The Impact of Cybersecurity Assurance on the Quality of Internal Audit in The Financial Technology Companies (FinTech) in Jordan

Researcher Hisham Muhammad Ahmad Al-Shayeb **Researcher Alaa Jaber Qasim Al Matarneh**
Professor **PhD**

Islamic Sciences University - Faculty of Finance and Business - Department of Accounting
alshayeb82@yahoo.com

Submission Date: 9/5/2024 **Acceptance Date: 19/8/2024**

Abstract

This study aimed to identify the impact of cybersecurity assurances in its dimensions (data security, system security, network security, operational security, and physical security) on the quality of internal auditing in FinTech companies in Jordan. To achieve the objectives of the study, the descriptive analytical approach was used, where the study population consists of financial technology companies known as FinTech operating in Jordan in accordance with the instructions of the Central Bank, and their number is (18) companies. A comprehensive survey strategy was followed in determining the sample for the study. The study sample is all financial technology companies in Jordan, and the sampling unit is in The study was conducted by employees of the Internal Audit Department, the Financial Department, and the Information Technology Department working in financial technology companies (FinTech) operating in Jordan. (115) electronic questionnaires were distributed to members of the study sample by sending the link via social media, and the number of questionnaires recovered was (107) A questionnaire suitable for statistical analysis, and the most important results reached were the presence of a statistically significant effect of cybersecurity assurances in its dimensions (data security, system security, network security, operational security, physical security) on the quality of internal auditing in Jordanian financial technology companies. The study recommended increasing investment by Jordanian financial technology companies in the technological infrastructure (physical security) to support cybersecurity and provide and develop the necessary infrastructure to improve their efficiency and reduce penetrations, and provide continuous training to employees about cybersecurity risks and how to recognize and deal with cyberattacks.

Keywords: cybersecurity, cybersecurity assurances, internal audit quality, financial technology companies.

أثر تأكيدات الأمن السيبراني في جودة التدقيق الداخلي في شركات التكنولوجيا المالية في الأردن

الباحث هشام محمد احمد الشايب
طالب دكتوراه

الباحث علاء جبر قاسم المطارنة
أستاذ دكتور

جامعة العلوم الإسلامية -كلية المال والأعمال -قسم المحاسبة

alshayeb82@yahoo.con

تاريخ التقديم :9/5/2024

تاريخ القبول :19/8/2024

الملخص

هدفت هذه الدراسة إلى التعرف على أثر تأكيدات الأمن السيبراني بأبعادها (أمن البيانات، أمن النظام، أمن الشبكة، الأمن التشغيلي، الأمن المادي) في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن، ولتحقيق أهداف الدراسة تم ستخدام المنهج الوصفي التحليلي، حيث تكون مجتمع الدراسة من شركات التكنولوجيا المالية المعروفة بـ FinTech)) العاملة في الأردن وفقاً لتعليمات البنك المركزي وعددها (18) شركة وتم إتباع استراتيجية المسح الشامل في تحديد العينة للدراسة، أما عينة الدراسة هي عبارة عن كامل شركات التكنولوجيا المالية في الاردن، كما أن وحدة المعاينة في الدراسة تكون من موظفي إدارة التدقيق الداخلي والإدارة المالية وإدارة تكنولوجيا المعلومات العاملين في شركات التكنولوجيا المالية FinTech)) العاملة في الأردن، حيث تم توزيع (115) إستبيانة إلكترونية على أفراد عينة الدراسة من خلال إرسال الرابط عبر وسائل التواصل الاجتماعي، وبلغ عدد الاستبانات المستردة استرداد (107) إستبانة صالحة للتحليل الإحصائي، وكانت أهم النتائج التي تم التوصل إليها، وجود أثر دال إحصائياً لتأكيدات الأمن السيبراني بأبعاده (أمن البيانات، أمن النظام، أمن الشبكة، الأمن التشغيلي، الأمن المادي) في جودة التدقيق الداخلي في شركات التكنولوجيا المالية الأردنية، وأوصت الدراسة بزيادة استثمار شركات التكنولوجيا المالية الأردنية في البنية التحتية التكنولوجية (الأمن المادي) لدعم الأمن السيبراني وتوفير البنية التحتية الضرورية وتطويرها لتحسين كفاءتها وتقليل من الاختراقات، وتوفير تدريب مستمر للموظفين حول مخاطر الأمن السيبراني وكيفية التعرف على الهجمات السيبرانية والتعامل معها

الكلمات المفتاحية: الأمن السيبراني، تأكيدات الأمن السيبراني، جودة التدقيق الداخلي، شركات التكنولوجيا المالية

1-1 المقدمة

في ظل التغيرات التي شهدتها المنظومة الاقتصادية محلياً وعالمياً مؤخراً، وما تبعها من تأثيرات على أنشطة الشركات في مختلف القطاعات الاقتصادية، أصبحت الشركات العاملة في مجال التكنولوجيا الماليةFinTech)) تظهر بشكل متزايد كوسيلة للتكيف مع الواقع الاقتصادي الجديد. وفقاً للنشرة الخاصة بالإستراتيجية الوطنية للمدفوعات الإلكترونية للأعوام (2023-2025)، الصادرة عن البنك المركزي الأردني، فقد شهد الأردن تطوراً كبيراً في هذا القطاع خلال السنوات العشر الأخيرة، الذي يتميز بالاستقرار والكفاءة العالية، حيث يعود الفضل في هذا التطور إلى الجهود المبذولة من مؤسسات القطاع بالتعاون مع الدور الرقابي والإشرافي للبنك المركزي الأردني على مقدمي خدمات الدفع وأنظمة الدفع الإلكتروني، وقد أولى البنك المركزي الأردني اهتماماً كبيراً بالأمن السيبراني، حيث تعتبر تأكيدات الأمن السيبراني ضرورية لتعزيز الثقة والاطمئنان بأن ضوابط الأمن السيبراني تطبق وفقاً للنهج المطلوب (Evans et. el, 2016).

من الجدير بالذكر أن نشاط شركات التكنولوجيا المالية يترافق مع كم كبير من البيانات Big Data)) التي تتسم بحساسية عالية، مما يجعل حفظها وتخزينها تحدياً كبيراً بسبب عوامل التكلفة والأمان، لذا أصبح من الضروري أن تولي شركات التكنولوجيا المالية اهتماماً كبيراً بالضوابط المتعلقة بأمن المعلومات وكفاءة أنظمة الرقابة الداخلية، وعلى رأسها جودة عمل التدقيق الداخلي، ويجب أن تتضمن هذه الضوابط حماية لأصحاب المصالح والمستخدمين والمدراء التنفيذيين.

يعد التدقيق الداخلي من الأدوات الحيوية التي تعتمد عليها شركات تكنولوجيا المالية لضمان فعالية العمليات الداخلية والتأكد من التزامها بالمعايير والقوانين المعمول بها، ومع تزايد حجم الأعمال وتفاقم تعقيداتها، أصبحت مهام التدقيق الداخلي أكثر تعقيداً وتحدياً، خاصة مع ظهور التحول الرقمي وتكنولوجيا المالية واعتماد الشركات المتزايد على التقنيات الحديثة، حيث تلعب التكنولوجيا دوراً محورياً في تحسين جودة التدقيق الداخلي، على سبيل المثال، يمكن لتقنيات تحليل البيانات أن توفر رؤى أعمق من خلال استخراج المعلومات الحيوية التي تعزز دقة عمليات التدقيق، بالإضافة إلى ذلك يمكن لهذه التقنيات أن تسهم في التنبؤ بالمخاطر السيبرانية المحتملة، مما يتيح للشركات الاستعداد بشكل أفضل للتحديات المستقبلية وحماية نظمها من التهديدات المتزايدة (علي وآخرون، 2022).

نتيجة لزيادة حجم شركات التكنولوجيا المالية وتنوع أنشطتها و زيادة تعقيد العمليات المناطة بطبيعة نشاطاتها التي تتسم بطابع الحساسية وكبر حجم البيانات، تتجلى أهمية وجود أنظمة رقابية داخلية دائمة و مستمرة، فأصبح من الضروري التركيز على جودة التدقيق الداخلي لدى تلك الشركات كونه يعتبر الركيز الأكثر أهميةً في أنظمة الرقابة الداخلية و نجاح هذه الشركات و استمرارها أصبح مقروناً بمدى أمن المعلومات لديها ،و بدوره يسعى المدقق الداخلي لضبط الأنظمة الداخلية والرقابية بكفاءة و فاعلية، و يتعين على التدقيق الداخلي كذلك أن يكون له أثر فعّال من خلال وضع إجراءات قياس

ومتابعة ومراقبة مناسبة للعمليات الداخلية في تلك الشركات، وتعتبر جودة أداء عمليات التدقيق أمرًا حيويًا يمكن أن يسهم بشكل كبير في تعزيز أمان شركات التكنولوجيا المالية، حيث يوفر تقديم رؤى استراتيجية حول المخاطر المتعلقة بشبكات تكنولوجيا المعلومات، وتحديد الفجوات الأمنية ونقاط الضعف المحتملة في النظام، ويقدم التدقيق لهذه الشركات الفرصة لتصحيح الثغرات ونقاط الضعف المكتشفة قبل أن يتم استغلالها من قبل القراصنة والمهاجمين السيبرانيين عبر شبكات الإنترنت، مما يساهم في تعزيز تأكيدات الأمن السيبراني والحفاظ على السمعة الإيجابية للشركات (Jadhav, 2023). و لهذا جاءت هذه الدراسة للبحث في أثر تأكيدات الأمن السيبراني في جودة التدقيق الداخلي في شركات التكنولوجيا المالية في الاردن

1-2أهمية الدراسة

تتجلى أهمية هذه الدراسة من الناحيتين العلمية و العملية وفقاً لما يلي:

1-2-1 الأهمية العلمية

يأمل الباحث أن تقدم هذه الدراسة إثراءً للمعرفة العلمية من خلال توضيح الدور الهام لتأكيدات الأمن السيبراني في تقديم آلية فحص موضوعي تهدف إلى تقييم مستقل لإدارة المخاطر، والرقابة، وعمليات الحوكمة، بالإضافة إلى الكشف عن أي مخاطر أو نقاط ضعف تتعلق بالرقابات الأمنية وتأثيرها على جودة التدقيق الداخلي في المنظمات التي تعمل في بيئة تقنية وتكنولوجية. وعلى حد علم الباحث، تكتسب هذه الدراسة أهمية علمية إضافية نظراً لقلة الدراسات التي تناولت أثر تأكيدات الأمن السيبراني على جودة التدقيق الداخلي في شركات التكنولوجيا المالية في الأردن.

