بين (0.822 – 0.931)، وهذا يشير إلى موثوقية أداة الدراسة واتساق إجاباتها.

الأساليب الإحصائية المستخدمة في الدراسة:

للإجابة عن أسئلة الدراسة وتحقيق أهدافها تم استخدام مجموعة من المقاييس الإحصائية الوصفية والاختبارات الإحصائية الاستدلالية المتوفرة على البرنامج الإحصائي "الحزمة الإحصائية للعلوم الاجتماعية (Statistical Package for Social Sciences, SPSS)" التي تمثلت فيما يأتي:

أولاً: المقاييس الإحصائية الوصفية (Descriptive statistical measures):

استخدمت الدراسة مجموعة من مقاييس الإحصاء الوصفي لتحليل إجابات أفراد عينة الدراسة ووصف متغيراتها الرئيسة والفرعية. حيث استخدمت الدراسة التكرارات والنسب

المئوية لوصف الخصائص الشخصية والوظيفية لأفراد عينة الدراسة، كما استخدمت الأوساط الحسابية والانحرافات المعيارية لوصف متغيرات الدراسة.

ثانياً: الاختبارات الإحصائية الاستدلالية (Inferential statistical tests):

استخدمت الدراسة مجموعة من الاختبارات الإحصائية الاستدلالية لفحص بيانات الدراسة والتحقق من ملاءمتها، وقد تمثلت هذه الاختبارات في اختبار كرونباخ ألفا لقياس درجات الثبات في أداة الدراسة، واختبار الارتباط بيرسون ومعامل تضخم التباين ومعامل التباين المسموح به للتحقق من عدم وجود مشكلة الازدواجية الخطية بين المتغيرات المستقلة.

وتم اختبار فرضية الدراسة الرئيسة وتفرعاتها لتحليل الانحدار الخطي المتعدد (Multiple linear regression analysis) (وهو من الأساليب الإحصائية التي توفر دقة الاستدلال بغرض تحسين النتائج في البحث من خلال العلاقة السببية بين المتغيرات موضوع الدراسة (سلمان، 2024)).

تحليل البيانات واختبار الفرضيات:

نتائج الإحصاء الوصفي للخصائص الشخصية والوظيفية:

تم استخراج التكرارات والنسب المئوية لإجابات أفراد عينة الدراسة على الجزء المتعلق بالخصائص الشخصية والوظيفية، ويهدف وصف هذه الإجابات إلى الحصول على تصور ومعرفة عامة حول أبرز الصفات التي يتمتع بها المدققون الخارجيون المزاولون في الأردن، وقد تركزت هذه الصفات حول العمر والمؤهل العلمي وعدد سنوات الخبرة.

الجدول (3): الخصائص الشخصية والوظيفية المدققين الخارجيين المزاولين في الأردن

المتغير	الفئة	التكرار	النسبة المئوية
العمر	أقل من 30 سنة	35	18.3
	30 – أقل من 40 سنة	58	30.4
	40 – أقل من 50 سنة	48	25.1
	50 سنة فأكثر	50	26.2
المؤهل العلمي	دبلوم كلية مجتمع فأقل	0	0.0
	بكالوريوس	131	68.6
	ماجستير	46	24.1
	دكتوراه	14	7.3
عدد سنوات الخبرة	أقل من 5 سنوات	6	3.1
	5 سنوات - أقل من 10 سنوات	37	19.4
	10 سنوات - أقل من 15 سنة	41	21.5

	أكثر من 15 سنة	107	56.0
المجموع		**191**	**%100**

يتضح من نتائج الجدول (3) أن (81.7%) من المدققين الخارجيين المزاولين هم من الفئات العمرية (30 – 50 سنة فأكثر)، مع وجود زيادة نسبية بسيطة في الفئة العمرية (30 – أقل من 40 سنة) التي بلغت (30.4%)، وهي النسبة الكبرى بالمقارنة بالفئات العمرية الأخرى، وهذا يتوافق مع متطلبات العمل كمدققين خارجيين مزاولين، حيث إن الحصول على رخصة مدقق مزاول تتطلب امتلاك الشهادات المهنية والخبرات اللازمة وهي تحتاج لمدة زمنية طويلة إلى حد ما.

ويتضح أن (68.6%) من المدققين الخارجيين المزاولين هم من الحاصلين على المؤهل العلمي (بكالوريوس)، وهي النسبة الأكبر بالمقارنة بفئات المؤهلات العلمية الأخرى، و(31.4%) منهم حاصلين على المؤهلات العلمية العليا (ماجستير ودكتوراة)، كما تبين عدم وجود مدققين خارجيين مزاولين حاصلين على المؤهل العلمي (دبلوم كلية مجتمع فأقل)، وهذا يتوافق مع متطلبات العمل كمدقق من حيث الحصول على شهادة البكالوريوس كحد أدنى، كما تشير نسب هذه المؤهلات العلمية إلى تمتع المدققين الخارجيين المزاولين في الأردن بالكفاءات والقدرات العلمية والمعرفية التي تساعدهم على أداء مهامهم التدقيقية بكفاءة عالية.

كما يتضح أن (56.0%) من المدققين الخارجيين المزاولين يمتلكون سنوات خبرة (أكثر من 15 سنة) وهي النسبة الأكبر بالمقارنة بفئات عدد سنوات الخبرة الأخرى، و(21.5%) منهم بلغ عدد سنوات خبرتهم بين (10 سنوات – أقل من 15 سنة)، كما تبين أن (3.1%) منهم بلغت عدد سنوات خبرتهم (أقل من 5 سنوات) وهي النسبة الأقل، وهذا يشير إلى امتلاك المدققين الخارجيين المزاولين في الأردن الخبرات والمهارات العملية في أنشطة وأعمال التدقيق الخارجي.

وصف متغيرات الدراسة:

تم استخراج المتوسطات الحسابية والانحرافات المعيارية والرتبة والأهمية النسبية لآراء أفراد عينة الدراسة حول درجات موافقاتهم على الفقرات المتعلقة بمتغيرات الدراسة الرئيسة والفرعية، وذلك بهدف وصف هذه المتغيرات ضمن بيئة الدراسة، وبيان أهميتها لدى المدققين الخارجيين المزاولين في الأردن. حيث يمثل متغير مقومات الأمن السيبراني المتغير المستقل في الدراسة، وقد تم قياسه من خلال (3) متغيرات فرعية، وهي: المقومات التكنولوجية والمقومات القانونية المقومات الاقتصادية. ويمثل متغير جودة التدقيق الخارجي حسب المعيار الدولي للتدقيق رقم 220 المتغير التابع في الدراسة، وقد تم قياسه من خلال (3) متغيرات فرعية، وهي:

المتطلبات الأخلاقية والاستقلالية وقبول الارتباط الجديد والاستمرار في الارتباط مع العميل وتنفيذ الارتباط. ويوضح الجدول الآتي قيم الإحصاء الوصفي المستخدمة لوصف هذه المتغيرات ومتغيراتها الفرعية.

