مجلة البحوث المالية والتجارية
المجلد (26) – العدد الرابع – أكتوبر 2025

أثر الدور المقترح لمراقب الحسابات في حوكمة الأمن السيبراني على جودة المراجعة

The Impact of the Proposed Role of the Auditor in Cybersecurity Governance on Audit Quality

بحث مقدم من الباحثة

سارة عبد المنعم محمد بدران

إشـراف

الأستاذ الدكتور	دكتور
حسين مصطفى عبد السلام هلالى	نورهان علي محمد المر
أستاذ المحاسبة المالية المتفرغ	أستاذ المحاسبة والمراجعة المساعد
	ورئيس قسم المحاسبة والمراجعة
كلية التجارة –جامعة بورسعيد	كلية التجارة – جامعة بورسعيد

تاريخ الإرسال	2025-09-12
تاريخ القبول	2025-10-01
رابط المجلة:	https://jsst.journals.ekb.eg/

الملخص:

تسعى الباحثة إلى معرفة أثر الدور المقترح لمراقب الحسابات في حوكمة الأمن السيبراني على جودة المراجعة وذلك بالتطبيق على الشركات المدرجة بالبورصة المصرية ، من خلال مناقشة الإطار المفاهيمي لحوكمة مخاطر الأمن السيبراني في ضوء الأدبيات المحاسبية، ومناقشة الدور المقترح لمراقب الحسابات في حوكمة الأمن السيبراني، كما تناول البحث أثر ذلك علي جودة المراجعة.

وقد بلغ حجم العينة 382 مشاهدة، وتوصلت نتائج الدراسة إلى وجود تأثير ذو دلالة إحصائية للدور المقترح لمراقب الحسابات في حوكمة مخاطر الأمن السيبراني على جودة عملية المراجعة، ولذلك أوصى البحث بضرورة دمج تقييم مخاطر الأمن السيبراني في تخطيط المراجعة كعامل مؤثر في مخاطر التحريف الجوهري، بالإضافة إلى ضرورة تصميم برامج تدريب تفاضلية حسب مستويات الخبرة لمراقبي الحسابات، تجمع بين وحدات تقنية وحوكمة وتقييم مخاطر.

الكلمات المفتاحية : مراقب الحسابات – حوكمة الأمن السيبراني – جودة المراجعة

Abstract:

The researcher seeks to understand the impact of the proposed role of the auditor in cybersecurity governance on audit quality, applying it to companies listed on the Egyptian Stock Exchange. This study discusses the conceptual framework for cybersecurity risk governance in light of accounting literature, discusses the proposed role of the auditor in cybersecurity governance, and examines its impact on audit quality.

The sample size was 382 participants. The study results revealed a statistically significant impact of the proposed role of the auditor in cybersecurity risk governance on the quality of the audit process. Therefore, the study recommended integrating cybersecurity risk assessment into audit planning as a factor influencing the risk of material misstatement. Furthermore, it recommended designing differentiated training programs tailored to the level of experience of auditors, combining technical, governance, and risk assessment modules.

Keywords: Auditor - Cybersecurity Governance - Audit Quality

القسم الأول : الإطار العام للبحث

أولاً: مشكلة البحث

في ظل زيادة الاعتماد على الإنترنت والحوسبة السحابية والأجهزة المحمولة تزايدت المخاطر، وقد أكد تقرير اختراق البيانات 2024 لدي شركة IBM على أن متوسط التكلفة العالمية للاختراق الواحد بنحو 4.88 مليون دولار فضلاً عن اتساع الأثر المالي والتنظيمي، ولذلك أصدرت لجنة الأوراق المالية والبورصات الأمريكية (SEC) توجيهات رسمية في عام 2018 تنص بشكل قاطع على أن مخاطر الأمن السيبراني تعتبر مخاطر جوهرية للوضع المالي للشركة وعملياتها التجارية، وفي عام 2024 ألزمت قواعد الهيئة بالإفصاح عن الحوادث السيبرانية المادية، والإفصاح السنوي عن إدارة المخاطر والحوكمة (Hossain et al., 2025).