1-2-2 الأهمية العملية

تستمد هذه الدراسة أهميتها من الناحية العملية من الدور الهام الذي تلعبه شركات التكنولوجيا المالية FinTech)) في دعم الاقتصاد الأردني بشكل عام. التوصيات والمقترحات التي ستتوصل إليها هذه الدراسة قد تسهم في تحفيز شركات التكنولوجيا المالية والمدراء التنفيذيين والرقابيين على إيلاء اهتمام أكبر لتأكيدات الأمن السيبراني وتطبيقاته. هذا الاهتمام من شأنه تعزيز الثقة بأن أنظمة الرقابة الداخلية تُطبَّق بكفاءة وجودة عالية، مما يعزز من استقرار وأمان العمليات المالية في تلك الشركات.

1-3أهداف الدراسة:

تتمثل الأهدف الرئيسية لهذه الدراسة بما يلي:

الهدف الرئيسي: التعرف على أثر تأكيدات الأمن السيبراني بأبعادها (أمن البيانات، أمن النظام، أمن الشبكة، الأمن التشغيلي، الأمن المادي) في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن.

و يتفرع عنه الاهداف الفرعية التالية:

الهدف الفرعي الأول: التعرف على أثر أمن البيانات في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن.

الهدف الفرعي الثاني: التعرف على أثر أمن النظام في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن.

الهدف الفرعي الثالث: التعرف على أثر أمن الشبكة في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن.

الهدف الفرعي الرابع: التعرف على أثر الأمن التشغيلي في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن.

الهدف الفرعي الخامس: التعرف على أثر الأمن المادي في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن.

4-1مشكلة الدراسة و أسئلتها

تعد شركات تكنولوجيا المالية من أكثر القطاعات تقدماً في مجال تطبيق التكنولوجيا والتقنيات الحديثة في أنشطتها وعملياتها، واستثمارها بالشكل الأمثل لتحسين كفاءة عملياتها، باعتبارها وسيلة لتحقيق أهدافها، إلاّ أن هذا الاستخدام لا بد وأن يترتب عليه بعض المخاطر والتهديدات التي تؤثر سلباً على سير العمل ومكانة الشركة في السوق، لذا كان لابد من تبني كافة الإجراءات والمتطلبات التي تسهم في الحفاظ على أمن البيانات والامتثال للقوانين وتحسين كفاءة العمليات والحد من المخاطر والتهديدات الأمنية الإلكترونية وحماية سمعة الشركة (Qasaimeh & Jaradeh, 2022).

وتعتبر جودة التدقيق الداخلي من المواضيع الهامة التي تشكل تحدياً رئيسياً لشركات التكنولوجيا المالية في الأردن، حيث ازدادت أهمية هذا الموضوع في القطاع المالي نظراً لحساسية الأنشطة المالية المرتبطة بتكنولوجيا المعلومات وتهديدات الهجمات السيبرانية التي قد تتعرض لها هذه الشركات، ولم تعد تهديدات الأمن السيبراني مقتصرة على البعد المادي فقط، بل أصبحت تشمل العديد من الأبعاد الأخرى، حيث تُعَد تأكيدات الأمن السيبراني خط الدفاع الأول لحماية الشركة، حيث تهدف إلى تحقيق درجة من الاطمئنان بأن الرقابات الأمنية تعمل بالشكل المطلوب، مما يوفر حماية للبيانات والتطبيقات والشبكات والفضاء السيبراني، لذلك تسعى شركات التكنولوجيا المالية جاهدة للوصول إلى مستوى عالٍ من التأكيدات حول أنظمة الرقابة الداخلية المرتبطة بالأمن السيبراني، جنباً إلى جنب مع جودة أعمال التدقيق الداخلي. (الهلسة، 2021).

و قد جاءت هذه الدراسة لتسليط الضوء على أهمية تأكيدات الأمن السيبراني التي بدورها ستخلق نوعاً من الإطمئنان حول الرقابات الأمنية المتعلقة بأمن البيانات، أمن

النظام، أمن الشبكة، الأمن التشغيلي، والأمن المادي وأنها تعمل بالشكل المطلوب لتعزيزجودة أعمال التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن، و عليه فإنه من الممكن صياغة أسئلة الدارسة على النحوالاتي:

السؤال الرئيسي: هل يوجد أثر لتأكيدات الأمن السيبراني بأبعادها (أمن البيانات، أمن النظام، أمن الشبكة، الأمن التشغيلي، الأمن المادي) في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن، و يتفرع عنه الأسئلة الفرعية التالية:

السؤال الفرعي الاول: هل يوجد أثر لأمن البيانات في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن؟

السؤال الفرعي الثاني: هل يوجد أثر لأمن النظام في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن؟

السؤال الفرعي الثالث: هل يوجد أثر لأمن الشبكة في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن؟

السؤال الفرعي الرابع: هل يوجد أثر للأمن التشغيلي في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن؟

السؤال الفرعي الخامس: هل يوجد أثر للأمن المادي في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن؟

5-1فرضيات الدراسة

للإجابة على أسئلة مشكلة الدراسة تم وضع الفرضيات التالية:

الفرضية الرئيسية:

H01: لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (P≤ 0.05) لتأكيدات الأمن السيبراني بأبعادها (أمن البيانات، أمن النظام، أمن الشبكة، الأمن التشغيلي، الأمن المادي) في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن.

و يتفرع عنها الفرضيات الفرعية التالية:

الفرضية الفرعية الأولى:

H01 -1 لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (P≤ 0.05) لأمن البيانات في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن.

الفرضية الفرعية الثانية:

H01 -2: لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (P≤ 0.05) لأمن النظام في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن.

الفرضية الفرعية الثالثة:

H01- 3: لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (P≤ 0.05) لأمن الشبكة في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن.

الفرضية الفرعية الرابعة:

H01 -4: لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (P≤ 0.05) للأمن التشغيلي في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن.

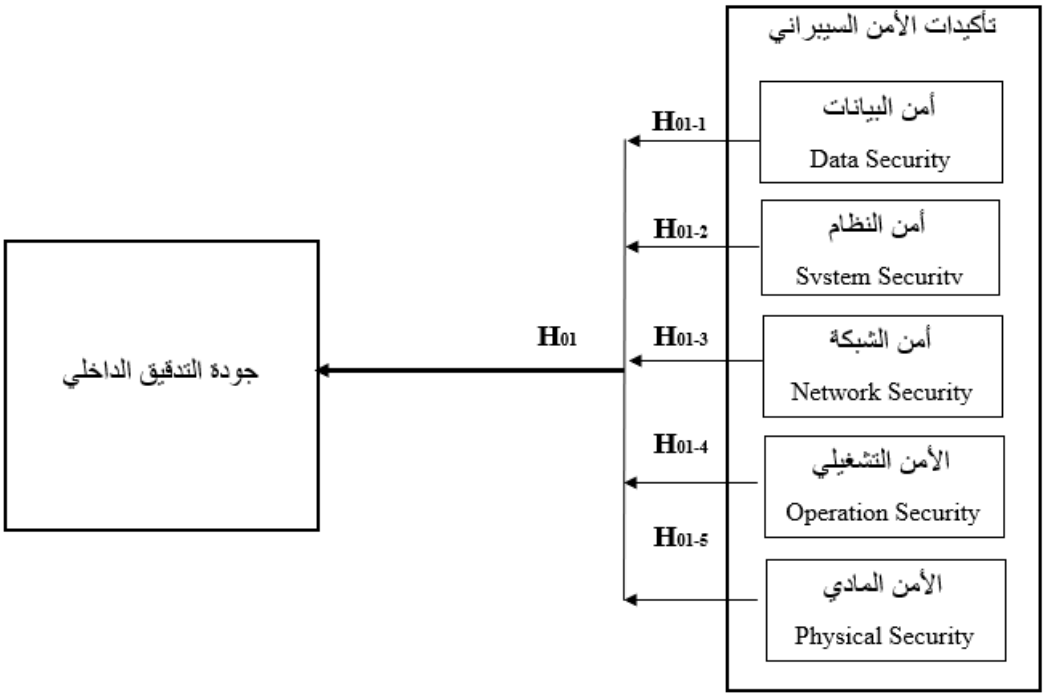
الفرضية الفرعية الخامسة:

H01- 5: لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (P≤ 0.05) للأمن المادي في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن.