الجدول (4): وصف مقومات الأمن السيبراني ومتغيراته الفرعية

الرقم	المتغير	الوسط الحسابي	الانحراف المعياري	الرتب	الأهمية النسبية
1	المقومات التكنولوجية	4.327	0.584	1	مرتفعة
2	المقومات القانونية	3.976	0.583	2	مرتفعة
3	المقومات الاقتصادية	3.683	0.712	3	مرتفعة
مقومات الأمن السيبراني		**3.995**	**0.525**		**مرتفعة**
1	المتطلبات الأخلاقية والاستقلالية	4.273	0.536	2	مرتفعة
2	قبول الارتباط الجديد والاستمرار في الارتباط مع العميل	4.117	0.554	3	مرتفعة
3	تنفيذ الارتباط	4.628	0.515	1	مرتفعة
جودة التدقيق الخارجي		**4.340**	**0.447**		**مرتفعة**

يتضح من نتائج الجدول (4) أن المتوسط الحسابي لمقومات الأمن السيبراني قد بلغ (3.995) وبانحراف معياري (0.525) وبأهمية مرتفعة، وبلغت قيم الأوساط الحسابية للمتغيرات الفرعية لمقومات الأمن السيبراني بين (3.683 – 4.327) وهي تشير إلى أن جميع هذه المتغيرات تحظى باهتمام مرتفع من قبل المدققين الخارجيين المزاولين، ومما يؤكد على ذلك قيم الانحرافات المعيارية التي بلغت بين (0.583 – 0.712). وبترتيب هذه المتغيرات يتبين أن (المقومات التكنولوجية) قد ظهرت في المرتبة الأولى بمتوسط حسابي بلغ (4.327) وبانحراف معياري (0.584) وبأهمية مرتفعة، وظهرت (المقومات القانونية) في المرتبة الثانية بمتوسط حسابي بلغ (3.976) وبانحراف معياري (0.583) وبأهمية مرتفعة، بينما ظهرت (المقومات الاقتصادية) في المرتبة الثالثة بوسط حسابي بلغ (3.683) وبانحراف معياري (0.712) وبأهمية مرتفعة.

ويتضح من النتائج أن المتوسط الحسابي لجودة التدقيق الخارجي حسب المعيار الدولي للتدقيق رقم 220 قد بلغ (4.340) وبانحراف معياري (0.447) وبأهمية مرتفعة، وبلغت قيم الأوساط الحسابية للمتغيرات الفرعية لجودة التدقيق الخارجي بين (4.117 – 4.628) وهي تشير إلى أن جميع هذه المتغيرات تحظى باهتمام مرتفع من قبل المدققين الخارجيين المزاولين، ومما يؤكد على ذلك قيم الانحرافات المعيارية التي بلغت بين (0.515 – 0.554). وبترتيب هذه المتغيرات يتبين أن (تنفيذ الارتباط) قد ظهر في المرتبة الأولى بمتوسط حسابي بلغ (4.628) وبانحراف

معياري (0.515) وبأهمية مرتفعة، وظهر (المتطلبات الأخلاقية والاستقلالية) في المرتبة الثانية بمتوسط حسابي بلغ (4.273) وبانحراف معياري (0.536) وبأهمية مرتفعة، بينما ظهر (قبول الارتباط الجديد والاستمرار في الارتباط مع العميل) في المرتبة الثالثة بوسط حسابي بلغ (4.117) وبانحراف معياري (0.554) وبأهمية مرتفعة.

نتائج اختبار فرضيات الدراسة:

تهدف فرضيات الدراسة إلى بيان أثر مقومات الأمن السيبراني في جودة التدقيق الخارجي في شركات التكنولوجيا المالية في الأردن. ولتحقيق هذا الهدف تم إجراء تحليل الانحدار الخطي المتعدد كأسلوب إحصائي استدلالي لاتخاذ القرار بقبول أو رفض الفرضيات الصفرية للدراسة الحالية.

نتائج اختبار الفرضية الرئيسة:

تهدف الفرضية الرئيسة إلى بيان أثر مقومات الأمن السيبراني في جودة التدقيق الخارجي في شركات التكنولوجيا المالية في الأردن. حيث تنص هذه الفرضية على أنه: **"لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لمقومات الأمن السيبراني بأبعادها مجتمعة (المقومات التكنولوجية، المقومات القانونية، المقومات الاقتصادية) في جودة التدقيق الخارجي بأبعادها (المتطلبات الأخلاقية والاستقلالية، قبول الارتباط الجديد والاستمرار في الارتباط، تنفيذ الارتباط) في شركات التكنولوجيا المالية في الأردن".** وتم اتخاذ القرار بهذه الفرضية من خلال تطبيق تحليل الانحدار المتعدد، وكانت النتائج كما يأتي:

الجدول (5): نتائج اختبار أثر مقومات الأمن السيبراني في جودة التدقيق الخارجي

المتغير التابع	معامل الارتباط	معامل التحديد	معامل التحديد المعدل	الخطأ المعياري للنموذج	درجة الحرية	القيمة المحسوبة F	مستوى الدلالة F
جودة التدقيق الخارجي	0.727	0.529	0.522	0.309	1	70.069	0.000

يتضح من نتائج الجدول (5) وجود علاقة قوية بين مقومات الأمن السيبراني وجودة التدقيق الخارجي، وذلك بالاستناد إلى قيمة معامل الارتباط (R=0.727)، وتشير قيمة معامل التحديد (R^2=0.529) إلى أن مقومات الأمن السيبراني قد استطاعت تفسير ما نسبته (52.9%) من التباين الحاصل في جودة التدقيق الخارجي. ويعتبر الفرق بين قيمتي معامل التحديد ومعامل التحديد

المعدل ($Adj.R^2$=0.522) قيمة صغيرة جداً التي بلغت (0.007)، وهذا يدل على قدرة مقومات الأمن السيبراني التنبؤ بجودة التدقيق الخارجي. ويتضح من نتائج الجدول وجود أثر ذي دلالة إحصائية لمقومات الأمن السيبراني في جودة التدقيق الخارجي، حيث كانت قيمة F المحسوبة (70.069) وكانت قيمة مستوى الدلالة (SigF=0.000) وهي أقل من القيمة (0.05).