فقد يكون لمخاطر الأمن السيبراني تأثيرات ومخاطر كبيرة أيضاً على الرقابة الداخلية والتي بدورها تؤثر بشكل كبير على جودة التقارير المالية (Eltweri, 2021) ، وأكد علي ذلك إحدى الدراسات (Rosati et al., 2022) بأن حوادث الأمن السيبراني تمثل إشارات على نقاط ضعف الرقابة الداخلية، وتعد من عوامل الخطر على جودة عملية المراجعة، وذلك يتوافق مع قانون SOX الذي وضع متطلبات صارمة علي الشركات توضح أهمية ضوابط نظام المعلومات عن طريق مطالبة الإدارة ومراقبي الحسابات بالتقرير عن فعالية الرقابة الداخلية علي عناصر التقارير المالية، كما تطلب ذلك القانون بأن يكون لدي الشركات سياسات تمنع وتفصح عن أنشطة ومخاطر الأمن السيبراني والتي من المحتمل أن تكون مهمة مادياً (Sebastian, 2022)، وهذا يعني احتمالية أن يقوم المديرون بالإفصاح عن وقوع عملية اختراق للأمن السيبراني في المستقبل.

وتري الباحثة أن وجود دور لمراقب الحسابات في حوكمة مخاطر الأمن السيبراني يعطي بعداً جديداً لممارسات الأمان التي تهدف إلى حماية أصول المعلومات الهامة للشركة، وسوف يحصل مراقب الحسابات على دليل لسياسات أمن المعلومات التنظيمية وفعاليتها في حماية سلامة الأصول وسرية البيانات والوصول إلى البيانات وتوافرها، ومن ثم يعمل مراقب الحسابات على تقييم فعالية وقدرة الشركة على حماية أصولها القيمة أو الحرجة ومدي تطبيقها لحوكمة الأمن السيبراني، كما يركز مراقب الحسابات على الرقابة الداخلية من خلال اقتراح اختبارات

جوهرية للتعرف علي هذه المخاطر وما مستوي التطبيق لحوكمة مخاطر الأمن السيبراني، وهذا ما توافق مع اقتراح مجلس الرقابة على محاسبة الشركة PCAOB الذي توقع بأن ينظر مراقبي الحسابات في كيفية حدوث هجمات للأمن السيبراني التي قد تؤثر على الرقابة الداخلية للشركة ومن ثم تؤثر علي جودة التقارير المالية وهذا بدوره يؤثر علي جودة المراجعة، وبالتالي يتمكن من تقديم تأكيد معقول فيما يتعلق بمصداقية التقارير المالية وإعدادها من البيانات المالية للأغراض الخارجية وفقاً للمحاسبة المتعارف عليها.

كما دعم ذلك AICPA, (2017) من خلال وضع مجموعتين من المعايير حيث تناولت المجموعة الأولي معايير الوصف لكي تستخدمها إدارة الشركة عند تنفيذ برنامج إدارة مخاطر الأمن السيبراني، وعند إعداد الإدارة لتقريرها عن مخاطر الأمن السيبراني، وتحتوي المجموعة الثانية على معايير الرقابة التي ينبغي علي مراقب الحسابات استخدامها للتوكيد علي مخاطر الأمن السيبراني.

ولذلك عند تقديم مراقب الحسابات لتوكيد على تطبيق الشركة لحوكمة مخاطر الأمن السيبراني مع تحديد للأنواع المختلفة من نقاط الضعف لنظام الأمن السيبراني مع اقتراحاته للتدابير العلاجية نظراً لقيامه بتحديد المخاطر وتحليلها وتوضيح مدي احتمالية حدوثها، ويتضح أن دور مراقب الحسابات في حوكمة مخاطر الأمن السيبراني يساعد علي تقييم البدائل واختيار أفضل بديل لمواجهة تهديدات الأمن السيبراني وهذا بدوره يحسن من جودة عملية المراجعة. ولذلك تتمثل مشكلة البحث في التعرف علي الدور المقترح لمراقب الحسابات في حوكمة مخاطر الأمن السيبراني للمعلومات وأثر ذلك علي جودة المراجعة.

