أثر محددات جودة وظيفة المراجعة الداخلية وهيكل الحوكمة السيبراني على مؤشرات إدارة مخاطر الأمن السيبراني: استخدام نماذج المعادلات الهيكلية القائمة على المربعات الصغرى (PLS-SEM)

د/ محمد عبد المنعم سراج

مدرس بقسم المحاسبة – أكاديمية السادات للعلوم الإدارية

mohserag1970@yahoo.com

ملخص البحث

يهدف هذا البحث إلى تحليل أثر محددات جودة وظيفة المراجعة الداخلية وهيكل الحوكمة السيبراني على تحسين مؤشرات إدارة مخاطر الأمن السيبراني في المنشآت، وذلك في ظل تزايد التهديدات السيبرانية وتعقيداتها. وتكمن أهمية هذا البحث في سعيه إلى تقديم إطار نظري وتطبيقي يدعم المنشآت في التصدي للتهديدات السيبرانية، وذلك من خلال تعزيز جودة المراجعة الداخلية وتفعيل هيكل حوكمة فعّال للأمن السيبراني، بما يسهم في رفع كفاءة أنظمة الرقابة وتحقيق مستويات أعلى من الأمان المعلوماتي.

تتمثل أهداف البحث في: (1) اختبار تأثير محددات جودة وظيفة المراجعة الداخلية من منظور مدخلات العمل (الكفاءة المهنية، التدريب، الاستقلالية)؛ (2) تحليل تأثير هيكل الحوكمة السيبرانية القائم على نموذج خطوط المساءلة الخمس (LoA5)؛ (3) دراسة الأثر التفاعلي المشترك بينهما على مؤشرات إدارة مخاطر الأمن السيبراني عبر مراحلها المختلفة (الوقاية، والاكتشاف، والاستجابة، والعلاج).

يعتمد البحث على منهجية كمية باستخدام نماذج المعادلات الهيكلية القائمة على المربعات الصغرى (PLS-SEM)، وتحليل بيانات ميدانية من منشآت مصرية تعمل في قطاعات ذات حساسية مرتفعة للمخاطر السيبرانية. كما يستند البحث إلى إطار نظري مستمد من أدبيات المراجعة الداخلية وحوكمة الأمن السيبراني، مع التركيز على نموذج "خطوط المساءلة الخمس (LoA5)"، والذي يدمج أدوار مجلس الإدارة، والإدارة التنفيذية، وتكنولوجيا المعلومات، وأمن المعلومات، والمراجعة الداخلية في إدارة الأمن السيبراني.

توصلت نتائج البحث إلى أن جودة وظيفة المراجعة الداخلية – لاسيما الكفاءة المهنية والاستقلالية – تؤثر إيجابيًا وبشكل ملموس على تحسين قدرة المنشآت على إدارة مخاطر الأمن السيبراني. كما تبين أن وجود هيكل حوكمة سيبراني قائم على نموذج خطوط المساءلة الخمس (LoA5) يساهم في تعزيز التكامل بين الوحدات التنظيمية، مما يرفع فعالية الوقاية من الهجمات والاستجابة لها. علاوة على ذلك، أثبت البحث أن التعاون والتفاعل بين جودة وظيفة المراجعة الداخلية وهيكل الحوكمة السيبراني يحقق أثرًا تراكميًا يُعزز من نضج إدارة المخاطر ويحد من آثار الحوادث السيبرانية.

خلص البحث إلى ضرورة الاستثمار في تطوير كفاءات المراجعين الداخليين وتوسيع نطاق استقلاليتهم، بالتوازي مع تبني نموذج حوكمة شامل يضمن المشاركة الفعالة لجميع الأطراف ذات العلاقة بالأمن السيبراني. كما أوصى البحث بتطبيق مؤشرات قياس محددة لنضج إدارة المخاطر، وتبني أطر تنظيمية مهنية كمرجع في تصميم عمليات الرقابة والمساءلة السيبرانية.

يسهم هذا البحث في سد فجوة بحثية قائمة في الأدبيات المحاسبية حول العلاقة التفاعلية بين المراجعة الداخلية والحوكمة السيبرانية، ويفتح آفاقًا مستقبلية لأبحاث تركز على تطبيق هذا النموذج في بيئات تنظيمية مختلفة، مع إمكانية تطوير نماذج تقييم للأداء الأمني مبنية على مؤشرات كمية ومعايير مهنية.

الكلمات المفتاحية: جودة وظيفة المراجعة الداخلية؛ الكفاءة المهنية؛ الاستقلالية؛ هيكل الحوكمة السيبراني؛ نموذج خطوط المساءلة الخمس (LoA5)؛ إدارة مخاطر الأمن السيبراني؛ نماذج المعادلات الهيكلية (SEM)

[1] تقديم البحث في 2025/7/27 وقبول نشره في 2025/8/6

The Impact of Internal Audit Function Quality Determinants and Cybersecurity Governance Structure on Cybersecurity Risk Management Indicators: Using Partial Least Squares Structural Equation Modeling (PLS-SEM)

Abstract

This research aims to analyze the impact of internal audit function quality determinants and the structure of cybersecurity governance on the enhancement of cybersecurity risk management indicators within organizations, especially amid the growing complexity and severity of cyber threats. The significance of this research lies in its attempt to provide both a practical and academic framework that supports organizations in mitigating such risks by strengthening internal audit quality and activating an effective cybersecurity governance structure.

The research has three main objectives: (1) to examine the effect of internal audit quality determinants from an input-based perspective (e.g., professional competence, training, and independence); (2) to analyze the effect of a cybersecurity governance structure based on the Five Lines of Accountability (5LoA) model; and (3) to investigate the joint interactive effect of both on cybersecurity risk management indicators across its various stages (prevention, detection, response, and recovery).

A quantitative methodology was employed using Partial Least Squares Structural Equation Modeling (PLS-SEM) and based on field data collected from Egyptian firms operating in sectors highly sensitive to cybersecurity risks. The theoretical framework of the research is grounded in the literature on internal auditing and cybersecurity governance, with a particular emphasis on the Five Lines of Accountability (5LoA) model. This model integrates the roles of the board of directors, executive management, IT, information security, and internal audit in the effective management of cyber risks.

The results revealed that internal audit function quality—especially professional competence and independence—has a significant positive impact on enhancing organizations' capabilities to manage cyber risks. Additionally, having a cybersecurity governance structure based on the 5LoA model contributes to improved coordination among organizational units, thereby increasing the effectiveness of both prevention and incident response. Moreover, the research demonstrated that the interaction between audit quality and cybersecurity governance creates a cumulative effect that boosts risk management maturity and reduces the consequences of cyber incidents.

The research concludes with a recommendation to invest in developing internal auditors' technical competencies and to broaden their operational independence, alongside adopting an inclusive governance model that ensures the active participation of all relevant stakeholders in cybersecurity. It also advises the application of specific performance indicators to measure cybersecurity risk management maturity and the use of professional frameworks as reference points in designing control and accountability structures.

This research addresses a notable gap in accounting literature concerning the interactive relationship between internal auditing and cybersecurity governance and opens future avenues for research applying this model in different organizational contexts, with the potential to develop quantifiable performance-based evaluation frameworks.

Keywords: Internal Audit Quality; Professional Competence; Independence; Cybersecurity Governance Structure; 5LoA Model; Cybersecurity Risk Management; Structural Equation Modeling (SEM)

1- المقدمة

في العصر الرقمي الحالي، أصبحت المنشآت تواجه مجموعة متنوعة من التهديدات الإلكترونية التي تمثل مخاطر متزايدة على أمنها السيبراني واستمرارية أعمالها. ومع تطور التقنيات الرقمية وتكاملها المتزايد في العمليات اليومية للمنشآت، أصبحت الهجمات السيبرانية أحد أكبر المخاطر التي تهدد المنشآت حول العالم (المجلس الأعلى للأمن السيبراني،2017). هذه الهجمات لا تؤثر فقط على البيانات والمعلومات الحساسة، بل تؤثر أيضًا على سمعة المنشآت وثقة عملائها ومساهميها، مما يؤدي إلى خسائر مادية ومعنوية قد تكون كارثية (شحاته،2022). ووفقًا لتقرير المنتدى الاقتصادي العالمي (2024)، تُعد الهجمات السيبرانية واحدة من أخطر التهديدات الاقتصادية والاجتماعية التي تواجه العالم اليوم، حيث أشار التقرير إلى أن الخروقات الأمنية والتسريبات المعلوماتية قد تكبد المنشآت خسائر كبيرة وتعطل سير أعمالها بشكل غير مسبوق (World Economic Forum, 2024).

في هذا السياق، برزت الحاجة إلى تبني هيكل فعال لحوكمة الأمن السيبراني، وذلك لضمان حماية البيانات وتأمين الأنظمة المعلوماتية وتعزيز القدرات الدفاعية للمنشآت. وتُعد حوكمة الأمن السيبراني جزءاً من الحوكمة العامة للمنشآت، وتهدف إلى وضع استراتيجيات وسياسات وإجراءات تضمن تحقيق الأهداف الأمنية والحد من التهديدات. علاوة على ذلك، تسهم حوكمة الأمن السيبراني في تعزيز الالتزام التنظيمي وتحسين مراقبة المخاطر وضمان تنفيذ السياسات الأمنية بفعالية. من جانب أخر تلعب جودة وظيفة المراجعة الداخلية دورًا حيويًا في دعم حوكمة الأمن السيبراني، حيث توفر إطارًا يتيح تقييم كفاءة أنظمة الرقابة الأمنية ويساعد في الكشف عن نقاط الضعف وتقديم التوصيات اللازمة لمعالجتها.

يستند هذا البحث إلى أهمية تكامل محددات جودة وظيفة المراجعة الداخلية وهيكل الحوكمة السيبراني كوسيلة لتقليل المخاطر السيبرانية. وفي هذا الإطار، يهدف البحث إلى اختبار تأثير محددات جودة وظيفة المراجعة الداخلية بناء على منهج المدخلات وهيكل الحوكمة السيبراني على تحسين العوائد الأمنية وتقليل المخاطر السيبرانية. وفي سبيل تحقيق ذلك، يعتمد البحث على تحليل تأثير كل من العوامل التي تسهم في رفع جودة وظيفة المراجعة الداخلية من منظور المدخلات، وفعالية أداء خطوط المساءلة (هيكل الحوكمة السيبراني)، والتعاون بينهم، وذلك على مؤشرات إدارة مخاطر الأمن السيبراني عبر المراحل المختلفة المتمثلة في الوقاية، والاكتشاف، والاستجابة، والعلاج/التصحيح.

2-مشكلة البحث

يشير الأمن السيبراني إلى قدرة المنشأة على حماية الأنظمة الرقمية أو الأصول المرتبطة بها من التهديدات الخارجية والداخلية. ويُعرف بأنه "تنظيم وجمع الموارد والعمليات والهياكل المستخدمة لحماية الفضاء السيبراني والأنظمة الممكّنة من الفضاء السيبراني من الحوادث التي تتعارض مع حقوق الملكية القانونية المعترف بها(Craigen et al., 2014, p.17)". وغالبًا ما يرتبط الأمن السيبراني بإدارة مخاطر السرية والنزاهة وتوافر الأنظمة أو الخدمات الرقمية (Cains et al., 2022).

وقد أصبحت أهمية إدارة مخاطر الأمن السيبراني أكثر إلحاحًا مع تزايد الاعتماد على الخدمات الرقمية عبر الإنترنت للعديد من المنشآت(Guthrie et al., 2021). ويواكب ذلك مع التطور المتزايد في التهديدات التي تؤثر على سرية الأنظمة ونزاهتها وتوافرها(Pienta et al., 2020)، مما يترتب عليه تأثير مباشر على العملاء والمساهمين وأصحاب المصلحة الآخرين (Li et al., 2019؛ علي وعلي، 2022).

وتشير الدلائل العملية في المنشآت التي تعرضت إلى هجمات سيبرانية إلى أن ضعف الحوكمة السيبرانية وعدم كفاءة وظيفة المراجعة الداخلية قد يؤديان إلى زيادة المخاطر السيبرانية وتعريض المنشآت لخسائر كبيرة. فعلى سبيل المثال، تعرضت شركة Equifax، وهي إحدى أكبر شركات المعلومات الائتمانية في العالم، لهجوم سيبراني كبير في عام 2017 أدى إلى تسريب بيانات شخصية لما يقرب من 147 مليون عميل. وكشفت التحقيقات أن هذا الاختراق نجم عن غياب الضوابط الكافية وعدم كفاءة الحوكمة السيبرانية، حيث لم تتمكن الشركة من مراقبة الثغرات الأمنية بفعالية، ولم يتم تحديث الأنظمة بما يتناسب مع المخاطر المحتملة، ما أدى إلى تداعيات مالية جسيمة وضرر كبير بسمعتها (Romanosky, 2018). كما تشير دراسة أجرتها Deloitte (2017) إلى أن حوالي نصف المنشآت التي تعرضت لهجمات سيبرانية تفتقر إلى أنظمة حوكمة سيبرانية قوية، وأن العديد من هذه المنشآت لم تكن تعتمد على آليات رقابية منتظمة لمراقبة التهديدات السيبرانية. وتظهر هذه الدلائل العملية كيف أن ضعف الحوكمة يمكن أن يؤدي إلى مخاطر عالية، خاصة مع ازدياد تعقيد الهجمات وعدم القدرة على التنبؤ بها.

وتشير دراسة D'Arcy and Herath (2009) إلى أن ضعف الحوكمة في مجال الأمن السيبراني قد يؤدي إلى تفاقم تأثير المخاطر السيبرانية، وأن تطبيق آليات حوكمة قوية قد يعزز من قدرة المنشآت على الاستجابة بشكل استباقي للتهديدات. كما توضح دراسة Cavusoglu et al. (2004) أن المنشآت التي تعتمد على آليات حوكمة قوية للأمن السيبراني تتمتع بقدرة أكبر على إدارة المخاطر وتجنب التهديدات، وأن ضعف هذه الحوكمة قد يؤدي إلى خسائر مالية جسيمة.

وتشير الأدلة الوصفية إلى أن أكثر من 60% من المنشآت تُسند المسؤولية عن الأمن السيبراني إلى قسم تكنولوجيا المعلومات(ACCA and CAANZ, 2019). بينما تعتبر حوالي ثلث المنشآت الكبيرة فقط أن إدارة المخاطر السيبرانية، مسؤولية تدخل ضمن نطاق مناصب الإدارة التنفيذية. علاوة على ذلك، فأن الأدلة الوصفية أوضحت أن 59% من المنشآت إن العلاقة بين الأمن السيبراني والمجالات المختلفة في المنشاة تعتبر في أفضل الأحوال محايدة، وغالبًا متوترة أو غير موجودة، و60% من المنشآت ليس لديها متخصص في الأمن السيبراني ضمن مجلس الإدارة أو المستوى التنفيذي(EY and IIA, 2021).

بالإضافة إلى ذلك، ففي بعض المنشآت، قد تؤدي الصراعات بين الوحدات المختلفة إلى تعقيد الجهود المشتركة وتطوير ممارسات عمل منفصلة، وتُعرف هذه الظاهرة بـ "الصومعة الذهنية"، حيث تعمل كل إدارة أو وحدة بشكل منعزل. وتدعو هذه الظروف إلى دور فعّال للإدارة العليا في تعزيز ثقافة أمنية شاملة، بحيث يُتاح لجميع الإدارات والوحدات ذات المسؤوليات المشتركة في الأمن السيبراني العمل بتناغم لتحقيق أهداف الحماية الأمنية للمنشأة(ISACA, 2011). ولذلك، يُعد وجود هيكل حوكمة قوي وفعال أمرًا حيويًا لتجاوز هذه التحديات وضمان التكامل بين مختلف فرق العمل في إدارة الأمن السيبراني .Love et al) (2010.

وقد أوضحت الدراسات أن أحد التحديات التي تواجه المنشآت في تطبيق هيكل فعال لحوكمة الأمن السيبراني هو نقص الكفاءات التقنية المتخصصة في مجال المراجعة الداخلية حيث يمثل عائقًا أمام تطوير القدرات الرقابية للمنشاة. إذ أن عمليات المراجعة الداخلية تتطلب مستوى عاليًا من المعرفة التقنية لتحليل التهديدات وتقييم الضوابط الأمنية، إلا أن العديد من المنشآت تعتمد على فرق مراجعة داخلية تفتقر إلى هذه الخبرات التخصصية. ونتيجة لذلك، فإن هذه الفرق قد تفشل في كشف الثغرات الأمنية أو تقديم توصيات فعالة للتعامل معها (Haislip et al., 2021؛ أميرهم،2022)، وهو ما يؤثر على القيمة المضافة التي تقدمها وظيفة المراجعة الداخلية من خلال الاستقلالية التي تمكنها من تقديم تقييم موضوعي للضوابط الأمنية، بعيداً عن التحيزات المحتملة في فرق تكنولوجيا المعلومات (راضي،2014؛ يوسف، 2024).

وفي هذا الإطار، تركز الأدبيات الحديثة على أهمية جودة وظيفة المراجعة الداخلية كوسيلة لتعزيز قدرة المنشآت على التصدي للتهديدات السيبرانية (شحاته،2022). وفقًا لدراسة Steinbart et al. (2018) فإن جودة وظيفة المراجعة الداخلية تُعتبر أحد العوامل الرئيسية التي تسهم في الكشف المبكر عن الثغرات الأمنية وتحسين فعالية الضوابط الأمنية، حيث أن المراجعين الداخليين المؤهلين مهنياً وأكاديمياً والمدربين بشكل جيد يستطيعون تقديم تقييمات دقيقة وموثوقة لمستويات الأمن السيبراني، مما يسهم في تحسين استجابة المنشآت للتهديدات.

في ضوء ذلك، تظهر الأدبيات والدلائل العملية أن المنشآت التي لا تعتمد علي هيكل حوكمة سيبراني فعال، ولا تركز على تعزيز جودة وظيفة المراجعة الداخلية تكون أكثر عرضه للتهديدات السيبرانية. إن التركيز على هذه المشكلة يبرز الحاجة إلى فهم العلاقة التفاعلية بين جودة وظيفة المراجعة الداخلية وهيكل الحوكمة السيبراني، وكيف يمكن أن يساهم هذا التفاعل في تحسين مؤشرات إدارة مخاطر الأمن السيبراني. ويركز البحث على سد هذه الفجوة البحثية من خلال تقديم أدلة عملية على كل من:

- أثر محددات جودة وظيفة المراجعة الداخلية علي تحسين مؤشرات إدارة مخاطر الأمن السيبراني.
- أثر وجود هيكل حوكمة سيبراني مستند إلى أحد أطر الأمن السيبرانية المهنية علي تحسين مؤشرات إدارة مخاطر الأمن السيبراني، بالمقارنة بالمنشآت التي تفتقر إلي هيكل واضح للحوكمة السيبراني.
- أثر المشاركة الفعالة للإدارة التنفيذية في مجلس الإدارة على تحسين مؤشرات إدارة مخاطر الأمن السيبراني.
- أثر التفاعل بين محددات جودة وظيفة المراجعة الداخلية، وتطبيق هيكل المساءلة المتكامل لحوكمة الأمن السيبراني على تحسين مؤشرات إدارة مخاطر الأمن السيبراني.

وعلى ذلك، فأن هذا البحث يمكن أن يسهم في تطوير نظرية ناشئة تصف تأثير محددات جودة وظيفة المراجعة الداخلية، وهيكل المساءلة المتكامل لحوكمة الأمن السيبراني على تحسين ممارسات إدارة مخاطر الأمن السيبراني، بحيث يمكن إعادة صياغة نظرية المنشأة لتشمل ليس فقط الأصول والموارد التي تؤدي إلى الربحية، بل أيضاً المخاطر والتهديدات التي قد تعيق ذلك، ومنها المخاطر السيبرانية الملموسة وغير الملموسة.

3- أهداف البحث

تتمثل أهداف البحث الرئيسية فيما يلي:

1. تحليل تأثير محددات جودة وظيفة المراجعة الداخلية من منظور منهج المدخلات على مؤشرات إدارة مخاطر الأمن السيبراني.
2. تحليل تأثير فعالية أداء خطوط المساءلة في هيكل الحوكمة السيبراني على مؤشرات إدارة مخاطر الأمن السيبراني.

3. تحليل أثر التفاعل المشترك بين جودة وظيفة المراجعة الداخلية من منظور منهج المدخلات، والهيكل المتكامل للحوكمة السيبرانية على مؤشرات إدارة مخاطر الأمن السيبراني عبر مراحلها المختلفة (الوقاية، والاكتشاف، والاستجابة، والعلاج/التصحيح).

تسعى هذه الأهداف إلى تقديم فهم شامل حول كيفية تأثير محددات جودة المراجعة الداخلية، وهيكل الحوكمة السيبراني على مؤشرات أداء مخاطر الأمن السيبراني، مع تقديم حلول تطبيقية تدعم المنشآت في تحسين استراتيجياتها في هذا المجال، وتتمثل في:

- اقتراح هيكل متكامل للحوكمة السيبراني يستند إلى مجموعة من المقومات الرئيسية كما تناولتها الأطر التنظيمية والمهنية الحالية، ويساهم في تنظيم الأدوار والمسؤوليات بشكل يضمن تفاعل فعال بين خطوط المساءلة المختلفة.

- توفير عدد من مؤشرات إدارة مخاطر الأمن السيبراني تعتمد على بيانات موضوعية لقياس التحسين في إدارة مخاطر الأمن السيبراني، وتساعد المنشآت في تقييم مستوي الأمن السيبراني، وتقليل فرص الخروقات السيبرانية. بالإضافة إلى أنها توفر دليل عملي للمنشآت حول المراحل الأساسية لإدارة مخاطر الأمن السيبراني.

4-أهمية البحث

تكمن أهمية هذا البحث في تقديم إسهام علمي وعملي يساعد المنشآت في تحسين إجراءاتها الأمنية وضمان حماية أصولها الرقمية. كما يسهم البحث في توضيح كيفية استثمار المنشآت في تعزيز جودة وظيفة المراجعة الداخلية وتطوير سياسات الحوكمة السيبرانية للحد من التهديدات السيبرانية المتزايدة. أيضاً، يساهم البحث في تقديم عدد من الأدلة العملية لسد فجوة بحثية مهمة، حيث لا تزال العلاقة بين جودة وظيفة المراجعة الداخلية وهيكل الحوكمة السيبراني وتأثيرها على تقليل المخاطر غير مدروسة بشكل كافٍ في الأدبيات المحاسبية، مما يفتح المجال أمام الباحثين لتطوير مزيد من الأبحاث في هذا المجال البحثي الحيوي الذي يهم مختلف القطاعات.

5-منهجية البحث

يعتمد البحث على منهجية مختلطة تجمع بين البحث الاستقرائي والاستنباطي. سيتم استعراض الأدبيات السابقة المتعلقة بمحددات جودة وظيفة المراجعة الداخلية وحوكمة الأمن السيبراني وتحليلها بشكل منهجي، إلى جانب إجراء دراسة ميدانية تشمل جمع بيانات من قطاعات مختلفة لتحليل مدى تأثير هذه العوامل على مؤشرات إدارة المخاطر السيبرانية.

6-حدود ونطاق البحث

تتمثل حدود البحث في الحدود التالية:

- يقتصر البحث على دراسة أثر محددات جودة وظيفة المراجعة الداخلية المستندة إلى منهج المدخلات، دون المناهج الأخرى المتاحة في الفكر المحاسبي لتحديد محددات جودة وظيفة المراجعة الداخلية.
- يقتصر البحث على دراسة أثر تطبيق هيكل المساءلة المتكامل لحوكمة الأمن السيبراني، دون المقومات الأخرى التي يعتمد عليها هيكل الحوكمة السيبراني كما تناولتها الأطر التنظيمية والمهنية المتاحة.
- يعتمد البحث على قياس التحسين في مؤشرات إدارة مخاطر الأمن السيبراني عبر مراحله المختلفة (الوقاية، والاكتشاف، والاستجابة، والعلاج/التصحيح)، بناء على بيانات ميدانية موضوعية وليس استجابات من المستجيبين في عينة البحث.
- تعتمد قابلية نتائج البحث للتعميم على قيود الصلاحية الداخلية لتصميم منهجية البحث والتي تشمل ضوابط اختيار العينة، وقياس المتغيرات، وأسلوب جمع البيانات، ونموذج الاختبار المستخدم.

7-خطة البحث

7-1 الإطار النظري للبحث

7-2 الدراسات السابقة وفروض البحث

7-3 منهجية البحث

7-4 نتائج البحث

7-5 الاستنتاجات، والتوصيات، ومجالات البحث المقترحة

7-1 الإطار النظري للبحث

7-1-1 محددات جودة المراجعة الداخلية في مجال الأمن السيبراني

أصبحت جودة وظيفة المراجعة الداخلية في مجال الأمن السيبراني من الموضوعات البحثية المتزايدة في مجال المراجعة، إلا أن الأبحاث المتعلقة بهذا المجال لا تزال محدودة. إذ يشير Haapamäki and Sihvonen (2019) في مراجعتهم لـ 13 دراسة متعلقة بمراجعة الأمن السيبراني إلى أن هذا المجال لا يزال في مراحله الأولية. ولم تقم أي من الدراسات بتطوير مفهوم شامل ومنهجي لمجالات مراجعة الأمن

السيبراني. ومن ناحية أخرى، اقترح Kahyaoglu and Caliyurt (2018) خصائص متعددة لمراجعة الأمن السيبراني الفعال، إلا أن دراستهم استندت إلى مبادئ عامة وعالية المستوى، مع التركيز على كيفية تعاون وظيفتي المراجعة الداخلية وأمن المعلومات لدعم المنشآت في تحقيق مستوى آمن من المعلومات بتكلفة فعالة.

وتعد دراسة Islam et al. (2018) واحدة من الدراسات الاختبارية القليلة التي تستقصي مدى تنفيذ عملية المراجعة الداخلية للأمن السيبراني، حيث ركزت الدراسة على قياس مدى تنفيذ عملية المراجعة الداخلية للأمن السيبراني باستخدام متوسط سبعة أسئلة حول مراجعة تكنولوجيا المعلومات من مسح (IIA Research Foundation, 2015) (CBOK). وعلى الرغم من أن CBOK يعد استبيانًا عامًا حول ممارسات المراجعة الداخلية، إلا أنه لا يغطي مجالات مراجعة الأمن السيبراني بشكل شامل.

كما هدفت دراسة Sabillon et al. (2017) إلى تقديم نموذج مراجعة للأمن السيبراني يضم 18 مجالاً للدول والمنشآت. ومع ذلك، فإن هذه الدراسة لم تقدم تقسيمًا واضحًا لهذه المجالات إلى مجالات فرعية، كما لم تحدد أي ضوابط، ما يجعل تطبيقها على المستوى التنظيمي صعبًا. وفي السياق ذاته، ناقشت دراسة Steinbart et al. (2018) أحد العوامل المهمة في مراجعة الأمن السيبراني الفعال، وهو التعاون بين وظيفة أمن المعلومات ووظيفة المراجعة الداخلية، حيث أظهرت الدراسة أن هذا التعاون يساهم بشكل كبير في تحسين مستوى الأمن السيبراني.

ووفقًا لمراجعات الأدبيات التي أجراها كل من Christ et al. (2021) و Hazaea et al. (2023)، لم تظهر أي دراسات تحليلية تتناول دور المراجعة الداخلية في إدارة الأمن السيبراني بشكل عام أو جودة المراجعة الداخلية وتطبيقها من قبل المستويات الفاعلة في هيكل الحوكمة السيبراني بشكل خاص. ومع ذلك، يمكن الافتراض أن العوامل المؤثرة في جودة المراجعة الداخلية عمومًا، والتي تمت دراستها في أبحاث متعددة (Erasmus and Coetzee, 2018)، قد تلعب دورًا مهمًا في تحديد جودة المراجعة الداخلية في مجال الأمن السيبراني.

علاوة على ذلك، تفرض طبيعة إدارة مخاطر الأمن السيبراني مجموعة من العوامل المحددة التي قد تؤثر على إجراءات المراجعة الداخلية وكفاءتها وجودتها، مثل الكفاءات التقنية المطلوبة للمراجعين الداخليين، والدعم الفعال من قبل مجالس الإدارة التي ينبغي أن تُعنى بوضع السياسات وتوجيه إدارة المخاطر بكفاء (Crowe and Internal Audit Foundation, 2018). وقد قدمت عدد من الدراسات تحليل لجودة وظيفة المراجعة الداخلية من زوايا متعددة، ولكل منها مزاياها وعيوبها (Arena and Azzone, 2009; Lin et al., 2011; Roussy and Brivot, 2016; Wang, 1997).

ففي دراسة Arena and Azzone (2009) صنفت مقاييس جودة وظيفة المراجعة الداخلية ضمن ثلاثة أبعاد: العملية، المخرجات، والنتائج. وتستند مقاييس العملية إلى فرضية مفادها أن وظيفة المراجعة الداخلية تكون فعالة وتضيف قيمة إذا التزمت بالمعايير المعتمدة في التخطيط وتنفيذ المهام وتقديم تقارير شاملة. من جهة أخرى، هناك وجهة نظر تقول بأن وظيفة المراجعة الداخلية تصبح فعالة إذا تم تطبيقها وفقًا لمنهجية قائمة على المخاطر وليس على مجرد الرقابة (Castanheira et al., 2010). أما مقاييس المخرجات فتقيس قدرة المراجعة الداخلية على تلبية احتياجات المراجعين وأصحاب المصلحة، وغالبًا ما يتم تفعيلها من خلال مدى رضا المراجعين والنسبة المئوية للتوصيات التي يتم تنفيذها. بينما ترتبط مقاييس النتائج بمساهمة إطار الرقابة في الأداء التنظيمي، والذي يصعب قياسه (Arena and Azzone, 2009).