1-6أنموذج الدراسة

تم و ضع أنموذج الدراسة ادناه لتحقيق هدف الدراسة و الإجابة على أسئلتها، و قد تم إعداد النموذج الذي يمثل العلاقة بين متغيرات الدراسة كالاتي:

الشكل رقم (1)



المصدر: من إعداد الباحث بالاعتماد على المراجع الآتية:

المتغير	المراجع التي تم الاستناد اليها
تأكيدات الأمن السيبراني	جمال الدين (2023)، الحوامده (2021)، منصور (2021)
جودة التدقيق الداخلي	Usman, et al., (2023)، Lindvall, (2022)الحوامده (2021)،

الإطار النظري

يُعتبر مفهوم الأمن السيبراني أحد المفاهيم الناشئة التي تجلب إهتماماً متزايداً، نظراً لظهور تقنيات وأدوات تكنولوجية جديدة مبتكرة، والتي من المتوقع أن تستخدم على نطاق واسع في جميع مجالات وأنشطة العمل لدى الشركات، بما في ذلك شركات تكنولوجيا المالية (FinTech)، و يعرف الأمن السيبراني على أنه مجموعة الممارسات للحفاظ على السرية المتكاملة مع التوافرية للمعلومات و أصولها للمنشآت التي تعمل ضمن إطار الفضاء السيبراني من تلك التهديدات السيبرانية من خلال مجموعة من التعليمات والضوابط والسياسات والإجراءات والسائل المُثلى بهذا الصدد (البنك المركزي الأردني، 5،2018)، حيث يعتبر الأمن السيبراني جزءاً حيوياً وهاماً في عالم الرقمنة الآمن، حيث تكمن

أهميته في توفير الحماية من المتسللين، القراصنة، أو المجرمين على شبكات الإنترنت، بالإضافة إلى مكافحة الاحتيال الإلكتروني وغيرها من التهديدات التي تشكل بالفعل تحدياً كبيراً. هذه التهديدات تجعل المستخدمين، سواء كانوا شركات أو أفراداً، في قلق دائم ومستمر حيال احتمال الوقوع كضحايا لتلك الانتهاكات السيبرانية والقرصنة الإلكترونية، فالأمن السيبراني هو أحد المجالات التكنولوجية التي تتطور بسرعة كبيرة، ولا يقتصر تطوره على قطاعات تكنولوجيا المعلومات فقط، بل يشمل أيضاً قطاعات الصحة، والبنوك، والتعليم، والجيش، والأمن، والحكومة، وشركات التكنولوجيا المالية (Kure et al., 2018, 3)).

تعتمد المنظمات والأفراد بشكل كبير على التكنولوجيا في أعمالهم اليومية، مما يجعل تجاهل خطر الجرائم الإلكترونية يمثل تهديداً جسيماً ومعقداً للمستخدمين، سواء كانوا موظفين أو منظمات أو عملاء، هذا الواقع يفرض على المنظمات العمل في بيئة مليئة بالتهديدات والمخاطر السيبرانية التي يجب التحوط ضدها، ومن هنا تبرز أهمية فهم أبعاد تأكيدات الأمن السيبراني وضمان الرقابة الفعّالة على الأنظمة المعلوماتية والتأكد من أمن المعلومات وحمايتها، حيث تهدف هذه الدراسة إلى تحليل المناهج المستخدمة في دراسة تأكيدات الأمن السيبراني لتحديد القضايا الهامة والمحورية ونقاط الضعف في الأنظمة من منظور التدقيق الداخلي وإدارة المخاطر لدى شركات التكنولوجيا المالية، حيث تعتمد هذه الشركات بشكل كبير على البيانات الرقمية في ممارسة أنشطتها التجارية، وهي بيانات ضخمة ومترابطة ضمن شبكة معلوماتية معقدة يستفيد منها العديد من أصحاب المصالح والمستخدمين للأنظمة (Kahyaoglu & Caliyurt , 2018, 360 &367)،إذ ينبغي على أي شركة التأكد من وجود آلية لفحص الأدلة بشكل موضوعي بهدف تقييم مستقل لإدارة المخاطر والرقابة وعمليات الحوكمة. يشمل هذا الكشف عن أي مخاطر أو نقاط ضعف متعلقة بالرقابات الأمنية، بما في ذلك أمان البيانات، وأمان النظام، وأمان الشبكة، والأمان التشغيلي، والأمان المادي (Jadhav, 2023, 1).

أولا أمن البيانات: يتعامل أمن البيانات مع سلامة البيانات، ويشمل تقييم نطاق الضرر المحتمل، بالإضافة إلى كشف الانتهاكات، وإجراء التعديلات الضرورية، ومنع سوء استخدام البيانات الفردية، تتمثل مراكز الخصوصية في أمن البيانات الفردية في مراقبة سلوكها وتأثير الاختراقات على البيانات (Hu, et al., 2018, 3) إذ يُعرف أمن البيانات بأنه مجموعة من السياسات والإجراءات التقنية والإدارية التي تشمل العمليات والآليات المتبعة لمنع أي تدخل غير مقصود أو غير مصرح به، مثل التجسس أو الاختراق أو الاستخدام غير القانوني للمعلومات والبيانات الإلكترونية الموجودة على الأنظمة المعلوماتية وأنظمة الاتصالات، حيث يضمن أمن البيانات أيضًا تأمين وحماية سرية وخصوصية البيانات الشخصية، ويشمل استمرار عملية حماية أجهزة الحاسوب وأنظمة المعلومات والاتصالات والخدمات من أي تغيير أو تلف يمكن أن يؤثر سلبًا على البيانات (السمحان، 2020، 11)، كما يُعرَف أمن البيانات بأنه مجموعة من الضوابط والسياسات التي وضعتها الهيئة الوطنية للأمن السيبراني بهدف تحديد الحد الأدنى من المتطلبات الأمنية لتمكين المؤسسات من حماية بياناتها بكافة أشكالها، سواء كانت بيانات مادية أو رقمية، تشمل هذه البيانات البيانات المهيكلة،

مثل قواعد البيانات والجداول، والبيانات غير المهيكلة، مثل الوثائق والمستندات، وذلك عبر جميع مراحل دورة حياة البيانات، ويهدف ذلك إلى مساعدة المؤسسات في التصدي للتهديدات المتنامية والحفاظ على أمان بياناتها ونشاطاتها التشغيلية، مع تقليل الأضرار إلى أدنى حد ممكن في حالة وقوع حوادث أمنية (الهيئة الوطنية للأمن السيبراني، 2023).

ثانيا أمن النظام: إن استخدام أنظمة تكنولوجيا المعلومات يسهم بشكل كبير وفاعل في تحسين كفاءة العمل وتبسيطه، كما يساعد في حل المشكلات المختلفة التي تواجهها المنظمات، وبالأخص تلك التي تعتمد في عملها على البيانات الضخمة مثل شركات التكنولوجيا المالية، ومع تعرض المنظمات للهجمات الإلكترونية، يصبح حماية خصوصية البيانات أمراً ملحاً وهاماً للغاية للحفاظ على سرية وجودة المعلومات (Qasaimeh & Jaradeh, 2022) لذا يتعين على المنشآت استخدام الأجهزة والبرامج الحاسوبية المناسبة لضمان حماية الأنظمة المعلوماتية من الهجمات السيبرانية الخارجية، بالإضافة إلى ذلك، يجب تطوير هذه الأنظمة باستمرار لمواكبة التطورات والمخاطر المستجدة، ومعالجة نقاط الضعف والأخطاء التي يمكن أن تستغل في التأثير المدمر على تلك الأنظمة (San, 2021).

إن حماية الأنظمة تُعتبر خطوة حيوية ضمن التدابير الشاملة التي يجب اتخاذها لتأمين الأنظمة المعلوماتية بشكل شامل، حيث تتضمن تدابير أمن الأنظمة استخدام تقنيات الأجهزة والبرامج للتصدي للتهديدات الخارجية وضمان سلامة الأنظمة خلال مراحل تطويرها، ومع تزايد توفر الأنظمة عبر الشبكات، أصبح قبول آليات الأمان ضرورة أساسية خلال عملية النمو وتطوير النظام، وباستخدام تطبيقات مكافحة الفيروسات، والخدمات المشفرة، وجدران الحماية، يمكن للمستخدمين وأصحاب المصالح تقليل مخاطر الاختراق وحماية تلك الأنظمة، حيث يجب على مالكي النظام اتخاذ الإجراءات اللازمة لتطبيق السيطرة الكاملة على النظام، بما في ذلك تنفيذ سياسات الأمان مثل استخدام كلمات مرور معقدة والمصادقة عليها من قبل المختصين والقائمين على الرقابات الداخلية، بالإضافة إلى تحديد وتأمين الوصول إلى المعلومات الحساسة(Mindcore, 2018) لذلك، يجب التأكد من أمن الأنظمة من خلال سلامة عمليات التصحيح عند وجود ثغرات في أنظمة المعلومات والعمليات، إذ تُعد هذه العملية دقيقة وغاية في الأهمية، وتتضمن آلية الوصول والصلاحيات لنظام المعلومات تعيين الأدوار والوظائف وإدارة الحسابات بشكل فعال، مما يمكن من مراقبة ومراجعة سجلات هويات الدخول ومنح الصلاحيات وفقًا للوظائف المحددة (Jadhav, 2023, 1).

ثالثا أمن الشبكة

يُعتبر أمن الشبكات جزءًا حيويًا من البنية التحتية لتكنولوجيا المعلومات، ولهذا فإن تقييم أمان الشبكة يحمل أهمية كبيرة، ويجب أن يأخذ هذا التقييم في الاعتبار الميزات والسلامة المتعلقة بمعدات الشبكة التي تُعرف كبوابات حماية، وتُعتبر معلمات الاختبار نوعًا من الهيكلية التي يتم تطبيقها لتوصيل الروابط وعقد الشبكات، مع التركيز على عدد ونوع بوابات الأمان، سواء كانت مادية أو منطقية (Gyorffy et al., 2017, 416)، حيث تتعلق

تأكيدات الأمن السيبراني على الشبكات بحماية الشبكات من المخاطر الخارجية والدفاع ضد التدخل غير المرغوب فيه، مع التركيز على تحديد ومنع النوايا الخبيثة التي تستهدف البنية التحتية الداخلية للشبكة (Mindcore, 2018).