ثانياً: أهمية البحث

في ضوء مشكلة البحث يمكن بلورة أهميته في تقديم تصور حول أثر دور مراقب الحسابات في حوكمة مخاطر الأمن السيبراني على تحسين جودة عملية المراجعة، مما يمكن مستخدمي التقارير من اتخاذ القرارات الاستثمارية والتأكد من دقة إفصاح الشركات المصرية المدرجة عن مخاطر الأمن السيبراني التي واجهتها.

ثالثاً: أهداف البحث

وفقاً لمشكلة البحث وأهميته بتمثل الهدف الرئيسي للبحث في دراسة أثر الدور المقترح لمراقب الحسابات حوكمة مخاطر الأمن السيبراني على جودة المراجعة.

رابعاً: فروض الدراسة

وفقاً لمشكلة البحث وأهميته وأهدافه يتمثل الفرض الرئيسي للبحث في لا يوجد أثر ذو دلالة إحصائية للدور المقترح لمراقب الحسابات حوكمة مخاطر الأمن السيبراني على جودة المراجعة.

خامساً: خطة البحث

ووفقاً لما سبق عرضه في البحث سوف يتم تقسيم ما تبقي منه إلى قسمين وهما الدراسة النظرية والدراسة التطبيقية، فضلاً عن النتائج والتوصيات والمقترحات البحثية المستقبلية.

القسم الثاني: الدراسة النظرية

أولاً: آليات حوكمة الأمن السيبراني

أوضحت دراسة (Ali et al., 2020) أن ضوابط حوكمة الأمن السيبراني تتمثل في أن يضم مجلس الإدارة في عضويته ومن يخولهم من لجانه أشخاصاً من الإدارة التنفيذية العليا يتمتعون بالمهارات والمعرفة المناسبة لفهم وإدارة المخاطر السيبرانية، وأن يتولى المجلس أو من يفوض لجانه المسؤوليات والمهام التالية حسب مناصبهم اعتماد سياسة الأمن السيبراني، اعتماد برنامج الأمن السيبراني، التحقق من الالتزام بسياسة وبرنامج الأمن السيبراني، بينما تتولى الإدارة التنفيذية العليا المسؤوليات والمهام التالية حسب مناصبها ضمان تطبيق وتحديث سياسة الأمن السيبراني، ضمان تنفيذ برنامج الأمن السيبراني بشكل متكامل مع الإطار العام لإدارة مخاطر تكنولوجيا المعلومات واستمرار تحديثه وتطويره، التأكد من وجود سجل شامل للمخاطر السيبرانية والتأكد من تحديثه بشكل مستمر وتوافقه مع ملف المخاطر في تكنولوجيا المعلومات الخاص بالشركة، مراقبة مستوى المخاطر السيبرانية بشكل مستمر، اعتماد قوائم الصلاحيات المتعلقة بإدارة الأمن والأمن السيبراني من حيث تحديد الكيان والأطراف المتعددة والأشخاص أو الأطراف المسؤولة والمسؤولين بشكل نهائي.

ويوجد العديد من المعايير المتبعة في تطبيق حوكمة الأمن السيبراني، وأشهرها معيار 27001، حيث يوجه هذا المعيار الشركة أو المؤسسة إلى تطوير آليات محددة للإشراف والرقابة ISO/IEC والتخفيف من المخاطر المحتملة، ويضمن إدارة تنفيذ جميع القواعد داخل البيئة الرقمية، وتعد مراقبة الخدمات الأمنية من أكثر التدابير أهمية المتبعة في حوكمة الأمن السيبراني، لذا يجب أن تدار الشركات أو المؤسسات من قبل أشخاص موثوق بهم ولديهم خبرة كافية في عملية إدارة البيئة الرقمية، وتعتبر حوكمة الإنترنت من القضايا الأساسية في حوكمة الأمن السيبراني، حيث تسعى إلى توفير البنية التحتية الأساسية وتحديد معايير الإنترنت ووساطة المعلومات وحقوق الملكية الفكرية (Mijwil, et al., 2023) .