وبالاعتماد على مخرجات التحليل الإحصائي الاستدلالي، فقد تقرر رفض الفرضية الصفرية الرئيسة وقبول الفرضية البديلة، التي تنص على أنه: **"يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لمقومات الأمن السيبراني بأبعادها مجتمعة (المقومات التكنولوجية، المقومات القانونية، المقومات الاقتصادية) في جودة التدقيق الخارجي بأبعدها (المتطلبات الأخلاقية والاستقلالية، قبول الارتباط الجديد والاستمرار في الارتباط، تنفيذ الارتباط) في شركات التكنولوجيا المالية في الأردن"**.

الجدول (6): معاملات الانحدار لأثر مقومات الأمن السيبراني في جودة التدقيق الخارجي

المتغير	المعاملات	الخطأ المعياري	المعاملات المعيارية	القيمة المحسوبة T	مستوى الدلالة T
ثابت الانحدار	1.857	0.173		10.723	0.000
المقومات التكنولوجية	0.306	0.042	0.433	7.234	0.000
المقومات القانونية	0.154	0.046	0.222	3.332	0.001
المقومات الاقتصادية	0.150	0.033	0.263	4.545	0.000

يتضح من نتائج الجدول (6) أن اتجاه العلاقة بين المقومات التكنولوجية وجودة التدقيق الخارجي طردية، وذلك بالاستناد إلى قيمة المعامل (B=0.306)، ويتضح أن المقومات التكنولوجية قد أثرت في جودة التدقيق الخارجي، حيث ظهرت قيمة T المحسوبة (7.234) وظهرت قيمة مستوى الدلالة (SigT=0.000)، وهي أقل من القيمة (0.05). ويتبين أن اتجاه العلاقة بين المقومات القانونية وجودة التدقيق الخارجي طردية، وذلك بالاستناد إلى قيمة المعامل (B=0.154)، ويتضح أن المقومات القانونية قد أثرت في جودة التدقيق الخارجي، حيث ظهرت قيمة T المحسوبة (3.332) وظهرت قيمة مستوى الدلالة (SigT=0.001)، وهي أقل من القيمة (0.05). كما يتبين أن اتجاه العلاقة بين المقومات الاقتصادية وجودة التدقيق الخارجي طردية، وذلك بالاستناد إلى قيمة المعامل (B=0.150)، ويتضح أن المقومات الاقتصادية قد أثرت في جودة التدقيق الخارجي، حيث ظهرت قيمة T المحسوبة (4.545) وظهرت قيمة مستوى الدلالة (SigT=0.000)، وهي أقل من القيمة (0.05).

نتائج اختبار الفرضيات المتفرعة عن الفرضية الرئيسة:

تهدف الفرضيات المتفرعة عن الفرضية الرئيسة إلى بيان أثر مقومات الأمن السيبراني في كل من (المتطلبات الأخلاقية والاستقلالية، قبول الارتباط الجديد والاستمرار في الارتباط، تنفيذ الارتباط) في شركات التكنولوجيا المالية في الأردن. وتم اتخاذ القرار بهذه الفرضيات من خلال تطبيق تحليل الانحدار المتعدد، وكانت النتائج كما يأتي:

الفرضية الفرعية الأولى:

تهدف الفرضية الفرعية الأولى إلى بيان أثر مقومات الأمن السيبراني في المتطلبات الأخلاقية والاستقلالية في شركات التكنولوجيا المالية. حيث تنص هذه الفرضية على أنه: **"لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لمقومات الأمن السيبراني في المتطلبات الأخلاقية والاستقلالية في شركات التكنولوجيا المالية في الأردن"**. وكانت النتائج كما يأتي:

الجدول (7): نتائج اختبار أثر مقومات الأمن السيبراني في المتطلبات الأخلاقية والاستقلالية

المتغير التابع	معامل الارتباط	معامل التحديد	معامل التحديد المعدل	الخطأ المعياري للنموذج	درجة الحرية	القيمة المحسوبة F	مستوى الدلالة F
المتطلبات الأخلاقية والاستقلالية	0.697	0.486	0.478	0.388	1	58.973	0.000

يتضح من نتائج الجدول (7) وجود علاقة قوية بين مقومات الأمن السيبراني والمتطلبات الأخلاقية والاستقلالية، وذلك بالاستناد إلى قيمة معامل الارتباط (R=0.697)، وتشير قيمة معامل التحديد (R^2=0.486) إلى أن مقومات الأمن السيبراني قد استطاعت تفسير ما نسبته (48.6%) من التباين الحاصل في المتطلبات الأخلاقية والاستقلالية. ويعتبر الفرق بين قيمتي معامل التحديد ومعامل التحديد المعدل (Adj.R^2=0.478) قيمة صغيرة جداً التي بلغت (0.008)، وهذا يدل على قدرة مقومات الأمن السيبراني التنبؤ بالمتطلبات الأخلاقية والاستقلالية. ويتضح من نتائج الجدول وجود أثر ذي دلالة إحصائية لمقومات الأمن السيبراني في المتطلبات الأخلاقية والاستقلالية، حيث كانت قيمة F المحسوبة (58.973) وكانت قيمة مستوى الدلالة (SigF=0.000) وهي أقل من القيمة (0.05).

وبالاعتماد على مخرجات التحليل الإحصائي الاستدلالي، فقد تقرر رفض الفرضية الصفرية الفرعية الأولى وقبول الفرضية البديلة، التي تنص على أنه: **"يوجد أثر ذو دلالة إحصائية عند**

مستوى معنوية (α≤0.05) لمقومات الأمن السيبراني في المتطلبات الأخلاقية والاستقلالية في شركات التكنولوجيا المالية في الأردن".