أمن الشبكات يُعنى بتأمين مستوى مناسب من الحماية لشبكات الكمبيوتر ضد التهديدات السيبرانية، مثل القراصنة والمتطفلين والبرامج الضارة، التي تهدف إلى الاختراق والتلاعب بالشبكات. يهدف ذلك إلى حماية البنية التحتية للشبكة ومنع الاختراق نتيجة للثغرات أو الهجمات السيبرانية (التوني، 2023، 625). تُعتبر تأكيدات حماية الشبكات جوهرية لضمان استقرار البنية التحتية، حيث تهدف إلى منع الوصول غير المصرح به إلى الشبكة. تستخدم أقسام الأمن تقنيات التعلم الآلي للكشف عن حركة مرور غير عادية وتنبيهها للتهديدات في الوقت الفعلي، مما يسهل مراقبة أمان الشبكة. يشمل حماية الشبكة جميع الآليات المسؤولة عن الحفاظ على سلامة الشبكة، بما في ذلك منع الوصول غير المصرح به والتدخلات غير المرغوب فيها (الدويري والحواجرة، 2023، 71). حيث تهدف تأكيدات الشبكات إلى ضمان موثوقية وسلامة الشبكات الداخلية، وتستند استراتيجيات الحماية على مجموعة متنوعة من الوسائل، بما في ذلك الأجهزة والبرمجيات المصممة خصيصًا لحماية البيانات والشبكات، وتتضمن هذه الوسائل مراقبة الاتصالات ومنع الوصول غير المصرح به ومكافحة انتشار الهجمات عبر الشبكات، كما تعتمد أيضًا على تكتيكات متعددة للردع من البرمجيات الضارة والانتهاكات الأخرى للشبكات والبيانات (Reid, 2021).

رابعا الأمن التشغيلي

الأمن التشغيلي يشير إلى السياسات والإجراءات والعمليات التي تدير معالجة وحماية البيانات الأساسية، بالإضافة إلى آليات منح الوصول للمستخدمين الذين يحتاجونه للولوج إلى الشبكات والبيانات، ويشمل أيضًا إدارة مكان وطريقة تخزين البيانات ومشاركتها (التوني، 2023، 626). ففي ظل التطور السريع في عالم التكنولوجيا، تزداد مستويات التهديدات التي تواجه الشبكات بصورة متواصلة، حيث يسعى المهاجمون والقراصنة السيبرانيون إلى الاستفادة من هذا التقدم، وعادةً ما يستهدفون الشبكات غير الآمنة كنقطة انطلاق لهجماتهم، بهدف التسلل إلى أنظمة المستخدمين والمؤسسات، وهنا تبرز أهمية التأكيدات على الأمن السيبراني؛ حيث تعتمد شركات ومؤسسات على هذه التدابير للتأكد من سلامة شبكاتها وأنظمتها، وتشمل هذه التأكيدات تقييم البنية التحتية للشبكة، ومراجعة السياسات والإجراءات الأمنية، وتحليل التهديدات المحتملة، واختبار البرمجيات والتطبيقات لاكتشاف الثغرات الأمنية، وبناءً على هذه النتائج، تُتخذ الإجراءات الضرورية لتعزيز الأمان وتعزيز الحماية، من بين هذه الإجراءات، تبرز أنظمة المصادقة متعددة العوامل كحل فعّال، حيث توفر طبقة إضافية من الحماية عند الولوج إلى الأنظمة والبيانات، من خلال مطابقة عدة عوامل مثل كلمة المرور، ورمز مكون من الأرقام، وبصمة الإصبع. ولذلك، يجب على المنظمات مراجعة الضوابط لمراقبة موردي الأنظمة التشغيلية ومقدمي الخدمات والشبكات السحابية، إلى جانب البرامج المستخدمة، وذلك لضمان كفاءة الأنظمة والتدابير الأمنية، بما في ذلك تحديد نقاط الضعف والمخاطر وتصحيحها (Jadhav, 2023, 2-3).

خامسا الأمن المادي

حفظ الأمان والسلامة للبنية التحتية المادية يتوقف بشكل كبير على الأمن السيبراني، حيث تعتبر البنية التحتية الحيوية - مثل الشبكات الكهربائية والمياه والاتصالات ووسائل النقل - أساسية لوظائف المجتمع الحديث، حيث تحتاج هذه البنية إلى حماية فعّالة من التهديدات السيبرانية، حيث يمكن لاختراق الأنظمة السيبرانية من قبل المهاجمين والقراصنة أن يؤدي إلى تعطيل البنية التحتية الحيوية، وبالتالي يمكن أن يسبب الفوضى والتأثير الكبير على المجتمع، لهذا السبب تلعب تأكيدات الأمن السيبراني دورًا بارزًا في الحفاظ على سلامة وأمان هذه البنية التحتية المادية وتأمينها (San, 2021). لذلك ينبغي على الشركات أن تولي اهتمامًا خاصًا ببنيتها التحتية وتعمل على تأمينها بشكل جيد، ويتطلب ذلك الحذر والنظر في جميع نقاط الضعف المحتملة في البنية التحتية، واتخاذ إجراءات فعّالة لمعالجتها، ومن بين هذه النقاط الضعف، يأتي تأمين وحماية المجتمع الذي تخدمه الشركة، حيث تعتمد الشركات على الثقة في الأسواق التي تعمل فيها. لذا، من الضروري أن تتخذ الشركات التدابير اللازمة لحماية بنيتها التحتية وأمانها المادي، وضمان سلامة جميع الأصول المادية (Mindcore, 2018).

ويشير مفهوم الأمن المادي إلى التدابير والرقابات المرتبطة ببنية التحتية المادية، حيث أنها، مثل سائر الأنظمة، قد تتعرض لتهديدات سيبرانية. لذا، يجب أن تتضمن تأكيدات الأمن السيبراني النظر في المكونات المادية للنظام، مثل أجهزة الحاسوب ومعالجاتها والمفاتيح ومسارات المعلومات وقنوات الاتصال، بالإضافة إلى ذلك يؤكد هذا النوع من الرقابات على ضرورة وجود خطة طوارئ لمواجهة حالات انقطاع التيار أو الكوارث مثل الحرائق، وذلك عن طريق الاحتفاظ بنسخ احتياطية في أماكن آمنة بعيدة عن مقر الشركة (ذنيبات، 2021). فالأمن المادي يُعَد جزءاً حيوياً ضمن استراتيجية الأمن السيبراني لأي منشأة، حيث يهدف إلى حماية الأصول والموارد من التهديدات الخارجية والداخلية، ويتضمن ذلك مجموعة من التدابير الإيجابية والسلبية التي تهدف إلى منع الوصول غير المصرح به وحفظ سلامة البيئة الداخلية للمنشأة، ويشمل الأمن المادي مجموعة من السياسات والإجراءات والتقنيات المصممة لحماية الأصول والموارد من التهديدات المختلفة، مثل السرقة والتخريب والإرهاب والنشاط الإجرامي، إذ يركز الأمن المادي أيضًا على حماية الموظفين والمعدات والبيانات والمعلومات الحساسة، بالإضافة إلى تأمين المنشآت والمواقع الحيوية ضد الهجمات والتسلل غير المرغوب فيه (2-CDSE, 2017, 1).

ويرى الباحث أنه يتعين على شركات التكنولوجيا المالية في الأردن استخدام آليات التشفير المناسبة للسيطرة على عملية الوصول إلى الشبكة وحماية البيانات، خصوصاً أن هذه الشركات تعتمد على الشبكات العنكبوتية في جميع عملياتها، وينبغي أن تشمل هذه الحماية البيانات أثناء عمليات الإرسال والاستقبال وتبادل البيانات، وكذلك عند عدم ممارسة أي نشاط تقني، وتُمكّن هذه الآليات الشركات من الكشف عن الانتهاكات ومنع الجرائم الإلكترونية وعمليات الاحتيال الإلكتروني، بالإضافة إلى توفير النسخ الاحتياطية الضرورية.

جودة التدقيق الداخلي

التدقيق الداخلي يُعَدُّ أداة رقابية فعّالة تُسهم في خدمة الإدارة وتضمين ضمان أساسي لكفاءة النظم الرقابية في الشركة. يتعدى التدقيق الداخلي النمطي المتمثل في التدقيق المالي والمحاسبي ليشمل مجالات الإدارة والعمليات أيضًا، ويقوم التدقيق الداخلي بتقييم الخطط والسياسات المعمول بها في الشركة، ويقترح البدائل المناسبة لتحسين استغلال الموارد المتاحة بكفاءة وفاعلية قصوى (الدوسري وآخرون، 2022، 667). تتجلى أهمية التدقيق الداخلي في الطلب المتزايد والكبير على خدماته في الشركات والوحدات الاقتصادية الخاصة والعامة، مما يعكس الاعتراف المتزايد بدوره الحيوي والفعّال في تحقيق أهداف الشركات وضمان تنفيذ العمليات بشكل صحيح ومطابق للمعايير والقوانين المعمول بها، ففي ظل وجود ظروف اقتصادية صعبة، يتعين على الشركات التركيز على كيفية أداء العمليات والأنشطة الداخلية، ويلعب التدقيق الداخلي دورًا حيويًا في هذا السياق من خلال تقديم تقييم مستقل وموضوعي للعمليات والأنشطة. كما يُعتبر التدقيق الداخلي أداة حيوية لضمان صحة البيانات والمعلومات المالية والمحاسبية في الوقت الفعلي، ويساهم في تحديد الاختلالات والمخاطر المحتملة وتصحيحها. ومن خلال تحول التدقيق الخارجي إلى نمط التدقيق الاختياري، يصبح لدى الشركات القدرة على توفير بيانات ومعلومات قابلة للاعتماد لاتخاذ القرارات الإدارية، ويُطلب من دائرة التدقيق الداخلي التأكد من تحقيق النتائج المتوقعة والتزام الإدارات القطاعية بالسياسات والخطط العامة (حمود وآخرون، 2019، 35 ; إبراهيم وآخرون، 2019، 858 ;قواقزة، 2022، 1398)

يتم تقسم خدمات التدقيق الداخلي إلى قسمين، فالقسم الاول تقديم الخدمات الاستشارية من قبل المدققين الداخليين يهدف في الأساس إلى تمكين الإدارة من اتخاذ القرارات المستنيرة، حيث يسعون المدققون الداخليون لتحقيق قيمة مضافة للشركة من خلال تقديم التوجيهات والاقتراحات التي تسهم في تحسين أداء الشركة ومراقبة العمليات، بالإضافة إلى تعزيز إدارة المخاطر والامتثال للحوكمة، وينبغي على المدققين الداخليين السعي إلى تحقيق التوازن الصحيح بين تقديم الاستشارات والحفاظ على الاستقلالية والموضوعية خلال تقديم خدماتهم، ويساعد هذا التوازن في بناء الثقة بين الإدارة والمدققين الداخليين، مما يسهم في تحقيق أهداف الشركة بشكل فعال ويساهم في تعزيز النجاح والاستدامة في الأعمال، أما القسم الثاني خدمات التأكيد تهدف إلى ضمان سير العمل بشكل سليم داخل الشركة واستكشاف وتفحص مختلف أنشطتها، بهدف تقديم تقييم موضوعي للأدلة وإصدار آراء تتعلق بعمليات الحوكمة والرقابة وإدارة المخاطر. وتشمل هذه الخدمات فحص الجوانب المتعلقة بدقة المعلومات المالية والحفاظ على الأصول واستخدام الموارد بكفاءة، بالإضافة إلى التحقق من تحقيق أهداف الشركة، ويسمح هذا التقييم الشامل بتحديد المخاطر المحتملة المتعلقة بأنشطة الشركة، ويوفر التوصيات اللازمة لضمان التعامل الملائم مع تلك المخاطر، مما يضمن توافق عمليات الشركة مع أهدافها واستراتيجياتها (Bunjaku, 2019, 39 ; كشاط، وتيجاني، 2017، 322).