وتتوافق مناهج العملية والمخرجات والنتائج ضمن إطار يتطلب الامتثال للمعايير، واتباع نهج قائم على المخاطر، ودمج أهداف المنشأة وتوقعات أصحاب المصلحة في أهداف الرقابة الداخلية. وفي هذا الإطار قدمت دراسة Brivot (2011) تحليل لمزايا وعيوب مقاييس العملية، والمخرجات، والنتائج. فمراقبة الجودة بناءً على العملية تُعد غير مناسبة عندما يتطلب العمل مقدارًا كبيرًا من التقدير الشخصي، حيث لا يمكن اختزاله إلى إجراءات تقنن العملية بأكملها. فإن مراقبة الجودة من خلال العملية (أو الإجراءات) ليست كافية في أفضل الأحوال، وقد تكون غير فعالة في أسوأها ما لم تأتِ من قبل محترفين آخرين، لأنهم وحدهم يمكنهم (بشكل جزئي) إنتاج الخوارزميات التي توجه أساليبهم. كذلك، فإن مراقبة الجودة بناءً على المخرجات ليست كافية للعمل المهني، حيث لا يمكنها الإشارة إلى العيوب إلا بأثر رجعي، عندما تظهر مشكلة كبيرة. تعتبر مراقبة الجودة المدخلة، من خلال اختيار الأكفاء والمميزين، أكثر فعالية وأسهل في التطبيق. إضافة إلى ذلك، فإن الرقابة الذاتية (من خلال الالتزام بقواعد السلوك المهني) والرقابة الجانبية من قبل الزملاء (من خلال العقوبات من أعضاء الجمعية المهنية) تتناسب أكثر مع طبيعة العمل المهني مقارنةً بالرقابة الإدارية.

ووفقاً لدراسة Roussy and Brivot (2016) فقد قدمت أربعة أطر تفسيرية لجودة وظيفة المراجعة الداخلية تختلف باختلاف وجهات النظر المتعددة للجهات الفاعلة في الحوكمة. فقد وُجدت أن المراجعين الخارجيين لا يُعبرون عن جودة المراجعة الداخلية استنادًا إلى مجموعة من الخصائص المرغوبة في المخرجات المنتجة (بما في ذلك تقرير المراجعة الداخلية). بدلاً من ذلك، يركزون على الشروط التي يعتبرونها ضرورية لضمان جودة المخرجات، مثل كفاءة المراجع الداخلي الفردي واستقلالية وظيفة المراجعة

الداخلية عن فريق إدارة المنشأة. وتُعتبر هذه المعايير للجودة عوامل مدخلات، حيث تتعلق بملف الشخص الذي ينبغي أن يقوم بالعمل والترتيبات التنظيمية التي يجب أن تكون متاحة قبل بدء العمل.

ومن وجهة نظر المراجعين الخارجيين، يُنظر إلى المراجعين الداخليين على أنهم "حراس" مكلفون بالكشف عن نقاط الضعف الهامة في الرقابة الداخلية. ويؤكدون أن الجودة يمكن تحقيقها فقط إذا استوفى المراجعين الداخليون معايير معينة (مثل الكفاءة الفنية) واتُخذت تدابير تنظيمية لحماية استقلاليتهم تجاه المديرين التنفيذيين.

في المقابل، يعبر معهد المراجعين الداخليين عن جودة المراجعة الداخلية من منظور عملية التنفيذ، كمهنيين مستقلين، حيث تكون جودة عملهم عالية فقط إذا التزموا بمعايير المراجعة الداخلية وأظهروا "العناية المهنية الواجبة" والتزموا بمدونة أخلاقيات المعهد (شحاته، ٢٠٢٢). فالجودة هنا تنبع من الامتثال المؤكد للمعايير وأفضل الممارسات التي يروج لها المعهد.

من ناحية أخرى، يؤطر المراجعون الداخليون وأعضاء لجان المراجعة جودة المراجعة الداخلية بناءً على مدى فائدة العمل المكتمل (الناتج النهائي) كما يرونه لمديري المنشأة. حيث يُعرفون جودة عملهم بمدى استفادة المدير الأعلى من التقرير الداخلي لتحسين أداء المنشأة. وتشير هاتان الإطارتان القائمتان على المخرجات إلى موقف عملي يتبناه المؤيدون لهذه الأطر، كما أكد ذلك Radcliffe (1999). فالمراجعون الداخليون وأعضاء لجان المراجعة مرتبطون بشكل واقعي بالبيئة التنظيمية المحددة التي يعملون فيها. تختلف وجهات نظرهم عن المراجعين الخارجيين، الذين يركزون على الاستقلال عن الإدارة العليا كمعيار أساسي للجودة (وإن كان مثالياً وقد يكون غير عملي). كما أنها تختلف عن إطار معهد المراجعين الداخليين (IIA)الذي يركز على الامتثال الكامل للمعايير المهنية، والذي يعتبرونه أقل أهمية من تقديم قيمة عملية وملموسة لصناع القرار في المنشأة.

إن طبيعة إطار المراجعين الداخليين، الذي يركز على مساعدة المدير الأعلى في تخفيف المخاطر الإستراتيجية الأكثر أهمية، يمكن أن تشجع المراجعين الداخليين على حماية ما وصفه Radcliffe (2008,2011) بـ "الأسرار العامة" بدلاً من عرضها علنًا، خصوصًا إذا كانت حماية هذه الأسرار العامة تعتبر أفضل وسيلة للسيطرة على المخاطر الإستراتيجية في ظروف معينة.

بناء على ذلك، يري الباحث بأن أطر المراجعين الخارجيين ومعهد المراجعين الداخليين (IIA) تتسق مع الرأي القائل بضرورة استخدام معايير الجودة المهنية، بما في ذلك ضوابط المدخلات عبر التوظيف الانتقائي بناءً على كفاءة المرشحين المثبتة، والرقابة المنتظمة من قبل أعضاء الجمعية المهنية لضمان الاستقلال والولاء للمهنة والجمهور بدلاً من المنشأة صاحبة العمل. كما يتسق إطار معهد المراجعين

الداخليين مع ضوابط موجهة ذاتيًا من خلال الامتثال لمعايير السلوك الأخلاقي. في المقابل، تتفق أطر المراجعين الداخليين وأعضاء لجان المراجعة مع الرأي الذي يرى أن الضوابط الإدارية يجب أن تسود، بما في ذلك ضوابط المخرجات من قبل الإدارة العليا القادرة على تحديد ما إذا كان تقرير المراجعة الداخلية ذا قيمة للمنشأة.

في ضوء ذلك، تركز الدراسة على دراسة محددات جودة وظيفة المراجعة الداخلية في مجال الأمن السيبراني من منظور المدخلات، وتتمثل في امتلاك المراجعين الداخليين للكفاءة المناسبة وتبنيهم العقلية الصحيحة فيما يتعلق بالاستقلالية تجاه الإدارة العليا للمنشأة. ويرتبط هذان المحددان بخصائص الأفراد الذين ينبغي اختيارهم للقيام بمهام المراجعة الداخلية، ما يجعلهما بمثابة معايير لمدخلات العمل في عملية المراجعة الداخلية في مجال الأمن السيبراني.

7-1-2 إدارة مخاطر الأمن السيبراني: آليات الحوكمة والأطر التنظيمية المهنية

على الرغم من الاهتمام المتزايد من قبل الحكومات والمؤسسات باستراتيجيات ومعايير وتوجيهات الأمن السيبراني، إلا أن لا تزال الأدبيات المحاسبية تفتقر إلى توفير إطار شامل لحوكمة الأمن السيبراني، مما يحد من قدرة المديرين التنفيذيين وأعضاء مجالس الإدارة على تطبيق ممارسات فعّالة في هذا المجال. حيث يُعد الأمن السيبراني مجالاً ناشئًا وحيويًا ضمن ممارسات الحوكمة (Sambamurthy and Zmud,1999; Wilkin and Chenhall, 2020).

في هذا الإطار، يتمثل التحدي الأساسي في تصميم آلية فعالة لتنظيم العلاقة بين التوجيه الاستراتيجي للأمن السيبراني من قِبل مجالس الإدارة وتنفيذه عبر المستويات التنظيمية المختلفة. وتُعد الحوكمة المؤسسية، على المستوى الكلي، أداة مركزية لتحديد العلاقات بين أصحاب المصلحة داخل المؤسسة، حيث توفر إطارًا للمساءلة يُمكّن من تحديد الأهداف المؤسسية ومتابعة تحقيقها (OECD, 2015).

ومع ذلك، لا يزال هيكل حوكمة الأمن السيبراني موضع جدل، حيث تتأثر معظم النقاشات حول هذا الموضوع بالإصدارات الإرشادية المهنية (IIA, 2016) أكثر من تأثيرها برؤى البحث الأكاديمي.

بناءً على ذلك، يبرز التساؤل حول تحديد المقومات الرئيسية لهيكل حوكمة الأمن السيبراني كما تناولتها الأطر التنظيمية والأدوات المهنية المتاحة. وتتضمن تلك المقومات المبادئ الإرشادية، وهيكل الأصول ذات الصلة بأصحاب المصالح، ومعايير إدارة المخاطر، وهيكل نظم المساءلة، وهيكل أعداد تقارير نتائج الأمن السيبراني.

- المبادئ الإرشادية

توجد في الأدبيات المحاسبية مبادئ توجيهية لحوكمة الأمن السيبراني موجهة للمديرين التنفيذيين وأعضاء مجالس الإدارة. بالإضافة إلى ذلك، فقد أصدرت المنظمات والهيئات المهنية عددًا من المبادئ الإرشادية للإدارات والوحدات الداخلية لحوكمة الأمن السيبراني، حيث حدد المنتدى الاقتصادي العالمي ستة مبادئ يجب تضمينها لضمان منشأة تتمتع بمقاومة سيبرانية عالية (WEF, 2021). يتضمن ذلك اعتبار الأمن السيبراني محركًا للأعمال، ومواءمة المخاطر مع احتياجات العمل، وضمان تصميم تنظيمي يدعم الأمن السيبراني، بما في ذلك الحوكمة على مستوى مجلس الإدارة.

وفي هذا الإطار قدم Leech and Hanlon (2017)، ومواد من الجمعية الوطنية لمديري الشركات CAQ (2018) خمسة مبادئ ينبغي على مجالس الإدارة أخذها في الاعتبار لتعزيز قدراتها في توفير الرقابة على الأمن السيبراني. يتضمن ذلك إطارًا من الأسئلة التي يجب طرحها لتقديم ضمانات حول مسائل الأمن السيبراني، وتستهدف هذه الأسئلة الإدارات والوحدات المختلفة المعنية بالعملية، بما في ذلك المراجعون الداخليون والإدارة والمديرون.

ونظرًا لغياب اللوائح المتعلقة بمدى مشاركة مجلس الإدارة في الأمن السيبراني، تعتبر الإرشادات التي تقدمها المنظمات الرائدة في هذا المجال حديثة للغاية؛ فقد نشر المعهد الأسترالي لمديري الشركات(AICD) في أكتوبر (2022) مجموعة من الإرشادات لمساعدة المديرين في مجالس الإدارة الأسترالية على الإشراف على إدارة المخاطر السيبرانية(AICD and CS Cooperative Research Centre, 2022).

- الأصول الرقمية في إطار الأمن السيبراني

يُطلق على الأصول الرقمية في إطار الأمن السيبراني اسم "التعرف على الجواهر الثمينة" التي يجب حمايتها، ثم ضمان حصول هذا النطاق على اهتمام الإدارة قبل غيره. وتعد الأدبيات المحاسبية محدودة في توفير هذا النوع من التوجيه،بما في ذلك الخطوات والطريقة لتحديد هذه الأصول في سياق الأمن السيبراني، وكذلك في ضوء التداخل الحتمي بين العمليات والأنظمة في البيئة الرقمية الحالية (علي،2022).

وقد أوضح Boehm et al. (2019) أهمية البدء بالتركيز على تحديد الأصول التي تتطلب الحماية والتوافق عليها، والتي يمكن أن تشمل تلك الأصول والعمليات التجارية، والأنظمة الداعمة لها، ومجموعات أو مخازن البيانات داخل المنشأة. ويُعتقد أن مثل هذا المدخل يعتمد على المخاطر، ويسمح بحوكمة الأمن السيبراني بطريقة أكثر فعالية من حيث التكلفة.

- **المراجعة الداخلية وإدارة مخاطر الأمن السيبراني**

تبرز أهمية إدارة مخاطر الأمن السيبراني من خلال إصدار المعهد الأمريكي للمحاسبين القانونيين المعتمدين (AICPA) إطارًا جديدًا لإدارة مخاطر الأمن السيبراني لمساعدة الشركات على مواجهة التحديات المتزايدة(AICPA, 2018)، حيث أن تحديات الأمن السيبراني تتطلب من المنشآت إدارة فعّالة للمخاطر.

وقد ظهرت إدارة المخاطر المؤسسية (ERM) كأحد المصطلحات البارزة في ظل زيادة عدم اليقين المالي وانتشار الفضائح المالية (Walker et al., 2002). وتعرف لجنة المنظمات الراعية (COSO, 2004) إدارة المخاطر المؤسسية (ERM) بأنها عملية تُنفذ بواسطة مجلس إدارة الكيان، وإدارته، والعاملين فيه، وتُطبق في إطار وضع الاستراتيجيات وفي جميع أنحاء المؤسسة، وتهدف إلى تحديد الأحداث المحتملة التي قد تؤثر على الكيان، وإدارة المخاطر لتكون ضمن مستوى مقبول من المخاطر، لتقديم ضمان معقول بشأن تحقيق أهداف الكيان. هناك ثماني مكونات لإدارة المخاطر المؤسسية (ERM): البيئة الداخلية، وضع الأهداف، تحديد الأحداث، تقييم المخاطر، الاستجابة للمخاطر، أنشطة التحكم، المعلومات والتواصل، والمراقبة.

يدعو إطار إدارة المخاطر المؤسسية (COSO ERM) وظيفة المراجعة الداخلية للمساعدة في الإدارة ومجلس الإدارة ولجنة المراجعة الخاصة به من خلال فحص وتقييم وإعداد تقارير وتقديم توصيات لتحسين كفاءة وفعالية عملية إدارة المخاطر المؤسسية(COSO, 2004). ويلعب المراجعون الداخليون دورًا رئيسيًا في تقديم خدمات التأكيد والاستشارات فيما يتعلق بإدارة المخاطر داخل منشأتهم (Sarens and De Beelde, 2006)، ويؤكد الباحثون في هذا المجال بشكل متزايد على حقيقة أن وظيفة المراجعة الداخلية تساهم بشكل كبير في دعم إدارة المخاطر المؤسسية (Walker et al., 2002؛ راضي،2014). ويُعتبر المدير التنفيذي للمراجعة الداخلية (CAE) أيضًا قياديًا مهمًا في إدارة المخاطر المؤسسية، حيث توجد أدلة على وجود تفاعل وثيق بين المراجعة الداخلية وكبير موظفي المخاطر(CRO)، وهناك أدلة على تركيز المراجعة الداخلية على تنسيق جهود إدارة المخاطر المؤسسية من خلال المساعدة في تحديد المخاطر، واقتراح أنشطة التحكم، ومراقبة عملية إدارة المخاطر (Beasley et al., 2005). وبالنظر إلى تركيز وظيفة المراجعة الداخلية الطبيعي على الحوكمة والمخاطر والامتثال، فإنها تلعب دورًا حيويًا في الإشراف على جميع مكونات إطار إدارة المخاطر المؤسسية الثمانية. وبالتالي، يكون لإدارة المخاطر المؤسسية الأثر الأكبر على أنشطة وظيفة المراجعة الداخلية عندما تكون عملية إدارة المخاطر للمنشأة مطبقة بالكامل(Beasley et al., 2006).

وفي مجال الأمن السيبراني، تشمل إدارة مخاطر الأمن السيبراني سلسلة من الأنشطة تهدف إلى تحديد، تقييم، معالجة، ومراقبة التهديدات الإلكترونية (NIST, 2018). يتم تقسيم دورة إدارة المخاطر عادة إلى ثلاث مراحل رئيسية: (1) الوقاية: الحد من احتمالية حدوث الحوادث من خلال ضوابط استباقية. (2) الاكتشاف: رصد التهديدات والحوادث فور وقوعها. (3) الاستجابة/التصحيح: احتواء الهجوم وتقليل آثاره واستعادة الوضع الطبيعي. وتُستخدم مؤشرات الأداء الرئيسية (KPIs) ومؤشرات المخاطر الرئيسية (KRIs) لتقييم مدى فعالية إدارة مخاطر الأمن السيبراني خلال المراحل الثلاث (Deloitte, 2017).

ويشمل دور المراجعة الداخلية تقييم فعالية ضوابط الأمن السيبراني وسياسات الحماية؛ التأكد من امتثال المنشأة للمعايير الدولية مثل: NIST CSF,2018; ISO/IEC27001/27005؛مراجعة خطط الاستجابة للحوادث السيبرانية؛ اختبار واختراق الضوابط الأمنية الداخلية بالتعاون مع الفرق الفنية.

- **إطار المساءلة في حوكمة الأمن السيبراني**

تتفق العديد من الدراسات على ضرورة تحميل مجلس الإدارة مسؤولية الأمن السيبراني، لكنها تقصر في شرح كيفية تنفيذ ذلك باستخدام الأطر والأدوات المناسبة. وتقترح عدد من الدراسات أهمية استخدام لجنة فرعية لمجلس الإدارة (Nolan and McFarlan, 2005) تمتلك المهارات والمعرفة الكافية لتوجيه الأمن السيبراني كأحد الطرق لبناء القدرات في مجلس الإدارة. وبالمثل يوضح Bailey et al. (2020) بأن استخدام اللجان الفرعية يمكن أن يسمح بتخصيص وقت أكبر لمناقشة مسائل الأمن السيبراني مقارنة باجتماعات مجلس الإدارة العادية. كما يؤكد Olyaei et al.(2021) على أن مجلس الإدارة يعتبر الأمن السيبراني مصدرًا رئيسيًا للمخاطر، ولذلك يجب أن يكونوا قادرين على ممارسة مسؤوليتهم بالمهارات المناسبة، وضمان تقديم التقارير إلى اللجان بلغة ملائمة.

وفي هذا الإطار قدم Bailey et al.(2020) جانب آخر من جوانب المساءلة وهو أن الرئيس التنفيذي وأعضاء آخرين من فريق القيادة العليا داخل الإدارة يتحملون جميعًا المسؤولية عن الأمن، وليس فقط مدير المعلومات(CIO) أو مدير أمن المعلومات(CISO). يعكس ذلك جوانب من الأمن مثل التحكم في الوصول والتفاعل مع العملاء، والتي تمتد عبر جميع أجزاء المنشأة. كما يشير إلى أنه لتلبية هذه المسؤولية، يجب أن يركز القادة على الاستراتيجية، ومراقبة الوحدات التجارية المتقاطعة، وسلوك المستخدم، والحكم السليم والإبلاغ. وتلعب الهياكل التنظيمية أيضًا دورًا رئيسيًا في المساءلة والإشراف كما تم تأطيرها من قبل Liu et al.(2020) يذكر المؤلفون أن حوكمة تقنية المعلومات المركزية مع إطار من المؤشرات والمقاييس للإبلاغ يعطي نتائج أفضل في تقليل مخاطر الأمن السيبراني.

وتتبني المنظمات المهنية (Committee of Sponsoring Organizations [COSO] 2004, 2013, 2017; IIA, 2013, 2016, 2020)، والمنظمون الماليون (لجنة بازل للإشراف المصرفي على مبادئ الإدارة السليمة للمخاطر التشغيلية,2011)، وجمعيات إدارة المخاطر (ISACA, 2011, 2012a, 2012b, 2016)، والشركات الاستشارية الكبرى نموذج "خطوط الدفاع الثلاثة" Three Line of Defense (3LoD) لإدارة المخاطر. ويتمثل الخط الأول للمساءلة هو وظيفة تكنولوجيا المعلومات المسؤولة عن تنفيذ الضوابط لحماية المنظمة من المخاطر السيبرانية. أما الخط الثاني للمساءلة هو الرقابة التكتيكية المسؤولة عن وضع سياسات إدارة المخاطر ومراقبة ضوابط الخط الأول وضمان الامتثال للوائح الأمن السيبراني وسياسات إدارة مخاطر تكنولوجيا المعلومات. وتشمل أدوار الخط الثاني إدارة المخاطر المؤسسية (ERM) والامتثال والأمن وضمان الجودة. أما الخط الثالث للمساءلة هو وظيفة المراجعة الداخلية فهو مستقل عن الإدارة ولا يشارك في اتخاذ القرارات الإدارية (Héroux and Fortin, 2013) ويقدم التأكيد المستقل والموضوعي والمشورة بشأن كفاية وفعالية الحوكمة وإدارة المخاطر لمجلس الإدارة (IIA, 2020).

وقد وجهت عدد من الدراسات عدد من الانتقادات لنموذج خطوط الدفاع الثلاث (3LoD) لأنه يركز على الدفاع ويجعل إدارة المخاطر مكتب "الرفض"، بدلاً من المساعدة في التعامل مع عدم اليقين، بالإضافة إلى عدم اعتراف النموذج بدور الإدارة التنفيذية ومجلس الإدارة بشكل صريح (Lyons, 2011; Leech and Hanlon, 2016). في هذا السياق، تشير بعض الدعاوى القضائية المتعلقة بحوادث سيبرانية إلى أن مجلس الإدارة والمديرين التنفيذيين هم المسؤولون في نهاية المطاف، مما يدل على أن الجهات المعنية تعتبرهم المسؤولين الأساسيين(Leech and Hanlon, 2016).

لقد وجهت الدراسات منذ ما يقرب من عقدين إلى ضرورة مشاركة مجلس الإدارة والإدارة التنفيذية في الأمن السيبراني (Jeyaraj and Zadeh, 2020; NIST framework 2019; COBIT 2019, Lyons, 2011). وعلى ذلك، فقد اعترف معهد الراجعين الداخليين (IIA,2020) بأهمية وجود مستويات إضافية في إدارة المخاطر السيبرانية والحوكمة، وأنه لتحقيق القيمة، يجب على المنشأة قبول وإدارة مستويات المخاطر. لذلك أستبعد معهد المراجعين الداخليين مصطلح "الدفاع" واعترف بالأدوار الصريحة للمديرين التنفيذيين ومجلس الإدارة في تحديث نموذج خطوط الدفاع الثلاث (3LoD). ويحدد النموذج المحدث خمسة خطوط للمساءلة. تُعد هذه الخطوط الأول والثاني والثالث من نموذج (3LoD)، بالإضافة إلى خطوط الإدارة ومجلس الإدارة. نُشير بعض الدراسات إلى النموذج المحدث باسم خطوط المساءلة الخمس (5LoA) Five Line of Accountability لتأكيد هذا الاختلاف.

تُعتبر الإدارة التنفيذية الخط الرابع للمساءلة (Lyons, 2011; Leech and Hanlon, 2016; Rothrock et al., 2018; Steinbart et al., 2018). تتحمل الإدارة التنفيذية مسؤولية إدارة المنشاة وتخصيص الموارد لإدارة المخاطر المختلفة، وتدعم وتشرف على إدارة المخاطر المؤسسية (COSO, 2017). وتضمن أن الخطوط الثلاثة الأولى لديها الكفاءات اللازمة وتؤدي وفقًا للتوقعات. وباعتبار أن إدارة المخاطر السيبرانية هي واحدة فقط من مجالات إدارة المخاطر المؤسسية، فإن الإدارة التنفيذية مسؤولة عن مواءمتها مع المجالات الأخرى(Deloitte, 2015a, 2015b).

وتشير معظم الأبحاث السابقة إلى أن وجود مديرين تنفيذيين (مثل: الرئيس التنفيذي، والمدير المالي، والمدير التنفيذي لتكنولوجيا المعلومات) لديهم خبرة في تكنولوجيا المعلومات أو مسؤول تنفيذي لتكنولوجيا المعلومات في مجلس الإدارة يقلل بشكل كبير من حوادث اختراق البيانات التي يجب الإبلاغ عنها (Feng and Wang, 2019; Haislip et al., 2016; Haislip et al., 2020; 2021; Vincent et al., 2019; Smith et al., 2021). ومع ذلك، وجدت دراسة (Haislip et al., 2021) أن وجود رئيس تنفيذي بخبرة في تكنولوجيا المعلومات قد يؤدي إلى زيادة في حوادث الاختراق السيبراني، ويُعزى ذلك إلى أنهم أكثر عرضة لاكتشاف وإبلاغ هذه الحوادث.

يمثل مجلس الإدارة الخط الخامس للمساءلة، وهو الذي يحدد شهية المخاطرة في المؤسسة ويشرف على ما إذا كانت الإدارة التنفيذية تعمل ضمن حدود المخاطرة المقبولة للمؤسسة. ويتطلب الدور الاستراتيجي من مجلس الإدارة المشاركة في تطوير وصقل الأهداف الاستراتيجية الأساسية (مثل تحديد شهية المخاطرة) ومقاييس المخاطر، وتحديد دقة تقييم المخاطر، وضمان استقلالية عمليات المراجعة (Leech and Hanlon, 2016; Von Solms and Von Solms, 2018).

بالإضافة إلى ذلك، يوفر نموذج خطوط المساءلة الخمس (5LoA) أساساً لتحديد الهياكل والأدوار والمسؤوليات اللازمة لحوكمة الأمن السيبراني، حيث يعتمد على نوعين من آليات الحوكمة وهما: الهيكلية والتشاركية في حوكمة الأمن السيبراني وتعالج سؤالين مستقلين ولكنهما مرتبطان. تركز الآليات الهيكلية للحوكمة على سؤال: "من لديه أي دور في كيفية اتخاذ القرارات؟"، بينما تتناول الآليات التشاركية سؤال: "من يتعاون مع من؟ وكيف يقومون بمراقبة بعضهم البعض؟" كما تتعامل الآليات التشاركية مع السلطة الرسمية وغير الرسمية، وتشمل التعاون والحوار الاستراتيجي والتعلم المشترك بين المديرين التنفيذيين للشركات وإدارة تكنولوجيا المعلومات وإدارة الأعمال (Van Grembergen et al., 2004).

وبالمقارنة مع نموذج (3LoD) التقليدي، يسمح النموذج الجديد بدرجة أكبر من المرونة في تصميم الخطوط، مشيرًا إلى التعاون الوثيق والتكامل بين الخطوط، ويؤكد على مسؤوليات الجهات المعنية ذات الصلة بالحوكمة (Eulerich, 2021).

علي حد علمنا، يُعد نموذج (5LoA) حتى الآن الإطار المهني الوحيد المعروف الذي يضع تصورًا منظمًا لتكوينات هيكل الحوكمة، من خلال تحديد الأدوار والعلاقات بين مجلس الإدارة، والإدارة التنفيذية، والجهات المعنية بإدارة مخاطر الأمن السيبراني داخل المؤسسة. ويُسهم هذا النموذج في دعم فهم أكثر تكاملاً لمسؤوليات الأطراف المختلفة ضمن منظومة الحوكمة السيبرانية. على الرغم من أن المشاركة في جميع مستويات الهيكل التنظيمي هي موضوع عام في أطر وطنية مماثلة، إلا أن نموذج (5LoA) يمثل معيار أفضل الممارسات، وهو منهج فعال لتلخيص المشاركة التنظيمية الشاملة المقترحة من قبل المنظمات المهنية والأكاديمية.

- **هيكل تقارير نتائج الأمن السيبراني**

يشير هيكل تقارير نتائج الأمن السيبراني إلى بعدين رئيسيين، الأول: يتعلق بتحديد المستوى التنظيمي المناسب للإشراف على حماية المعلومات الأمنية، بينما الثاني: يتعلق بمحتوى وطبيعة التقارير المطلوبة. فيما يخص المستوى التنظيمي، تشير الدراسات المتخصصة إلى أهمية تعيين منصب مستقل لرئيس أمن المعلومات(CISO)، ويكون هذا الدور ضروريًا لمواجهة التهديدات السيبرانية، حيث أن المنشآت التي تعين رئيس أمن المعلومات (CISO) تكون أكثر قدرة على التصدي للهجمات السيبرانية ولديها فرق استجابة للحوادث أكثر من تلك التي لا تعين هذا المنصب(ThreatTrack, 2016). إضافة إلى ذلك، يعد من المهم أن يكون رئيس أمن المعلومات (CISO) مستقلاً عن رئيس قسم المعلومات (CIO) لمنع تضارب المصالح، حيث تميل تكنولوجيا المعلومات إلى التركيز على الأداء وتقليل التكاليف، في حين أن أمن المعلومات يعتبر جزءًا من إدارة المخاطر المؤسسية ويحتاج إلى توازن مع تلك الأهداف (ISACA, 2012b). ويمكن تحقيق هذه الاستقلالية عبر إبلاغ رئيس أمن المعلومات مباشرة إلى الرئيس التنفيذي أو رئيس قسم المخاطر، مما يعزز قدرة المنشأة على مواجهة التهديدات السيبرانية وتحقيق إدارة فعّالة للمخاطر.

من ناحية أخرى، تتيح هذه الاستقلالية لرئيس أمن المعلومات تقديم التقارير الخاصة بالموارد اللازمة لإدارة مؤشرات فعالية الأمن السيبراني. وقد أوضحت دراسة Arena et al. (2010) أن المنشآت التي يكون فيها رئيس أمن المعلومات على تواصل مباشر مع الرئيس التنفيذي تتمتع بدعم إداري قوي، مما يسهم في تخصيص الميزانية بشكل فعال لموارد الأمن السيبراني، وبالتالي تعزيز الحماية في المنشأة. كما

تبرز أهمية هيكل التقارير في تحسين العلاقة بين المراجعة الداخلية ووظائف أمن المعلومات. ووفقًا لـ San Miguel and Govindarajan (1984)، فإن المنشآت التي تتمتع فيها مسؤولي المراجعة بعلاقات تقرير مستقلة يميل فيها المراجعون إلى تحسين الكفاءة بدلاً من مجرد التركيز على الالتزام.