الجدول (8): معاملات الانحدار لأثر مقومات الأمن السيبراني في المتطلبات الأخلاقية والاستقلالية

المتغير	المعاملات	الخطأ المعياري	المعاملات المعيارية	القيمة المحسوبة T	مستوى الدلالة T
ثابت الانحدار	1.447	0.217		6.667	0.000
المقومات التكنولوجية	0.325	0.053	0.383	6.126	0.000
المقومات القانونية	0.161	0.058	0.194	2.782	0.006
المقومات الاقتصادية	0.214	0.041	0.312	5.166	0.000

يتضح من نتائج الجدول (8) أن اتجاه العلاقة بين المقومات التكنولوجية والمتطلبات الأخلاقية والاستقلالية طردية، وذلك بالاستناد إلى قيمة المعامل (B=0.325)، ويتضح أن المقومات التكنولوجية قد أثرت في المتطلبات الأخلاقية والاستقلالية، حيث ظهرت قيمة T المحسوبة (6.126) وظهرت قيمة مستوى الدلالة (SigT=0.000)، وهي أقل من القيمة (0.05). ويتبين أن اتجاه العلاقة بين المقومات القانونية والمتطلبات الأخلاقية والاستقلالية طردية، وذلك بالاستناد إلى قيمة المعامل (B=0.161)، ويتضح أن المقومات القانونية قد أثرت في المتطلبات الأخلاقية والاستقلالية، حيث ظهرت قيمة T المحسوبة (2.782) وظهرت قيمة مستوى الدلالة (SigT=0.006)، وهي أقل من القيمة (0.05). كما يتبين أن اتجاه العلاقة بين المقومات الاقتصادية والمتطلبات الأخلاقية والاستقلالية طردية، وذلك بالاستناد إلى قيمة المعامل (B=0.214)، ويتضح أن المقومات الاقتصادية قد أثرت في المتطلبات الأخلاقية والاستقلالية، حيث ظهرت قيمة T المحسوبة (5.166) وظهرت قيمة مستوى الدلالة (SigT=0.000)، وهي أقل من القيمة (0.05).

الفرضية الفرعية الثانية:

تهدف الفرضية الفرعية الثانية إلى بيان أثر مقومات الأمن السيبراني في قبول الارتباط الجديد والاستمرار في الارتباط في شركات التكنولوجيا المالية. حيث تنص هذه الفرضية على أنه: **"لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (α≤0.05) لمقومات الأمن السيبراني في قبول الارتباط الجديد والاستمرار في الارتباط في شركات التكنولوجيا المالية في الأردن".** وكانت النتائج كما يأتي:

الجدول (9): نتائج اختبار أثر مقومات الأمن السيبراني في قبول الارتباط الجديد والاستمرار في الارتباط

المتغير التابع	معامل الارتباط	معامل التحديد	معامل التحديد المعدل	الخطأ المعياري للنموذج	درجة الحرية	القيمة المحسوبة F	مستوى الدلالة F
قبول الارتباط الجديد والاستمرار في الارتباط	0.729	0.532	0.525	0.382	1	70.875	0.000

يتضح من نتائج الجدول (9) وجود علاقة قوية بين مقومات الأمن السيبراني وقبول الارتباط الجديد والاستمرار في الارتباط، وذلك بالاستناد إلى قيمة معامل الارتباط (R=0.729)، وتشير قيمة معامل التحديد (R^2=0.532) إلى أن مقومات الأمن السيبراني قد استطاعت تفسير ما نسبته (53.2%) من التباين الحاصل في قبول الارتباط الجديد والاستمرار في الارتباط. ويعتبر الفرق بين قيمتي معامل التحديد ومعامل التحديد المعدل (Adj.R^2=0.525) قيمة صغيرة جداً التي بلغت (0.007)، وهذا يدل على قدرة مقومات الأمن السيبراني التنبؤ بقبول الارتباط الجديد والاستمرار في الارتباط. ويتضح من نتائج الجدول وجود أثر ذي دلالة إحصائية لمقومات الأمن السيبراني في قبول الارتباط الجديد والاستمرار في الارتباط، حيث كانت قيمة F المحسوبة (70.875) وكانت قيمة مستوى الدلالة (SigF=0.000) وهي أقل من القيمة (0.05).

وبالاعتماد على مخرجات التحليل الإحصائي الاستدلالي، فقد تقرر رفض الفرضية الصفرية الفرعية الثانية وقبول الفرضية البديلة، التي تنص على أنه: **"يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لمقومات الأمن السيبراني في قبول الارتباط الجديد والاستمرار في الارتباط في شركات التكنولوجيا المالية في الأردن"**.

الجدول (10): معاملات الانحدار لأثر مقومات الأمن السيبراني في قبول الارتباط الجديد والاستمرار في الارتباط.

المتغير	المعاملات	الخطأ المعياري	المعاملات المعيارية	القيمة المحسوبة T	مستوى الدلالة T
ثابت الانحدار	1.075	0.214		5.022	0.000
المقومات التكنولوجية	0.312	0.052	0.356	5.968	0.000
المقومات القانونية	0.215	0.057	0.250	3.769	0.000
المقومات الاقتصادية	0.229	0.041	0.323	5.594	0.000

يتضح من نتائج الجدول (10) أن اتجاه العلاقة بين المقومات التكنولوجية وقبول الارتباط الجديد والاستمرار في الارتباط طردية، وذلك بالاستناد إلى قيمة المعامل (B=0.312)، ويتضح أن المقومات التكنولوجية قد أثرت في قبول الارتباط الجديد والاستمرار في الارتباط، حيث ظهرت قيمة T المحسوبة (5.968) وظهرت قيمة مستوى الدلالة (SigT=0.000)، وهي أقل من القيمة (0.05). ويتبين أن اتجاه العلاقة بين المقومات القانونية وقبول الارتباط الجديد والاستمرار في الارتباط طردية، وذلك بالاستناد إلى قيمة المعامل (B=0.215)، ويتضح أن المقومات القانونية قد أثرت في قبول الارتباط الجديد والاستمرار في الارتباط، حيث ظهرت قيمة T المحسوبة (3.769) وظهرت قيمة مستوى الدلالة (SigT=0.000)، وهي أقل من القيمة (0.05). كما يتبين أن اتجاه العلاقة بين المقومات الاقتصادية وقبول الارتباط الجديد والاستمرار في الارتباط طردية، وذلك بالاستناد إلى قيمة المعامل (B=0.229)، ويتضح أن المقومات الاقتصادية قد أثرت في قبول الارتباط الجديد والاستمرار في الارتباط، حيث ظهرت قيمة T المحسوبة (5.594) وظهرت قيمة مستوى الدلالة (SigT=0.000)، وهي أقل من القيمة (0.05).