الدراسات السابقة

هدفت دراسة جمال الدين (2023) إلى استعراض أهم القضايا الجدلية المطروحة بين الباحثين في السياسية و في الأمن السيبراني تحديداً ، من خلال أربعة محاور رئيسية حيث تناولت الوحدات الدولية الفاعلة في النظام الدولي، و تأثير الأمن السيبراني على مجموعة المؤسسات الدولية، و التغير الذي أحدثه الأمن السيبراني على هيكلية الانظمة الدولية، و أهم العمليات الدولية في الفضاء السيبراني وفقاً للتنسيقات الدولية، وأظهرت النتائج أنه يوجود حالة من الفوضى تسود التنظيم على الصعيد الدولي بسبب غياب أنظمة الرقابة على أمن المعلومات وأنه يجب ترسيخ مفهوم الأمن السيبراني لمواجهة حرب التهديدات المتعلقة بمخاطر أمن المعلومات. وهدفت دراسة أبو الخير (2023) إلى عرض مفهوم ومخاطر الأمن السيبراني، وتوضيح محددات جودة المراجعة الداخلية للأمن السيبراني، وإختبار أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الاستقرار المالي في البنوك الإلكترونية، وتوصلت الدراسة إلى أن التطور الحاصل في المخاطر السيبرانية يحفز المنظمات المالية وخاصةً البنوك الإلكترونية على البحث المستمر نحو إتخاذ إجراءات وقائية من تلك المخاطر من خلال لوائح تجعل تلك الإجراءات أكثر وضوحاً أمام مجالس إدارات تلك البنوك، الأمر الذي يؤدي إلى دعم الاستقرار المالي في تلك البنوك. وهدفت دراسة عبدالقادر، وآخرون (2023) إلى تسليط الضوء على أثر جاهزية البيئة المادية والبشرية للأمن السيبراني على استخدام الخدمات المصرفية الالكترونية من خلال تقليل المخاطر المدركة لدى عينة عملاء بنك التنمية المحلية BDL بوالية غرداية، وتوصلت الدراسة إلى وجود علاقة تأثير غير مباشرة لبعدي جاهزية البيئة المادية والبشرية للأمن السيبراني في استخدام الخدمات المصرفية الالكترونية من خلال تقليل المخاطر المدركة للعملاء. وهدفت دراسة أميرهم (2022) إلى إختبار أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الإستقرار المالي في البنوك الإلكترونية، وكانت أهم النتائج التي تم التوصل إليها: التطور الحادث في المخاطر السيبرانية يحفز المنظمات المالية وخاصة البنوك الإلكترونية على البحث المستمر والمكثف نحو إتخاذ إجراءات وقائية من تلك المخاطر من خلال لوائح تجعل تلك الإجراءات أكثر وضوحاً أمام مجالس إدارات تلك البنوك، الأمر الذي يؤدي إلى دعم الإستقرار المالي في تلك البنوك. وهدفت دراسة الحوامده (2021) إلى بيان أثر الحوكمة السيبرانية على جودة التدقيق الداخلي في البنوك التجارية الأردنية، وذلك من خلال إجراء الدراسة الميدانية التي خصصت على البنوك التجاريه الأردنية، توصلت الدراسة إلى عدة نتائج من أبرزها: أشارت نتائج التحليل الوصفي الى ارتفاع مستوى اهتمام البنوك التجارية الاردنية بالحوكمة السيبرانية، حيث بلغ الوسط الحسابي 4.16 ، في حين ظهرت جميع الابعاد بأهمية نسبية مرتفعة اذ احتلّ بُعد برنامج الأمن السيبراني المرتبة الأولى، بينما احتلّ بُعد سياسة الأمن السيبراني المرتبة الأخيرة. وهدفت دراسة منصور (2021) إلى التعرف على أهمية الأمن السيبراني من خلال تأثيره على الرقابة الداخلية وقيمة الوحدة الاقتصادية باعتماد إطار حوكمة تقنية المعلومات (COBIT5)، وتم قياس متطلبات الأمن السيبراني بكل من (الاستراتيجية، العمليات والإجراءات، الحماية

السرية والخصوصية، والمخاطر السيبرانية)، وتوصلت الدراسة إلى وجود علاقة بين أبعاد ومتطلبات الأمن السيبراني (العمليات والإجراءات، المخاطر السيبرانية، الحماية السرية والخصوصية، الأمن المنطقي، الاستراتيجية) على الأطر الحديثة للرقابة الداخلية (COBIT5) وقيمة الوحدة الاقتصادية.

وهدفت دراسة Tawfiq and Abdullah (2023) إلى إلى التعرف بشكلٍ عام على دور شركات التكنولوجيا المالية في تنمية الاقتصاد في الأردن، وسردت الدراسةً بدايةً مفهوم التكنولوجيا المالية، وأبرز مراحل تطور هذه التقنية، حيث كان التركيز في بداية الدراسة على التكنولوجيا المالية وتطورها في دول العالم، وفي نهاية الدراسة تمت الاشارة إلى التكنولوجيا المالية في الأردن وكيفية تتطورها بشكل متسارع بفضل الأبحاث و المؤتمرات العلمية والندوات التوعوية و التثقيفية في هذا المجال، والدور الرقابي و الإشرافي للبنك المركزي في تطوير هذا القطاع مما ساهم بشكل إيجابي في تنمية الاقتصاد الأردني. و قد كانت من أهم نتائج هذه الدراسة النظرية أن الأردن تعد من الدول الناشئة في استخدام مجال التكنولوجيا المالية و أن وزارة الاتصال الرقمي تعمل جاهدةً على عقد الندوات و المؤتمرات التي من شئنها الاسهام في نشر الوعي في مجال التكنولوجيا المالية، و أن الاردن من المحتمل أن يكون من الدول الرائدة عالمياً في هذا المجال اذا استمر في هذا النهج. وهدفت دراسة Usman, et al., (2023) إلى إنشاء إطار نظري ليعزز عملية فحص دور المدققين الداخليين في تقييم مخاطر الأمن السيبراني في منظمات الأعمال القائمة على التمويل، حيث تكون مجتمع الدراسة من منظمات الأعمال المالية والتي تقدم خدمات مالية لأصحاب المصلحة من القطاعين العام والخاص، وأظهرت نتائج هذه الدراسة أن أداء مهمة تقييم مخاطر الأمن السيبراني من قبل المدقق الداخلي يتأثر بخصائص الأخلاقيات المهنية للمدقق الداخلي المطلوبة (كالنزاهة، والموضوعية والسمات الشخصية والمهارات المهنية والكفاءة والمعرفة المهنية). بينما هدفت دراسة Jadhav (2023) إلى استكشاف الدور الذي تلعبه عمليات تدقيق الأمن السيبراني بأبعاده تدقيق الأمن السيبراني، الأمن السيبراني، والتهديدات السيبرانية، إدارة المخاطر السيبرانية، تدقيق تكنولوجيا المعلومات، أنظمة الأعمال ، ولجنة التدقيق) في إدارة أنظمة وتطبيقاتها، وكانت أهم النتائج التي تم التوصل اليها أن عمليات تدقيق الأمن السيبراني تساعد في ضمان تدقيق كامل ومتعمق للمواقف الأمنية للمنظمة، كما تساعد في الكشف عن المخاطر والثغرات والتهديدات التي تواجهها المنظمة، جنبًا إلى جنب مع تأثير هذه المخاطر عبر مجالات مختلفة بما في ذلك أمن البيانات والأمن التشغيلي والأنظمة. وهدفت دراسة (Lindvall, 2022) إلى الكشف عن ممارسات المدققين الداخليين في السويد، ودورهم في تحقيق الأمن السيبراني، وأظهرت النتائج أن هناك أثر للمدققين الداخليين للتأكيد بشكل كبير على الأمن السيبراني للمؤسسات، حيث يمكنهم تعزيز ممارسة الأمن السيبراني، وبالتالي يؤثر المدققون الداخليون على المنظمات من خلال الممارسة والمهارات الشخصية على تحقيق الأمن السيبراني، كما أظهرت النتائج أن المدققون الداخليون ووظيفة التدقيق الداخل تؤثر على الإدارات الأخرى، وخاصة الوحدات التي تعمل في مجال الأمن السيبراني. وهدفت دراسة Al Fayi (2022) إلى التركيز

على فحص كيفة تلأثيير كفاءة وموضوعية المدققين الداخليين على مقاومتهم الضغط من الشركات المضيفة فيما يتعلق بتقاريرها من خلال فحص تأثير عوامل جودة وظائف التدقيق الداخلي على قدرة المديرين التنفيذيين للتدقيق الداخلي على عدم التعديل في تقارير التدقيق الداخلي، وتوصلت الدراسة إلى النتائج عديدة من أهمها تقديم دليل على أن خبرة فرق و مدراء التدقيق الداخلي ومؤهلاتهم العلمية و شهاداتهم وتدريبهم وموضوعيتهم كانت جميعها مرتبطة بشكل كبير بمقاومة الضغط. وهدفت دراسة Laib (2021) إلى إلى تحديد أهمية الأمن السيبراني في القطاع المالي في عصر التحول الرقمي في ليبيا، من خلال الحصول على نظرة عامة على الأمن السيبراني حيث عمد الباحث إلى مراجعة محدد في الأدبيات المتخصصة، التشريعات الدولية ، وإجراء تحليل للهجمات التي تم الإبلاغ عنها في القطاع المالي على مدى السنوات الماضية عرض حتى أزمة كوفيد 19-، و بهدف تحديد جوانب واتجاهات الجرائم الإلكترونية و الهجمات السيبرانية، كانت من أهم نتائج الدراسة أن القراصنة الذين استطاعوا التسلل و اختراق الانظمة المعلوماتية بإستخدام الهجمات السيبرانية قد إختاروا الشركات المالية كوجهة لهم حيث أن بعض تلك الشركات المالية كانت تستخدم الأنظمة الرقمية التقليدية فكانت فريسة سهلة المنال.