من ناحية أخرى، لا يزال هناك نقص في التوجيه بشأن محتوي وطبيعة التقارير المطلوبة لضمان أن مجلس الإدارة يستطيع أداء مسؤولياته بشكل فعال. وفقًا لوظيفة المراجعة الداخلية، يوفر إطار التقارير الموجه إلى المستويات العليا رؤى حول فعالية الضوابط ويشمل أيضًا وجهة نظر ممارس مستقل كوسيلة للحصول على ضمان من الإدارة (AICPA, 2018). كما يُستخدم إطار عمل Ponemone لتصنيف نضج الأمان والانتهاكات في ثلاثة مجالات رئيسية: نقص النظام، والاحتيال الإجرامي، والخطأ البشري (Banker and Feng ,2019).

وتؤكد الدراسات على أهمية تقارير الأسباب الجذرية كما أوضحتها دراسة(2021) .Cheong et al، التي تقدم طريقة للإبلاغ إلى الجهات التنظيمية مثل هيئة الأوراق المالية والبورصات (SEC) من خلال تقارير الإفصاح الموجهة من الإدارة إلى مجالس الإدارة. ورغم وجود هذه الأطر، إلا أن هناك نقصًا في التوجيه الذي يغطي دورة الحياة الكاملة للأمن السيبراني، بالإضافة إلى الحاجة لتحديد البيانات الضرورية التي تتجاوز مجرد قياس حجم وشدة الهجمات على الشبكات.

7-2 الدراسات السابقة وفروض البحث

يهدف هذا الجزء إلى اشتقاق فروض البحث بناءً على تحليل واستقراء الدراسات السابقة في الفكر المحاسبي التي تناولت محددات جودة وظيفة المراجعة الداخلية في مجال الأمن السيبراني، وهيكل الحوكمة السيبراني، والعلاقة بين كل منها، ومدى مساهمتها في تحسين مؤشرات إدارة مخاطر الأمن السيبراني.

7-2-1 محددات جودة وظيفة المراجعة الداخلية وأثرها على تحسين مؤشرات مخاطر الأمن السيبراني

يركز البحث بشكل خاص على جودة وظيفة المراجعة الداخلية في مجال الأمن السيبراني. ومن خلال التحليل السابق في الإطار النظري للبحث لمحددات جودة وظيفة المراجعة الداخلية في الأمن السيبراني، يركز البحث على دراسة محددات جودة وظيفة المراجعة الداخلية في الأمن السيبراني من منظور منهج المدخلات، وتتمثل المعايير الرئيسية لتقييم جودة وظيفة المراجعة الداخلية بناء على مدخلات العمل في كفاءة المراجعين الداخليين، واستقلالية وظيفة المراجعة الداخلية.

يتميز هذا البحث بأنه لا يركز فقط على جودة مخرجات عمل المراجعين الداخليين بذاتها، بل على الجمع بين الكفاءة المناسبة والموقف أو العقلية الصحيحة (الاستقلالية) تجاه الإدارة العليا للمنشأة. يرتبط كلا المحددين بملف الشخص الذي يتم اختياره للقيام بالعمل، وبالتالي يعتبران معايير لمدخلات العمل التي تخص عملية المراجعة الداخلية في مجال الأمن السيبراني، وبالتالي تعزز من ضمان الامتثال للمعايير وإجراءات الأمن السيبراني. وقد قدمت عدد من الدراسات السابقة مجموعة من المؤشرات لقياس هذين المتغيرين لجودة وظيفة المراجعة الداخلية في مجال الأمن السيبراني.

فيما يتعلق بكفاءة المراجعين الداخليين، تتطلب المنظمات المهنية في مجال المراجعة الداخلية أن يمتلك المراجعون الداخليون المعرفة والمهارات والكفاءات اللازمة لأداء مهامهم الفردية. ويُشجع المراجعون الداخليون على إثبات كفاءتهم من خلال الحصول على الشهادات المهنية المناسبة، مثل شهادة المراجع الداخلي المعتمد (CIA) والشهادات الأخرى التي يقدمها معهد المراجعين الداخليين (IIA) أو منظمات مهنية أخرى (IIA, 2017).

وفي مجال الأمن السيبراني، تتطلب المراجعة معرفة متقدمة بتكنولوجيا المعلومات(IT)، ويجب أن يمتلك المراجعون الداخليون معرفة كافية بمخاطر تكنولوجيا المعلومات الأساسية وأنظمة التحكم، بالإضافة إلى تقنيات المراجعة المعتمدة على التكنولوجيا المتاحة لأداء مهامهم (IIA, 2017). وقد أشارت الدراسات إلى أهمية تطوير المهارات المهنية للمراجعين، مثل التدريب المستمر والحصول على الشهادات المهنية (Patton, 2005)، رغم أن هناك شعورًا عامًا بأن المزيد من العمل مطلوب في هذا المجال. كما يؤكد معهد حوكمة تكنولوجيا المعلومات (ITGI) على ضرورة أن يكون الأفراد المسؤولون عن تقييم أمن المعلومات على دراية بتقنيات المراجعة الخاصة بنظم المعلومات ومعايير الأمن المعلوماتي (ITGI, 2012)، وهو ما يشير إلى قيمة الشهادات المهنية في هذه المجالات.

وقد أوضحت دراسة Steinbart et al. (2013) أن مستوى المعرفة لدى المراجع الداخلي حول أمن المعلومات (والذي يُفهم بشكل محدد على أنه مجموعة المهارات الخاصة بالمدير التنفيذي للمراجعة CAE) هو محدد رئيسي لقدرته على النجاح في أداء دوره كمراقب ومستشار مستقل لبرنامج أمن المعلومات في المنشأة. وعندما يمتلك المراجعون الداخليون خبرة تقنية متعمقة في مجال أمن المعلومات، يمكنهم بناء علاقات أكثر تأثيرًا مع وظائف الأمن المعلوماتي، مما يساهم في بناء برنامج إدارة أمني أكثر فعالية.

ويمتلك المراجعون الداخليون المعرفة والكفاءة المهنية المتخصصة من خلال (1) الخلفية الأكاديمية (مثل تكنولوجيا المعلومات، علوم الحاسوب، نظم المعلومات)، (2) شهادات الأمن السيبراني[1]، و (3) التدريب الدوري لمواكبة التهديدات السيبرانية المتغيرة بسرعة وكيفية مواجهتها (Islam et al., 2018; Steinbart et al., 2012).

بناءً على ما سبق، يمكن الاستنتاج أن امتلاك المراجعين الداخليين للمعرفة والمهارات والكفاءات المتخصصة في مجال الأمن السيبراني يرتبط ارتباطًا وثيقًا بتحسين جودة عمليات المراجعة الداخلية المتعلقة بالامتثال لمعايير الأمن السيبراني، مما ينعكس إيجابًا على فعالية مؤشرات الرقابة، والكشف، والاستجابة، والمعالجة أو التصحيح لمخاطر الأمن السيبراني.

وفيما يتعلق باستقلالية وظيفة المراجعة الداخلية، تشير الدراسات السابقة إلى تنوع مؤشرات قياس استقلالية وظيفة المراجعة الداخلية المستخدمة في بحوث المراجعة الداخلية. وقد ركزت بعض الدراسات على مؤشر مدى الاستجابة والتعاقد الخارجي لتنفيذ مراجعة الأمن السيبراني كدليل على الاستقلالية، حيث يتم اللجوء إلى هذا الخيار في حالة عدم توفر الخبرة الكافية داخل إدارات المراجعة الداخلية في هذا المجال، ويتم التعاقد مع مستشارين خارجيين لتنفيذ عملية المراجعة أو جزء منها (Khan et al., 2020; Selim and Yiannakas, 2000). ويضيف كل من Brand (2010) و Abbott et al. (2007) أن المستشارين الخارجيين يميلون إلى أن يكونوا أكثر استقلالية من الموظفين الداخليين عند تنفيذ مهام المراجعة الداخلية.

كما تم استخدام العلاقة بين وظيفة المراجعة الداخلية ومجلس الإدارة ولجنة المراجعة كمؤشرات بديلة للاستقلالية، حيث يُعتبر المراجع الداخلي أكثر استقلالية في نظر المراجعين الخارجيين إذا كانت هذه الوظيفة تحت السلطة المباشرة للجنة المراجعة (Desai et al., 2010,2011; Glover et al., 2008; Gramling and Vandervelde, 2006). وتؤثر لجنة المراجعة بشكل كبير على وظيفة المراجعة الداخلية، حيث يقوم المديرون التنفيذيون للمراجعة (CAE) بتقديم تقاريرهم إلى لجنة المراجعة، كما أن نطاق عمل المراجعين الداخليين يتقيد بمسؤوليات اللجنة (Barua et al., 2010).

ومن الضروري أن تلعب وظيفة المراجعة الداخلية دورًا مركزيًا في مساعدة لجنة المراجعة على الإشراف على الأمن السيبراني، حيث يُتوقع من المراجعين الداخليين وضع خارطة طريق تتعامل مع قضايا

[1]. توجد العديد من الشهادات المهنية في مجال الأمن السيبراني مثل: شهادة مدير تنفيذي للمراجعة (CAEs) في مجال الأمن السيبراني (CDP, CSP, CISM)، وشهادة مراجعة نظم المعلومات (مثل: QICA, CISA, CRISC).

المخاطر السيبرانية المختلفة (Deloitte, 2015a). فيما يتعلق بالأمن السيبراني، يمكن لوظيفة المراجعة الداخلية أن تقدم منظورًا موضوعيًا إلى لجنة المراجعة وأعضاء مجلس الإدارة الآخرين، وبالتالي تستخدم هذه النتائج لتطوير خطة تدقيق داخلية شاملة تغطي مجالات المخاطر المتعلقة بإدارة التهديدات السيبرانية التي تواجه المنشأة (Deloitte, 2017).

ومن بين التهديدات التي تهدد استقلالية وظيفة المراجعة الداخلية، فقد حددت دراسة Christopher et al. (2009) تلك المتعلقة بموافقة مجلس الإدارة على الميزانية والموارد المخصصة لمراجعة عمليات الأمن السيبراني، حيث توصي أفضل الممارسات بأن تقوم لجنة المراجعة بهذا الدور بدلاً من مجلس الإدارة.

في ضوء ما تقدم، يمكن الاستنتاج أن انخفاض مستوى استقلالية لجنة المراجعة عن مجلس الإدارة يؤدي إلى تصاعد التهديدات التي قد تمس استقلالية وظيفة المراجعة الداخلية في علاقتها مع المجلس. وعلاوة على ذلك، فإن افتقار لجنة المراجعة إلى الكفاءة المطلوبة في توجيه اهتمام المراجعين الداخليين نحو أبرز مخاطر الأمن السيبراني، يمنح مجلس الإدارة مساحة أوسع للتأثير على عمل المراجعة الداخلية، مما يُضعف من استقلالية هذه الوظيفة الحيوية.

بناء على ما سبق، فأنه يمكن اشتقاق الفرض الأول للبحث:

الفرض الأول (H1): تؤثر جودة وظيفة المراجعة الداخلية المبنية على منهج المدخلات تأثيرًا إيجابيًا على تحسين مؤشرات إدارة مخاطر الأمن السيبراني.

7-2-2 هيكل حوكمة الأمن السيبراني (خطوط المساءلة الخمس) وأثره على تحسين مؤشرات مخاطر الأمن السيبراني

توصي مبادئ إدارة المخاطر السليمة بأن يتم تنظيم إدارة مخاطر الأمن السيبراني وفقًا لثلاث خطوط للمساءلة (COSO, 2017; IIA, 2013, 2020). يمثل مديرو تقنية المعلومات (IT) في الخط الأول للمساءلة، حيث يعتبرون مخاطر الأمن السيبراني جزءًا أساسيًا من أعمالهم، ويقومون بإنشاء الهياكل والضوابط المناسبة لإدارة هذه المخاطر. أما الخط الثاني للمساءلة فيتمثل في وظيفة أمن المعلومات، التي توفر الخبرة اللازمة لتنفيذ ومراقبة فعالية الأمن السيبراني. في حين أن الخط الثالث هو وظيفة المراجعة الداخلية التي تقدم لمجلس الإدارة ولجان المراجعة ولجان المخاطر التابعة له ضمانًا مستقلاً بأن استراتيجية وسياسات وإجراءات وضوابط إدارة مخاطر الأمن السيبراني فعالة (Deloitte, 2017; IIA, 2020). يتضمن ذلك مراجعة كفاية الأعمال التي قامت بها خطوط المساءلة الأول والثاني. ونظرًا لخصوصية

مراجعة الأمن السيبراني، يجب على وظيفة المراجعة الداخلية أن تأخذ في اعتبارها أطر الأمن السيبراني[2] لضمان اتساق المعايير والمصطلحات عبر خطوط المساءلة الثلاث، بالإضافة إلى الإرشادات المهنية وأفضل الممارسات.

وتوفر أطر إدارة الأمن السيبراني وتكنولوجيا المعلومات خرائط منهجية للعمليات التي يتبعها الخط الأول والثاني، والتي من المفترض أن يقوم المراجعون الداخليون (الخط الثالث) بمراجعتها وتقديم التأكيدات حولها. وتقدم المنشورات المهنية حول مراجعة تكنولوجيا المعلومات وإدارة المخاطر مزيدًا من الإرشادات حول خصائص مراجعة الأمن السيبراني وأفضل الممارسات (مثل IT Governance Institute, 2007a: 2007b; IIA, 2020; Deloitte, 2017).

علاوة على ذلك، تم تطوير العديد من الأطر الأخرى التي تلبي احتياجات صناعات محددة أو أغراض خاصة. كما قد تلجأ بعض المنشآت إلى تصميم أطر مخصصة تتوافق مع طبيعة أعمالها، ومستوى شهيتها للمخاطر، وما تمتلكه من موارد. وتسهم هذه الأطر في تحديد المعايير التي يُبنى عليها برنامج المراجعة الداخلية ويُوجَّه بموجبها.

تعمل الأطر على تحديد مجموعة من العمليات المرتبطة بالأنشطة التشغيلية الرئيسة، إلى جانب أهداف الحوكمة ومؤشرات الأداء، كما تتضمن نموذجًا أوليًا للنضج يُستخدم لتقييم مستوى الامتثال وتحديد المسؤوليات الإدارية بوضوح(De Haes and Van Grembergen 2015). وتعتمد هذه الأطر على منطق مفاده أن المنشأة بحاجة إلى استعادة قدرتها على العمل بعد الهجمات السيبرانية، وتشمل عادةً العمليات في أربع مجالات رئيسية: الوقاية، والاكتشاف، والاستجابة، والعلاج/التصحيح. ورغم أن الدور التقليدي لوظيفة المراجعة الداخلية كان يركز بشكل أساسي على الوقاية، إلا أن نطاق مراجعة الأمن السيبراني يجب أن يشمل الضوابط والعمليات في جميع المجالات الأربعة.

بالإضافة إلى ذلك، يجب أن تتضمن الأطر أيضًا المتطلبات القانونية والتنظيمية الوطنية والصناعية، بحيث يمكنها تلبية الأهداف المختلفة للمنشآت وتلبية احتياجات أصحاب المصلحة. ومن أهم احتياجات أصحاب المصلحة (مثل مجلس الإدارة) هي فهم كيفية مقارنة عمليات الأمن السيبراني في المنشأة

[2]. توجد ثلاث أطر رئيسية في المجال المهني للأمن السيبراني:

- أهداف التحكم في تكنولوجيا المعلومات والتقنيات ذات الصلة (COBIT 5) (ISACA, 2012a, 2012b)
- معايير الأمن السيبراني الصادرة من المنظمة الدولية للتوحيد والقياس (ISO 27001/2)
- المعايير الصادرة عن المعهد الوطني للمعايير والتكنولوجيا في الولايات المتحدة (NIST,2018)

بالممارسات الجيدة ومدى توافقها مع الأطر المعتمدة. ويتم قياس ذلك من خلال نضج إدارة مخاطر الأمن السيبراني. وتستخدم نماذج النضج كأداة لقياس مدى تنفيذ المنشآت لإدارة مخاطر الأمن السيبراني بشكل منهجي. عادةً ما يتم التقييم الذي يتم تقديمه من مراجع خارجي مستقل بناءً على منهجية تقيم المنشأة بأكملها على مقياس من: (0) غير موجود، (1) عشوائي، (2) قابل للتكرار ولكن بديهي، (3) محدد، (4) مدار وقابل للقياس، (5) محسن، كما هو محدد في(ISACA,2012a, 2012b, COBIT 5). وكلما زادت درجة النضج، زادت فعالية إدارة المخاطر وحوكمة الأمن السيبراني(Steinbart et al., 2013) .

في النهاية، تقع مسؤولية نضج إدارة مخاطر الأمن السيبراني على عاتق الإدارة. وتقدم وظيفة المراجعة الداخلية ملاحظات وتوصيات، والتي إذا تم تنفيذها ستؤدي إلى مستوى أعلى من النضج، مثل تحسين إمكانية تتبع العمليات، وقابلية قياس النجاح من خلال مؤشرات المخاطر والأداء الرئيسية، وتحديد الأدوار بوضوح (IIA, 2020).

استنادًا إلى ما سبق، يقترح الباحث الفرض التالي الذي يتناول أثر هيكل حوكمة الأمن السيبراني، المتمثل في خطوط المساءلة الثلاث، على تحسين نتائج مؤشرات إدارة مخاطر الأمن السيبراني.

الفرض الثاني (أ) (H2a): يساهم وجود هيكل حوكمة سيبراني مبني على نموذج خطوط المساءلة الثلاث ومستند إلى أحد أطر الأمن السيبراني المهنية في تحسين مؤشرات إدارة مخاطر الأمن السيبراني بالمقارنة بالمنشآت التي تفتقر إلى هيكل واضح للحوكمة السيبرانية.

وفيما يتعلق بتأثير المشاركة الفعالة لكل من الإدارة التنفيذية ومجلس الإدارة (الخط الرابع والخامس للمساءلة) على تحسين نتائج مؤشرات مخاطر الأمن السيبراني، تشير الأدلة إلى تأثير إيجابي بالغالب للمديرين التنفيذيين ذوي الخبرة في تكنولوجيا المعلومات على حوادث الاختراق السيبراني. حيث تشير معظم الأبحاث السابقة إلى أن وجود مديرين تنفيذيين (مثل الرئيس التنفيذي، المدير المالي، والمدير التنفيذي لتكنولوجيا المعلومات) لديهم خبرة في تكنولوجيا المعلومات أو مسؤول تنفيذي لتكنولوجيا المعلومات في مجلس الإدارة يقلل بشكل كبير من حوادث اختراق البيانات التي يجب الإبلاغ عنها (Feng and Wang, 2019; Haislip et al., 2016, 2020, 2021; Vincent et al., 2019; Smith et al.,2021). ومع ذلك، وجدت دراسة (Haislip et al., 2021) أن وجود رئيس تنفيذي بخبرة في تكنولوجيا المعلومات قد يؤدي إلى زيادة في حوادث الاختراق السيبراني، ويُعزى ذلك إلى أنهم أكثر عرضة لاكتشاف وإبلاغ هذه الحوادث.

إلا أن عددًا قليلاً من الدراسات حول حوكمة الأمن السيبراني لم يقدم أدلة حاسمة حول دور مجلس الإدارة، نظرًا لعدم وجود مقاييس مباشرة وقابلة للملاحظة حول دور مجلس الإدارة. وعلى الرغم من ذلك،

هناك مؤشر غير مباشر على مشاركة مجلس الإدارة يتمثل في المستوى الذي يتم فيه معالجة قضايا حوكمة تكنولوجيا المعلومات داخل المنشأة. فقد وجد Wang et al., (2013) أن المنشآت التي تضم مسؤولاً تنفيذيًا في تكنولوجيا المعلومات ضمن فريق الإدارة العليا تكون أقل عرضة للإبلاغ عن خروقات أمنية. كما وجدوا ارتباطًا سلبيًا بين تعويضات مسؤولي تكنولوجيا المعلومات واحتمالية حدوث اختراقات أمنية. بينما وجد Higgs et al. (2016) أن الإفصاح عن الخروقات الأمنية مرتبط عكسيًا مع المدة التي كان لدى مجلس إدارة الشركة فيها لجنة تقنية. وبالتالي، تدعم كلا الدراستين فكرة وجود ارتباط بين مشاركة مجلس الإدارة وتحسن نتائج الأمن المعلوماتي.

يُعد وجود الإفصاحات المتعلقة بالأمن المعلوماتي وطبيعتها في التقرير السنوي للشركة مؤشرًا إضافيًا يعكس مدى دعم مجلس الإدارة لدوره في الإشراف على قضايا الأمن السيبراني. حيث وجدت دراسة Li (2015) ارتباطًا إيجابيًا بين إفصاح الشركات الصينية عن محتوى متعلق بالأمن في تقاريرها السنوية وجودة إجراءاتها الأمنية عبر الإنترنت. وفي هذا السياق وجدت دراسة Wang et al., (2013) أن المنشآت التي تبلغ عن اتخاذها خطوات استباقية لإدارة المخاطر السيبرانية تكون أقل عرضة للإفصاح عن خروقات أمنية مقارنةً بالشركات التي لا تبلغ عن إجراءات نشطة لتخفيف المخاطر السيبرانية.

وفي الممارسة العملية، توجد فجوات أو تداخلات بين الخطوط الأول والثاني والثالث (Soomro et al., 2016). إضافة إلى ذلك، هناك انفصال كبير حاليًا بين المعلومات المقدمة من مستويات العمليات التقنية وفهم مجلس الإدارة والمديرين التنفيذيين لهذه المعلومات (Gale et al., 2022). يثير هذا الانفصال مصدر قلق، إذ قد يترتب عليه ضعف في أداء الوحدات التنظيمية لأدوارها ضمن خطوط المساءلة، مما يؤدي إلى غياب التكامل والانسجام بين تلك الخطوط بالشكل المطلوب.

علاوة على ذلك، تفتقر الخطوط الرابعة والخامسة (الإدارة ومجلس الإدارة) إلى الكفاءات الكافية، وغالبًا ما تجد صعوبة في فهم تقارير الأمن السيبراني، مما يؤدي إلى ضعف في المساءلة وبالتالي ضعف في الحوكمة السيبرانية الفعالة (NASDAD and Tanium, 2016; McKinsey Global Survey, 2018).

يُعد خطر الاختراقات الأمنية وما قد يترتب عليها من أضرار مصدر قلق متنامٍ لدى غالبية الشركات، الأمر الذي جعلها تحظى باهتمام متزايد من قبل مجالس الإدارة (Gregory and Austin, 2014). وأظهر مسح حديث لأكثر من 250 عضوًا في مجلس الإدارة أن الأمن السيبراني يعد مصدر قلق متزايدًا، بل ويتجاوز أحيانًا مخاطر الامتثال التنظيمي. فقد أشار نحو 74% من أعضاء مجلس الإدارة إلى أن الرؤساء التنفيذيين لديهم فهم قوي للتحديات المتعلقة بالامتثال التنظيمي، بينما قال نصفهم فقط (51%) إن

رؤساءهم التنفيذيين يمتلكون فهمًا جيدًا لمواضيع الأمن السيبراني (Tysiac, 2014). وعند دراسة ما إذا كانت أدوار المسؤولين التنفيذيين ونظم التعويضات مرتبطة بحدوث الاختراقات الأمنية، لوحظ أن الاختراقات الأمنية أقل شيوعًا عندما يكون المسؤولون التنفيذيون لتقنية المعلومات مشاركين أكثر في فريق القيادة ويتم تعويضهم بناءً على سلوكياتهم وليس فقط على النتائج (Kwon et al., 2013). لذلك، من المنطقي توقع أن يكون لمشاركة الإدارة السيبرانية على مستوى مجلس الإدارة تأثير على عنصر الأمن السيبراني ضمن المخاطر التكنولوجية (Higgs et al., 2016; Steinbart et al., 2013).

ويُعتبر مجلس إدارة الشركات الذي يتفاعل بجدية مع قضايا الأمن السيبراني عنصرًا أساسيًا لتحقيق إجراءات أمن سيبراني قوية. وقد أشارت دراسة (2015) Protiviti إلى أن العامل المشترك بين المنشآت التي لديها أطر حوكمة للأمن السيبراني قوية هو مجلس إدارة مشارك يتمتع بفهم حقيقي للقضايا الأمنية والخصوصية .وقد وجدت دراسة (2019) .Vincent et al تأثيرًا إيجابيًا لمشاركة مجلس الإدارة وخبرته في تكنولوجيا المعلومات على مستوى نضج إدارة المخاطر السيبرانية. بناءً على ذلك، يُعد وجود خبرة متخصصة في الأمن السيبراني ضمن مجلس الإدارة شرطًا أساسيًا لضمان فعالية برنامج إدارة الأمن السيبراني. وعلى الرغم من أن العديد من المنشآت تكلف لجنة المراجعة بمهام الأمن السيبراني، إلا أن الشركات التي تشكل التقنية العمود الفقري لأعمالها غالبًا ما يكون لديها لجنة مخصصة لإدارة المخاطر السيبرانية تركز بشكل حصري على الأمن السيبراني وقضايا إدارة المخاطر الأخرى. مع ذلك، تُعتبر اللجان المتخصصة في إدارة المخاطر أمرًا نادرًا في القطاعات غير المالية (KPMG, 2014).

بناءً على ما سبق، يمكن استنتاج أن المشاركة الفعّالة للإدارة التنفيذية ضمن مجلس الإدارة تُسهم بشكل جوهري في تعزيز وتحسين نتائج مؤشرات مخاطر الأمن السيبراني.

الفرض الثاني (ب) (H2b): تؤثر المشاركة الفعالة للإدارة التنفيذية في مجلس الإدارة بشكل إيجابي على تحسين مؤشرات إدارة مخاطر الأمن السيبراني.

7-2-3 التأثير المشترك للتعاون بين محددات جودة وظيفة المراجعة الداخلية وهيكل المساءلة للحوكمة السيبراني على تحسين مؤشرات مخاطر الأمن السيبراني

تختبر المجموعة الثالثة من الفروض التأثير المشترك للتعاون بين محددات جودة وظيفة المراجعة الداخلية وهيكل الحوكمة السيبراني (خطوط المساءلة الخمسة)على نتائج مؤشرات مخاطر الأمن السيبراني، حيث تتحمل خطوط المساءلة الخمسة أدوارًا متعددة في المسؤولية عن إدارة المخاطر السيبرانية، والتي تعد الهدف النهائي للمراجعة الداخلية للأمن السيبراني. ويوضح (2020) .Yoo et al أن فعالية الأمن

السيبراني هي جهد جماعي، وأن فعالية خطوط المساءلة الخمسة يتم تعزيزها من خلال الكفاءة الجماعية للخطوط المساءلة وتنسيق المعرفة الأمنية. في هذا السياق، يكون لجودة وظيفة المراجعة الداخلية تأثير إيجابي على تحسين نتائج مؤشرات إدارة مخاطر الأمن السيبراني إذا كانت تمثل حلقة وصل فعالة بين مجلس الإدارة والمديرين التنفيذيين (الخط الرابع والخامس) من جهة، ومديري تقنية المعلومات وأمن المعلومات (الخط الأول والثاني) من جهة أخرى.

فيما يتعلق بالتأثير المشترك للعلاقة بين جودة وظيفة المراجعة الداخلية وخطوط المساءلة الأول والثاني، قدمت(2013) Halvelka and Merhout نموذجًا شاملاً للعوامل المؤثرة في جودة وظيفة المراجعة الداخلية، بناءً على مراجعة شاملة للأدبيات العلمية ومقابلات مفصلة مع مراجعي تكنولوجيا المعلومات الداخليين. يعد أحد المكونات الأساسية في نموذجهم هو تأثير طبيعة العلاقة بين وظيفة المراجعة الداخلية وخطوط المساءلة الأولى والثانية (التي يطلقون عليها بيئة المؤسسة)، لا سيما العلاقة مع العميل الخاضع للمراجعة، على جودة أداء المراجعة الداخلية، وبشكل خاص على قدرة هذه الوظيفة في تقديم توصيات تسهم في تحسين العمليات. وقد أوضحت نتائج الدراسة بأن العلاقات الجيدة بين وظيفة المراجعة الداخلية وخطوط المساءلة الأول والثاني تعزز كفاءة المراجعة وفعاليتها، حيث تزيد من الوصول إلى الأدلة وتزيد من شفافية وصراحة الوحدات التنظيمية في تواصلها مع وظيفة المراجعة الداخلية. وتتسق تلك النتائج مع ما جاء في الأدبيات المهنية التي تشير إلى أن العلاقة الجيدة مع العميل تسهم في تحسين وصول المراجع إلى الأدلة، وخاصة الأدلة "الناعمة" المتعلقة بالمواقف والسلوكيات (Dittenhofer, 1997).

وتتوافق نتائج الأبحاث الميدانية مع هذه الافتراضات. فعلى سبيل المثال، ذكر أحد المشاركين في دراسة(2012) .Steinbart et al أن "في العديد من الأماكن التي زرتها، كان الأمر يشبه لعبة القط والفأر، حيث يحاول المراجعون ضبط تكنولوجيا المعلومات في موقف غير صحيح، بينما تحاول تكنولوجيا المعلومات منع المراجع من اكتشاف ذلك" (ص. 235). وذكر المشارك أيضًا أن التعاون بين وظيفة المراجعة الداخلية وخطوط المساءلة الأول والثاني يساهم في تحديد المخاطر، وتقليلها، ومعالجة المشاكل التي يتم اكتشافها.