الفرضية الفرعية الثالثة:

تهدف الفرضية الفرعية الثالثة إلى بيان أثر مقومات الأمن السيبراني في تنفيذ الارتباط في شركات التكنولوجيا المالية. حيث تنص هذه الفرضية على أنه: **"لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لمقومات الأمن السيبراني في تنفيذ الارتباط في شركات التكنولوجيا المالية في الأردن".** وكانت النتائج كما يأتي:

الجدول (11): نتائج اختبار أثر مقومات الأمن السيبراني في تنفيذ الارتباط

المتغير التابع	معامل الارتباط	معامل التحديد	معامل التحديد المعدل	الخطأ المعياري للنموذج	درجة الحرية	القيمة المحسوبة F	مستوى الدلالة F
تنفيذ الارتباط	0.694	0.481	0.473	0.310	1	57.852	0.000

يتضح من نتائج الجدول (11) وجود علاقة بين مقومات الأمن السيبراني وتنفيذ الارتباط، وذلك بالاستناد إلى قيمة معامل الارتباط (R=0.694)، وتشير قيمة معامل التحديد (R^2=0.481) إلى أن مقومات الأمن السيبراني قد استطاعت تفسير ما نسبته (48.1%) من التباين الحاصل في تنفيذ الارتباط. ويعتبر الفرق بين قيمتي معامل التحديد ومعامل التحديد المعدل (Adj.R^2=0.473) قيمة صغيرة جداً التي بلغت (0.008)، وهذا يدل على قدرة مقومات الأمن السيبراني التنبؤ بتنفيذ الارتباط. ويتضح من نتائج الجدول وجود أثر ذي دلالة إحصائية لمقومات الأمن السيبراني في تنفيذ الارتباط، حيث كانت قيمة F المحسوبة (57.852) وكانت قيمة مستوى الدلالة (SigF=0.000) وهي أقل من القيمة (0.05).

وبالاعتماد على مخرجات التحليل الإحصائي الاستدلالي، فقد تقرر رفض الفرضية الصفرية الفرعية الثالثة وقبول الفرضية البديلة، التي تنص على أنه: **"يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لمقومات الأمن السيبراني في تنفيذ الارتباط في شركات التكنولوجيا المالية في الأردن"**.

الجدول (12): معاملات الانحدار لأثر مقومات الأمن السيبراني في تنفيذ الارتباط

المتغير	المعاملات	الخطأ المعياري	المعاملات المعيارية	القيمة المحسوبة T	مستوى الدلالة T
ثابت الانحدار	2.168	0.174		12.483	0.000
المقومات التكنولوجية	0.144	0.042	0.212	3.380	0.001
المقومات القانونية	0.182	0.046	0.275	3.935	0.000
المقومات الاقتصادية	0.210	0.033	0.385	6.341	0.000

يتضح من نتائج الجدول (12) أن اتجاه العلاقة بين المقومات التكنولوجية وتنفيذ الارتباط طردية، وذلك بالاستناد إلى قيمة المعامل (B=0.144)، ويتضح أن المقومات التكنولوجية قد أثرت في تنفيذ الارتباط، حيث ظهرت قيمة T المحسوبة (3.380) وظهرت قيمة مستوى الدلالة (SigT=0.001)، وهي أقل من القيمة (0.05). ويتبين أن اتجاه العلاقة بين المقومات القانونية وتنفيذ الارتباط طردية، وذلك بالاستناد إلى قيمة المعامل (B=0.182)، ويتضح أن المقومات القانونية قد أثرت في تنفيذ الارتباط، حيث ظهرت قيمة T المحسوبة (3.935) وظهرت قيمة مستوى الدلالة (SigT=0.000)، وهي أقل من القيمة (0.05). كما يتبين أن اتجاه العلاقة بين المقومات الاقتصادية وتنفيذ الارتباط طردية، وذلك بالاستناد إلى قيمة المعامل (B=0.210)،

ويتضح أن المقومات الاقتصادية قد أثرت في تنفيذ الارتباط، حيث ظهرت قيمة T المحسوبة (6.341) وظهرت قيمة مستوى الدلالة (SigT=0.000)، وهي أقل من القيمة (0.05).

النتائج والتوصيات:

النتائج:

بالاعتماد على المخرجات النهائية لتحليل البيانات واختبار فرضيات الدراسة، خلُصت الدراسة إلى النتائج الآتية:

1- اهتمام المدققين الخارجيين المزاولين بمقومات الأمن السيبراني ومتغيراته (المقومات التكنولوجية، والمقومات القانونية، والمقومات الاقتصادية) على التوالي وبمستوى مرتفع. ويمكن ربط هذا الاهتمام بتعقيدات وتأثيرات التكنولوجيا على أداء منشآت العملاء. فمن الناحية التكنولوجية، تزداد التهديدات السيبرانية تعقيداً وتطوراً مما يتطلب أنظمة حماية متقدمة ومتطورة، وفي هذا المجال يهتم المدققون بالتحقق من قدرة وكفاءة البنية التحتية التقنية لمنشآت العملاء على التصدي للهجمات السيبرانية، وضمان الحماية، والسلامة للأنظمة، والبيانات. ومن الناحية القانونية، فقد ظهرت العديد من التشريعات واللوائح التي تتعلق بحماية البيانات وضمان خصوصيتها واكتشاف هجمات الأمن السيبراني وتصحيحها والتعافي منها، إضافة إلى طرق وأدوات الإبلاغ والتفتيش مما يجعل الالتزام بها أمراً أساسياً وضرورياً، وفي هذا المجال يهتم المدققون بمتابعة مدى امتثال العملاء لهذه التشريعات واللوائح مما يضمن التزامها بتطبيق إطار واستراتيجية الأمن السيبراني وتوفير الحماية من مخاطر الهجمات السيبرانية واتخاذ الإجراءات المناسبة لها. أما من الناحية الاقتصادية، فإن تعرض منشآت العملاء لهجمات السيبرانية يؤدي إلى تكبدها خسائر مالية كبيرة وتعطيل عملياتها، وفي هذا المجال يهتم المدققون بالتأكد من توافر المخصصات المالية وكفايتها للحماية من الهجمات السيبرانية والتعافي منها، وتوافق التدابير الأمنية المتخذة مع ميزانية منشأة العميل.

2- اهتمام المدققين الخارجيين المزاولين بجودة التدقيق الخارجي حسب المعيار الدولي للتدقيق رقم 220 ومتغيراته (تنفيذ الارتباط، المتطلبات الأخلاقية والاستقلالية، وقبول الارتباط الجديد والاستمرار في الارتباط مع العميل) على التوالي وبمستوى مرتفع. وهذا الاهتمام يدل على التزام المدققين الخارجيين المزاولين بتقديم خدمات تدقيق دقيقة وموثوقة مما يعزز من الثقة في النتائج، وذلك من خلال الالتزام بتنفيذ عمليات التدقيق وفقاً لقواعد والمعايير المحددة مع مراعاة الدقة والكفاءة، ودعم وتعزيز استقلالية المدققين، بالإضافة إلى اختيار العملاء بعناية وحذر والتقييم للمخاطر المحتملة لضمان استمرارية العلاقة.