3 - الطريقة والإجراءات

3 -1 منهج الدراسة

استند منهج الدراسة على الأسلوب الوصفي التحليلي في تحقيق أهدافها والإجابة عن أسئلتها وتحليل بياناتها وإختبار فرضياتها.

3-2 مجتمع وعينة الدراسة

يتكون مجتمع الدراسة من شركات التكنولوجيا المالية المعروفة بـFinTech)) العاملة في الأردن وفقاً لتعليمات البنك المركزي و عددها (18) شركة والتي تتوفر المعلومات الأساسية عنها في السجل العام للشركات المرخصة وفقاً لأحكام نظام الدفع والتحويل الإلكتروني للأموال رقم (111) لسنة (2017)، وتم إتباع استراتيجية المسح الشامل في تحديد العينة للدراسة، أما عينة الدراسة هي عبارة عن كامل شركات التكنولوجيا المالية في الاردن، كما أن وحدة المعاينة في الدراسة تكون من موظفي إدارة التدقيق الداخلي و الإدارة المالية وإدارة تكنولوجيا المعلومات العاملين في شركات التكنولوجيا المالية FinTech)) العاملة في الأردن.

3-3 وحدة التحليل المستهدفة

تم إجراء الدراسة على الأفراد «العاملين في شركات التكنولوجيا المالية، وتم توزيع (115) إستبيانة إلكترونية على أفراد عينة الدراسة أي بمعدل (6-7) استبانات في كل شركة من خلال إرسال الرابط عبر وسائل التواصل الاجتماعي، وبلغ عدد الاستبانات المستردة (107) إستبانة صالحة للتحليل الإحصائي.

4-3 مصادر جمع البيانات

استخدمت الدراسة المصادر النظرية والأدبية (الثانوية) لجمع البيانات والمعلومات لإعداد الجانب النظري وتحديد المتغيرات، كما استخدمت المصادر الأولية في إعداد الجانب العملي للدراسة والتي تمثلت في أداة الدراسة (الإستبانة)، حيث تهدف الاستبانة إلى استخلاص الردود والاتجهات حول الدراسه من الأفراد المعنيين في شركات التكنولوجيا المالية.

5-3 اختبار الموثوقية في أداة الدراسة

يقيس معامل ألفا كرونباخ (Cronbach Alpha Coefficient) درجة الموثوقية في المستخدمة في الدراسة من خلال تحديد درجة الترابط بين عناصرها. وتعتبر قيمة معامل ألفا كرونباخ التي تبلغ (0.70) وأكبر مؤشراً على ارتفاع الثبات العالي في أداة الدراسة، وبالتالي موثوقيتها وإمكانية استخدامها لإجراء عمليات التحليل الاحصائي. والجدول الآتي يوضح نتائج إختبار موثوقية أداة الدراسة:

الجدول (1): نتائج إختبار موثوقية أداة الدراسة

الرقم	المتغير	قيمة ألفا
1	أمن البيانات	0.846
2	أمن النظام	0.834
3	أمن الشبكة	0.832
4	الأمن التشغيلي	0.829
5	الأمن المادي	0.899
تأكيدات الأمن السيبراني		**0.910**
جودة التدقيق الداخلي التدقيق الداخلي		**0.909**

تشير قيم الجدول (1) إلى ارتفاع درجة الثبات والموثوقية في أداة الدراسة، حيث ظهرت جميع قيم ألفا كرونباخ أكبر من (0.70)، إذ بلغت أقل قيمة (0.829) وهي عند متغير الأمن التشغيلي و(0.910) كأعلى قيمة عند متغير تأكيد الأمن السيبراني.

6-3 الأساليب الإحصائية

تم تحليل بيانات الدراسة من خلال استخدام أدوات التحليل الإحصائي الملائمة، من خلال الاستعانة بالبرنامج الإحصائي (Statistical Package for Social Sciences- SPSS)، وتم استخدام الإختبارات الإحصائية الأتية:

«**الإحصاء الوصفي**: التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية»؛ لتقديم وصف شامل لدرجة موافقة أفراد عينة الدراسة على الفقرات المختلفة.

معامل الاتساق الداخلي - كرونباخ ألفا: لقياس ثبات أداة الدراسة.

معامل تضخم التباين والتباين المسموح بع لقياس درجة الارتباط بيـن المتـغيرات.

تحليل الانحدار الخطي المتعدد والمتدرج: لإختبار فرضيات الدراسة.

«الأهميـه النسبيـه تـم تحديـدها طبـقاً للـصيـغة التاليـه ووفـقـاً لمقـياس ليـكرت الخماسـي لبدائـل الاجابـة لكـل فقـرة»

$$\text{طول الفترة} = \frac{\text{الحد الأعلى للبديل} - \text{الحد الأدنى للبديل}}{\text{عدد المستويات}} = \frac{5 - 1}{3} = 1.33$$

حيث عدد المستويات هي: منخفض، متوسط، ومرتفع، وبذلك يكون:

المستوى المنخفض: الوسط الحسابي من 1 إلى أقل من 2.33

المستوى المتوسط: الوسط الحسابي من 2.33 إلى أقل من 3.66

المستوى المرتفع: الوسط الحسابي من 3.66 لغاية 5.00

4 - تحليل البيانات وإختبار الفـرضيات

4 - 1 وصف متغيرات الدراسة

يبيـن الجـدول (2) نتائـج وصـف متغيـرات الدراسـة باسـتخدام مقاييـس الاحـصـاء الوصـــفي،

الجدول (2): وصف متغيرات الدراسة

الرقم	المتغير	الوسط "الحسابي"	الانحراف "المعياري"	الترتيب	الأهمية "النسبية"
1	أمن البيانات	4.412	0.421	3	"مرتفعة"
2	أمن النظام	4.457	0.407	2	"مرتفعه"
3	أمن الشبكة	4.484	0.419	1	"مرتفعه"
4	الأمن التشغيلي	4.325	0.451	5	مرتفعة
5	الأمن المادي	4.351	0.429	4	مرتفعة
تأكيدات الأمن السيبراني		**4.405**	**0.351**	**-**	**مرتفعة**
جودة التدقيق الداخلي		**4.101**	**0.384**	**-**	**مرتفعة**

تشـير القيـم إلى إرتفـاع الأهميـة النسـبية لمتغيـر تأكيـدات الأمـن السـيبراني فـي شـركات تكنولوجيـا المعلومـات بوسـط حسـابي (4.405) وانحـراف معيـاري (0.351)، كمـا تبيـن ارتفـاع الأهميـة النسـبية لجميـع أبعـاد تأكيـدات الأمـن السـيبراني، وقـد جـاء ترتيبهـا علـى التوالـي: أمـن

الشبكات (4.484)، أمن النظام (4.457)، أمن البيانات (4.412)، الأمن المادي (4.351)، الأمن التشغيلي (4.325).

كما تشير القيم إلى إرتفاع الأهمية النسبيه لمتغير الدراسة من جودة التدقيق الداخلي بوسط حسابي (4.101) وانحراف معياري (0.384).

4 - 2 نتائج اختبار الفرضيات

4 - 2 - 1 نتائج إختبار الفرضيه الرئيسة H01

« لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية0.05 ≥P)) لتأكيدات الأمن السيبراني بأبعادها (أمن البيانات، أمن النظام، أمن الشبكة، الأمن التشغيلي، الأمن المادي) في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن».

الجدول (3): علاقة وأثر تأكيدات الأمن السيبراني في جودة التدقيق الداخلي

المتغير المستقل	المعاملات غير المعيارية		المعاملات المعيارية			درجات الارتباط الخطي	
	B	الخطأ المعياري	β	T	Sig. T	VIF	التباين المسموح به
أمن البيانات	0.191	0.041	0.189	4.659	0.000	1.916	0.522
أمن النظام	0.204	0.062	0.201	3.290	0.000	2.415	0.414
أمن الشبكة	0.216	0.051	0.205	4.235	0.000	2.115	0.473
الأمن التشغيلي	0.141	0.054	0.132	2.611	0.037	1.979	0.505
الأمن المادي	0.154	0.065	0.144	2.369	0.041	2.977	0.336
R	0.801						
R^2	0.642						
F	119.208						
Sig. F	0.000						

المتغير التابع: جودة التدقيق الداخلي

تشير قيم الجدول (3) إلى علاقة تأكيدات الأمن السيبراني وأثره في جودة التدقيق الداخلي في شركات التكنولوجيا المالية الأردنيه»، حيث تبين أن تأكيدات الأمن السيبراني يرتبط بعلاقة قوية وموجبة مع جودة التدقيق الداخلي (R=0.801)، وساهم في تفسير

(64.2%) من التغير في جودة التدقيق الداخلي (R2=0.642)، كما تبين أن تأثيره كان معنوياً في جودة التدقيق الداخلي (F=119.208, Sig.F=0.000). وبالاعتماد على ما سبق يتضح أنه: «يوجد أثر ذو دلالة إحصائية عند مستوى معنوية0.05 ≥P)) لتأكيدات الأمن السيبراني بأبعادها (أمن البيانات، أمن النظام، أمن الشبكة، الأمن التشغيلي، الأمن المادي) في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن».