وبناءً على ذلك، فقد وجدت دراسة (2014) Fanning and Piercey أن قبول المديرين لتوصيات المراجعة الداخلية الجيدة الصياغة يزداد عندما يتمتع المراجع بعلاقة ودية معهم. في المقابل، وجدت دراسة (2015) Roussy أن المراجعين الداخليين الذين يواجهون صراعًا في الأدوار مع خطوط المساءلة الأول

والثاني يتبنون سلوكيات تأقلم تؤثر سلبًا على استقلاليتهم، مما يؤثر بدوره سلبًا على قدرتهم على تنفيذ المراجعة بنجاح واكتشاف وتطوير وتوصيل نتائج المراجعة.

وبالتالي، يجب أن تسهل العلاقة الجيدة بين وظيفة المراجعة الداخلية وخطوط المساءلة الأول والثاني قدرة وظيفة المراجعة الداخلية على تحديد قضايا الأمن واقتراح طرق لمعالجتها. ويطلق على هذا "تأثير الكشف التعاوني". وقد أظهرت الدراسات السابقة أن إدارة المخاطر السيبرانية يمكن تعزيزها بشكل كبير إذا تعاونت وظيفة المراجعة الداخلية مع خبراء الأمن (Bantleon et al., 2020; Kahyaoglu and Çaliyurt, 2018; Steinbart et al., 2012, 2013, 2018). حيث يستفيد المراجعون الداخليون عند الاعتماد على الخطين الأول والثاني لفهم البنية التحتية للأمن السيبراني المتغيرة باستمرار أو لتحديد وتقييم المخاطر السيبرانية. من ناحية أخرى، يستفيد خبراء الأمن من خبرة المراجعين في ربط المخاطر السيبرانية بالعمليات الحيوية وتأثيرها على الأعمال. وقد وُجدت Steinbart et al. (2018) أن هذا التعاون له تأثير على نقاط الضعف المكتشفة في الضوابط، وحالات عدم الامتثال، والحوادث الأمنية المكتشفة. وتوجد أدلة ميدانية على أن التعاون بين وظيفة المراجعة الداخلية وإدارة العمليات الخاضعة للمراجعة يحسن من جودة عمليات إدارة المخاطر (Arena et al., 2010) ، ويزيد من احتمالية قبول المديرين لتوصيات المراجعة وتطبيقها (Arena and Azzone, 2009)، ويحسن بشكل غير مباشر من كفاءة الوحدات من خلال تسهيل تعلم المراجعين من عمليات المراجعة (Ma'ayan and Carmeli, 2016).

ومع ذلك، فإن العلاقة الجيدة بين وظيفة المراجعة الداخلية وخطوط المساءلة الأولى والثانية لا تقتصر على تحقيق هذه النتيجة الإيجابية فقط. ميزة أخرى محتملة للعلاقة الجيدة بين وظيفة المراجعة الداخلية وخطوط المساءلة الأول والثاني هي أنها يمكن أن تؤدي إلى نقل "المعرفة"، حيث يستخدم خط المساءلة الأول والثاني نصائح من وظيفة المراجعة الداخلية لتحسين تصميم وعمل الضوابط الأمنية. وقد أشار Halvelka and Merhout (2013, P. 178) إلى ذلك بالقول: "من المعقول افتراض أن النظام أو العملية قد يتم تحسينها أو تغييرها بناءً على نتائج مراجعة تكنولوجيا المعلومات". أيضاً، أفادت دراسة Steinbart et al. (2012) أن قدرة المراجع الداخلي على رؤية القضايا الأمنية من منظور عمليات الأعمال أثرت على فهم مدير الأمن المعلوماتي (الخط الثاني) لكيفية تحقيق فصل الواجبات بفعالية. وقد ساعد الحوار بين مدير الأمن والمراجع الداخلي في تحسين فهم المدير لهذه القضية وأدى إلى تحسين الضوابط على حقوق الوصول والأذونات.

ويحدث نقل المعرفة عندما تعتبر الوحدات المختلفة داخل نفس المنشأة أنها تشترك في مجموعة مشتركة من القيم أو تتشارك نفس التركيز أو الهدف (Morris and Empson, 1998). في مثل هذه الحالات، تكون الوحدة المستقبلة على استعداد لبذل المزيد من الوقت والجهد لتقييم مزايا المعرفة التي تمتلكها الوحدة الأخرى. وفى هذا الإطار وجد Bauer and Estep (2018) أن فعالية المراجعة تحسنت عندما كانت هناك علاقة جيدة بين المراجعين الماليين ومراجعي تكنولوجيا المعلومات في الشركات الكبرى، حيث أدى تبادل المعرفة إلى كشف وحل قضايا المراجعة بوقت أسرع.

من جانب أخر، لا تنظر المجموعات دائمًا إلى وجود هدف مشترك فقط لأن هناك علاقة رسمية تجمعها. فكل من الخط الأول و/أو الخط الثاني (وظيفة تقنية المعلومات، ووظيفة أمن المعلومات) والخط الثالث (وظيفة المراجعة الداخلية) لديهم أدوار وأهداف مختلفة، والتي قد تُعتبر متعارضة بسبب حاجة المراجعة الداخلية للاستقلالية. لذلك، من المعقول توقع أن تتفاوت جودة العلاقات بين وظائف المراجعة الداخلية ووظائف الأمن المعلوماتي من منشأة إلى أخرى، وأن تعكس هذه الاختلافات في مؤشرات نتائج الأمن المختلفة.

فإذا كانت مراجعة الأمن السيبراني تساهم في تعزيز فعالية الخطين الأول والثاني، فمن المفترض أن يزيد ذلك من احتمالية إدارة مخاطر الأمن السيبراني والضوابط بشكل فعال، مما يقلل في النهاية من احتمالية الهجمات السيبرانية (Boehm et al., 2019). ومع ذلك، بالنظر إلى أن عدد الهجمات السيبرانية التدميرية في تزايد رغم الجهود المتزايدة في الصناعة وتحسين الممارسات (EY, 2019)، ولا يمكن ضمان النجاح في منع الهجمات السيبرانية الناجحة (Deloitte, 2017). فالصناعات التي تستثمر أعلى الموارد في تطوير جميع خطوط المساءلة الثلاث في إدارة مخاطر الأمن السيبراني هي أيضًا الأكثر تعرضًا للهجمات، مثل الصناعات الدفاعية، والخدمات المالية، وشركات الطاقة والمرافق، والبنية التحتية الحرجة (Karabacak et al., 2016).

بناء على ذلك، فأنه يمكن اشتقاق تأثير العلاقة بين جودة وظيفة المراجعة الداخلية بناء على منهج المدخلات، ونموذج خطوط المساءلة الثلاث من خلال الفرض التالي:

الفرض الثالث (أ) (H3a): يؤثر التفاعل بين جودة وظيفة المراجعة الداخلية، بناء على منهج المدخلات، وتطبيق نموذج خطوط المساءلة الثلاث بشكل إيجابي على تحسين مؤشرات إدارة مخاطر الأمن السيبراني.

على الجانب الآخر، وفيما يتعلق بالتأثير المشترك للعلاقة بين جودة وظيفة المراجعة الداخلية وخطوط المساءلة الرابع والخامس (المديرين التنفيذيين ومجلس الإدارة)، فقد أوضحت عدد من الدراسات أن

مستوى دعم مجلس الإدارة (الخط الخامس) للأمن المعلوماتي قد يكون له تأثير إيجابي (مباشر وغير مباشر) على العلاقة بين وظيفة المراجعة الداخلية وخطوط المساءلة الأول والثاني (وظائف الأمن المعلوماتي).

يحدث التأثير المباشر من خلال تشجيع مجلس الإدارة على إقامة علاقة تعاونية بين وظيفة المراجعة الداخلية ووظائف الأمن المعلوماتي. وفي هذا السياق، وجدت دراسة Sarens and De Beedle لا (2006) أنه في المنشآت التي تعطي فيها مجلس الإدارة الأولوية لإدارة المخاطر وتحسين الرقابة الداخلية، تعمل الإدارة على تعزيز قبول وتقدير جودة وظيفة المراجعة الداخلية. وبالمثل، أوضح .Arena et al (2010) أنه في إحدى المنشآت التي دعمت فيها مجلس الإدارة بشدة أنشطة إدارة المخاطر المؤسسية (ERM)، عمل فريق المراجعة الداخلية ومسؤول المخاطر الرئيسي معًا على إدارة المخاطر المؤسسية.

ويحدث التأثير غير المباشر من خلال تشجيع وتمكين زيادة الانتباه إلى قضايا الأمن السيبراني في عمليات المراجعة. بالرغم من تمتع المدير التنفيذي للمراجعة باستقلالية عن الإدارة، إلا أن معايير المراجعة الداخلية تؤكد ضرورة أن يأخذ في الاعتبار مداخلات مجلس الإدارة المتعلقة بالمخاطر التي تواجه المنشأة عند التخطيط لأنشطة المراجعة الداخلية(IIA, 2013) .

وبالفعل، أدرك مديرو الأمن المعلوماتي الذين تمت مقابلتهم من قبل (2012) .Steinbart et al أن مستوى الموارد التي يكرسها وظيفة المراجعة الداخلية لقضايا الأمن المعلوماتي يعتمد بشكل كبير على اهتمام مجلس الإدارة في هذا المجال. يعتبر توفير مجلس الإدارة لهذه الموارد أمرًا مهمًا، نظرًا لأن موظفي الأمن المعلوماتي يرون أن مستوى معرفة المراجعة الداخلية بالأمن المعلوماتي وتكرار المراجعة لوظيفة المراجعة الداخلية لهما تأثير إيجابي على جودة العلاقة بين الوظيفتين.

أخيرًا، من المحتمل أن يزيد دعم مجلس الإدارة للأمن المعلوماتي وأهميته كهدف تنظيمي شامل من التصورات لدى وظائف المراجعة الداخلية والأمن المعلوماتي بأنهما يشتركان في هدف مشترك وهو تحسين نتائج مؤشرات مخاطر الأمن السيبراني، مما يؤدي بدوره إلى تحسين العلاقات بين هذه الوحدات التنظيمية. وقد أشار (2022) .Slapnicar et al إلى أن جودة وظيفة المراجعة الداخلية يكون لها تأثير إيجابي على نضج إدارة مخاطر الأمن السيبراني إذا كانت تمثل حلقة وصل حاسمة في التواصل بين خطوط المساءلة الرابع والخامس (مجلس الإدارة والمديرين التنفيذيين). ويتحقق ذلك إذا أدركت وظيفة المراجعة الداخلية توقعات مجلس الإدارة والمديرين التنفيذيين، وتحققت من مما إذا كان مديرو تقنية المعلومات وأمن المعلومات يلبون هذه التوقعات، وقدمت معلومات إلى مجلس الإدارة حول مجالات الأمن السيبراني التي تحتاج إلى موارد وظيفة المراجعة الداخلية، وأخيرًا، تم تنفيذ توصيات المراجعة الداخلية.

بناء على ذلك، فأنه يمكن اشتقاق تأثير العلاقة بين جودة وظيفة المراجعة الداخلية بناء على منهج المدخلات، والهيكل المتكامل للحوكمة السيبراني من خلال الفرض التالي:

الفرض الثالث (ب) (H3b): يساهم التفاعل بين جودة وظيفة المراجعة الداخلية المبنية على منهج المدخلات، وتطبيق هيكل حوكمة متكامل للحوكمة السيبرانية (نموذج خطوط المساءلة الخمسة) في تحسين مؤشرات إدارة مخاطر الأمن السيبراني مقارنة بالمنشآت التي تطبق نموذج خطوط المساءلة الثلاث فقط.

7-3 منهجية البحث

7-3-1 نموذج البحث وقياس متغيرات البحث

بناء على مراجعة الدراسات السابقة واشتقاق فروض البحث، فأن نموذج البحث يتضح من الشكل (1).
بناء على نموذج البحث الموضح في الشكل (1) يتضح ما يلي:

1. جميع المتغيرات الكامنة Latent variables في النموذج (X1, X2, Y) تتبع نموذجاً تكوينياً Formative model، وذلك للأسباب التالية:

- المؤشرات تكون المتغير الكامن، وليس انعكاساً له.
- إزالة أي مؤشر تؤثر على المعني الكلي للمتغير الكامن، بمعني أنه إذا اختفت الكفاءة أو الاستقلالية، فأن مفهوم جودة وظيفة المراجعة الداخلية على أساس منهج المدخلات سيتغير. أيضاً، إزالة أحد المؤشرات مثل دعم الإدارة التنفيذية، سيغير تعريف الهيكل المتكامل للحوكمة، وإذا تم إزالة مرحلة الاستجابة، فلن تكون هناك قدرة على التعامل مع الحوادث، مما يعني تغيير معني المتغير الكامن، وهو إدارة المخاطر السيبرانية.
- المؤشرات ليست بالضرورة مرتبطة إحصائياً، بل كل منها يضيف بعداً جديد للمتغير الكامن، حيث يمكن أن تكون الاستقلالية عالية، والكفاءة منخفضة أو العكس، المتغيرات التي تشكل الهيكل المتكامل للحوكمة السيبراني تساهم في تشكيل الهيكل العام، ولكنها ليست بالضرورة مترابطة إحصائياً.

2. يعكس النموذج بنية تكوينية هرمية من الدرجة الثالثة Third-Order Formative Model حيث يتكون النموذج من مستويات متعددة من التكوين، مما يعني أن (X1, X2, Y) تتكون من متغيرات وسيطة متعددة تتألف من مكونات تفصيلية على المستوي الأدنى، كما يتضح من الشكل (1).

وقد تم استخدام النماذج الهيكلية القائمة على المربعات الصغرى PLS-SEM، وهي تستخدم لتقدير النماذج السببية، خاصة في الحالات التي تكون فيها البيانات معقدة أو صغيرة الحجم، أو عندما تكون

الأهداف تركز على التنبؤ بدلاً من اختبار النظريات. بالإضافة إلى ذلك، أن النماذج الهيكلية القائمة علي المربعات الصغري PLS-SEM يدعم النماذج التكوينية Formative models، حيث تكون المتغيرات الظاهرة هي التي تحدد المتغيرات الكامنة، كما أنه يدعم تحليل النماذج الهيكلية المعقدة التي تحتوي على علاقات سببية متعددة بين المتغيرات.

تم بناء نموذج البحث على ثلاثة أنواع من المتغيرات، هي :المتغيرات المستقلة، المتغير التابع، والمتغيرات الرقابية. وقد تم اعتماد أسلوب هرمي في تصنيف المتغيرات (درجة أولى، وثانية، وثالثة)، مما يتيح فهماً دقيقاً لمكونات كل متغير وطريقة قياسه، كما يتضح من الجدول (1). فيما يلي توضيح منهجي لكيفية قياس كل من هذه المتغيرات:

- المتغيرات المستقلة

1 . جودة المراجعة الداخلية على أساس منهج المدخلات(X1): تُقاس عبر بعدين رئيسيين:

- الكفاءة(X11)، ويتفرع عنها ثلاثة مؤشرات فرعية: الشهادات المهنية، والخلفية الأكاديمية، والتدريب والتطوير المستمر. وقد أعتمد البحث على دراسة كل من Steinbart et al. (2018) Islam et al. (2012) في تحديد المؤشرات الفرعية المرتبطة بالمتغير، وقد تم قياس هذه المؤشرات باستخدام مقياس ليكرت الخماسي، وقد تم احتساب متوسط الاستجابات لكل مشارك على مستوى كل مؤشر.

- الاستقلالية(X12) ، وتضم مؤشرين فرعيين: الاستعانة بمستشارين والتعاقد الخارجي، والارتباط مع لجنة المراجعة والإدارة. وقد أستند البحث إلى دراسات كل من Khan et al. (2020); Selim and Yiannakas (2000); Desai et al. (2011) في تحديد المؤشرات الفرعية للمتغير. وقد تم استخدام مقياس ثنائي، حيث تم جمع درجات عناصر القياس لتكوين المؤشر الإجمالي.

2 . الهيكل المتكامل للحوكمة السيبرانية(X2): يشمل بُعدين فرعيين:

- هيكل الحوكمة السيبرانية بناءً على خطوط المساءلة الثلاث (X21) ويقيس فعالية أداء كل من الخط الأول والثاني والثالث للمساءلة، بالإضافة إلى جودة التعاون فيما بينها. تم الاعتماد على مقياس ليكرت الخماسي، وحساب متوسط الاستجابات لكل مؤشر.

- دعم الإدارة التنفيذية ومجلس الإدارة(X22) والذي يشمل خطي المساءلة الرابع والخامس، ويقيس مدى دعم القيادة العليا لحوكمة الأمن السيبراني، وتم كذلك القياس عبر متوسط الاستجابات باستخدام مقياس ليكرت. وقد استند البحث إلي دراسات كل من Van Gremberen et al.

(2004); Eulerich (2021);Leech and Hanlon (2016); Rothrock et al. (2018); Stafford et al. (2018) في تحديد المؤشرات لمتغير الهيكل المتكامل للحوكمة السيبرانية.

- **المتغير التابع: مؤشرات إدارة مخاطر الأمن السيبراني(Y)**

يتمثل هذا المتغير في أربعة مراحل رئيسية لإدارة المخاطر: الوقاية/المنع(Y1)، والاكتشاف(Y2)، والاستجابة(Y3)، والعلاج/التصحيح(Y4). تم تصميم عدد من المؤشرات لكل مرحلة، وجميعها تقيس مدى تطبيق الممارسات المتعلقة بالمخاطر، بالاعتماد على مقياس ليكرت الخماسي، مع احتساب المتوسط الحسابي لاستجابات كل مشارك في كل مجموعة مؤشرات. وأستند البحث في تحديد المؤشرات الفرعية للمتغير (Y) على كل من دراسة COBIT 5 (2012a,b) ISACA; (2013) .Steinbart et al .

- **المتغيرات الرقابية**

اعتمد البحث على ثلاث متغيرات رقابية رئيسية لضبط العلاقة بين محددات جودة وظيفة المراجعة الداخلية وهيكل الحوكمة السيبراني من جهة، ومؤشرات إدارة مخاطر الأمن السيبراني من جهة أخرى، وذلك على النحو الآتي:

1. مستوى الجهد المخصص لعملية مراجعة الأمن السيبراني: يمثل هذا المتغير مؤشراً على مدى التزام المنشاة بتقويم الضوابط الأمنية الرقمية من خلال المراجعة الداخلية، حيث إن تخصيص قدر أكبر من الجهد والموارد لمراجعة الأمن السيبراني يعزز من قدرة المراجعين على كشف الثغرات التقنية والتوصية بالتحسينات الملائمة. وقد أشار Gramling et al. (2004) إلى أن اتساع نطاق مراجعة الأمن السيبراني يعكس التفاعل الإيجابي بين وظيفة المراجعة ومتطلبات الحوكمة، بما يعزز من فاعلية إدارة المخاطر الرقمية. في هذا البحث، يقاس هذا الجهد بنسبة الوقت الذي يخصصه قسم المراجعة الداخلية لمراجعة الأمن السيبراني.
2. حجم قسم المراجعة الداخلية: يُعد حجم قسم المراجعة عاملاً حاسماً في تحديد قدرته على التعامل مع تعقيدات بيئة الأعمال الحديثة، لا سيما فيما يتعلق بمراجعة الجوانب التقنية للأمن السيبراني. فالأقسام الأكبر تمتلك موارد بشرية وخبرات متخصصة تمكنها من أداء مهامها بفاعلية أعلى. وقد أكد Arena and Azzone (2009) و Mihret and Yismaw (2007) على أن الحجم يعد من العوامل التنظيمية المؤثرة في فاعلية أداء المراجعة الداخلية، خاصة عند التعامل مع مخاطر ذات طابع تكنولوجي. في هذا البحث، يقاس حجم قسم المراجعة الداخلية بنسبة عدد المراجعين الداخليين في قسم المراجعة الداخلية المخصصة لعمليات الأمن السيبراني.

3. مستوى الرقمية في العمليات: يُقصد به درجة الاعتماد على النظم الرقمية والتقنيات المتقدمة في تنفيذ العمليات التشغيلية والإدارية، وهو ما يؤثر بصورة مباشرة على طبيعة وحجم المخاطر السيبرانية التي تواجهها المنشأة. كما أن بيئة العمل الرقمية تتطلب تطوير أساليب المراجعة واستخدام أدوات تحليل البيانات، وهو ما أشار إليه Alles (2020)&Vasarhelyi et al. (2015) فى سياق تطور دور المراجعة الداخلية في عصر البيانات الضخمة والتحول الرقمي. ويقاس مستوي الرقمية في العمليات بنسبة العمليات التي تعتمد على النظم الرقمية والتقنيات المتقدمة.

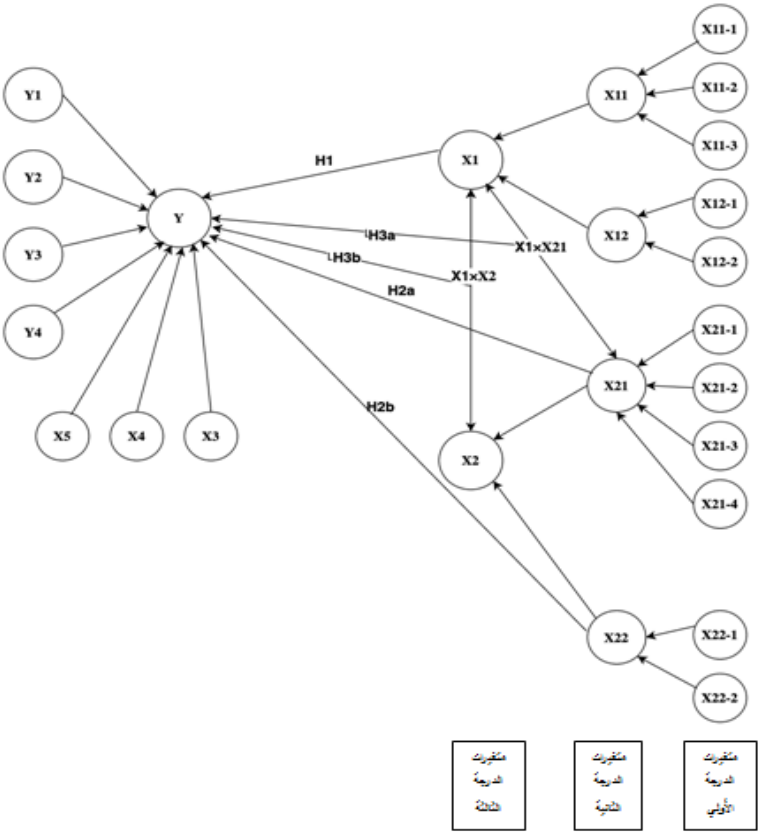
وقد تم قياس جميع المتغيرات الرقابية باستخدام مقياس ليكرت الخماسي، من خلال احتساب المتوسط الحسابي للاستجابات لكل متغير.

جدول 1: قياس متغيرات البحث

متغيرات الدرجة الثالثة		متغيرات الدرجة الثانية		متغيرات الدرجة الأولي		المؤشرات	حساب الدرجات	المدي النظري لمقياس ليكرت
أ. المتغيرات المستقلة								
X1	جودة المراجعة الداخلية على أساس المدخلات	X11	الكفاءة	X11-1	الشهادات المهنية	X11-11	حساب متوسط الاستجابات لعناصر القياس لكل مشارك	1-5
						X11-12		
				X11-2	الخلفية الأكاديمية	X11-21		1-5
						X11-22		
				X11-3	التدريب والتطوير المستمر	X11-31		1-5
						X11-32		
						X11-33		
		X12	الاستقلالية	X12-1	الاستعانة بمستشارين والتعاقد الخارجي	X12-11	جمع درجات عناصر القياس	0-4
						X12-12		
						X12-13		
						X12-14		
				X12-2	الارتباط مع لجنة المراجعة والإدارة	X12-21		0-4
						X12-22		
						X12-23		
						X12-24		
X2	الهيكل المتكامل للحوكمة السيبراني	X21	هيكل حوكمة سيبراني يستند إلى خطوط المساءلة الثلاث	X21-1	فعالية أداء خط المساءلة الأول في هيكل الحوكمة	X21-11	حساب متوسط الاستجابات لعناصر القياس لكل مشارك	1-5
						X21-12		
						X21-13		
				X21-2	فعالية أداء خط المساءلة الثاني في هيكل الحوكمة	X21-21		1-5
						X21-22		
						X21-23		
				X21-3	فعالية أداء خط المساءلة الثالث في هيكل الحوكمة	X21-31		1-5
						X21-32		
						X21-33		
				X21-4	جودة التعاون بين خطوط المساءلة الثلاث	X21-41		1-5
						X21-42		

متغيرات الدرجة الثالثة		متغيرات الدرجة الثانية		متغيرات الدرجة الأولي		المؤشرات	حساب الدرجات	المدي النظري لمقياس ليكرت
						X21-43		
						X21-44		
						X21-45		
			X22	دعم الإدارة التنفيذية (خط المساءلة الرابع)	X22-1	X22-11	حساب متوسط الاستجابات لعناصر القياس لكل مشارك	1-5
						X22-12		
				دعم مجلس الإدارة (خط المساءلة الخامس)	X22-2	X22-21		1-5
						X22-22		
ب. المتغير التابع								
				مؤشرات مرحلة الوقاية/المنع	Y1	Y11		1-5
						Y12		
						Y13		
						Y14		
				مؤشرات مرحلة الاكتشاف	Y2	Y21		1-5
						Y22		
						Y23		
						Y24		
				مؤشرات مرحلة الاستجابة	Y3	Y31		1-5
						Y32		
				مؤشرات مرحلة العلاج	Y4	Y41		1-5
						Y42		
ج. المتغيرات الرقابية								
				مستوي الجهد المخصص لعمليات مراجعة الأمن السيبراني	X3	X31	حساب متوسط الاستجابات لعناصر القياس لكل مشارك	1-5
				حجم قسم المراجعة الداخلية	X4	X41		1-5
				مستوي الرقمية في العمليات	X5	X51		1-5

المصدر: أعداد الباحث



شكل1: نموذج البحث

المصدر: أعداد الباحث

ويستخدم هذا البحث خمس نماذج للمعادلات الهيكلية (SEM) لاختبار فروض البحث، وذلك على النحو التالي:

النموذج الأول:

ويستخدم لاختبار الفرض الأول (H1): تؤثر جودة وظيفة المراجعة الداخلية المبنية على منهج المدخلات تأثيرًا إيجابيًا على تحسين مؤشرات إدارة مخاطر الأمن السيبراني.

النموذج الإحصائي المستخدم:

$$Y=\beta0+\beta1X1+\beta2X3+\beta3X4+\beta4X5+\varepsilon$$

حيث:

Y= مؤشرات إدارة مخاطر الأمن السيبراني

X1= جودة وظيفة المراجعة الداخلية (المتغير الأساسي)

X3= مستوي الجهد المبذول في مراجعة الأمن السيبراني (متغير رقابي)

X4= حجم قسم المراجعة الداخلية (متغير رقابي)

X5= مستوى الرقمية في العمليات (متغير رقابي)

β_1= معامل تأثير جودة وظيفة المراجعة الداخلية على مؤشرات إدارة المخاطر (المتغير الأساسي في الفرض).

β_2، β_3، β_4= تأثيرات المتغيرات الرقابية علي Y

ε= الخطأ العشوائي في النموذج (unexplained error)

النموذج الثاني:

ويستخدم لاختبار الفرض الثاني (أ) (H2a): يساهم وجود هيكل حوكمة سيبراني مبني على نموذج خطوط المساءلة الثلاث ومستند إلى أحد أطر الأمن السيبراني المهنية، في تحسين مؤشرات إدارة مخاطر الأمن السيبراني.

النموذج الإحصائي المستخدم:

$$Y=\beta0+\beta1D+\beta2X3+\beta3X4+\beta4X5+\varepsilon$$

حيث:

Y= مؤشرات إدارة مخاطر الأمن السيبراني

D= متغير صوري (وجود هيكل حوكمة سيبرانية: 1 = نعم، 0 = لا) يتيح عزل الأثر الحقيقي للمتغير الأساسي D (الهيكل) عن التأثيرات الأخرى

X3= مستوي الجهد المبذول في مراجعة الأمن السيبراني (متغير رقابي)

X4= حجم قسم المراجعة الداخلية (متغير رقابي)

X5= مستوى الرقمية في العمليات (متغير رقابي)

β_1= يقيس الفرق بين المنشآت التي تطبق هيكل الحوكمة وتلك التي لا تطبقه (المتغير الأساسي في الفرض)

β_2، β_3، β_4= تأثيرات المتغيرات الرقابية علىY

ε = الخطأ العشوائي في النموذج (unexplained error)

النموذج الثالث:

ويستخدم لاختبار الفرض الثاني (ب) (H2b): تؤثر المشاركة الفعالة للإدارة التنفيذية في مجلس الإدارة بشكل إيجابي على تحسين مؤشرات إدارة مخاطر الأمن السيبراني.

النموذج الإحصائي المستخدم:

$$Y=\beta0+\beta1X22+\beta2X3+\beta3X4+\beta4X5+\varepsilon$$

حيث:

Y= مؤشرات إدارة مخاطر الأمن السيبراني

X22= دعم الإدارة التنفيذية ومجلس الإدارة (المتغير الأساسي)

X3= مستوى الجهد المبذول في مراجعة الأمن السيبراني (متغير رقابي)

X4= حجم قسم المراجعة الداخلية (متغير رقابي)

X5= مستوى الرقمية في العمليات (متغير رقابي)

β_1= يمثل التأثير المباشر للمشاركة الفعالة للإدارة التنفيذية في مجلس الإدارة على مؤشرات إدارة المخاطر

β_2، β_3، β_4= تأثيرات المتغيرات الرقابية علىY

ε = الخطأ العشوائي في النموذج(unexplained error)

النموذج الرابع:

ويستخدم لاختبار الفرض الثالث (أ) (H3a): يؤثر التفاعل بين جودة وظيفة المراجعة الداخلية، بناءً على منهج المدخلات، وتطبيق نموذج خطوط المساءلة الثلاث، بشكل إيجابي على تحسين مؤشرات إدارة مخاطر الأمن السيبراني.