3- تؤثر مقومات الأمن السيبراني بأبعادها مجتمعة (المقومات التكنولوجية، المقومات القانونية، المقومات الاقتصادية) إيجاباً في جودة التدقيق الخارجي بأبعادها (المتطلبات الأخلاقية والاستقلالية، قبول الارتباط الجديد والاستمرار في الارتباط، تنفيذ الارتباط) في شركات التكنولوجيا المالية في الأردن. ووجود هذا الأثر يدل على الدور الهام الذي تقوم به مقومات الأمن السيبراني في تحسين وتعزيز أنشطة وعمليات التدقيق الخارجي، حيث تعمل المقومات التكنولوجية كأنظمة الحماية الرقمية والبنية التحتية السيبرانية على تعزيز قدرة المدققين على تقييم المخاطر والمحافظة على سلامة وصحة البيانات والمعلومات. وتسهم المقومات القانونية بما تتضمنه من قواعد وقوانين وتشريعات تتعلق بالأمن السيبراني في توفير إطار قانوني وتنظيمي يضمن التزام شركات التكنولوجيا المالية بالعمل وفقاً للمعايير المحددة والمطلوبة، مما يساعد في أداء أنشطة وأعمال التدقيق، وتوفير بيئة عمل آمنة من الهجمات السيبرانية. بالإضافة إلى أن الاستثمار في البنية التحتية

والإجراءات والتدابير الأمنية للأمن السيبراني يعمل على تقليل احتمال التعرض للمخاطر والاختراقات السيبرانية، وبالتالي زيادة الجودة في التدقيق. ولذا فإن تطبيق هذه المقومات بشكل متكامل من شأنه أن يسهم في تعزيز الثقة في عمليات التدقيق، والحد من المخاطر المتعلقة بالانتهاكات والاختراقات السيبرانية، ويضمن الدقة والاستقلالية في عملية التدقيق في شركات التكنولوجيا المالية.

4- تؤثر مقومات الأمن السيبراني إيجاباً في المتطلبات الأخلاقية والاستقلالية في شركات التكنولوجيا المالية في الأردن. ووجود هذا الأثر يدل على الدور الهام الذي تقوم به مقومات الأمن السيبراني في تعزيز المعايير الأخلاقية وضمان الاستقلالية في العمليات الرقابية والتدقيق. حيث تسهم المقومات التكنولوجية من خلال الأنظمة المُشفّرة وتدابير الحماية للعمليات في الحد من التلاعب في البيانات والمعلومات، وهذا يضمن دقة البيانات المستخدمة في عمليات التدقيق وخلوها من الأخطاء والتلاعب، وبالتالي دعم الالتزام بالمعايير الأخلاقية. وتسهم المقومات القانونية من خلال القواعد والتشريعات المختصة بالأمن السيبراني في إعداد إطار يحمي حقوق ومصالح كافة الأطراف، وبالتالي يضمن عمل المدققين الخارجيين وفقاً لمعايير أخلاقية. كما تسهم المقومات الاقتصادية من خلال تخصيص الموارد والإمكانات اللازمة للأمن السيبراني في الحد من تعرض المدققين الخارجيين لضغوط وتأثيرات خارجية تؤثر على نزاهتهم مما يسهم في تعزيز استقلاليتهم في عملية اتخاذ القرارات. ولذا، فإن تطبيق هذه المقومات من شأنه أن يعزز من التزام المدققين الخارجيين بالمعايير الأخلاقية ويضمن استقلاليتهم، وبالتالي زيادة الثقة والمصداقية في عمليات التدقيق في شركات التكنولوجيا المالية.

5- تؤثر مقومات الأمن السيبراني إيجاباً في قبول الارتباط الجديد والاستمرار في الارتباط في شركات التكنولوجيا المالية في الأردن. ووجود هذا الأثر يدل على الدور الهام الذي تقوم به مقومات الأمن السيبراني في اتخاذ القرارات بشأن قبول واستمرار الارتباط والعلاقات المهنية مع العملاء. حيث تضمن المقومات التكنولوجية الحفاظ على أمن وسرية معلومات العملاء المالية والشخصية، مما يعزز من ثقتها لدى الأطراف المختلفة وبالتالي استعداد المدققين الخارجيين لقبول ارتباطات جديدة والاستمرار في الارتباطات الحالية. وتساعد المقومات القانونية المتعلقة بالأمن السيبراني في ضمان الامتثال للقوانين واللوائح والتشريعات المحلية والعالمية، مما يعزز من المصداقية وتقليل التعرض للمخاطر القانونية وبالتالي تقبل المدققين الخارجيين لها كعملاء جدد واستمرار العلاقات القائمة معها. بالإضافة إلى أن توافر المقومات الاقتصادية بما في ذلك الاستثمار في أنظمة الأمن السيبراني من شأنها أن تساعد على تقليل المخاطر والأزمات المتعلقة بالهجمات والاختراقات السيبرانية، مما يجعل المدققين الخارجيين أكثر استعداداً للتعامل مع مثل هذه الشركات والحفاظ على العلاقات والشراكات الحالية دون التخوف من التعرض للمخاطر السيبرانية. ولذا، فإن الاستثمار في الأمن السيبراني وتعزيز شركات التكنولوجيا المالية لبنيتها الأمنية يزيد من استعداد المدققين الخارجيين لقبول ارتباطات جديدة معها والاستمرار في الشركات القائمة معها.