ويتبين من الجدول (3) عدم وجود ارتباطات خطية عالية بين المتغيرات التفسيرية (المستقلة)، حيث ظهرت جميع قيم معامل تضخم التباين (VIF) أقل من (10)، وقيم معامل التباين المسموح به أقل من (1.0).

4-2-2 نتائج إختبار الفرضيات الفرعية

الفرضيه الفرعيه الأولى H01.1

« لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (P≤ 0.05) لأمن البيانات في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن. «.

يتبين من الجدول (3) أن أمن البيانات ترتبط بعلاقة موجبة مع جودة التدقيق الداخلي (B=0.191)، وأن أثرها كان معنوياً في جودة التدقيق الداخلي (T=4.659, Sig.T=0.000). وبالاعتماد على ما سبق يتضح أنه: «يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (P≤ 0.05) لأمن البيانات في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن «.

الفرضية الفرعية الثانية H01.2

«لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (P≤ 0.05) لأمن النظام في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن».

يتبين من الجدول (3) أن أمن النظام يرتبط بعلاقة موجبة مع جودة التدقيق الداخلي (B=0.204)، وأن أثره كان معنوياً في جودة التدقيق الداخلي (T=3.290, Sig.T=0.000). وبالاعتماد على ما سبق يتضح أنه: « يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (P≤ 0.05) لأمن النظام في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن «.

الفرضيه الفرعيه الثالثة H01.3

«لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (P≤ 0.05) لأمن الشبكة في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن «.

تبيّن من الجدول (3) أن أمن الشبكات ترتبط بعلاقة موجبة مع جودة التدقيق

الداخلي (B=0.216)، وأن أثرها كان معنوياً في جودة التدقيق الداخلي (T=4.235, Sig.T=0.000). وبالاعتماد على ما سبق يتضح أنه: «يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (P≤ 0.05) لأمن الشبكة في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن».

الفرضيه الفرعيه الرابعه H01.4

«لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (P≤ 0.05) للأمن التشغيلي في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن».

يتبين من الجدول (3) أن أمن التشغيلي يرتبط بعلاقة موجبة مع جودة التدقيق الداخلي (B=0.141)، وأن أثره كان معنوياً في جودة التدقيق الداخلي (T=2.611, Sig.T=0.037). وبالاعتماد على ما سبق يتضح أنه: «يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (P≤ 0.05) للأمن التشغيلي في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن».

الفرضية الفرعية الخامسة H01.5

«لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (P≤ 0.05) للأمن المادي في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن»

يتبين من الجدول (3) أن الأمن المادي يرتبط بعلاقة موجبة مع جودة التدقيق الداخلي (B=0.154)، وأن أثره كان معنوياً في جودة التدقيق الداخلي (T=2.977, Sig.T=0.041). وبالاعتماد على ما سبق يتضح أنه: « يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (P≤ 0.05) للأمن المادي في جودة التدقيق الداخلي في شركات التكنولوجيا المالية FinTech في الأردن».

ولترتيب أثر أبعاد تأكيدات الأمن السيبراني في جودة التدقيق الداخلي تم استخدام تحليل الإنحدار المتدرج.

الجدول (4): ترتيب أثر أبعاد تأكيدات الأمن السيبراني في جودة التدقيق الداخلي

النموذج	تأكيدات الأمن السيبراني	B	T	Sig. T	R2	F	Sig. F
الأول	أمن البيانات	0.821	15.731	0.000	0.509	268.243	0.000
الثاني	أمن الشبكات	0.411	7.841	0.000	0.581	188.984	0.000
الثالث	أمن النظام	0.351	4.636	0.000	0.612	159.207	0.000
الرابع	الأمن التشغيلي	0.195	2.574	0.037	0.641	121.113	0.000
الخامس	الامن المادي	0.154	2.574	0.041	0.642	119.208	0.000

تشير قيم الجدول (4) إلى أن (أمن البيانات) يعد الأكثر تأثيراً في جودة التدقيق الداخلي، حيث ساهم في تفسير (50.9%) من التغير في جودة التدقيق الداخلي (R2=0.509)، وبدخول متغير (أمن الشبكات) لنموذج الانحدار ازداد نسبة التفسير بمقدار (7.2%) (R2=0.581)، وأدى دخول متغير (امن النظام) لنموذج الانحدار المتضمن (أمن البيانات، أمن الشبكات) إلى زيادة نسبة التفسير بمقدار (3.1%) (R2=0.612)، وعند دخول متغير (الأمن التشغيلي) لنموذج الانحدار الذي يضم الأبعاد الثلاث السابقة مجتمعة ازدادات نسبة التفسير بمقدار (2.9%) (R2=0.641)، وبدخول متغير (الأمن المادي) لنموذج الإنحدار السابق ازدادت نسبة التفسير بمقدار (0.1%) (R2=0.642).

5 - النتائج والتوصيات

5 - 1 النتائج

أشارت مخرجات التحليل واختبار الفرضيات إلى النتائج الآتية:

1 - ارتفاع مستوى الأهمية النسبية لتأكيدات الأمن السيبراني وأبعاده (أمن البيانات، أمن النظام، أمن الشبكة، الأمن التشغيلي، الأمن المادي) في شركات التكنولوجيا المالية. وهذا يشير إلى اهتمام هذه الشركات بالتكنولوجيا الحديثة وتطوير تقنياتها والاستعداد للمخاطر السيبرانية من خلال استخدام أمن البيانات، أمن النظام، أمن الشبكة، الأمن التشغيلي، الأمن المادي لتحسين الأمن على جميع الهجماتوبالتالي تعزيز تنافسيتها في السوق. حيث توافقت هذه النتيجة مع دراسة عبدالقادر، وآخرون (2023) ودراسة الحوامدة (2021) من حيث ارتفاع الاهمية النسبية، إلا أنها تعارضت مع دراسة جمال الدين (2023).

2 - ارتفاع مستوى الأهمية النسبيّه لجودة التدقيق الداخلي في شّركات التكنولوجيا المالية. وهذا يدل على زيادة مستوى الوعي والإدراك لدى هذه الشركات فيما يتعلق بتحقيق الجودة والدقة في العمليات التشغيلية والمالية، واتخاذ التدابير الضرورية لتعزيز الثقة وتحسين الأداء، بالإضافة إلى تعزيز مستوى الشفافية والإفصاح، كما يعملون على تعزيز جودة التدقيق الداخلي وتحسين عمليات المراقبة والتدقيق بهدف ضمان الامتثال للسياسات والإجراءات، وتقليل المخاطر المحتملة. حيث توافقت هذه النتيجة مع دراسة Usman, et al., 2023) من حيث ارتفاع الأهمية النسبية لجودة التدقيق الداخلي

3 - وجود أثر دال إحصائياً لتأكيدات الأمن السيبراني في جودة التدقيق الداخلي في شركات التكنولوجيا المالية الأردنية. وهذا يشير إلى دور الأمن السيبراني في تحسين الأمن والموثوقية في العمليات التشغيلية والحفاظ على البيانات والمعلومات والأنظمة، والشبكات، والأمن المادي. حيث توافقت مع دراسة Jadhav 2023) من حيث تدقيق الأمن السيبراني تساعد في ضمان تدقيق كامل ومتعمق للمواقف الأمنية للمنظمة، كما تساعد في الكشف عن المخاطر والثغرات والتهديدات التي تواجهها المنظمة،

ودراسة (Lindvall, 2022) من حيث أثر المدققين الداخليين للتأكيد بشكل كبير على الأمن السيبراني للمؤسسات، حيث يمكنهم تعزيز ممارسة الأمن السيبراني

4 - وجود أثر دال إحصائياً لأمن البيانات، أمن النظام، أمن الشبكة، الأمن التشغيلي، الأمن المادي في جودة التدقيق الداخلي في شّركات التكنولوجيا المالية الأردنية. وهذا يشير إلى أهمية ودور هذا الأمن في تحسين الكفاءة والفعالية في الحفاظ وأمن تشغيل الأنظمة والمحافظة على البيانات والمعلومات والشبكات

5 - يعتبر أمن البيانات من أهم تأكيدات الأمن السيبراني تأثيراً في جودة التدقيق الداخلي في شركات التكنولوجيا المالية في الأردن، وهذا قد يعود لدوها في التركيز على مراكز الخصوصية في أمن البيانات الفردية، وقيام الشركات بكشف الانتهاكات وتحديد أي تجاوزات، ومن ثم إجراء التعديلات الضرورية لمعالجة هذه الانتهاكات، بالإضافة إلى ذلك قد يعود السبب في منع سوء استخدام البيانات الفردية والحفاظ على سرية وأمان هذه البيانات.

2-5 التوصيات

بناءً على النتائج السابقة، يقترح البحث التوصيات الآتية :

1 - زيادة استثمار شركات التكنولوجيا المالية الأردنية في البنية التحتية التكنولوجية (الأمن المادي) لدعم الأمن السيبراني وتوفير البنية التحتية الضرورية وتطويرها لتحسين كفاءتها وتقليل من الاختراقات.

2 - توفير تدريب مستمر للموظفين حول مخاطر الأمن السيبراني وكيفية التعرف على الهجمات السيبرانية والتعامل معها

3 - تأكد من تحديث البرامج والأنظمة بانتظام لسد الثغرات الأمنية والحفاظ على النظام آمنًا

4 - تحديد صلاحيات الوصول بحيث يتم منح الوصول فقط للأشخاص الذين يحتاجونه لأداء مهامهم اليومية.