النموذج الاحصائي المستخدم:

$$Y=\beta0+\beta1X1+\beta2X21+\beta3(X1\times X21)+\beta4X3+\beta5X4+\beta6X5+\varepsilon$$

حيث:

Y= مؤشرات إدارة مخاطر الأمن السيبراني

X1= جودة وظيفة المراجعة الداخلية

X21= تطبيق نموذج خطوط المساءلة الثلاث

X1 × X21= التفاعل بين المتغيرين الأساسيين

X3= مستوي الجهد المبذول في مراجعة الأمن السيبراني (متغير رقابي)

X4= حجم قسم المراجعة الداخلية (متغير رقابي)

X5= مستوى الرقمية في العمليات (متغير رقابي)

β_1، β_2= التأثيرات المستقلة لكل من X1 و X21

β_3= معامل التفاعل بين المتغيرين الأساسين في الفرض، والذي يُعبر عن ما إذا كان التأثير المشترك بين X1 و X21 يؤدي إلى تحسين Y

β_4، β_5، β_6= تأثيرات المتغيرات الرقابية على Y.

ε= الخطأ العشوائي في النموذج (unexplained error).

النموذج الخامس:

ويستخدم لاختبار الفرض الثالث (ب) (H3b): يساهم التفاعل بين جودة وظيفة المراجعة الداخلية المبنية على منهج المدخلات، وتطبيق هيكل حوكمة سيبرانية متكامل (نموذج خطوط المساءلة الخمسة)، في تحسين مؤشرات إدارة مخاطر الأمن السيبراني، مقارنةً بالمنشآت التي تطبق نموذج خطوط المساءلة الثلاث فقط.

النموذج الإحصائي المستخدم:

$$Y=\beta0+\beta1X1+\beta2D+\beta3(X1\times C)+\beta4X3+\beta5X4+\beta6X5+\varepsilon$$

حيث:

Y= مؤشرات إدارة مخاطر الأمن السيبراني

X1= جودة وظيفة المراجعة الداخلية

C= متغير صوري (Dummy Variable) يمثل نوع نموذج الحوكمة:

- C= 1: منشآت تطبق نموذج الخطوط الخمسة
- C= 0: منشآت تطبق الخطوط الثلاثة فقط

X1 × C= تأثير التفاعل بين جودة وظيفة المراجعة الداخلية ونوع النموذج

X3= مستوي الجهد المبذول في مراجعة الأمن السيبراني (متغير رقابي)

X4= حجم قسم المراجعة الداخلية (متغير رقابي)

X5= مستوى الرقمية في العمليات (متغير رقابي)

β_1= التأثير المستقل لجودة وظيفة المراجعة الداخلية

β_2= الفرق في الأداء بين النموذجين عند المستوى الصفري لجودة وظيفة المراجعة الداخلية

β_3= معامل التفاعل بين المتغيرين الأساسين في الفرض: يوضح ما إذا كان تأثير X1 على Y يختلف باختلاف C (نوع نموذج الحوكمة)

β_4، β_5، β_6= تأثيرات المتغيرات الرقابية على Y

ε = الخطأ العشوائي في النموذج(unexplained error)

7-3-2 جمع البيانات

تم جمع البيانات من خلال استبيان عبر الإنترنت (ملحق (1))، تم توزيعه على المراجعين الداخليين، والمسؤولين بإدارات تقنية وأمن المعلومات، وأعضاء مجالس الإدارة بالشركات عينة البحث. وقد استخدمت شبكة LinkedIn لمشاركة الاستبيان مع المهنيين العاملين في مجال المراجعة الداخلية، وتقنية وأمن المعلومات. وقد تم اختبار الاستبيان مبدئياً بمشاركة أستاذ أكاديمي واحد، وأثنين من المهنيين.

وللتغلب على التحيز الناتج عن الطريقة العامة Common method variance تم أتباع الإجراءات التالية وفقاً لـ Podsakoff et al. (2003):

- وضع خطاب تعريفي يتضمن وصفاً لأهداف الدراسة، ويوضح الطابع التطوعي للمشاركة وسرية الإجابات الكاملة. وقدمت معلومات تواصل للإجابة عن أي استفسارات، وحث المشاركين على تقديم إجابات صادقة.
- استخدام مقياس ليكرت مكون من خمس نقاط، مع تسمية النقاط لتوضيحها وتسهيل الإجابة.
- تم خلط عناصر القياس Measurement items، وتم تقديم أسئلة (المتغيرات الملاحظة Manifest variables) للمتغيرات الكامنة على صفحات مختلفة لتجنب إنتاج ارتباطات متوقعة بين الاستجابات للأسئلة تحت المتغيرات الكامنة.
- القيام باختبارين للتحيز الناتج عن الطريقة العامة Common method variance:

1. اختبار العامل الفردي Harman's Single Factor Test وقد أوضحت النتائج أن 18 عاملاً بقيم ذاتية أكبر من 1، مفسراً حوالي 90% من التباين.
2. اختبار التداخل الكامل Full Collinearity Assessment، وقد أوضحت النتائج أن أعلي قيمة لعوامل تضخم التباين (VIF) كانت 2.7 وهي أقل من الحد الأقصى المسموح به (3.3) (Kock, 2015).

بناء على ذلك، تشير نتائج الاختبارين إلى أن التحيز الناتج عن الطريقة العامة Common method variance لم يكن موجوداً في البيانات.

7-3-3 عينة البحث

تم تلقي 190 استجابة، وتم استبعاد 75 استجابة بسبب وجود نقص في البيانات يزيد عن10% في تقييم 48 مؤشراً للقياس. وبناء على ذلك، استندت الدراسة إلى عينة غير احتمالية مكونة من 115 استجابة. ووفقاً لـ Hulland et al. (2018) تعد عينة Convenience sample كافية لاختبار التأثيرات النظرية بناء على نموذج البحث. ومع ذلك، فأن استخدام عينة Convenience sample يحد من إمكانية تعميم النتائج المستخلصة من هذه العينة على المجتمع.

ويوضح الملحق (2) توصيف العينة من حيث الخصائص الديموغرافية والمهنية (الجزء الأول)، والسمات العامة للمنشآت المشمولة في عينة البحث (الجزء الثاني)، بما يُسهم في فهم الخلفية التي يستند إليها المشاركون في البحث، والبالغ عددهم (115) مفردة. ويمكن تحليل الخصائص الديموغرافية والمهنية لعينة البحث على النحو التالي:

1. **التوزيع الوظيفي:** أظهرت النتائج أن غالبية المستجوبين يشغلون مناصب قيادية في أقسام المراجعة، حيث جاءت النسب على النحو التالي:
   - مديرو المراجعة التنفيذيون: (24.3%) — في المرتبة الأولى.
   - أعضاء أقسام المراجعة الداخلية: (17.4%).
   - أعضاء في قسم تقنية المعلومات: (14.8%).
   - أعضاء لجان المراجعة: (12.2%).
   - أعضاء في مجالس الإدارة: (8.7%).
   - فئة "أخرى": (22.6%).

   ويُشير هذا التوزيع إلى تمثيل قوي للمجالات ذات الصلة بالمراجعة والتقنية، وهو ما يعكس أهمية الرقابة والإشراف ضمن بيئة عمل المشاركين.

2. **التأهيل المهني:** يتضح من النتائج أن أكثر من نصف العينة يحملون شهادة محاسب قانوني معتمد (CPA/CIA)بنسبة (54.8%)، مما يعزز البُعد المهني للمستجوبين في جانب المحاسبة والمراجعة. في المقابل، كانت نسب الحاصلين على الشهادات المتخصصة في نظم المعلومات وأمن المعلومات منخفضة نسبيًا، حيث تراوحت نسب الحاصلين على شهادات مثل:CISA ، CISM، CCNA: ما بين (1.7% – 2.6%).كما أفاد (27%) من المشاركين بعدم امتلاكهم لأي مؤهل مهني متخصص.

ويعكس هذا التوزيع تركّزًا مهنيًا في المحاسبة والمراجعة، مقابل ضعف في التأهيل المرتبط بالأمن السيبراني ونظم المعلومات، ما قد يشير إلى فجوة تدريبية محتملة.

3. **التوزيع حسب الجنس:** توزعت العينة من حيث الجنس على النحو التالي: إناث: (56.5%)؛ ذكور: (43.5%)، ويُعد هذا التوزيع تمثيلاً جيدًا للعنصر النسائي في المجال، وربما يشير إلى ازدياد انخراط المرأة في المناصب الرقابية والإدارية.
4. **سنوات الخبرة العملية:** تنوعت سنوات الخبرة بين المستجوبين، وجاء التوزيع كالتالي: أكثر من 21 سنة: (26.2%) — أعلى نسبة. أقل من 5 سنوات: (21.7%). من 16 إلى 20 سنة: (21.7%). باقي الفئات تراوحت نسبها بين (14.8%) و(15.6%). ويعكس هذا التوزيع مزيجًا متوازنًا من حيث سنوات الخبرة، مما يتيح للبحث الاستفادة من وجهات نظر متنوعة تمثل مستويات مهنية مختلفة.
5. **الفئة العمرية:** أظهرت النتائج أن غالبية المستجوبين تنتمي إلى الفئتين العمريتين: من 40 إلى 50 عامًا: (31.3%). أكثر من 50 عامًا: (31.3%). بينما توزعت بقية العينة على: أقل من 30 عامًا: (21%). من 30 إلى 40 عامًا: (16.4%). ويوضح هذا التركيب العمري سيطرة الفئة الناضجة مهنيًا على العينة، مع وجود تمثيل مقبول للفئات الأصغر سنًا.

بناءً على ما سبق، يُمكن القول إن العينة تمثل بدرجة كبيرة العاملين في مجالات المراجعة والمحاسبة، ممن يمتلكون خبرة طويلة .كما تميزت بتنوع من حيث الجنس والعمر، فيما تشير النتائج إلى حاجة ملحّة لرفع مستوى التأهيل في مجالات الأمن السيبراني ونظم المعلومات، بهدف تحقيق التوازن المهني المطلوب في بيئة العمل الرقمية.

أما من حيث تحليل السمات العامة للمنشآت المشمولة في عينة الدراسة، يتناول التحليل أبعادًا متعددة تشمل: القطاع الاقتصادي، وعدد العاملين، وحجم الأصول، وعدد العاملين في أقسام المراجعة الداخلية وأمن المعلومات.

من حيث **القطاع الاقتصادي**، أظهرت النتائج تنوع القطاعات التي تنتمي إليها المنشآت، حيث كانت النسبة الأعلى من منشآت قطاع تقنية المعلومات والاتصالات (24.3%)، تلتها الخدمات المالية والبنوك (16.5%)، ثم القطاع الصناعي (15.6%) والقطاع السياحي (13.3%) . كما تمثلت القطاعات الحكومية (8.6%)، الصحية والتعليمية (10.4%)، وقطاعات أخرى (11.3%) بنسب متفاوتة. ويعكس هذا التوزيع تنوعًا قطاعيًا جيدًا في العينة، مع تركّز ملحوظ في القطاعات المرتبطة بالتكنولوجيا والخدمات المالية.

ومن حيث **حجم المنشأة (حسب عدد العاملين)**، بيّنت النتائج أن المنشآت الصغيرة (أقل من 100 موظف) تمثل نسبة مهمة (28%)، بينما بلغت نسبة المنشآت المتوسطة (100–499 موظف) حوالي (27.8%)، والمنشآت الكبيرة (500 موظف فأكثر) حوالي (28.6%). ويؤشر هذا التوزيع إلى تمثيل متوازن نسبيًا لمختلف أحجام المنشآت.

ومن **حيث حجم المنشأة (حسب إجمالي الأصول)**، تشير البيانات إلى أن أكثر من ربع المنشآت (27.8%) لا تتوفر لديها معلومات حول إجمالي الأصول، مما يشكّل فجوة معرفية لدى عدد من المشاركين. أما المنشآت التي تقع أصولها في فئة أقل من 10 ملايين فقد شكّلت (20.3%)، وبين 250 – 500 مليون شكلت (17.3%)، وباقي الفئات تراوحت بين (9.5% – 14.7%). وتُظهر النتائج تنوعًا في مستويات رأس المال بين المنشآت.

أما من حيث **عدد العاملين في قسم المراجعة الداخلية**، غالبية المنشآت تضم فرق مراجعة داخلية تتراوح بين 6 إلي 50 مراجعًا داخليًا، حيث جاءت النسب: من 6–10 (21.7%)، 11–20 (17.5%)، و21–50 (19%). بينما تضم فئة قليلة أكثر من 50 مراجعًا (14.8%). وتشير النتائج إلى أن (14%) من المنشآت لا تعرف عدد العاملين في هذا القسم. يدل هذا التوزيع على وجود اهتمام ببناء وحدات مراجعة داخلية متوسطة الحجم.

أما **عدد العاملين في إدارات تكنولوجيا وأمن المعلومات**، أفادت النتائج بأن أغلب المنشآت لديها أقسام تقنية تتراوح بين 1 إلى 50 موظفًا، حيث كانت النسبة الأعلى للفئة (1–10) بنسبة (22.6%)، ثم (26–50) بنسبة (19%)، تليها فئة (11–25) بنسبة (17.4%). وقد أجابت (26%) من المنشآت بأنها لا تعرف عدد العاملين في هذا القسم. ويشير ذلك إلى اهتمام متوسط بتكوين فرق تقنية، مع وجود فجوة معرفية بشأن الهيكل التنظيمي في بعض المنشآت، خاصة تلك التي اختارت "لا أعرف."

يُبرز التحليل الوصفي للمنشآت محل الدراسة درجة جيدة من التنوع والتوازن في التوزيع القطاعي والحجمي، ما يعزز تمثيل العينة وقدرتها على دعم تعميم النتائج. إلا أن نسبة الاستجابات التي اتسمت بعدم المعرفة ببعض المؤشرات الأساسية (كعدد العاملين أو حجم الأصول) توحي بوجود فجوات معرفية محتملة داخل بعض المنشآت، مما قد يُعزى إلى محدودية الشفافية أو عدم إشراك بعض الإدارات في البيانات المالية والتنظيمية.

7-4 نتائج البحث

7-4-1 نتائج الإحصاء الوصفي لمتغيرات البحث

يوضح ملحق (3) نتائج الإحصاء الوصفي للمتغيرات وذلك من خلال مؤشرات: المتوسط الحسابي، الانحراف المعياري، النسبة الترتيبية الدنيا(P10)، الوسيط (P50)، والنسبة الترتيبية العليا (P90). وتُعد هذه المؤشرات أدوات مهمة لفهم اتجاهات إجابات أفراد العينة.

- **المتغيرات المستقلة**

X1: جودة المراجعة الداخلية على أساس منهج المدخلات، بلغ المتوسط الحسابي (4.12) مع انحراف معياري (3.42)، وهو ما يشير إلى تقييم مرتفع لجودة المراجعة. ويعزز ذلك الوسيط (4.03) والنسبة العليا(P90 = 4.82)، مما يعكس إجماعًا إيجابيًا على كفاءة المدخلات في عملية المراجعة.

X11 الكفاءة، حقق هذا المتغير متوسطًا قدره (3.55) ، ما يشير إلى مستوى متوسط إلى مرتفع من الكفاءة المدركة، إلا أن الانحراف المعياري (2.76) يدل على وجود تباين بين آراء المشاركين. وقد جاءت الأبعاد الفرعية على النحو التالي:

X11-1 الشهادات المهنية (3.72) :تعكس تقديرًا جيدًا لحيازة المؤهلات المهنية. X11-2 الخلفية الأكاديمية (3.66) :تشير إلىوعي بأهمية التأهيل العلمي.X11-3التدريب والتطوير المستمر (4.00) : يُبرز حرصًا على التعلّم المستمر وبناء القدرات.

X12الاستقلالية، حقق هذا المتغير متوسط (3.63) و4.54 = P90، مما يشير إلي إن الاستقلالية تُقيّم بمستوى جيد، مع تباين معتدل في الإدراك (الانحراف المعياري= 2.72). وتُظهر الأبعاد:

X12-1الاستعانة بمستشارين خارجيين (3.70) :يعكس انفتاحًا على الدعم الفني. X12-2الارتباط مع لجنة المراجعة (3.63) :يشير إلى تفعيل العلاقة بين المراجعة والحوكمة.

X2 :الهيكل المتكامل للحوكمة السيبرانية، سُجل متوسط (3.66)، بانحراف معياري (2.56) ، مما يدل على إدراك معتدل لأهمية وجود هيكل واضح للحوكمة. ويُظهر التوزيع أن فئات عديدة لا تزال تختلف في تقييم هذا المتغير.

X21 خطوط المساءلة الثلاث، حقق هذا البُعد أعلى متوسط في المتغيرات المستقلة (4.39)، مما يعكس إدراكًا عاليًا لأهمية خطوط المساءلة:X21-1 الخط الأول:(3.28) ،X21-2الخط الثاني:(3.23) X21-3الخط الثالث:(3.53)، X21-4 جودة التعاون بين الخطوط :(3.82). وتشير هذه النتائج

إلى أن الخط الثالث (وظيفة المراجعة الداخلية) والتعاون بين الخطوط أكثر فاعلية من الخطين الأول والثاني.

X22 دعم الإدارة التنفيذية ومجلس الإدارة، بلغ المتوسط (4.00) ، حيث أظهرت النتائج أن دعم الإدارة التنفيذية (4.05) كان أعلى من دعم مجلس الإدارة (3.38) ، وهو ما يعكس فجوة محتملة في اهتمام القيادات العليا بقضايا الأمن السيبراني والحوكمة.

- **المتغيرات الرقابية**

X3: مستوى الجهد المخصص لمراجعة الأمن السيبراني، بلغ المتوسط (4.09) ، ويُظهر هذا الرقم إدراكًا متقدمًا لأهمية تخصيص جهود في مجال مراجعة أمن المعلومات، ويعزز ذلك ارتفاع قيمة P90إلى (4.84).

X4: حجم قسم المراجعة الداخلية، بمتوسط (4.11) و4.94 = P90، تدل النتائج على وجود هياكل تنظيمية داعمة وفعالة في هذا القسم لدى غالبية المنشآت.

X5: مستوى الرقمية في العمليات، يُظهر المتوسط (4.11) مستوى مرتفعًا من التبني الرقمي في العمليات، مما يُعزز من فعالية الأمن السيبراني والحوكمة الرقمية بشكل عام.

- **المتغير التابع: إدارة مخاطر الأمن السيبراني(Y)**، بلغ المتوسط العام لمتغير إدارة المخاطر (3.82)، مما يعكس فاعلية جيدة في إدارة التهديدات السيبرانية. أما الأبعاد الفرعية، فجاءت كما يلي:

Y1 الوقاية: المتوسط = 3.52 يعكس استعدادًا وقائيًا جيدًا، إلا أن قيمة P10 = 2.61 تشير إلى ضعف في بعض الحالات.

Y2 الاكتشاف: المتوسط = 4.10، وهو الأعلى بين أبعادY ، مما يدل على كفاءة أنظمة الكشف المبكر والإنذار عن المخاطر.

Y3 الاستجابة: المتوسط = 4.38 و5.0 = P90، وهو الأعلى إطلاقًا، مما يُبرز تفوق المنشآت في التصرف عند وقوع المخاطر.

Y4 العلاج: المتوسط = 3.64، وهو الأدنى نسبيًا، ما يشير إلى أن إجراءات التعافي لا تزال بحاجة إلى تطوير في بعض المنشآت.

تكشف النتائج أن العينة تتمتع بمستوى جيد من النضج المؤسسي في الجوانب المتعلقة بالمراجعة الداخلية، والحوكمة، وجهود الأمن السيبراني. ومع ذلك، فقد أظهرت بعض الفجوات، خصوصًا في دعم

مجالس الإدارة، وفعالية خطي المساءلة الأول والثاني، وكذلك في القدرة على علاج الهجمات السيبرانية بعد وقوعها.

تُعد هذه المؤشرات مدخلاً مهمًا لتطوير السياسات، وتعزيز ثقافة الأمن السيبراني والحوكمة في بيئة الأعمال الرقمية.

7-4-2 نموذج القياس

تُعد معاملات التحميل المعيارية (Standardized Loadings) إحدى الأدوات الأساسية في تحليل النماذج الهيكلية(SEM)، حيث تُستخدم لقياس مدى تمثيل المؤشرات للمتغيرات الكامنة. تعكس هذه القيم العلاقة بين كل مؤشر وبين المتغير الذي يُفترض أنه يقيسه، وتُعبر عن الصدق البنائي (Construct Validity) للمقياس. وفقًا للمعايير الإحصائية المعتمدة، تُعد القيم المقبولة لمعاملات التحميل:

- مرتفعة ≥ 0.70: ممتازة وتعكس اتساقًا قويًا.
- بين 0.60 – 0.69: مقبولة بشروط خاصة أو ضمن تحليل استكشافي.
- ضعيفة < 0.60: وتُشير غالبًا إلى أن المؤشر لا يمثل البُعد بشكل كافٍ.

وفيما يلي التحليل التفسيري لمعاملات التحميل المعيارية للمتغيرات الكامنة كما يتضح من ملحق (4)

- **المتغيرات من الدرجة الأولى (First-Order Constructs)**

X11: الكفاءة (تشمل المؤشرات X11-11 إلىX11-33) معظم المؤشرات أظهرت تحميلات معيارية تتراوح بين 0.71 إلى0.89، ما يدل على ارتباط قوي بين المؤشرات الفرعية (مثل الشهادات المهنية والتدريب) ومفهوم الكفاءة. هذا يعكس أن تصميم أدوات القياس في هذا البُعد جيد من حيث الصدق الداخلي.

X12: الاستقلالية (X12-11إلىX12-24) تمثلت بقيم متوسطة إلى مرتفعة(0.91 – 0.68) ، مما يدل على اتساق مقبول إلى قوي بين البنود المستخدمة والاستقلالية كمتغير. وتشير هذه القيم إلى أن الاستعانة بمستشارين أو التبعية للجنة المراجعة تندرج فعليًا ضمن مفهوم الاستقلالية.

X21: فعالية خطوط المساءلة الثلاثة (X21-11إلىX21-45) جميع المؤشرات سجلت تحميلات بين 0.94 – 0.75، مما يعزز موثوقية هذه الأبعاد كركيزة أساسية في نموذج الحوكمة السيبرانية. وينعكس ذلك في وضوح أداء الخطوط الثلاثة كمكونات مترابطة وفاعلة.

X22: دعم الإدارة التنفيذية ومجلس الإدارة (X22-11 إلى X22-22) سجلت مؤشرات هذا البعد تحميلات قوية بين 0.89 – 0.70، مما يُظهر تماسكًا جيدًا بين التصورات المرتبطة بالدعم التنفيذي والمجالس الرقابية.

- **المتغيرات من الدرجة الثانية (Second-Order Constructs)**

X1: جودة المراجعة الداخلية، تعتمد على بعدي الكفاءة والاستقلالية (X11، X12). تحميلات هذه الأبعاد كعوامل مكونة للمتغير العام تراوحت بين 0.92 – 0.84. وتعكس هذه القيم تمثيلاً قويًا للمتغيرات الفرعية في تشكيل البُعد العام لجودة المراجعة.

X2: الهيكل المتكامل للحوكمة السيبرانية، يتكون من X21 وX22 كمكونين رئيسيين، وقد أظهرا تحميلات معيارية تفوق 0.87. هذا يعكس أن أداء الخطوط الثلاثة، ودعم الإدارة التنفيذية ومجس الإدارة يشكلان فعلاً الهيكل الأساسي للحوكمة السيبرانية كما يُقترح نظريًا.

Y: إدارة مخاطر الأمن السيبراني، تضم مراحل الوقاية، الاكتشاف، الاستجابة، والعلاج. القيم الناتجة تراوحت بين 0.94 – 0.80، وهي مؤشرات تؤكد أن مكونات المتغير التابع تعكس فعلاً أبعاده النظرية.

- **المتغيرات من الدرجة الثالثة (Third-Order Constructs)**

توضح النتائج أن معاملات التحميل لمتغيرات الدرجة الثالثة (X1، X2، Y) مرتفعة، مما يشير إلى ترابط هيكلي قوي بين مستويات المتغيرات.القيم تتراوح بين 0.95– 0.85، وهي ضمن النطاقات المثالية لنماذج القياس التأكيدي(CFA).

وبالتالي فأن التقييم العام للمتغيرات الكامنة في النموذج هو كما يلي:

متغيرات من الدرجة الأولى: تحميلات جيدة إلى ممتازة (0.68–0.94)، وبالتالي فأن صلاحية المؤشرات مقبولة.

متغيرات من الدرجة الثانية: تحميلات قوية جدًا (>0.85)، وبالتالي فأن صلاحية المؤشرات موثوقة.

متغيرات من الدرجة الثالثة: تحميلات مثالية (0.88–0.95)، وبالتالي فأن صلاحية المؤشرات تدعم النموذج البنائي.

بناءً على هذه النتائج، يمكن القول إن النموذج المقترح يتمتع بدرجة عالية من الاتساق البنائي والصدق المفاهيمي، وأن أدوات القياس المُستخدمة قادرة على تمثيل المتغيرات بفعالية عالية.

بالإضافة إلى ذلك، يُعد فحص الموثوقية والصلاحية جزءًا حاسمًا في تحليل النماذج الكامنة ضمن الإطار البنائي(SEM) . تهدف هذه الخطوة إلى التأكد من جودة أداة القياس وقدرتها على قياس المتغيرات النظرية بدقة واتساق. تعتمد الدراسة على ثلاث مؤشرات:

- موثوقية التركيب الداخلي(CR): تعكس قوة الاتساق بين المؤشرات المرتبطة ببُعد كامن.
- ألفا كرونباخ (α) : تقيس الاتساق الداخلي بين البنود.
- متوسط التباين المستخرج(AVE): يختبر مقدار التباين الحقيقي المفسَّر بواسطة المتغير الكامن.

في ضوء النتائج الموضحة في الجدول (2) فأن التقييم العام لمؤشرات تحليل الموثوقية والصلاحية في النموذج هو:

- CR: معظم القيم > 0.85 ممتازة.
- α: جميعها ضمن المقبول والمرتفع مما يدعم الثبات الداخلي
- AVE: جميعها ≤ 0.50 مما يدعم الصدق التقاربي

وهذا يشير إلى:

- اتساق داخلي ممتاز في معظم المتغيرات (CR و α).
- صدق تقاربي قوي كما تدل عليه قيم AVE.
- دقة في بناء مؤشرات القياس، مما يدعم صلاحية النموذج البنائي لاختبار الفرضيات.

جدول2: نتائج الموثوقية والصلاحية

متغيرات الدرجة الثانية		متغيرات الدرجة الأولي		موثوقية التركيب الداخلي Composite Reliability (CR)	ألفا كرونباخ Cronbach's alph (α)	متوسط التباين المستخرج Average variance extracted (AVE)
X11	الكفاءة	X11-1	الشهادات المهنية	0.93	0.84	0.71
		X11-2	الخلفية الأكاديمية	0.83	0.77	0.65
		X11-3	التدريب والتطوير المستمر	0.84	0.81	0.74
X12	الاستقلالية	X12-1	الاستعانة بمستشارين والتعاقد الخارجي	0.85	0.89	0.53
		X12-2	الارتباط مع لجنة المراجعة والإدارة	0.93	0.88	0.63
X21	هيكل حوكمة سيبراني يستند إلى خطوط	X21-1	فعالية أداء خط المساءلة الأول في هيكل الحوكمة	0.82	0.85	0.69
		X21-2	فعالية أداء خط المساءلة الثاني في هيكل	0.92	0.8	0.69

متغيرات الدرجة الثانية		متغيرات الدرجة الأولي		موثوقية التركيب الداخلي Composite Reliability (CR)	ألفا كرونباخ Cronbach's alph (α)	متوسط التباين المستخرج Average variance extracted (AVE)
	المساءلة الثلاث		الحوكمة			
		X21-3	فعالية أداء خط المساءلة الثالث في هيكل الحوكمة	0.84	0.77	0.56
		X21-4	جودة التعاون بين خطوط المساءلة الثلاث	0.94	0.87	0.53
X22	دعم الإدارة التنفيذية ومجلس الإدارة (خط المساءلة الرابع والخامس)	X22-1	دعم الإدارة التنفيذية (خط المساءلة الرابع)	0.85	0.84	0.66
		X22-2	دعم مجلس الإدارة (خط المساءلة الخامس)	0.84	0.82	0.7
Y	مؤشرات إدارة مخاطر الأمن السيبراني	Y1	مؤشرات مرحلة الوقاية/المنع	0.91	0.9	0.7
		Y2	مؤشرات مرحلة الاكتشاف	0.81	0.81	0.74
		Y3	مؤشرات مرحلة الاستجابة	0.9	0.88	0.74
		Y4	مؤشرات مرحلة العلاج	0.83	0.89	0.68
X3-X4	المتغيرات الرقابية	X3	مستوي الجهد المخصص لعمليات مراجعة الأمن السيبراني	0.89	0.91	0.66
		X4	حجم قسم المراجعة الداخلية	0.94	0.78	0.7
		X5	مستوي الرقمية في العمليات	0.82	0.84	0.66

المصدر: أعداد الباحث

ويُعد اختبار الصلاحية التمييزية من المؤشرات الجوهرية في تقييم نماذج القياس البنيوية، حيث تهدف إلى التحقق من تميّز كل بُعد عن الأبعاد الأخرى داخل النموذج. ويُقاس هذا النوع من الصلاحية عادة من خلال ثلاث طرق أساسية:

1. الجذر التربيعي لـ AVE: يجب أن يكون أعلى من أي قيمة ارتباط بين المتغير نفسه وأي متغير آخر.
2. الارتباطات البينية: تعكس قوة العلاقة بين البنى المختلفة.
3. نسبة HTMT :والتي يجب أن تقل عادة عن 0.85 إلى 0.90 لبيان تميّز المفاهيم.