6- تؤثر مقومات الأمن السيبراني إيجاباً في تنفيذ الارتباط في شركات التكنولوجيا المالية في الأردن. ووجود هذا الأثر يدل على الدور الهام الذي تقوم به مقومات الأمن السيبراني في تحسين كفاءة، وفعالية عمليات، ومهام التدقيق، وتنفيذها. حيث توفر المقومات التكنولوجية أنظمة حماية متطورة تحد من فرص التلاعب أو الوصول غير المصرح به إلى البيانات والمعلومات الهامة، مما يضمن اعتماد المدققين الخارجيين على بيانات دقيقة وآمنة عند أداء عملية التدقيق، وبالتالي تعزيز الثقة والمصداقية في عمليات التدقيق. وتساعد المقومات القانونية في ضمان التزام المدققين وشركات التكنولوجيا المالية باللوائح والمعايير المتعلقة بحماية البيانات وخصوصيتها، وهذا من شانه أن يعزز من جودة تنفيذ الارتباطات وتقليل المخاطر القانونية التي قد تؤثر سلباً على أنشطة وعمليات التدقيق بالإضافة إلى أن تطبيق المقومات الاقتصادية من خلال

الاستثمار في أنظمة الحماية والتدابير والسياسات الأمنية من شأنه أن يسهم في تقليل احتمالات التعرض للمخاطر والهجمات السيبرانية خلال عملية التدقيق، مما يتيح للمدققين الخارجيين التركيز على تنفيذ الارتباط بشكل فعّال دون الاكتراث لتهديدات الأمن السيبراني وبالتالي زيادة السرعة والدقة في تنفيذ عمليات التدقيق. ولذا، فإن الاستثمار في الأمن السيبراني وتحقيق التكامل في تطبيق مقوماته من شانه أن يسهم في تحسين جودة تنفيذ أنشطة وعمليات التدقيق الخارجي، وزيادة الدقة والفعالية فيها، وتعزيز الثقة في نتائجها.

التوصيات

بالاعتماد على النتائج الوصفية والتحليلية التي تم التوصل إليها، تقترح الدراسة التوصيات الآتية:

1- استمرار المدققين الخارجيين المزاولين بتدقيق الأنظمة والبرامج وتطبيق المعايير الملزمة وإصدار التقارير حول كفاية أنظمة الأمن السيبراني، وتصميم المزيد من أنظمة الحماية بشكل متوافق (غير متعارض) مع الأنشطة التشغيلية مع إعطاء الأولوية لأنظمة الحماية في حال التعارض.

2- استمرار المدققين الخارجيين المزاولين بتعريف وتدريب العاملين لدى العميل بشكل مستمر على الإطار والاستراتيجية للأمن السيبراني، وتحسين دور مجلس الإدارة على تحديد أخطار الأمن السيبراني ودرجة تحملها وتوجيهها إلى الإدارة لاتخاذ الإجراء المناسب بخصوصها.

3- توفر المؤسسات المزيد من الموازنات الكافية لتوعية الموظفين وتدريب فريق التدقيق بشكل مستمر وتمكينه من الحصول على المعرفة والخبرات اللازمة من جهات معتمدة لحماية أصولها المادية والمعنوية، بالإضافة إلى توفير القدر الكافي من الموازنات لمواجهة أخطار الهجمات السيبرانية وكلفة الاسترداد والتعافي واستئناف أعمالها بعد الهجوم السيبراني أو الكوارث الطبيعية.

4- بذل المدققون الخارجيون المزاولون المزيد من العناية اللازمة بغض النظر عن وقت مهمة التدقيق أو تأخرها، والاستمرار بالتحقق من التزام فريق التدقيق بالمتطلبات الأخلاقية في كل مرحلة من مراحل الارتباط، واتخاذ الشريك المسؤول المزيد من الإجراءات المناسبة عند وجود تهديد للاستقلالية أو المتطلبات الأخلاقية لأي عضو في الفريق.

5- الاستمرار بتقييم العلاقة بين العميل والمدقق السابق للوقوف على أسباب تغيير المدقق أو طلب مهمة التدقيق من مدقق آخر، والتقييم المستمر لعدم الاستقلالية والضغوطات التي يمكن يواجهها المدقق من خلال التعرف على سمعة الإدارة ومجلس الإدارة للعميل.

6- توفير المزيد من المدققين من ذوي الخبرة في الأنظمة والبرامج لتنفيذ مهمة التدقيق في شركات التكنولوجيا المالية، وتحسين دور مسؤول الارتباط في التوجيه والإشراف المناسب والمتابعة المستمرة مما يساهم في جودة التدقيق.

7- إكساب المدققين الخارجيين المزاولين المزيد من المعرفة بالأمن السيبراني وإجراءات الحماية، والتبادل المستمر للمعلومات حول الهجمات السيبرانية والاطلاع عليها مما يساهم في رفع جودة التدقيق.

التوصيات العملية لشركات التكنولوجيا المالية وهيئات التدقيق في الأردن:

1- توفير تعاون مجدول ومحدد النطاق بين الجهات التشريعية والتنظيمية المختصة بقضايا الأمن السيبراني وبين شركات التدقيق من خلال جمعية المحاسبين القانونيين وبين شركات التكنولوجيا المالية ومطوري الأنظمة والبرامج.

2- إلزام الشركات المطورة أو المستوردة لأنظمة وبرامج وادوات الأمن السيبراني بالحصول على مراجعة مشتركة من قبل جمعية المحاسبين القانونيين والجهات المنظمة للأمن السيبراني.

3- اعتماد ممارسات محددة ومعممة للأمن السيبراني لتعزيز جودة التدقيق الخارجي.

المراجع باللغة العربية:

-بكاي، احمد (2022). المهن المحاسبية (التدقيق) في عصر العولمة الرقمية والتكنولوجية: قراءة إحصائية لآثار التطور الرقمي على فعالية الممارسات المهنية في المنطقة الأوروبية والآسيوية خلال الفترة 2007 – 2021. *مجلة إدارة الأعمال والدراسات الاقتصادية، 8*(2)، 67- 86.

-البنك المركزي الأردني (2018). *تعليمات التكييف مع المخاطر السيبرانية*، رقم 1984/1/1/26. https://www.cbj.gov.jo/Pages/viewpage.aspx?pageID=62

-دائرة مراقبة الشركات (2017). دليل قواعد حوكمة الشركات الأردنية: الشركات المساهمة الخاصة، الشركات ذات المسؤولية المحدودة، الشركات المساهمة العامة غير المدرجة في البورصة. *وزارة الصناعة والتجارة الأردنية*.

-ذنيبات، علي عبد القادر (2015). *تدقيق الحسابات في ضوء المعايير الدولية: نظرية وتطبيق، ط5*. وائل.

-الشهري، أحمد محمد غنيم (2021). مدى التزام مدققي الحسابات في مكاتب التدقيق الكويتية بتطبيق معيار جودة التدقيق الدولي رقم 220. *مجلة القلم*، 34، 472-496. http://search.mandumah.com/Record/1151860

- العامري، محمد سعيد، حميد، عادل عبد الله، ومحجوب، محمد الامين البشر (2021). *الأمن السيبراني والتحقيقات الرقمية*. المتحدة للطباعة والنشر.