5 - وضع خطة استجابة للحوادث الأمنية وتوفير إجراءات للتعامل مع الهجمات والانتهاكات على الفور، بالإضافة إلى تحليل ومراقبة السجلات للكشف عن أنماط الهجمات المحتملة

6 - تقييم المخاطر الأمنية المحتملة التي قد تواجهها المؤسسة وتصنيفها حسب الأولوية، وهذا يتضمن تحليل الضعف في الأنظمة والعمليات وتقييم التهديدات المحتملة.

المراجع

المراجع العربية

إبراهيم، عمار غازي، وحمادي، صالح مهدي، وخلف، أمينة إبراهيم .(2019). دور استقلالية التدقيق الداخلي على تطبيق قواعد الحوكمة وأثره في جودة المعلومات المحاسبية دراسة تطبيقية في جامعة ديالى. مجلة كلية الإدارة والاقتصاد للدراسات الاقتصادية والإدارية والمالية، 11(4)، 852-882.

البنك المركزي الأردني (15 آذار 2024). الصفحة الرئيسية ، قائمة التشريعات - التعليمات - تعليمات التكيف مع المخاطر السيبرانية رقم (1984/1/1/26) بتاريخ 6/شباط/2018، زيارة @ 11:33. https://www.cbj.gov.jo/EchoBusV3.0/SystemAssets/c78cf52b-2183-9a32-a7f6c5937c3e.pdf-4144

التوني، شريهان مصطفى محمد (2023). أثر وعي العملاء بالقرصنة الإلكترونية كأداة لتحقيق الأمن السيبراني: دراسة ميدانية على البنوك الحكومية بمحافظة بورسعيد. مجلة التجارة والتمويل، (4)، 609-653.

جمال الدين، هبة (2023). الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد و العلوم السياسية، 7 (24)، 189-230. https://dx.doi.org/10.21608/jpsa.2023.279877

حمود، مريم ، إبراهيم، الحسن ، وعلي، هديل (2019). أهمية التدقيق الداخلي على جودة المعلومات المحاسبية في القوائم المالية: دراسة حالة في مصرف الرافدين المركزي/ بغداد. مجلة الكوت للعلوم الإدارية الاقتصادية، 1(34)، 30-47.

الحوامده، أحمد موسى (2021). أثر الحوكمة السيبرانية على جودة التدقيق الداخلي في البنوك التجارية الأردنية. (رسالة ماجستير غير منشورة) جامعة جرش، جرش، الأردن.

الدوسري، أحمد يعقوب يوسق عبدالله شحادته، محمد موسى علي وعلي، شريف محمد (2022). دراسة تحليلية لمحددات جودة التدقيق الداخلي في ظل عمليات الرقمنة وفقا لمعايير المنظمة والتجارب الدولية. المجلة العلمية للدراسات والبحوث المالية والإدارية، 13 (2)، 663-683.

الدويري، فراد عقيل علي والحواجرة، كامل محمد يوسف (2023). دور خصائص البيانات الضخمة في الحد من الجرائم الإلكترونية من خلال استراتيجية الأمن السيبراني في جهاز الأمن العام الأردني [أطروحة دكتواره غير منشورة]. جامعة مؤته، مؤته، الأردن.

ذنيبات، علي (2021). تدقيق الحسابات في ضوء المعايير الدولية - نظرية وتطبيق

(ط7). دار وائل.

السمحان، منى عبدالله (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الادارية بجامعة الملك سعود. مجلة كلية التربية، (111)، 1-29.

عبدالقادر، صواق، بوندين، بوداود، عبداللطيف، حيمودة (2023) أثر جاهزية الأمن السيبراني على الخدمات المصرفية الإلكترونية من خلال تقليل المخاطر المدركة دراسة حالة بنك BDL بغرداية. مجلة أبحاث اقتصادية معاصرة، 6، (1)، 353-372.

ابو الخير، محمد حارس محمد طه (2023). أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الاستقرار المالي في البنوك الالكترونية: دراسة ميدانية. المجلة العلمية للدراسات والبحوث المالية والادارية، 15 (1)، 1-71.

أميرهم، جيهان عادل (2022). أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وانعكاساته على ترشيد قرارات المستثمرين، دراسة ميدانية، مجلة البحوث المالية والتجارية، العدد3.

علي، شريف ، الدوسري موسى و عبدالله، أحمد. (2022). دراسة تحليلية لمحددات جودة التدقيق الداخلي في ظل عمليات الرقمنة وفقاً للمعايير المنظمة و التجارب الدولية. المجلة العلمية للدراسات والبحوث المالية والإدارية662 ،(2)13 ،-683.

قواقزة، يوسف (2022). أثر التدقيق الداخلي على إدارة المخاطر. المجلة العربية للنشر العلمي، 5(50)، 1395-1406.

كشاط، منى، وتيجاني، بالرقي (2017). الادوار الحديثة للتدقيق الداخلي على ضوء مستجدات الاطار المرجعي الدولي للممارسات المهنية. مجلة رؤى اقتصادية، 7(2)، 319-335، جامعة الشهيد حمة لخضر، الجزائر.

الهلسة، تامر (2021). أثر مقومات الأمن السيبراني في خصائص المعلومات المحاسبية: الدور المعدل COBIT 2019: دراسة ميدانية في البنوك التجارية الأردنية [أطروحة دكتواره غير منشورة] .جامعة العلوم الإسلامية العالمية، عمان.

الهيئة الوطنية للأمن السيبراني (2023). نبذة عن الهيئة الوطنية للأمن السيبراني. بتاريخ 13 آذار 2024 زيارة @ 2:40 pm. https://nca.gov.sa/about

المراجع الاجنبية

Types of cybersecurity (2018, May 9). Mindcore Technologies. https://mind-core.com/blogs/sybersecurity/5-types-of-cyber-security/

AL Fayi, S. (2022). Internal audit quality and resistance to pressure, Journal of Money and Business, 2 (1), 5769-. DOI 10.1108/JMB-110053-2021-

Alkhamees, S. B., & Durugbo, C. M. (2024). Organisational ambidexterity and innovation: A systematic review and unified model of "CODEC" management priorities. Management Review Quarterly, 75(2).

Al Qassaymeh, M., & Al-Barashdi, S. (2024). Role of Option of Sight (Khayar Al-Ro'ya) in Protecting the Buyer in International Sale Contract. International journal for scientific research.

Al-Gasaymeh, A., Qasaimeh, G. M., Alrawashdeh, N., Alsmadi, A. A., & Alzoubi, H. M. (2023). The Impact of Cobit 5 On the Effectiveness of Applying Governance Tools in Jordanian Commercial Banks. Calitatea, 24(194), 377.384-

Al-Naimi, A. A., Al Abed, S., Farooq, U., Qasaimeh, G., & Alnaimat, M. A. (2023, March). Impact of open banking strategy and fintech on digital transformation. In 2023 International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 15-). IEEE.

Al-Own, B., Saidat, Z., Kasem, J., & Qasaimeh, G. (2023, March). Impact of Digital Payment Systems and Blockchain on Economic Growth. In 2023 International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 15-). IEEE.

Al-Qassaymeh, M. M. A. S. (2020). Delivery of Electronic Products in Electronic Sale Contracts Under Jordanian Law: An Overall Comment. Business Law Review, 41(6).

Bunjaku, F. (2019). Audit components: literature review on audit plan, risk and materiality and internal control. Journal of Economics, 4(1), 3643-.

Center for Development of Security Excellence (CDSE) (2017). Introduction to Physical Security. Student Guide.

Evans, M., Maglaras, L., He, Y. & Janicke H. (2016). Human behaviour as an aspect of cybersecurity assurance, Security and Communication Network, 9, 4667-4679. DOI: 10.1002/sec.1657

Gyorffy, K., Leitold, F., & Arrott, A. (2017). Individual awareness of cyber-security vulnerability- Citizen and Public servant. Central and eastern European e-dem and e-gov days, 325, 411421-. DOI https://doi.org/10.24989/ocg.v325.34

Hu, T., Wang, K., Chih, W. & Yang, X. (2018). Trade-off cybersecurity concerns for co-created value. Journal of Computer Information Systems, https://doi.org/10.1080088/74417.2018.1538708

Jadhav, K. (2023). The role of cyber security audits in managing company systems and applications, Organization: Tech Mahindra Americas Bedminster, NJ, USA .17-.

Kahyaoglu,S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective, Managerial Auditing Journal, 33(4), 360376-. https://doi.org/10.1108/MAJ-021804-2018-

Laib, S. (2021), The importance of cyber security in the financial sector in the age of digital transformation, Journal for Economic and Administrative Research, 5 (1), 448-464.

Qasaimeh, Ghazi M & Jaradeh, Hussam Eddin. (2022). The impact of artificial intelligence on the effective applying of cyber governance in jordanian commercial banks. International Journal of Technology, Innovation and Management (IJTIM), 2(1).

Reid, K (2021). What are the different types of cyber security? (2021, August 12). https://triadanet.com/blog/different-types-of-syber-security/

Saidat, Z., Abdelrahim, H. J., Alkhodary, D. A., & Qasaimeh, G. (2023, March). Impact of open big data and insurtech on business digitalization. In 2023 International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 15-). IEEE.

San, Juan N. (2021, October 13). What is cybersecurity. Vpn Pro. https://vpnpro.com/web/what-is-cyber-security/

Tawfiq, M., & Abdullah, H. (2023). Financial technology and its role in achieving economic development in the Hashemite Kingdom of Jordan, American Journal of Sociology, Economics and Tourism 3, 1- 8.

Usman, Alih, Che-Ahmad, Ayoib, Abdulmalik, Salau Olarinoye. (2023). The Role of Internal Auditors Characteristics in Cybersecurity Risk Assessment in Financial-Based Business Organisations: A Conceptual Review. Intern. Journal of Profess. Bus. Review, 8 (8), p. 0131-