ويوضح جدول (3) نتائج الصلاحية التمييزية Discriminant Validity بحيث:

- القيم على القطر الرئيسي تمثل الجذر التربيعي للـ AVE (تتراوح بين 0.70 و0.90).

- القيم أسفل القطر تمثل الارتباطات بين المتغيرات (تتراوح بين 0.30 و0.70).
- القيم أعلى القطر تمثل نسبHTMT (تتراوح بين 0.50 و0.85).

أولاً: تحليل نتائج الجذر التربيعي لـ AVE (قطر الجدول): تُظهر القيم الموجودة على القطر الرئيسي (مثل 0.79، 0.86، 0.87، 0.74...) أنها جميعًا أكبر من معظم الارتباطات البينية، وهو ما يُعد مؤشرًا قويًا على تحقق الصلاحية التمييزية وفقًا لمعيار Fornell–Larcker (1981) . وبالتالي، تحقق معظم الأبعاد التميّز البنائي المطلوب، مما يُعزز من مصداقية النموذج النظري المستخدم في الدراسة.

ثانياً: تحليل الارتباطات البينية (أسفل القطر): يلاحظ أن معظم قيم الارتباط بين الأبعاد تقع بين 0.30 و0.84، مما يشير إلى وجود علاقات مترابطة ولكن ليست متداخلة بشكل مفرط. على سبيل المثال:

- العلاقة بين X11–2(الخلفية الأكاديمية) و Y3(الاستجابة) بلغت 0.32، وهي ضعيفة، مما يشير إلى تمايز جيد.
- بينما العلاقة بين X11–2 و X21–2 (خط المساءلة الثاني) بلغت 0.79، وهي مرتفعة لكنها لا تتجاوز قيمة الجذر التربيعي على القطر (0.86)، مما يُبقي ضمن الحد المسموح.

وبالتالي يمكن الاستنتاج أنه لا توجد مؤشرات قوية على التداخل البنائي أو التكرار المفاهيمي بين الأبعاد.

ثالثاً: تحليل HTMT (فوق القطر): يستخدم HTMT كاختبار أكثر صرامة من Fornell–Larcker (1981). عند مراجعة القيم فوق القطر نلاحظ:

- بعض القيم تقترب من الحد الأعلى المقبول (0.85)، مثل العلاقة بين X11–1 و(0.75) X11–2 ، وبين X11–1و (0.85) X11–3.

- في المقابل، هناك قيم أقل بكثير (0.51، 0.58، 0.63...) مما يشير إلى تميّز كافٍ.

وبالتالي فأن غالبية قيم HTMT تقع ضمن النطاق المقبول (أقل من 0.85)، ما يعزز الصلاحية التمييزية.
وعلى ذلك فأن التفسير العام لنتائج الصلاحية التمييزية في السياق البحثي هي كما يلي:

- أبعاد الكفاءة(X11) : تُظهر علاقات مرتفعة فيما بينها، وهو متوقع بسبب الاشتراك في البُعد المفاهيمي ذاته. لكن جميعها تحافظ على تميّزها عن بقية الأبعاد مثل X12 و X21و Y.
- أبعاد الحوكمة السيبرانية(X21–X22): حافظت على تمايز مقبول فيما بينها وبين مؤشرات إدارة مخاطر الأمن السيبراني(Y1–Y4)، وهو أمر ضروري لفصل مفاهيم الهيكل الحوْكمي عن مخرجات الأداء.

- مؤشرات إدارة مخاطر الأمن السيبراني(Y) : أظهرت ترابطًا داخليًا معتدلًا (0.59–0.75) وهو متوقع، إلى جانب تمايز جيد عن المتغيرات الأخرى.

في ضوء ذلك، تشير نتائج جدول الصلاحية التمييزية إلى تحقق معايير التميّز البنائي بين المتغيرات الكامنة في النموذج، سواء باستخدام معيار الجذر التربيعي لـ AVE أوHTMT ، مما يُعد مؤشراً قويًا على جودة الأداة البحثية والمصداقية المفاهيمية للنموذج التحليلي المستخدم في البحث.

جدول 3: نتائج الصلاحية التمييزية Discriminant Validity

Y4	Y3	Y2	Y1	X22-2	X22-1	X21-4	X21-3	X21-2	X21-1	X12-2	X12-1	X11-3	X11-2	X11-1	
0.56	0.58	0.63	0.77	0.58	0.73	0.69	0.51	0.75	0.77	0.78	0.63	0.85	0.75	0.79	X11-1
0.81	0.76	0.84	0.77	0.65	0.7	0.82	0.5	0.79	0.74	0.7	0.69	0.64	0.86	0.39	X11-2
0.63	0.84	0.68	0.75	0.79	0.79	0.58	0.56	0.75	0.73	0.64	0.75	0.74	0.67	0.58	X11-3
0.55	0.64	0.63	0.71	0.66	0.58	0.82	0.62	0.51	0.81	0.5	0.87	0.3	0.33	0.3	X12-1
0.72	0.79	0.73	0.53	0.59	0.82	0.77	0.77	0.68	0.8	0.83	0.51	0.58	0.5	0.37	X12-2
0.83	0.62	0.61	0.63	0.56	0.68	0.7	0.67	0.53	0.77	0.63	0.38	0.35	0.35	0.63	X21-1
0.66	0.59	0.75	0.66	0.63	0.53	0.74	0.7	0.87	0.67	0.38	0.39	0.34	0.62	0.63	X21-2
0.77	0.59	0.67	0.53	0.58	0.58	0.83	0.84	0.5	0.48	0.66	0.41	0.41	0.52	0.48	X21-3
0.82	0.74	0.54	0.62	0.74	0.54	0.71	0.45	0.63	0.6	0.4	0.68	0.42	0.36	0.58	X21-4
0.55	0.79	0.73	0.82	0.79	0.74	0.69	0.36	0.33	0.58	0.59	0.44	0.41	0.53	0.3	X22-1
0.65	0.57	0.84	0.75	0.74	0.67	0.34	0.5	0.55	0.67	0.35	0.57	0.49	0.41	0.55	X22-2
0.69	0.57	0.67	0.75	0.61	0.68	0.48	0.66	0.56	0.42	0.52	0.31	0.42	0.64	0.68	Y1
0.51	0.56	0.82	0.49	0.34	0.48	0.67	0.51	0.59	0.65	0.34	0.37	0.34	0.32	0.39	Y2
0.57	0.75	0.6	0.57	0.67	0.36	0.35	0.35	0.49	0.6	0.61	0.61	0.7	0.32	0.58	Y3
0.87	0.58	0.59	0.65	0.36	0.64	0.6	0.48	0.44	0.38	0.5	0.54	0.35	0.43	0.5	Y4

المصدر: أعداد الباحث

ولقياس خصائص البني التكوينية لمتغيرات الدرجة الثالثة والثانية يعتمد نموذج القياس على ثلاث مؤشرات:

- Weight (الأوزان) — تشير إلى أهمية أو تأثير المتغير في النموذج.
- t statistics– لاختبار دلالة الوزن (كلما زادت، زادت دلالة المتغير).
- VIF (Variance Inflation Factor) – لقياس التعدد الخطي(Multicollinearity)، والقيم المقبولة عادة أقل من 5.

بناء على النتائج الموضحة في الجدول (4–A) فأن التحليل التفسيري لنتائج المؤشرات الثلاث لمتغيرات الدرجة الثالثة كما يلي:

- **تحليل نتائج متغير X1: جودة المراجعة الداخلية على أساس منهج المدخلات**

المتغير الفرعي X11 الكفاءة: يشير وزن هذا المتغير إلى تأثير معتدل على جودة المراجعة الداخلية. القيمة المرتفعة لإحصائية t (> 2) تدل على أن التأثير دال إحصائيًا بدرجة عالية (عند مستوى دلالة 0.01). كما أن قيمة VIF (2.1) تؤكد غياب مشكلة التعدد الخطي الجسيم، مما يعزز موثوقية التقدير.

المتغير الفرعي X12 الاستقلالية :أظهرت الاستقلالية تأثيرًا أقوى نسبيًا مقارنة بالكفاءة. وهذا يشير إلى أن استقلالية وظائف المراجعة الداخلية تلعب دورًا أكبر في تحديد جودة المراجعة. الدلالة الإحصائية العالية (t = 7.85) تقوي هذا الاستنتاج، مع تأكيد على عدم وجود تأثيرات تداخل خطية مرتفعة (VIF < 5).

- **تحليل نتائج متغير X2: الهيكل المتكامل للحوكمة السيبرانية**

المتغير الفرعي X21 هيكل حوكمة يستند إلى خطوط المساءلة الثلاث: يعكس هذا الوزن أن وجود هيكل حوكمة منظم يؤثر تأثيرًا واضحًا على تكاملية الحوكمة السيبرانية. إحصائية t المرتفعة توضح أن هذا التأثير دال بدرجة عالية. كما أن VIF المنخفض يدعم ثبات نتائج التقدير.

المتغير الفرعي X22 دعم الإدارة التنفيذية ومجلس الإدارة :يُعد هذا المتغير الأقوى من حيث التأثير بين جميع المتغيرات الفرعية المدروسة، مما يعكس أهمية الدعم المؤسسي في تحقيق حوكمة سيبرانية فعالة. تعزز القيمة المرتفعة لإحصائية t هذا الاستنتاج، فيما يؤكد VIF على عدم وجود تضخم تباييني.

في ضوء تلك النتائج فأن:

1. جميع المتغيرات الفرعية لها دلالة إحصائية عالية جميع(t > 6)، مما يعكس قوة العلاقات بين المتغيرات من الدرجة الثانية والثالثة.
2. قيم الأوزان تتراوح بين (0.35 – 0.47)، مما يشير إلى وجود فروقات نسبية واضحة في تأثير المتغيرات.
3. قيم VIF منخفضة(3 >)، مما يؤكد على عدم وجود مشاكل تداخل خطي تؤثر على مصداقية النموذج.

بناء على النتائج الموضحة في الجدول (4–B) فأن التحليل التفسيري لنتائج المؤشرات الثلاث لمتغيرات الدرجة الثانية كما يلي:

- **متغير الكفاءة (X11)** يتضح أن جميع المؤشرات الثلاث تُساهم بدرجة معنوية في تكوين متغير الكفاءة، وتُظهر القيم العالية لـ t- statistics أن العلاقة دالة إحصائيًا عند مستوى معنوية 0.01. ويُشير الوزن الأعلى للتدريب والتطوير المستمر (0.36) إلى أهمية التعلم المستمر في رفع كفاءة المراجعين. كما أن جميع قيم VIF أقل من 3، ما يدل على عدم وجود مشكلة تداخل خطي.

- **متغير الاستقلالية(X12)** تُشير الأوزان المرتفعة والدلالات الإحصائية القوية إلى الدور الحاسم لاستقلالية أقسام المراجعة. تفوق الاستعانة بخبرات خارجية (0.40) على الارتباط مع لجنة المراجعة والإدارة، ما يبرز أهمية الخبرات المحايدة والمتخصصة.

- **متغير هيكل الحوكمة السيبرانية (X21)** تشير النتائج إلى أن التعاون بين الخطوط يمثل العنصر الأكثر تأثيرًا في هذا البعد، مما يعكس أهمية التنسيق المشترك في منظومة الحوكمة السيبرانية. في حين أن أداء الخط الأول له تأثير منخفض نسبيًا، لكنه يظل ذا دلالة معنوية.

- **دعم الإدارة التنفيذية ومجلس الإدارة (X22)** يشكل هذا البُعد القوة الدافعة الرئيسة في نموذج الحوكمة. الوزن المرتفع لدعم الإدارة التنفيذية (0.45) يؤكد على الأهمية العملية للقيادة الإدارية في نجاح الممارسات السيبرانية. كما أن التوافق العالي بين المؤشرين يعكس تكامل الأدوار القيادية.

- **مؤشرات إدارة مخاطر الأمن السيبراني(Y)** تشير النتائج إلى أن مرحلة الاستجابة تُمثل العنصر الأهم في إدارة المخاطر، تليها مرحلة الاكتشاف. هذه النتائج تُبرز أهمية القدرة على التعامل الفعّال مع التهديدات بعد وقوعها، إلى جانب ضرورة اكتشافها مبكرًا.

في ضوء تلك النتائج فأن:

- جميع المؤشرات لها دلالة إحصائية قوية($t > 5$).
- الأوزان تتراوح بين 0.28 و0.45، مما يعكس توزيعًا متوازنًا ومتمايزًا في الأهمية.
- جميع قيم VIF أقل من 3، ما يعكس استقرار النموذج وخلوه من التعدد الخطي المؤثر.
- يتبيّن أن دعم الإدارة التنفيذية ومجلس الإدارة (X22) والتدريب والتطوير (X11-3) والتعاون بين خطوط المساءلة الثلاث (X21-4)هي أبرز العوامل المؤثرة.

جدول 4-A: قياس خصائص البني التكوينية لمتغيرات الدرجة الثالثة

متغيرات الدرجة الثالثة		متغيرات الدرجة الثانية		Weight	t statistics	VIF
X1	جودة المراجعة الداخلية على أساس المدخلات	X11	الكفاءة	0.35	6.20	2.1
		X12	الاستقلالية	0.42	7.85	2.4
X2	الهيكل المتكامل للحوكمة السيبراني	X21	هيكل حوكمة سيبراني يستند إلى خطوط المساءلة الثلاث	0.38	7.10	2.0
		X22	دعم الإدارة التنفيذية ومجلس الإدارة (خط المساءلة الرابع والخامس)	0.47	8.30	2.7

جدول 4-B: قياس خصائص البني التكوينية لمتغيرات الدرجة الثانية

متغيرات الدرجة الثانية		متغيرات الدرجة الأولي		Weight	t statistics	VIF
X11	الكفاءة	X11-1	الشهادات المهنية	0.32	5.90	2.2
		X11-2	الخلفية الأكاديمية	0.28	5.10	2.0
		X11-3	التدريب والتطوير المستمر	0.36	6.40	2.5
X12	الاستقلالية	X12-1	الاستعانة بمستشارين والتعاقد الخارجي	0.40	7.00	2.3
		X12-2	الارتباط مع لجنة المراجعة والإدارة	0.38	6.70	2.1
X21	هيكل حوكمة سيبراني يستند إلى خطوط المساءلة الثلاث	X21-1	فعالية أداء خط المساءلة الأول في هيكل الحوكمة	0.30	5.40	2.2
		X21-2	فعالية أداء خط المساءلة الثاني في هيكل الحوكمة	0.34	6.00	2.0
		X21-3	فعالية أداء خط المساءلة الثالث في هيكل الحوكمة	0.31	5.50	2.4
		X21-4	جودة التعاون بين خطوط المساءلة الثلاث	0.35	6.30	2.3
X22	دعم الإدارة التنفيذية ومجلس الإدارة	X22-1	دعم الإدارة التنفيذية (خط المساءلة الرابع)	0.45	7.50	2.6
		X22-2	دعم مجلس الإدارة (خط المساءلة الخامس)	0.42	7.10	2.4
Y	مؤشرات إدارة مخاطر الأمن السيبراني	Y1	مؤشرات مرحلة الوقاية/المنع	0.33	6.10	2.0
		Y2	مؤشرات مرحلة الاكتشاف	0.37	6.80	2.1
		Y3	مؤشرات مرحلة الاستجابة	0.39	7.00	2.2
		Y4	مؤشرات مرحلة العلاج	0.36	6.50	2.3

المصدر: أعداد الباحث

7-4-3 النموذج الهيكلي

بناء على نتائج اختبارات نموذج القياس، فأنه سوف يتم الاعتماد على أسلوب تحليل المسار Path Analysis ضمن نماذج المعادلات الهيكلية لاختبار فروض البحث. وبناء على نتائج اختبارات الفروض في الجدول (5)، يمكن تحليل النتائج على النحو التالي:

النموذج الأول:

يتضح من تحليل نتائج النموذج الأول لاختبار الفرض الأول (H1) أن:

- جميع المتغيرات المؤثرة دالة إحصائيًا($p < 0.01$) ، بما فيها X1.
- $\beta_1 = 0.34$، وهي أعلى قيمة بين المتغيرات، مما يشير إلى أن جودة وظيفة المراجعة الداخلية تمثل المتغير الأكثر تأثيرًا في النموذج.
- $R^2 = 0.68$ أي أن النموذج يفسر نسبة عالية من التباين فيY ، مما يدل على ملاءمته التفسيرية. هذا يعني أن تحسين جودة وظيفة المراجعة الداخلية المبنية على منهج المدخلات ينعكس بشكل مباشر وإيجابي على مؤشرات إدارة مخاطر الأمن السيبراني، حتى بعد ضبط المتغيرات الرقابية الأخرى.

النموذج الثاني:

يتضح من تحليل نتائج النموذج الثاني لاختبار الفرض الثاني (أ) (H2a) أن:

- جميع المتغيرات دالة إحصائيًا($p < 0.01$)، مما يدل على أن كل من D و X3 و X4 و X5 يساهم بشكل معنوي في تفسير التباين فيY.
- قيمة $R^2 = 0.67$ تعني أن النموذج يفسر 67% من التباين في مؤشرات إدارة المخاطر السيبرانية.
- D ($\beta = 0.31$) هو المتغير الأكثر تأثيرًا في النموذج، مما يدعم الفرض القائل بأن وجود هيكل حوكمة سيبراني يحسن من نتائج ممارسات إدارة المخاطر السيبرانية. حيث إن وجود هيكل واضح للحوكمة السيبرانية له أثر معنوي موجب على مؤشرات إدارة المخاطر، حتى بعد ضبط تأثير المتغيرات الرقابية الأخرى.

النموذج الثالث:

يتضح من تحليل نتائج النموذج الثالث لاختبار الفرض الثاني (ب) (H2b) أن:

- جميع المعاملات دالة إحصائيًا عند مستوى دلالة 0.05 , 0.01 ($p < 0.05,0.01$).
- X22 هو الأقوى تأثيرًا ($\beta = 0.33, t = 4.10$) مما يدعم الفرض الأساسي.
- $R^2 = 0.64$ يشير إلى أن النموذج يفسر نسبة عالية من التباين في Y (جودة نموذج جيدة).

تُظهر النتائج أن المشاركة الفعالة للإدارة التنفيذية ومجلس الإدارة لها تأثير مباشر ومعنوي على تحسين مؤشرات إدارة مخاطر الأمن السيبراني، حتى بعد ضبط أثر المتغيرات الرقابية الأخرى.

النموذج الرابع:

يتضح من تحليل نتائج النموذج الرابع لاختبار الفرض الثالث (أ) (H3a) أن:

- جميع التأثيرات دالة إحصائيًا ($p < 0.05,0.01$)

- β_3 (X1 × X21) = 0.22, t = 2.70, p = 0.007: يؤكد وجود تفاعل معنوي إيجابي بين جودة وظيفة المراجعة الداخلية وتطبيق نموذج خطوط المساءلة الثلاث.
- R^2 = 0.69 أي أن النموذج يفسر نسبة كبيرة من التباين في مؤشرات إدارة المخاطر، مما يدل على قوة النموذج البنائي.

تشير نتائج تحليل المسار إلى أن التفاعل بين جودة وظيفة المراجعة الداخلية وتطبيق نموذج خطوط المساءلة الثلاث يؤثر بشكل إيجابي ومعنوي على تحسين مؤشرات إدارة مخاطر الأمن السيبراني، حتى بعد التحكم في المتغيرات الرقابية.

النموذج الخامس:

يتضح من تحليل نتائج النموذج الخامس لاختبار الفرض الثالث (ب) (H3b) أن:

- التأثير التفاعلي (C × X1) دال إحصائيًا(β = 0.26, p = 0.004)، مما يشير إلى أن جودة وظيفة المراجعة الداخلية تؤثر بدرجة أقوى على إدارة المخاطر في المنشآت التي تطبق نموذج الخطوط الخمسة.
- المتغيرات الضابطة (X3, X4, X5) جميعها ذات دلالة إحصائية، ما يعزز قوة النموذج.
- R^2 = 0.7 يعكس تفسيرًا عاليًا لمؤشراتY ، مما يدل على جودة النموذج التنبؤي.

تُظهر نتائج تحليل المسار أن التفاعل بين جودة وظيفة المراجعة الداخلية ونوع نموذج الحوكمة السيبرانية (C) يسهم بشكل معنوي في تحسين مؤشرات إدارة مخاطر الأمن السيبراني، وبدرجة أعلى في المنشآت التي تطبق نموذج خطوط المساءلة الخمسة.

جدول 5: نتائج اختبارات فروض البحث

المتغيرات	النموذج الأول (H1)	النموذج الثاني (H2a)	النموذج الثالث (H2b)	النموذج الرابع (H3a)	النموذج الخامس (H3b)
X1					
معاملβ	0.34^{***}			0.30^{***}	0.29^{***}
اختبار t	4.25^{*}			3.80^{*}	3.65^{*}
X21					
معاملβ				0.25^{***}	
اختبار t				3.20^{*}	
X22					
معاملβ			0.33^{***}		
اختبار t			4.10^{*}		
D					
معاملβ		0.31^{***}			
اختبار t		3.95^{*}			

المتغيرات	النموذج الأول (H1)	النموذج الثاني (H2a)	النموذج الثالث (H2b)	النموذج الرابع (H3a)	النموذج الخامس (H3b)
X1 × X21					
معاملβ				0.22^{***}	
اختبارt				2.70^{*}	
C					
معاملβ					0.21^{***}
اختبارt					2.80^{*}
X1 × C					
معاملβ					0.26^{***}
اختبارt					2.95^{*}
X3					
معاملβ	0.26^{***}	0.28^{***}	0.25^{***}	0.20^{***}	0.22^{***}
اختبارt	3.05^{*}	3.10^{*}	2.85^{*}	2.60^{*}	2.65^{*}
X4					
معاملβ	0.17^{**}	0.16^{**}	0.19^{**}	0.18^{**}	0.15^{**}
اختبارt	2.10^{*}	2.15^{*}	2.40^{*}	2.15^{*}	2.00^{*}
X5					
معاملβ	0.22^{***}	0.21^{***}	0.22^{***}	0.24^{***}	0.23^{***}
اختبارt	2.80^{*}	2.75^{*}	2.95^{*}	3.00^{*}	2.85^{*}
R^2 (Y)	0.68	0.67	0.64	0.69	0.71

$^{***}p < 0.01$, $^{**}p < 0.05$, $^{*}p < 0.1$, $^{*}t \geq 1.96$

7-5 استنتاجات البحث، والتوصيات، ومجالات البحث المقترحة

7-5-1 استنتاجات البحث

استهدف البحث دراسة التفاعل بين الهياكل التنظيمية للحوكمة السيبرانية وجودة وظيفة المراجعة الداخلية ودورهما المشترك في تعزيز فاعلية إدارة مخاطر الأمن السيبراني. يستند هذا البحث إلى إطار نظري وميداني متكامل يسعى إلى اختبار تأثير محددات جودة وظيفة المراجعة الداخلية، من منظور مدخلات العمل، على مؤشرات إدارة مخاطر الأمن السيبراني، بالإضافة إلى تحليل أثر تطبيق نموذج الحوكمة السيبرانية متعدد الخطوط، لا سيما في صورته المطورة (نموذج خطوط المساءلة الخمسة).

يعتمد الإطار النظري للبحث على عدد من المفاهيم الأساسية المستقاة من الأدبيات المحاسبية والإدارية، والتي تم تطويرها. حيث تبني البحث منظور مدخلات العمل كأداة لتقييم جودة وظيفة المراجعة الداخلية، من خلال التركيز على بُعدين رئيسيين: الأول، الكفاءة المهنية يشمل المؤهلات الأكاديمية والتدريب المستمر والحصول على الشهادات المهنية ذات الصلة بأمن المعلومات. الثاني، الاستقلالية التنظيمية

وتمثل قدرة المراجعة الداخلية على ممارسة دورها التقييمي دون تأثر بالسلطة التنفيذية. وفي هذا الإطار، يقترح البحث أن جودة وظيفة المراجعة الداخلية لم تعد تُقاس فقط بمدى الالتزام بالمعايير المهنية التقليدية، بل يجب أن تشمل قدرة المراجعين الداخليين على فهم تقنيات أمن المعلومات، والمخاطر السيبرانية، والتفاعل معها بكفاءة.

بالإضافة إلى ذلك، قدم البحث تحليل للأطر التنظيمية والمهنية لحوكمة الأمن السيبراني، وقد أوضحت الدراسات السابقة التي استند عليها البحث أن فعالية نموذج خطوط المساءلة الخمس(5LoA)، والذي يعيد تعريف الحوكمة من كونها نظامًا رقابيًا قائمًا على المساءلة، إلى كونها نموذجًا تفاعليًا يتطلب تعاونًا بين جميع الخطوط التنظيمية، مع إبراز الدور الاستراتيجي لمجلس الإدارة والإدارة العليا.

وفي هذا السياق، تشكل نظرية الحوكمة المؤسسية ونظرية الوكالة إطارًا لفهم كيف يمكن للتنظيم المؤسسي والدور الرقابي للمراجعة أن يساهما في تقليل المخاطر الناجمة عن عدم تماثل المعلومات وضعف المساءلة. وفي ضوء تحليل الأدبيات السابقة، افترضت الدراسة وجود تأثير تفاعلي بين جودة وظيفة المراجعة الداخلية وتطبيق هيكل الحوكمة السيبرانية على مؤشرات إدارة مخاطر الأمن السيبراني.

وبناء على تحليل نتائج نموذج المعادلات الهيكلية (البنائية) (SEM-PLS)، وتفسير دلالات النماذج السببية المستخدمة لاختبار فروض البحث، أشارت النتائج إلي إلى تأثير إيجابي ودال إحصائيًا لمحددات جودة وظيفة المراجعة الداخلية على مؤشرات إدارة مخاطر الأمن السيبراني، ما يدعم الفرضية ويُبرز الدور الحيوي للكفاءة والاستقلالية في تحسين مخرجات الحوكمة السيبرانية. وهو ما يتفق مت نتائج دراسات كل من Steinbart et al. (2012); Islam et al. (2018); Christopher et al. (2009).

وأظهرت نتائج البحث وجود هيكل حوكمة سيبراني مبني على نموذج خطوط المساءلة الثلاث تأثيرًا معنويًا إيجابيًا على أداء إدارة المخاطر. كما تبين أن دعم الإدارة التنفيذية ومجلس الإدارة له تأثير أقوى نسبيًا على مؤشرات إدارة مخاطر الأمن السيبراني مقارنة بنموذج خطوط المساءلة الثلاث، ما يسلط الضوء على أهمية القيادة المؤسسية في إنجاح جهود الأمن السيبراني. وتتفق تلك النتائج مع نتائج دراسة كل من Steinbart et al. (2013); Feng and Wang (2018); Haislip et al. (2016,2020,2021); Vincent et al. (2019); Simth et al. (2021).

كما أن التفاعل بين محددات جودة وظيفة المراجعة الداخلية وتطبيق نموذج الحوكمة أظهر نتائج إيجابية، حيث أن معامل التفاعل كان دالاً إحصائيًا، مما يشير إلى أن التكامل بين المدخلات المهنية وهياكل الحوكمة يُعزز فعالية إدارة المخاطر، وكانت المنشآت التي تطبق نموذج الخطوط الخمسة أكثر فاعلية في التفاعل مع جودة المراجعة مقارنة بتلك التي تطبق نموذج الخطوط الثلاث. تتفق تلك النتائج مع

نتائج دراسات كل من Steinbart et al. (2012,2013,2018); Bantleon et al. (2020); Slapnicar et al. (2022); Boehm et al. (2019); Barrer and Estep (2018).

استناداً على ذلك، يمكن استنتاج عدد من النتائج الجوهرية، أبرزها أن الاستقلالية تؤدي دورًا محوريًا في تحديد جودة المراجعة الداخلية، وتتجاوز في أهميتها عامل الكفاءة. كما أن التعاون بين خطوط المساءلة الثلاث يُعد من أبرز المحددات الفاعلة للحوكمة السيبرانية. ويعد دعم الإدارة التنفيذية هو العامل الأكثر تأثيرًا في تشكيل هيكل الحوكمة. وقد أظهرت مرحلة الاستجابة للمخاطر أعلى مستويات الأداء مقارنة بمراحل إدارة الخطر الأخرى، مما يعكس نضجًا مؤسسيًا في التعامل مع التهديدات بعد وقوعها، في حين برزت الحاجة إلى مزيد من التحسين في مرحلة العلاج والتصحيح.

7-5-2 توصيات البحث

يمثل هذا البحث مساهمة علمية بارزة في إثراء الأدبيات المحاسبية المعاصرة من خلال تقديم إطار نظري وميداني لفهم العلاقة بين محددات جودة وظيفة المراجعة الداخلية المبنية على منهج المدخلات، وهيكل الحوكمة السيبراني، وإدارة مخاطر الأمن السيبراني. وفى ضوء نتائج البحث يمكن تقديم عدد من التوصيات البحثية والعملية تمثل فرص لتطوير مجالات البحوث المستقبلية، وتطوير السياسات والممارسات في مجالات المراجعة الداخلية، وحوكمة الأمن السيبراني، وإدارة المخاطر السيبرانية، وهي على النحو التالي:

- تطوير مجالات البحوث المستقبلية:

(أ) إعادة صياغة دور المراجعة الداخلية بوصفها وظيفة استراتيجية في إدارة المخاطر، حيث لم تعد المراجعة الداخلية مجرد وظيفة فنية تقويمية، بل أصبحت، في ضوء التهديدات الرقمية، عنصرًا محوريًا في التنبؤ بالمخاطر وبناء نظم الحماية، وهو ما يتطلب كفاءات عابرة للتخصصات.