-العلوان، جعفر أحمد عبد الكريم (2022). أدوار وتحديات الأمن السيبراني المعتمد على الذكاء الاصطناعي: دراسة حالة. *المجلة الأردنية في إدارة الأعمال، 18* (3)، 437-456. DOI: https://doi.org/10.35516/jjba.v18i3.196

-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، 4*(2 ج2)، 1-58. Doi: 10.21608/CFDJ.2023.289978

-فريد، حنان هارون (2022). *المجلة العلمية للدراسات التجارية والبيئية، 13*(4)، 412-488. Doi: 10.21608/JCES.2022.285187

-قوجيل، محمد وطيبة، عبد العزيز (2022). مخاطر التكنولوجيا المالية وادارتها في القطاع المصرفي: دراسة تنظيمية احترازية. *مجلة الاقتصاد والمالية، 8*(2)، 185-199.

-سلمان، ثائر داوود (2024). الانحدار الخطي المتعدد: مفهومه ونموذج مطبق باستخدام البرنامج الإحصائي SPSS. جامعة بغداد

المراجع باللغة الاجنبية:

-Alsakini, Saad A. Karee, Alawawdeh Hanan Ali & Alsayyed Saleh (2024). The impact of cybersecurity on the quality of financial statements. *Applied Mathematics & Information Sciences, 18*(1), 169-181. http://dx.doi.org/10.18576/amis/180117

-Almasria, Nashat Ali, Airout, M. Rana, Samara, Abeer Ihsan, Saadat, Mohammad & Jrairah, Souliman Talal (2021). The role of accounting information system in enhancing the quality of external audit procedures. *Journal of management Information and Decision Sciences, 24*(7), 1-23.

-Andreasson, Kim (2012). *Cybersecurity: Public sector threats and responses*. Taylor Francis Group.

-Arens A. Alvin, Elder J. Randal, Beasly S. Mark & Hogan, Chris E. (2017). *Auditing and assurance services: An integrated approach. 16th ed.* Pearson.

-Arnes, Andre (2023). *Cyber investigations*. John Wiley & Sons Ltd.

-Ciftci Ilhan, Tatoglu Ekrem, Wood Geoffrey, Demirbag Mehmet and Zaim Selim (2019). Corporate governance and firm performance in emerging markets: Evidence from Turkey. *International Business Review, 28*, 90-103. www.elsevier.com/locate/ibusrev

-Dang, Li (2004). *Assessing actual audit quality*. [Unpublished Doctoral Dissertations]. Drexel University.

-Didenko Anton N. (2020). Cybersecurity regulation in the financial sector: Prospects of legal harmonization in the European Union and beyond. *Uniform Law Review*, 25, 125-167. https://doi.org/10.1093/ulr/unaa006

-Financial Industry Regulatory Authority (FINRA)(26/3/2024). *Cybersecurity*. Retrieved from: https://www.finra.org/rules-guidance/key-topics/cybersecurity

-Health and Human Services (10/4/2024). *Health insurance portability and accountability act*. Retrieved from: https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%2-0knowledge.

-Kshetri , Nir (2013). *Cybercrime and cybersecurity in the global south*. Palgrave Macmillan.

-Knapp, T.R. (1991). Coefficient alpha: Conceptualization and anomalies. Research in Nursing & Health, 14 456-480. DOI: 10.1002/nur.4770140610

-Kurniawan, Yohannes & Mulyawan, Archie Nathanael (2023). The role of external auditors in improving cybersecurity of the companies through internal control in financial reporting. *Journal of System and Management Sciences, 13*(1), 485-510. DOI:10.33168/JSMS.2023.0126

-International Auditing and Assurance Standards Board (2017). *Handbook of international quality control, auditing, review, other assurance, and related services pronouncements*, Ed. 2016-2016.

-ISO, the International Organization for Standardization (26/3/2024). ISO/IEC 27001:2022: *Information security, cybersecurity and privacy protection: Information security management systems requirements*. Retrieved from: https://www.iso.org/standard/27001

-Lessambo, Felix I. (2018*). Auditing, assurance services, and forensic: A comprehensive approach*. Palgrave Macmillan.

-Morgan, Steve (2023). *Cybersecurity facts, figures, predictions and statistics. Cybersecurity Ventures*. Retrieved from: https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

-Ngo, Tran Nguen Bao & Tick, Andrea (2021). Cyber-security risks assessments by external auditors. *Interdisciplinary Description of Complex Systems, 19*(3), 375-390. https://doi.org/10.7906/indecs.19.3.3

-Romney, Marshall B., & Steinbart, Paul John (2018). *Accounting information systems* (15th ed). Pearson.

-Rosati, Pierangelo, Gogolin, Fabian & Lynn, Theo (2020). Cyber-security incidents and audit quality. *European Accounting Review, 31*(3), 701-728. DOI: 10.1080/09638180.2020.1856162

-Saputra, Komang Adi Kurniawan & Paranoan Selmita (2024). *Do cyber security, digitalization and data visualization affect the quality of internal environmental audit?*. AABFJ, 18(2), 158-174.

-Saudi Arabian Monetary Authority (May, 2017). Cyber security framework, V1.

-Serag, Asmaa Abd El-Monem & Al-aqiliy, Laila Mahrous (2020). A Proposed framework for big data analytics in external auditing and its impact on audit quality with a field study in Egypt. *Alexandria Journal of Accounting Research, 4*(3).

-Sekran, Uma, & Bougie, Roger (2016). *Research methods for business: A skill–building approach (1st ed.)*. John Wiley & Sons, Inc.

-Security Standard Council (10/4/2024). *Payment Card Industry Data Security Standards (PCI-DSS)*. Retrieved from: https://www.pcisecuritystandards.org/

-The International Civil Aviation Organization (ICAO) (7/4/2024). *Cost Benefit Analysis for Implementing CNS/ATM systems*. Retrieved from: https://www.icao.int/sustainability/Pages/eap-fp-cost-benefit-analysis.aspx

-Usman, Alih, Che-Ahmad, Ayoib & Abdulmalik, Salau Olarinoye (2024). The role of internal auditor characteristics in cybersecurity risk assessment in financial-based business organization: a conceptual review. *RGSA – Revista de Gestao Social e Ambiental, 18*(6), 1-33. DOI: https://doi.org/10.24857/rgsa.v18n6-008

-Wheelen, Thomas L., Hunger, J. David, Hoffman, Alan N. & Bamford, Charles E. (2012). *Strategic management and business policy: Globalization, innovation, and sustainability, 13th Ed.* Pearson.