(ب) الحاجة إلى بناء نظرية ناشئة حول حوكمة الأمن السيبراني، يشير البحث إلى أن الأدبيات المحاسبية لا تزال تعاني من غياب إطار نظري متكامل لحوكمة الأمن السيبراني، ويدعو إلى تطوير نظرية ناشئة تعيد تعريف العلاقة بين الحوكمة، والمراجعة، والأمن السيبراني.

(ت) أظهرت نتائج الدراسة أن نماذج القياس التكوينية متعددة الدرجات توفر إطارًا أكثر دقة لفهم العلاقات المعقدة بين جودة المراجعة، وهياكل الحوكمة، وإدارة الأمن السيبراني. وهذا من شأنه أن يوجه البحوث المستقبلية إلى تبني نماذج تحليل أكثر تعقيدًا وتكاملاً تعكس البنية الهرمية الحقيقية للمتغيرات.

- تطوير السياسات والممارسات في مجال المراجعة الداخلية:

(أ) أولوية الاستقلالية التنظيمية، كشفت النتائج أن الاستقلالية تفوق الكفاءة في التأثير على جودة المراجعة، ما يستدعي إعادة النظر في هياكل التقارير المؤسسية.

(ب) التركيز على المهارات السيبرانية للمراجعين، انخفاض نسبة الشهادات التقنية ضمن المشاركين يُشير إلى ضرورة تعزيز البرامج التدريبية التقنية للمراجعين.

(ت) الدمج الاستراتيجي للمراجعة في الحوكمة السيبرانية، يُعد خط المساءلة الثالث من أكثر المكونات فعالية، مما يستدعي إشراك أقسام المراجعة الداخلية في تطوير سياسات الأمن السيبراني.

- تطوير نظم وآليات حوكمة الأمن السيبراني:

(أ) تعزيز التعاون بين خطوط المساءلة، حيث ظهرت النتائج أن فعالية الحوكمة تزداد بوجود تنسيق فعّال بين خطوط المساءلة الثلاثة.

(ب) الدعم المحدود من مجالس الإدارة يستدعي برامج توعوية وتدريبية لتعزيز دورهم في الرقابة السيبرانية.

(ت) اعتماد نموذج الخطوط الخمسة حيث ثبت أن المنشآت التي تطبق هذا النموذج تحقق أداءً أفضل، مما يبرر تعميمه في منشآت أكثر.

- تطوير سياسات وممارسات إدارة مخاطر الأمن السيبراني

(أ) الحاجة لتقوية قدرات العلاج والتعافي، حيث أن ضعف تقييم مرحلة العلاج يشير إلى فجوة في الاستعداد لما بعد وقوع الهجمات.

(ب) الاستثمار في أدوات الاكتشاف المبكر حيث تفوق مرحلة الاكتشاف يؤكد أهميتها، ويحفز على استخدام الذكاء الاصطناعي والتحليلات المتقدمة.

(ت) التكامل بين الجهد الفني والتنظيم، يشير ارتفاع تقييم الجهد المبذول في المراجعة إلى أهمية الدمج بين التقنية والإدارة في إدارة المخاطر.

7-5-3 مجالات البحث المستقبلية المقترحة

تؤكد نتائج هذه الدراسة أهمية التكامل بين المراجعة الداخلية، والحوكمة المؤسسية، وممارسات الأمن السيبراني كمدخل لتعزيز جاهزية المنشآت ضد التهديدات الرقمية. كما أن النتائج تمهد الطريق لمجالات لبحوث مستقبلية أكثر تخصصًا وتكاملاً، على النحو التالي:

- إجراء دراسات مقارنة قطاعية لفحص اختلاف تأثير المتغيرات باختلاف طبيعة القطاع (عام، خاص، مالي، تقني...).

- قياس أثر عدد من المتغيرات الوسيطة (مثل: القدرة الإدارية، والثقافة التنظيمية، والثقة المؤسسية) في العلاقة بين الحوكمة وجودة وظيفة المراجعة الداخلية والأداء السيبراني.
- دمج الذكاء الاصطناعي والتحول الرقمي في الدراسات المستقبلية لفهم كيفية مساهمة الأدوات الذكية في تعزيز أو تهديد وظيفة المراجعة الداخلية، واستقلالية المراجعين.
- إجراء دراسات طولية (Longitudinal Studies) لقياس تطور الأداء السيبراني في المؤسسات بعد تطبيق الحوكمة على مدى الزمن.
- استخدام منهج المقارنة بين الدول لإجراء دراسات مقارنة بين بيئات تنظيمية وقانونية مختلفة (على سبيل المثال، دول الخليج مقابل دول من أوروبا).

المراجع

اولاً: المراجع باللغة العربية

أميرهم، جيهان عادل ناجي. (2022). أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وانعكاساته على ترشيد قرارات المستثمرين: دراسة ميدانية. **مجلة البحوث المالية والتجارية**، جامعة بور سعيد– كلية التجارة، (23)3، *325-377. 10.21608/JSST.2022.153499.1452*

المجلس الأعلى للأمن السيبراني (2017). الاستراتيجية الوطنية للأمن السيبراني 2017–2021. رئاسة مجلس الوزراء، جمهورية مصر العربية، 1–10. متاح على:*HTTPS://WWW.ESCC.GOV.EG/*

شحاته، شحاته السيد (2022). نحو دور فاعل للمراجع الداخلي في إدارة مخاطر الأمن السيبراني في الشركات المقيدة بالبورصة المصرية. **المجلة العلمية للدراسات والبحوث المالية والإدارية**، كلية التجارة – جامعة مدينة السادات، (13)2، 26–37. *MASF.2022.239808*/10.21608

راضي، محمد سامي (2014). تطوير دور المراجعة الداخلية في إدارة المخاطر في بيئة الأعمال المصرية: دراسة ميدانية. **مجلة التجارة والتمويل، كلية التجارة** – جامعة طنطا، (34)2،1–48 *10.21608/CAF.2014.130176*

علي، عبد الوهاب نصر. (2022). مهنة المحاسبة في مواجهة تداعيات التحول الرقمي في مصر: قصور الممارسة وحتمية التطوير. **المجلة العلمية للدراسات والبحوث المالية والإدارية**، كلية التجارة – جامعة مدينة السادات، مج (13)2، 15–25. *10.21608/MASF.2022.239797*

علي، محمود أحمد، وعلي، صالح علي صالح (2022). أثر الافصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية: دراسة تجريبية. مجلة الإسكندرية للبحوث المحاسبية، (6)3، 1–48. *10.21608/ALJALEXU.2022.268516*

يوسف، حنان محمد إسماعيل (2024). القيمة المضافة من فاعلية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني: دراسة انتقادية وتجريبية. مجلة البحوث المحاسبية، جامعة طنطا– كلية التجارة، (11)1، 525–594 *10.21608/AB J.2024.340155*

ثانياً: المراجع باللغة الاجنبية

Abbott, L. J., Parker, S., & Peters, M. F. (2007). The role of internal auditors in risk management and governance. *Journal of Accounting Research*, 45(2), 523–540. *https://doi.org/10.1111/j.1475-679X.2007.00247.x*

ACCA, & CAANZ. (2019). Cyber and the CFO. *https://www.accaglobal.com/content/dam/ACCA_Global/professional-insights/Cyber-cfo/pi-cyber-and-the-CFO.pdf*

Alles, M. (2020). The drivers of the adoption of continuous auditing: A practical response to the need for assurance on continuous data. *International Journal of Accounting Information Systems*, 36, 100465. *https://doi.org /10. 1016/ j.accinf.2019.100465*

American Institute of Certified Public Accountants (AICPA). (2018). Cybersecurity disclosure and reporting frameworks. American Institute of Certified Public Accountants.*https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-for-cybersecurity*

Arena, M., & Azzone, G. (2009). Identifying organizational drivers of internal audit effectiveness. *International Journal of Auditing, 13*(1), 43–60. *https://doi.org/10.1111/j.1099-1123.2008.00392.x*

Arena, M., Azzone, G., and Arnaboldi, M. (2010). The role of internal audit in corporate governance: A conceptual framework. *International Journal of Auditing, 14*(2), 158–173. *https://doi.org/10.1111/j.1099-1123.2009.00393.x*

Australian Institute of Company Directors (AICD), & Cyber Security Cooperative Research Centre. (2022). Cyber security governance principles. *https://www.aicd.com.au/content/dam/aicd/pdf/tools-resources/director-tools/board/cyber-security-governance-principles-web3.pdf*

Bailey, T., Banerjee, S., Feeney, C., & Hogsett, H. (2020). Cybersecurity: Emerging challenges and solutions for the boards of financial-services companies. McKinsey. *https://www.mckinsey.com/industries/financial-*

services/our-insights/cybersecurity-emerging-challenges-and-solutions-for-the-boards-of-financial-services-companies

Banker, R. D., & Feng, C. (2019). The impact of information security breach incidents on CIO turnover. *Journal of Information Systems, 33*(3), 309–329. *https://doi.org/10.2308/isys-52229*

Bantleon, U., d'Arcy, A., Eulerich, M., Hucke, A., Pedell, B., & Ratzinger-Sakel, N. (2020). Coordination challenges in implementing the three lines of defense model. SSRN. *https://ssrn.com/abstract=3663955*

Barua, A., Rama, D. V., & Sharma, V. (2010). Audit committee characteristics and investment in internal auditing. *Journal of Accounting and Public Policy, 29*(5), 503–513. *https://doi.org/10.1016/j.jaccpubpol.2010.07.005*

Basel Committee on Banking Supervision. (2011). Principles for sound management of operational risk. Bank for International Settlements. *https://www.bis.org/publ/bcbs195.htm*

Bauer, T. D., & Estep, C. (2018). One team or two? Exploring relationship quality between auditors and IT specialists and its implications for a collective audit team identity and the audit process. Working Paper. *https://ssrn.com/abstract=2579198*

Beasley, M. S., Clune, R., & Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy, 24*(6), 521–531. *https://doi.org/10.1016/j.jaccpubpol.2005.10.002*

Beasley, M. S., Clune, R., & Hermanson, D. R. (2006). The impact of enterprise risk management on the internal audit function. *Journal of Forensic Accounting, 7*(1), 1–20. *https://digitalcommons.kennesaw.edu/facpubs/1349/*

Boehm, J., Curcio, N., Merrath, P., Shenton, L., & Stähle, T. (2019). The risk-based approach to cybersecurity. McKinsey & Company. *https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity*

Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal, 33*(4), 360–376. https://doi.org/10.1108/MAJ-02-2018-1804

Brand, T. (2010). External auditors and their impact on internal audit independence: A conceptual analysis. *International Journal of Auditing, 14*(1), 21–30. https://doi.org/10.1111/j.1099-1123.2009.00382.x

Brivot, M. (2011). Controls of knowledge production, sharing and use in bureaucratized professional service firms. Organization Studies, 32(4), 489–508. https://doi.org/10.1177/0170840610397

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context Using Expert Elicitation. Risk Analysis, 42(8), 1643–1669. https://onlinelibrary.wiley.com/doi/10.1111/risa.13687

Castanheira, N., Lima Rodrigues, L., & Craig, R. (2010). Factors associated with the adoption of risk-based internal auditing. *Managerial Auditing Journal, 25*(1), 79–98. https://doi.org/10.1108/02686901011007315

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value of breached firms and Internet security developers. *International Journal of Electronic Commerce, 9*(1), 69–105. https://www.tandfonline.com/doi/abs/10.1080/10864415.2004.11044320

Center for Audit Quality (CAQ). (2018). Board governance and cybersecurity: Key principles for enhancing oversight. https://www.thecaq.org/wpcontent/uploads/2019/03/caq_cybersecurity_risk_management_oversight_tool_2018-04.pdf

Cheong, A., Yoon, K., Cho, S., & No, W. G. (2021). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. *Journal of Information Systems, 35*(2), 179–194. https://doi.org/10.2308/ISYS-2020-031

Christ, M. H., Eulerich, M., Krane, R., & Wood, D. A. (2021). New frontiers for internal audit research. Accounting Perspectives, 20(4), 449–475. https://doi.org/10.1111/1911-3838.12272

Christopher, J., Sarens, G., & Leung, P. (2009). A critical analysis of the independence of the internal audit function: Evidence from Australia. Accounting, *Auditing & Accountability Journal, 22*(2), 200–220. https://doi.org/10.1108/09513570910933942

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004). Enterprise risk management—Integrated framework. COSO. https://www.coso.org/guidance-erm

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Internal control—Integrated framework. COSO. https://www.coso.org/guidance-on-ic

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise risk management: Integrating with strategy and performance. COSO. https://www.coso.org/enterprise-risk-management

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4(10), 13–21. https://timreview.ca/article/835

Crowe, C., & Internal Audit Foundation. (2018). the future of cybersecurity in internal audit. *Internal Audit Foundation*. https://www.crowe.com/-/media/Crowe/LLP/folio-pdf/The-Future-of-Cybersecurity-in-IA-RISK-18000-002A-update.pdf

De Haes, S., & Van Grembergen, W. (2015). Enterprise governance of information technology: Achieving strategic alignment and value. Springer. https://www.springer.com/gp/book/9783319145471

Deloitte. (2015a). Cybersecurity and the role of internal audit: An urgent call to action. Deloitte Insights. https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-internal-audit-role.html

Deloitte. (2015b). Governance in brief: Is your organisation prepared for a cyber-attack? Deloitte Insights. *https://www2.deloitte.com/content/ dam/Deloitte/ uk/Documents/audit/deloitte-uk-gov-in-brief-nov-2015.pdf*

Deloitte. (2017). Cybersecurity governance and risk management: Insights for executives. Deloitte Insights. *https://www2.deloitte.com/us/en/pages/ risk/articles/cybersecurity-governance-risk-management-insights.html*

Desai, N. K., Gerard, G. J., & Tripathy, A. (2011). Internal audit sourcing arrangements and reliance by external auditors. Auditing: *A Journal of Practice & Theory, 30*(1), 149–171. *https://doi.org/10.2308/aud.2011.30.1.149*

Desai, V., Roberts, R. W., & Srivastava, R. (2010). An analytical model for external auditor evaluation of the internal audit function using belief functions. Contemporary Accounting Research, 27(2), 537–575. *https://doi.org/10.1111/j.1911-3846.2010.01016.x*

Dittenhofer, M. (1997). Behavioural aspects of internal auditing "revisited". *Managerial Auditing Journal, 12*(1), 23–27. *https://doi.org/10.1108/ EUM0000000004309*

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79–98. *https://doi.org/10.1287/isre.1070.0160*

Erasmus, L. J., & Coetzee, P. (2018). Drivers of stakeholders' view of internal audit effectiveness: Management versus audit committee. *Managerial Auditing Journal, 33*(1), 90–114. *https://doi.org/10.1108/MAJ-05-2017-1558*

EY. (2019). How financial services organizations manage cyber risk. EY Insights. *https://www.ey.com/en_gl/consulting/how-financial-services-organizations-can-manage-cyber-risk*

EY, & The Institute of Internal Auditors. (2021). The risky six. Key questions to expose gaps in board understanding of organizational cyber resiliency. *https://www.theiia.org/globalassets/site/ey-the-risky-six-board-disconnections.pdf*

Eulerich, M. (2021). The new three lines model for structuring corporate governance – A critical discussion of similarities and differences. Corporate Ownership & Control, 18(2), 180–187. https://doi.org/10.22495/cocv18i2art15

Fanning, K., & Piercey, M. D. (2014). Internal auditors' use of interpersonal likability, arguments, and accounting information in a corporate governance setting. Accounting, Organizations and Society, 39(8), 575–589. https://doi.org/10.1016/j.aos.2014.07.002

Feng, C., & Wang, T. (2019). Does CIO risk appetite matter? Evidence from information security breach incidents. *International Journal of Accounting Information Systems*, 32, 59–75. https://doi.org/10.1016/j.accinf.2018.11.001

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Gale, M., Bongiovanni, I., & Slapničar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. Computers & Security, 121, 102840. https://doi.org/10.1016/j.cose.2022.102840

Glover, S. M., Prawitt, D. F., & Wood, D. A. (2008). Internal audit sourcing arrangement and the external auditor's reliance decision. Contemporary Accounting Research, 25(1), 193–213. https://doi.org/10.1506/car.25.1.7

Gramling, A. A., Maletta, M. J., Schneider, A., & Church, B. K. (2004). The role of the internal audit function in corporate governance: A synthesis of the extant internal auditing literature and directions for future research. *Journal of Accounting Literature, 23*, 194–244. https://www.researchgate.net/publication/284061551

Gramling, A. A., & Vandervelde, S. D. (2006). Assessing internal audit quality. Internal Auditing, 21(3), 26–33. https://digitalcommons.Kennesaw.edu/facpubs/1332/

Gregogry and Austin LLP (2014), "Board oversight of cybersecurity risks", avaialble at:*https:// content.next.westlaw.com/5-558-2825?transitionType= Default &contextData=(sc.Default)&__lrTS=20170609212306243&firstPage=true & bhcp=1*

Guthrie, C., Fosso-Wamba, S., & Arnaud, J. B. (2021). Online Consumer Resilience During a Pandemic: An Exploratory Study of E-Commerce Behavior Before, During and After a COVID-19 Lockdown. *Journal of Retailing and Consumer Services, 61*, 102570. *https://www.sciencedirect.com/science/article/pii/S0969698921001363*

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal, 34*(7), 808–834. *https://doi.org/10.1108/MAJ-09-2018-2004*

Haislip, J. Z., Masli, A., Richardson, V. J., & Sanchez, J. M. (2016). Repairing organizational legitimacy following information technology (IT) material weaknesses: Executive turnover, IT expertise, and IT system upgrades. *Journal of Information Systems, 30*(1), 41–70. *https://doi.org/10.2308/isys-51294*

Haislip, J., Karim, K., Lin, K. J., & Pinsker, R. (2020). The influences of CEO IT expertise and board-level technology committees on Form 8-K disclosure timeliness. *Journal of Information Systems, 34*(2), 167–185. *https://doi.org/10.2308/isys-52623*

Haislip, J., Lim, J. H., & Pinsker, R. (2021). The impact of executives' IT expertise on reported data security breaches. Information Systems Research, 32(2), 318–334. *https://doi.org/10.1287/isre.2020.0986*

Havelka, D., & Merhout, J. W. (2013). Internal information technology audit process quality: Theory development using structured group processes. *International Journal of Accounting Information Systems, 14*(3), 165–192. *https://doi.org/10.1016/j.accinf.2012.12.001*

Hazaea, S. A., Zhu, J., Khatib, S. F., & Elamer, A. A. (2023). Mapping the literature of internal auditing in Europe: A systematic review and agenda for

future research. *Meditari Accountancy Research, 31*(6), 1675–1706. https://doi.org/10.1108/MEDAR-01-2022-1584

Higgs, J. L., Pinsker, R., Smith, T., & Young, G. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems, 30*(3), 79–98. https://doi.org/10.2308/isys-51402

Héroux, D., & Fortin, J. (2013). The internal audit function in information technology: A holistic perspective. *Managerial Auditing Journal, 28*(5), 455–485. https://doi.org/10.1108/02686901311327273

ISACA. (2011). COBIT 5: The Framework. Rolling Meadows: ISACA.

ISACA. (2012a). COBIT 5 Enabling Processes. Rolling Meadows, IL: ISACA.

ISACA. (2012b). COBIT 5 for Information Security. Rolling Meadows, IL: ISACA.

ISACA. (2016). State of Cybersecurity: Implications for 2016. https://www .isaca.org/cyber/Documents/state-of-cybersecurity _res _eng _0316.pdf

ISACA. (2019). COBIT 2019: An ISACA Framework. ISACA. https://www.isaca.org/resources/cobit

IT Governance Institute. (2007a). Control objectives for information and related technology, 4.1. Rolling Meadows, IL: IT Governance Institute.

IT Governance Institute. (2007b). IT assurance guide using COBIT. IL: IT Governance Institute.

ITGI. (2012). IT Governance and Internal Audit: Key Issues and Best Practices. Information Technology Governance Institute.

Institute of Internal Auditors (IIA). (2013). the three lines of defense in effective risk management and control. https://na.theiia.org/standards-guidance/ Public%20Documents/PP%20The%20.Three%20Lines%20of%20Defense %20in%20Effective%20Risk%20Management%20and%20Control.pdf

Institute of Internal Auditors (IIA). (2016). Assessing cybersecurity risk: Roles of the three lines of defense. https://guidance/Member%20Documents/GTAG-Assessing-Cybersecurity-Risk.pdf

Institute of Internal Auditors (IIA). (2017). Assessing cybersecurity risk: The internal audit activity's role. The Institute of Internal Auditors. *https://www.theiia.org/globalassets/documents/content/articles/guidance/gtag/gtag-assessing-cybersecurity-risk.pdf*

Institute of Internal Auditors (IIA). (2020). The IIA's three lines model: An update of the three lines of defense. *https://www.iia.org.au/technical-resources/professionalGuidance/the-iia's-three-linesmodel*

Institute of Internal Auditors Research Foundation. (2015). Common Body of Knowledge (CBOK).

https://global.theiia.org/iiarf/Public%20Documents/CBOK-2015-Vision-Brochure.pdf

*International Organization for Standardization / Intern*ational Electrotechnical Commission (ISO/IEC). (2013). ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements. *https://www.iso.org/standard/54534.html*

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

Jeyaraj, A., & Zadeh, A. (2020). Institutional isomorphism in organizational cybersecurity: A text analytics approach. *Journal of Organizational Computing and Electronic Commerce, 30*(4), 361–380. *https://doi.org/10.1080/10919392.2020.1776033*

Kahyaoglu, S. B., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal, 33*(4), 360–376. *https://doi.org/10.1108/MAJ-02-2018-1804*

Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). Regulatory approaches for cybersecurity of critical infrastructures: The case of Turkey. Computer Law & Security Review, 32(3), 526–539. *https://doi.org/10.1016/j.clsr.2016.02.005*

Khan, S. N., Asad, M., Fatima, A., Anjum, K., & Akhtar, K. (2020). Outsourcing internal audit services: A review. *International Journal of Management, 11*(8), 503–517. https://doi.org/10.34218/IJM.11.8.2020.04

KPMG. (2014). *Cyber security: It's not just about technology*. KPMG LLP. Retrieved from https://assets.kpmg.com/content/dam/kpmg/pdf/2014/05/cyber-security-not-just-technology.pdf

Kwon, J., Ulmer, J. R., & Wang, T. (2013). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems, 27*(1), 219–236. https://doi.org/10.2308/isys-50339

Leech, T. J., & Hanlon, L. C. (2016). Three lines of defense versus five lines of assurance. In R. LeBlanc (Ed.), The Handbook of Board Governance: A Comprehensive Guide for Public, Private, and Not-for-Profit Board Members (pp. 335–355). Hoboken, NJ: John Wiley & Sons.

Leech, T. J., & Hanlon, L. C. (2017). Board Cyber Risk Oversight. In D. Antonucci (Ed.), The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities (pp. 11–21). Hoboken, NJ: John Wiley & Sons.

Li, D. C. (2015). Online security performances and information security disclosures. *Journal of Computer Information Systems, 55*(2), 20–28. https://doi.org/10.1080/08874417.2015.11645753

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior. *International Journal of Information Management, 45*, 13–24. https://www.sciencedirect.com/science/article/pii/S0268401218302093

Lin, S., Pizzini, M., Vargus, M., & Bardhan, I. (2011). The role of the internal audit function in the disclosure of material weaknesses. The Accounting Review, 86(1), 287–323. https://doi.org/10.2308/accr.00000016

Liu, C.-W., Huang, P., & Lucas, H. C. (2020). Centralized IT decision making and cybersecurity breaches: Evidence from U.S. higher education institutions. *Journal of Management Information Systems, 37*(3), 758–787. https://doi.org/10.1080/07421222.2020.1790190

Love, P., Reinhard, J., Schwab, A., & Spafford, G. (2010). Global Technology Audit Guide (GTAG) 15: Information Security Governance. Altamonte Springs, FL: The Institute of Internal Auditors. https://www.scribd. com/ document/124305052/Global-Technology-Audit-Guide-Practice-Guide-Information-Security-Governance

Lyons, S. (2011). Corporate oversight and stakeholder lines of defense. The Conference Board Executive Action Report, (365), October 2011. https://ssrn.com/abstract=1938360

Ma'ayan, Y., & Carmeli, A. (2016). Internal audits as a source of ethical behavior, efficiency, and effectiveness in work units. Journal of Business Ethics, 137(2), 347–363. https://doi.org/10.1007/s10551-015-2561-0

McKinsey & Company. (2018). A time for boards to act. McKinsey Global Survey. https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/ our-insights/a-time-for-boards-to-act

Mihret, D. G., & Yismaw, A. W. (2007). Internal audit effectiveness: An Ethiopian public sector case study. *Managerial Auditing Journal, 22*(5), 470–484. https://doi.org/10.1108/02686900710750757

Morris, T., & Empson, L. (1998). Organisation and expertise: An exploration of knowledge bases and the management of accounting and consulting firms. Accounting, Organizations and Society, 23(5–6), 609–624. https://doi.org/10.1016/S0361-3682(98)00032-4

Nasdaq & Tanium. (2016). The Accountability Gap: Cybersecurity & Building a Culture of Responsibility. Goldsmiths, University of London. Retrieved from https://www.tanium.com/blog/cybersecurity-accountability-gap/

National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S.

Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Nolan, R., & McFarlan, F. W. (2005). Information technology and the board of directors. *Harvard Business Review, 83*(10), 96–106.

Olyaei, S., Thielemann, K., Addiscott, R., & Pratap, K. (2021). Predicts 2021: Cybersecurity Program Management and IT Risk Management. Gartner. Retrieved from https://www.gartner.com/en/documents/4000465

Organisation for Economic Co-operation and Development (OECD). (2015). Digital security risk management for economic and social prosperity. OECD Publishing. https://doi.org/10.1787/9789264245471-en

Patten, D. M. (2005). An analysis of the impact of locus-of-control on internal auditor job performance and satisfaction. *Managerial Auditing Journal, 20*(9), 1016–1029. https://doi.org/10.1108/02686900510625343

Pienta, D., Thatcher, J. B., & Johnston, A. (2020). Protecting a Whale in a Sea of Phish. *Journal of Information Technology, 35*(3), 214–231. https://aisel.aisnet.org/jit/vol35/iss3/11/

Protiviti (2015), "The Battle Continues – Working to Bridge the Data Security Chasm", available at: www.protiviti.com/sites/default/files/united_states/insights/2015-it-security-privacy-survey-protiviti.pdf

Radcliffe, V. S. (1999). Knowing efficiency: The enactment of efficiency in efficiency auditing. Accounting, Organizations and Society, 24(4), 333–362. https://doi.org/10.1016/S0361-3682(98)00067-1

Radcliffe, V. S. (2008). Public secrecy in auditing: What government auditors cannot know. Critical Perspectives on Accounting, 19(1), 99–126. https://doi.org/10.1016/j.cpa.2006.07.004

Radcliffe, V. S. (2011). Public secrecy in government auditing revisited. Critical Perspectives on Accounting, 22(7), 722–732. https://doi.org/10.1016/j.cpa.2011.01.014

Romanosky, S. (2018). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 4*(1), tyy010. https://doi.org/10.1093/cybsec/tyy010

Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. MIT Sloan Management Review, 59(2), 12–15.https://sloanreview.mit.edu/article/the-boards-role-in-managing-cybersecurity-risks/

Roussy, M. (2015). Welcome to the Day-to-Day of Internal Auditors: How Do They Cope with Conflicts? Auditing: *A Journal of Practice & Theory, 34*(2), 237–264. https://doi.org/10.2308/ajpt-50904

Roussy, M., & Brivot, M. (2016). Internal audit quality: A polysemous notion? *Accounting, Auditing & Accountability Journal, 29*(5), 714–738. https://doi.org/10.1108/AAAJ-10-2014-1843

Sabillon, R., Cavaller, V., Serra-Ruiz, J., & Cano, J. (2017). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In Proceedings of the 2017 International Conference on Information Systems and Computer Science (INCISCOS) (pp. 253–259). IEEE. https://doi.org/10.1109/INCISCOS.2017.20

Sambamurthy, V., & Zmud, R. W. (1999). Arrangements for information technology governance: A theory of multiple contingencies. MIS Quarterly, 23(2), 261–290. https://doi.org/10.2307/249754

San Miguel, J. G., & Govindarajan, V. (1984). The contingent relationship between the controller and internal audit functions in large organizations. Accounting, Organizations and Society, 9(2), 179–188. https://doi.org/10.1016/0361-3682(84)90006-0

Sarens, G., & De Beelde, I. (2006). Internal auditors' perception about their role in risk management: A comparison between US and Belgian companies. *Managerial Auditing Journal, 21*(1), 63–80. https://doi.org/10.1108/02686900610634766

Selim, G., & Yiannakas, A. (2000). Outsourcing the internal audit function: A survey of the UK public and private sectors. *International Journal of Auditing, 4*(3), 213–226. https://doi.org/10.1111/1099-1123.00314

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, 44, 100548. https://doi.org/10.1016/j.accinf.2021.100548

Smith, T., Tadesse, A. F., & Vincent, N. E. (2021). The impact of CIO characteristics on data breaches. *International Journal of Accounting Information Systems, 43*, 100532. https://doi.org/10.1016/j.accinf.2021.100532

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Steinbart, P. J., Raschke, R. L., & Dilla, W. N. (2018). Cybersecurity auditing: Building a framework for effective audits. *International Journal of Auditing, 22*(1), 101–120. https://doi.org/10.1111/ijau.12112

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

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2013). Information security professionals' perceptions about the relationship between the information security and internal audit functions. *Journal of Information Systems, 27*(2), 65–86. https://doi.org/10.2308/isys-50510

ThreatTrack. (2016). Security analysts say defending against advanced malware still a major struggle. Retrieved from http://www.threattracksecurity.com/resources/whitepapers/security-analysts-say-defending-against-advanced-malware-still-a-major-struggle.aspx

Tysiac, K. (2014, March 24). Auditors have important role in cybersecurity. *Journal of Accountancy*. https://www.journalofaccountancy.com/news/2014/mar/20149771.html

Van Grembergen, W., De Haes, S., & Guldentops, E. (2004). Structures, Processes and Relational Mechanisms for IT Governance. In W. Van Grembergen (Ed.), Strategies for Information Technology Governance (pp. 1–36). IGI Global.

Vasarhelyi, M. A., Kogan, A., & Tuttle, B. M. (2015). Big data in accounting: An overview. Accounting Horizons, 29(2), 381–396. https://doi.org/10.2308/acch-51071

Vincent, N. E., Higgs, J. L., & Pinsker, R. E. (2019). Board and management-level factors affecting the maturity of IT risk management practices. *Journal of Information Systems, 33*(3), 117–135. https://doi.org/10.2308/isys-52276

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security – what goes where? Information & Computer Security, 26(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Walker, P., Shenkir, W. G., & Barton, T. L. (2002). Enterprise Risk Management: Putting It All Together. Altamonte Springs, FL: Institute of Internal Auditors Research Foundation.

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research, 24*(2), 201–218. https://doi.org/10.1287/isre.1120.0437

Wang, X. (1997). Development trends and future prospects of internal auditing. *Managerial Auditing Journal, 12*(4/5), 200–204. https://doi.org/10.1108/02686909710173885

Wilkin, C. L., & Chenhall, R. H. (2020). Information technology governance: Reflections on the past and future directions. *Journal of Information Systems, 34*(2), 257–292. https://doi.org/10.2308/isys-52632

World Economic Forum. (2021). Cyber resilience and governance: A framework for organizations. *https://www3.weforum.org/docs/WEF_Unpacking_Cyber_Resilience_2024.pdf*

World Economic Forum. (2024). the Global Risks Report 2024. *https://www.weforum.org/publications/global-risks-report-2024/*

Yoo, C. W., Goo, J., & Rao, H. R. (2020). Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. MIS Quarterly, 44(2), 907–931. *https://doi.org/10.25300/ MISQ/ 2020/15477*

ملحق 1: الاستبيان

السادة المشاركين الكرام ،،،

تحية طيبة وبعد،،،

في إطار إعداد دراسة أكاديمية بعنوان: "**أثر محددات جودة وظيفة المراجعة الداخلية وهيكل الحوكمة السيبراني على مؤشرات إدارة مخاطر الأمن السيبراني: استخدام نماذج المعادلات الهيكلية القائمة على المربعات الصغرى**" والتي تُعَد جزءًا من الجهود العلمية الهادفة إلى تعزيز فعالية إدارة الأمن السيبراني داخل المنشآت، أُقدِّم هذا الاستبيان لأخذ آرائكم وخبراتكم العملية في هذا المجال المهم. تهدف هذه الدراسة إلى استكشاف العلاقة بين جودة وظيفة المراجعة الداخلية وهيكل الحوكمة السيبراني، وتأثير ذلك على تحسين مؤشرات إدارة مخاطر الأمن السيبراني في المؤسسات المختلفة، وذلك بالاعتماد على أساليب تحليل إحصائي متقدمة.

ملاحظات هامة:

- المعلومات المقدمة سيتم استخدامها لأغراض البحث العلمي فقط.
- سيتم التعامل مع كافة الإجابات بسرية تامة ولن يتم الإفصاح عن أي بيانات شخصية أو مؤسسية.
- المشاركة في هذا الاستبيان اختيارية، مع التأكيد على أهمية المساهمة الصادقة لما لها من أثر كبير في جودة مخرجات البحث.

الفئة المستهدفة:

مديرو المراجعة الداخلية، وأعضاء لجان المراجعة، ومسؤولو الحوكمة، مسؤولو تكنولوجيا وأمن المعلومات، وأعضاء مجالس الإدارة، والمختصون في المجالات ذات الصلة.

يستغرق تعبئة هذا الاستبيان ما بين **10 إلى 15 دقيقة**، ويسرني كثيرًا تعاونكم الكريم.

مع خالص الشكر والتقدير،

الباحث

د. محمد عبد المنعم سراج

مدرس بقسم المحاسبة – أكاديمية السادات للعلوم الإدارية

الجزء الأول: الخصائص الديموغرافية والمهنية للمستجوبين والبيانات الوصفية للمنشآت عينة الدراسة

الجزء الأول	الخصائص الديموغرافية والمهنية للمستجوبين
1. الوظيفة	o مدير المراجعة التنفيذي
	o عضو في لجنة المراجعة
	o عضو في قسم المراجعة الداخلية
	o عضو مجلس إدارة
	o عضو في قسم IT
	o أخري
2. التأهيل المهني	o محاسب قانوني معتمد/ مراجع داخلي معتمد CPA/CIA
	o مراجع نظم معلومات معتمد CISA
	o مدير أمن المعلومات المعتمد CISM
	o محترف معتمد في أمن السحابة CCSP
	o محترف معتمد في أمن نظم المعلومات CISSP
	o معتمد في التحكم في المخاطر ونظم المعلومات CRISC
	o إطار عمل الأمن السيبراني NIST (NCSF)
	o مساعد شبكات معتمد من CISCO (CCNA)
	o شهادات مهنية أخري
	o لا يوجد
3. الجنس	o ذكر
	o أنثي
4. الخبرة	o أقل من 5 سنوات
	o من 6 – 10سنوات
	o من 11 – 15سنوات
	o من 16 – 20سنوات
	o أكثر من 21 سنة
5. العمر	o أقل من 30 عام
	o من 30 – 40عام
	o من 40 – 50عام
	o أكثر من 50 عام

الجزء الثاني	البيانات الوصفية للمنشأة التي تعمل بها
1. القطاع	o صناعي o حكومي o خدمات مالية وبنوك o خدمات تقنية المعلومات والاتصالات o خدمات صحة وتعليم o سياحة o أخري
2. الحجم (عدد العاملين في المنشأة)	o أقل من 20 موظف o من 20 – 99 موظف o من 100 – 299 موظف o من 300 – 499 موظف o من 500 – 999موظف o أكثر من 1000 موظف o لا أعرف
3. الحجم (إجمالي الأصول)	o من0 – 10مليون o من أكبر من 10 مليون – 50مليون o من أكبر من 50 مليون – 250مليون o من أكبر من 250 مليون – 500مليون o أكبر من 500 مليون o لا أعرف
4. عدد العاملين في قسم المراجعة الداخلية	o من 1 –5مراجع داخلي o من 6 – 10مراجع داخلي o من 11 – 20 مراجع داخلي o من 21 – 50 مراجع داخلي o أكثر من 50 مراجع داخلي o لا أعرف
5. عدد العاملين في إدارات تكنولوجيا وأمن المعلومات	o من 1 – 10موظف o من 11 – 25موظف o من 26 – 50موظف o أكثر من 50موظف o لا أعرف

الجزء الثاني: توصيف درجات المقياس المستخدم في الاستبيان

درجة المقياس				
1	2	2	4	5
توصيف المقياس				
o لا أوافق بشدة/نادرة الحدوث/لا يتم/لا يوجد/ لا يوجد تأثير واضح أو o أقل من شهر أو o أقل من 20% أو o لا يتم إجراء التقييم أو الاختبار	o لا أوافق/نادراً /غير كافي /منخفض/ ضعيف أو o من شهر إلى أقل من شهرين أو o من 20% إلى أقل من 40% أو o إجراء التقييم أو الاختبار مرة واحدة	o محايد/أحياناً/غير كافي إلى حد ما/متوسط أو o من 2 إلى أقل من 3 شهور o من 40% إلى أقل من 60% o إجراء التقييم أو الاختبار من 2-3 مرات	o أوافق/غالباً/كافي ولكن بشكل محدود/مرتفع o من 3-5 شهور o من 60% إلى أقل من 80% o إجراء التقييم أو الاختبار من3-5مرات	o أوافق بشدة/دائماً/كافي جداً/مرتفع جداً o أكثر من٥ شهور o أكثر من 80% o أكثر من 5 مرات

	العبارات	1	2	2	4	5
X1	جودة المراجعة الداخلية على أساس منهج المدخلات					
X11	الكفاءة					
X11-1	الشهادات المهنية					
X11-11	ما نسبة أعضاء الفريق الحاصلين على شهادات مهنية متخصصة في الأمن السيبراني؟					
X11-12	كيف يتم تقييم تأثير الشهادات المهنية على الأداء الفعلي للفريق؟					
X11-2	الخلفية الأكاديمية					
X11-21	ما هو أعلى مستوى أكاديمي لأعضاء الفريق؟ (١) البكالوريوس، (٢) دبلوم عالي، (٣) الماجستير، (٤) الدكتوراه، (٥) دراسات متقدمة ومتخصصة					
X11-22	هل ترى أن الخلفية الأكاديمية الحالية للفريق كافية لتلبية متطلبات المراجعة السيبرانية؟					
X11-3	التدريب والتطوير المستمر					
X11-31	ما مدى تكرار برامج التدريب المقدمة للفريق؟					
X11-32	هل توفر المؤسسة فرصًا للتعلم من خلال المؤتمرات أو ورش العمل الخارجية؟					
X11-33	هل توفر المؤسسة نظامًا لتحفيز أعضاء الفريق على حضور التدريبات؟					
X12	الاستقلالية					
X12-1	الاستعانة بمستشارين والتعاقد الخارجي					
X12-11	هل ترى أن الاستعانة بخدمات خارجية يمكن أن تؤثر على استقلالية قسم المراجعة الداخلية؟					
X12-12	هل يتم تقييم أداء المستشارين الخارجيين بناءً على معايير محددة من قبل قسم المراجعة الداخلية؟					
X12-13	هل تؤثر الكفاءة العالية التي يقدمها المستشارون الخارجيون على قدرة الفريق الداخلي على اتخاذ قرارات مستقلة؟					
X12-14	هل تعتقد أن التكاليف المرتبطة بالخدمات الخارجية مبررة بالنسبة للقيمة المضافة؟					
X12-2	الارتباط مع لجنة المراجعة والإدارة					

X12-21	هل توجد سياسات واضحة تُحدد مسؤوليات لجنة المراجعة والإدارة وقسم المراجعة الداخلية في مجال الأمن السيبراني؟	نعم	لا
X12-22	هل يتم تحديد نطاق عمل المراجعة الداخلية في مجال الأمن السيبراني بالتنسيق مع لجنة المراجعة؟	نعم	لا
X12-23	هل يتم تقديم تقارير المراجعة الداخلية مباشرة إلى لجنة المراجعة؟	نعم	لا
X12-24	هل توفر لجنة المراجعة الموارد اللازمة لقسم المراجعة الداخلية لضمان فعالية المراجعة في مجال الأمن السيبراني؟	نعم	لا
D	هل تطبق الشركة هيكل حوكمة سيبرانية مبني على خطوط للمساءلة	نعم	لا

C	إذا كانت الاجابة بنعم، هل تطبق الشركة نموذج مبني على خطوط للمساءلة الثلاث/الخمس	نموذج الخطوط الخمس	نموذج الخطوط الثلاث

نموذج حوكمة سيبراني مبني على ثلاث خطوط للمساءلة	نموذج حوكمة سيبراني مبني على خمس خطوط للمساءلة
1. وظيفة تكنولوجيا المعلومات	1. وظيفة تكنولوجيا المعلومات
2. وظيفة أمن المعلومات السيبرانية	2. وظيفة أمن المعلومات السيبرانية
3. وظيفة المراجعة الداخلية	3. وظيفة المراجعة الداخلية
	4. الإدارة التنفيذية مجلس الإدارة

	العبارات	1	2	2	4	5
	5. مجلس الإدارة					
X2	الهيكل المتكامل للحوكمة السيبراني					
X21	هيكل حوكمة سيبراني يستند إلى خطوط المساءلة الثلاث					
X21-1	فعالية أداء خط المساءلة الأول في هيكل الحوكمة					
X21-11	كم مرة يتم تحديث الأنظمة والتطبيقات بأحدث التحديثات الأمنية؟					
X21-12	ما مدي الالتزام بتطبيق سياسات أمن المعلومات على الأنظمة والبنية التحتية؟					
X21-13	ما مدى التعاون بين قسم تكنولوجيا المعلومات وأمن المعلومات في وضع خطط الحماية؟					
X21-2	فعالية أداء خط المساءلة الثاني في هيكل الحوكمة					
X21-21	ما نسبة الهجمات السيبرانية التي تم اكتشافها ومعالجتها بنجاح؟					
X21-22	ما نسبة الموظفين الذين تلقوا تدريبًا حول التهديدات السيبرانية خلال العام الماضي؟					
X21-23	ما مدى سرعة تنفيذ التوصيات الأمنية المقدمة من المراجعة الداخلية؟					
X21-3	فعالية أداء خط المساءلة الثالث في هيكل الحوكمة					
X21-31	كم عدد المراجعات الأمنية التي أجريت خلال العام الماضي؟					
X21-32	ما نسبة توصيات المراجعة الداخلية التي تم تنفيذها من قبل الأقسام الأخرى؟					
X21-33	هل يتم مراجعة الحوادث الأمنية من قبل المراجعة الداخلية لتحديد مدى فاعلية استجابة قسم أمن المعلومات؟					
X21-4	جودة التعاون بين خطوط المساءلة الثلاث					
X21-41	كيف تصف جودة التنسيق بين الأقسام الثلاثة (تكنولوجيا المعلومات، أمن المعلومات، المراجعة الداخلية)؟					
X21-42	هل يتم تحديد المسؤوليات بوضوح بين الأقسام الثلاثة (تكنولوجيا المعلومات، أمن المعلومات، المراجعة الداخلية)؟					
X21-43	هل يشعر الموظفون بالتعاون الكافي بين الأقسام الثلاثة لتحقيق أهداف الأمن السيبراني؟					
X21-44	هل يشارك قسم أمن المعلومات نتائج التقييم الأمني مع المراجعة الداخلية؟					
X21-45	هل يتم التخطيط للمشاريع المشتركة بين الأقسام الثلاثة بشكل متكامل؟					
X22	دعم الإدارة التنفيذية ومجلس الإدارة (خط المساءلة الرابع والخامس)					
X22-1	دعم الإدارة التنفيذية (خط المساءلة الرابع)					
X22-11	ما مدى توافق استراتيجية الأمن السيبراني مع الأهداف التشغيلية للمنشأة؟					
X22-12	هل الميزانية المخصصة للأمن السيبراني كافية لتلبية احتياجات المنشأة؟					
X22-2	دعم مجلس الإدارة (خط المساءلة الخامس)					
X22-21	كم مرة يتم مناقشة تقارير الأمن السيبراني في اجتماعات مجلس الإدارة؟					
X22-22	هل يقدم مجلس الإدارة توجيهات واضحة لضمان الامتثال للسياسات الأمنية؟					
Y	مؤشرات إدارة مخاطر الأمن السيبراني					
Y1	مؤشرات مرحلة الوقاية/المنع					
Y11	ما نسبة الأنظمة المحدثة بشكل منتظم؟					
Y12	كم عدد اختبارات الاختراق (Penetration Testing) التي أجريت في العام الماضي؟					

	العبارات	1	2	2	4	5
Y13	كم مرة يتم إجراء تقييم نقاط الضعف (Vulnerability Assessments) سنويًا؟					
Y14	كم عدد نقاط الضعف في نظام الرقابة الداخلية للأمن السيبراني التي أبلغ عنها قسم المراجعة الداخلية إلى لجنة المراجعة أو مجلس الإدارة أو الإدارة التنفيذية؟					
Y2	مؤشرات مرحلة الاكتشاف					
Y21	كم عدد الحوادث التي تم اكتشافها قبل أن تؤثر على العمليات خلال العام الماضي؟					
Y22	ما نسبة الأنظمة المغطاة بأنظمة مراقبة الأحداث الأمنية(SIEM) ؟					
Y23	كم عدد التنبيهات التي تم تصنيفها كحقيقية (True Positives) خلال العام الماضي؟					
Y24	كم عدد اختبارات المحاكاة (Simulated Attacks) التي تم تنفيذها لاختبار أنظمة الاكتشاف؟					
Y3	مؤشرات مرحلة الاستجابة					
Y31	كم حادثًا سيبرانيًا تم الاستجابة له خلال العام الماضي؟					
Y32	ما نسبة الحوادث التي تم احتواؤها دون تأثير كبير على العمليات؟					
Y4	مؤشرات مرحلة العلاج					
Y41	كم عدد الحوادث التي تم تنفيذ إجراءات تصحيحية لها خلال العام الماضي؟					
Y42	كم عدد التحديثات الأمنية التي تم تطبيقها لتصحيح نقاط الضعف المكتشفة؟					
X3	مستوي الجهد المخصص لعمليات المراجعة الداخلية للأمن السيبراني					
X31	ما هي نسبة الوقت الذي يخصصه قسم المراجعة الداخلية لمراجعة الأمن السيبراني؟					
X4	حجم قسم المراجعة الداخلية					
X41	ما هي نسبة عدد المراجعين الداخليين المخصصين لمراجعة عمليات الأمن السيبراني؟					
X5	مستوي الرقمية في العمليات					
X51	ما هي نسبة العمليات التي تم تحويلها إلى عمليات رقمية في الشركة؟					

ملحق 2: البيانات الديموغرافية والمهنية والبيانات الوصفية للمنشآت عينة البحث

الجزء الأول	الخصائص الديموغرافية والمهنية للمستجوبين		
البعد	الابعاد الفرعية	العدد	النسبة
(1) الوظيفة	مدير المراجعة التنفيذي	28	24.3٪
	عضو في لجنة المراجعة	14	12.2٪
	عضو في قسم المراجعة الداخلية	20	17.4٪
	عضو مجلس إدارة	10	8.7٪
	عضو في قسم IT	17	14.8٪
	أخري	26	22.6٪
(2) التأهيل المهني	محاسب قانوني معتمد/ مراجع داخلي معتمد CPA/CIA	63	54.8٪
	مراجع نظم معلومات معتمد CISA	2	1.7٪
	مدير أمن المعلومات المعتمد CISM	2	1.7٪
	محترف معتمد في أمن السحابة CCSP	--	--
	محترف معتمد في أمن نظم المعلومات CISSP	--	--
	معتمد في التحكم في المخاطر ونظم المعلومات CRISC	--	--
	إطار عمل الأمن السيبراني NIST (NCSF)	5	4.3٪
	مساعد شبكات معتمد من CISCO (CCNA)	3	2.6٪
	شهادات مهنية أخري	9	7.9٪
	لا يوجد	31	27٪
(3) الجنس	ذكر	50	43.5٪
	أنثي	65	56.5٪
(4) الخبرة	أقل من 5 سنوات	25	21.7٪
	من 6 – 10سنوات	17	14.8٪
	من 11 – 15سنوات	18	15.6٪
	من 16 – 20سنوات	25	21.7٪
	أكثر من 21 سنة	30	26.2٪
(5) العمر	أقل من 30 عام	24	21٪
	من 30 – 40عام	19	16.4٪
	من 40 – 50عام	36	31.3٪
	أكثر من 50 عام	36	31.3٪

الجزء الثاني	البيانات الوصفية للمنشآت عينة الدراسة		
البعد	الابعاد الفرعية	العدد	النسبة
(1) القطاع	صناعي	18	٪15.6
	حكومي	10	٪8.6
	خدمات مالية وبنوك	19	٪16.5
	خدمات تقنية المعلومات والاتصالات	28	٪24.3
	خدمات صحة وتعليم	12	٪10.4
	سياحة	15	٪13.3
	أخري	13	٪11.3
(2) الحجم (عدد العاملين في المنشأة)	أقل من 20 موظف	10	8.7%
	من 20 – 99 موظف	22	19.3%
	من 100 – 299 موظف	13	11.3%
	من 300 – 499 موظف	19	16.5%
	من 500 – 999موظف	17	14.7%
	أكثر من 1000 موظف	16	13.9%
	لا أعرف	18	15.6%
(3) الحجم (إجمالي الأصول)	من0 – 10مليون	23	20.3%
	من أكبر من 10 مليون – 50مليون	12	10.4%
	من أكبر من 50 مليون – 250مليون	17	14.7%
	من أكبر من 250 مليون – 500مليون	20	17.3%
	أكبر من 500 مليون	11	9.5%
	لا أعرف	32	27.8%
(4) عدد العاملين في قسم المراجعة الداخلية	من 1 –5مراجع داخلي	15	13%
	من 6 – 10مراجع داخلي	25	21.7%
	من 11 – 20 مراجع داخلي	20	17.5 %
	من 21 – 50 مراجع داخلي	22	19%
	أكثر من 50 مراجع داخلي	17	14.8%
	لا أعرف	16	14%
(5) عدد العاملين في إدارات تكنولوجيا وأمن المعلومات	من 1 – 10موظف	26	22.6%
	من 11 – 25موظف	20	17.4%
	من 26 – 50موظف	22	19%
	أكثر من 50موظف	17	14.8%
	لا أعرف	30	26%

المصدر : اعداد الباحث

ملحق 3: نتائج الإحصاء الوصفي للمتغيرات

المتغيرات الكامنة		المدي النظري لمقاس ليكرت	المدي الفعلي	المتوسط الحسابي Mean	الانحراف المعياري SD	النسبة المئوية الترتيبية 10% (P10)	الوسيط (P50)	النسبة المئوية الترتيبية 90% (P90)
أ. المتغيرات المستقلة								
X1	جودة المراجعة الداخلية على أساس المدخلات	1 - 5	3.58 - 4.66	4.12	3.42	3.42	4.03	4.82
X11	الكفاءة	1 - 5	2.94 - 4.16	3.55	2.76	2.76	3.5	4.34
X11-1	الشهادات المهنية	1 - 5	3.16 - 4.28	3.72	2.99	2.99	3.89	4.45
X11-2	الخلفية الأكاديمية	1 - 5	3.01 - 4.31	3.66	2.81	2.81	3.85	4.5
X11-3	التدريب والتطوير المستمر	1 - 5	3.31 - 4.69	4.0	3.1	3.1	4.15	4.9
X12	الاستقلالية	1 - 5	2.93 - 4.33	3.63	2.72	2.72	3.75	4.54
X12-1	الاستعانة بمستشارين والتعاقد الخارجي	1 - 5	3.29 - 4.11	3.7	3.17	3.17	3.71	4.23
X12-2	الارتباط مع لجنة المراجعة والإدارة	1 - 5	3.1 - 4.16	3.63	2.94	2.94	3.61	4.32
X2	الهيكل المتكامل للحوكمة السيبراني	1 - 5	2.81 - 4.51	3.66	2.56	2.56	3.7	4.77
X21	هيكل حوكمة سيبراني يستند إلى خطوط المساءلة الثلاث	1 - 5	3.55 - 5.0	4.39	3.3	3.3	4.67	5.0
X21-1	فعالية أداء خط المساءلة الأول في هيكل الحوكمة	1 - 5	2.56 - 4.0	3.28	2.34	2.34	3.38	4.22
X21-2	فعالية أداء خط المساءلة الثاني في هيكل الحوكمة	1 - 5	2.34 - 4.12	3.23	2.07	2.07	3.32	4.39
X21-3	فعالية أداء خط المساءلة الثالث في هيكل الحوكمة	1 - 5	3.09 - 3.97	3.53	2.96	2.96	3.59	4.1
X21-4	جودة التعاون بين خطوط المساءلة الثلاث	1 - 5	3.12 - 4.52	3.82	2.91	2.91	4.02	4.73
X22	دعم الإدارة التنفيذية ومجلس الإدارة	1 - 5	3.53 - 4.47	4.0	3.39	3.39	3.75	4.61
X22-1	دعم الإدارة التنفيذية	1 - 5	3.46 - 4.64	4.05	3.28	3.28	3.81	4.82
X22-2	دعم مجلس الإدارة	1 - 5	2.71 - 4.05	3.38	2.51	2.51	3.13	4.25

المتغيرات الكامنة		المدي النظري لمقاس ليكرت	المدي الفعلي	المتوسط الحسابي Mean	الانحراف المعياري SD	النسبة المئوية الترتيبية 10% (P10)	الوسيط (P50)	النسبة المئوية الترتيبية 90% (P90)
ب. المتغيرات الرقابية								
X3	مستوي الجهد المخصص لعمليات مراجعة الأمن السيبراني	1 - 5	3.51 - 4.67	4.09	3.34	3.34	4.39	4.84
X4	حجم قسم المراجعة الداخلية	1 - 5	3.47 - 4.75	4.11	3.28	3.28	3.96	4.94
X5	مستوي الرقمية في العمليات	1 - 5	3.65 - 4.57	4.11	3.51	3.51	3.98	4.71
ج. المتغير التابع								
Y	إدارة مخاطر الأمن السيبراني	1 - 5	3.1 - 4.54	3.82	2.88	2.88	4.08	4.76
Y1	مرحلة الوقاية/المنع	1 - 5	2.82 - 4.22	3.52	2.61	2.61	3.78	4.43
Y2	مرحلة الاكتشاف	1 - 5	3.62 - 4.58	4.1	3.48	3.48	4.03	4.72
Y3	مرحلة الاستجابة	1 - 5	3.7 - 5.0	4.38	3.5	3.5	4.28	5.0
Y4	مرحلة العلاج	1 - 5	3.21 - 4.07	3.64	3.08	3.08	3.67	4.2

المصدر: أعداد الباحث

ملحق 4: معاملات التحميل المعيارية للمتغيرات الكامنة في النموذج

متغيرات الدرجة الثالثة		معاملات التحميل المعيارية لمتغيرات الدرجة الثالثة Formative Loadings	متغيرات الدرجة الثانية		معاملات التحميل المعيارية لمتغيرات الدرجة الثانية Formative Loadings	متغيرات الدرجة الأولي		المؤشرات	معاملات التحميل للمؤشرات Formative Loadings
X1	جودة المراجعة الداخلية على أساس المدخلات	0.74	X11	الكفاءة	0.88	X11-1	الشهادات المهنية	X11-11	0.73
								X11-12	0.85
						X11-2	الخلفية الأكاديمية	X11-21	0.88
								X11-22	0.7
						X11-3	التدريب والتطوير المستمر	X11-31	0.74
								X11-32	0.76
								X11-33	0.91
			X12	الاستقلالية	0.7	X12-1	الاستعانة بمستشارين والتعاقد الخارجي	X12-11	0.65
								X12-12	0.76
								X12-13	0.78
								X12-14	0.72
						X12-2	الارتباط مع لجنة المراجعة والإدارة	X12-21	0.73
								X12-22	0.82
								X12-23	0.79
								X12-24	0.72
X2	الهيكل المتكامل للحوكمة السيبراني	0.71	X21	هيكل حوكمة سيبراني يستند إلى خطوط المساءلة الثلاث	0.81	X21-1	فعالية أداء خط المساءلة الأول في هيكل الحوكمة	X21-11	0.95
								X21-12	0.71
								X21-13	0.67
						X21-2	فعالية أداء خط المساءلة الثاني في هيكل الحوكمة	X21-21	0.75
								X21-22	0.76
								X21-23	0.69
						X21-3	فعالية أداء خط المساءلة الثالث في هيكل الحوكمة	X21-31	0.68
								X21-32	0.71
								X21-33	0.85
						X21-4	جودة التعاون بين خطوط المساءلة الثلاث	X21-41	0.85
								X21-42	0.68
								X21-43	0.77
								X21-44	0.68
								X21-45	0.7
			X22	دعم الإدارة التنفيذية ومجلس	0.72	X22-1	دعم الإدارة التنفيذية (خط المساءلة الرابع)	X22-11	0.79
								X22-12	0.72

متغيرات الدرجة الثالثة			معاملات التحميل المعيارية لمتغيرات الدرجة الثالثة Formative Loadings	متغيرات الدرجة الثانية		معاملات التحميل المعيارية لمتغيرات الدرجة الثانية Formative Loadings	متغيرات الدرجة الأولي		المؤشرات	معاملات التحميل للمؤشرات Formative Loadings
				الإدارة (خط المساءلة الرابع والخامس)			دعم مجلس الإدارة (خط المساءلة الخامس)	X22-2	X22-21	0.74
									X22-22	0.76
				مؤشرات إدارة مخاطر الأمن السيبراني	Y	0.8	مؤشرات مرحلة الوقاية/المنع	Y1	Y11	0.78
									Y12	0.65
									Y13	0.7
									Y14	0.93
							مؤشرات مرحلة الاكتشاف	Y2	Y21	0.71
									Y22	0.83
									Y23	0.69
									Y24	0.72
							مؤشرات مرحلة الاستجابة	Y3	Y31	0.74
									Y32	0.68
							مؤشرات مرحلة العلاج	Y4	Y41	0.71
									Y42	0.88
				المتغيرات الرقابية	X3-X5	0.74	مستوي الجهد المخصص لعمليات مراجعة الأمن السيبراني	X3	X31	0.68
							حجم قسم المراجعة الداخلية	X4	X41	0.77
							مستوي الرقمية في العمليات	X5	X51	0.9

المصدر: أعداد الباحث