حيث تتطلب حوكمة الأمن السيبراني الفعّالة مشاركة الإدارة العليا وفهماً واضحاً لملف مخاطر الشركة، كما تتضمن المراجعة والتحديثات المنتظمة للبقاء على اطلاع دائم بالتهديدات الأمنية السيبرانية المتطورة وأفضل الممارسات، وتتضمن حوكمة الأمن السيبراني الفعّالة أيضاً تنفيذ السياسات والإجراءات والضوابط لمنع الجرائم الإلكترونية واكتشافها والاستجابة لها، فإن الامتثال للقوانين واللوائح جانباً مهماً من حوكمة الأمن السيبراني، لأن عدم الامتثال قد يؤدي إلى عقوبات مالية كبيرة وإلحاق الضرر بسمعة الشركة بشكل عام، وقد يشمل ذلك تنفيذ تقنيات أمنية متقدمة، ومراقبة ومراجعة السجلات والتنبيهات بانتظام، وإجراء اختبارات اختراق منتظمة، وهذا يتضمن أيضاً تحديد وتقييم ملف مخاطر الشركة وتنفيذ الضوابط الفنية مثل جدران الحماية وأنظمة اكتشاف التسلل وتنفيذ الضوابط غير الفنية مثل تعليم الموظفين وخطط الاستجابة للحوادث (Elnagar et al., 2024).

ومن ثم تعد حوكمة الأمن السيبراني جانب بالغ الأهمية من استراتيجية إدارة المخاطر الشاملة للشركة، لأنها تتضمن تطوير وتنفيذ السياسات والإجراءات والضوابط لحماية أنظمة المعلومات والبيانات في الشركة من التهديدات السيبرانية، ويشمل ذلك تحديد المخاطر وتقييمها، وتنفيذ الضوابط الفنية وغير الفنية للتخفيف من تلك المخاطر، ومراجعة وتحديث وضع الأمن السيبراني للمنظمة بانتظام. كما تتطلب حوكمة الأمن السيبراني الفعالة مشاركة نشطة من الإدارة العليا والتواصل الواضح في جميع أنحاء المنظمة لضمان فهم جميع الموظفين لدورهم في حماية أصول الشركة (القاضي، 2024).

ثانياً: مخاطر عملية المراجعة ودور مراقب الحسابات في الحد منها

يحقق مراقب الحسابات جودة المراجعة عندما ينفذ دوره في جميع مراحل عملية المراجعة بكفاءة وفاعلية، مع الالتزام التام بالمعايير المهنية والقواعد السلوكية، بدايةً من قبوله لعملية المراجعة وعمل تخطيط جيد يتناسب مع بيئة العميل وظروفه الخاصة، ثم تنفيذ إجراءات المراجعة وفق معايير المراجعة والتعليمات القانونية المتعارف عليها، مع الاسترشاد بمعايير وأدلة المنظمات المهنية المسؤولة عن تنظيم المهنة، حيث يهدف هذا الالتزام المنهجي إلى خفض مخاطر المراجعة إلى أدنى مستوى ممكن من خلال الإفصاح عن الأخطاء والانحرافات الجوهرية والإفصاح عنها في تقريره، بما يضمن في النهاية تلبية احتياجات مستخدمي القوائم المالية.

وتعتبر المخاطر الكامنة جزءاً جوهرياً من نموذج مخاطر المراجعة، والتي يجب على مراقب الحسابات تقييمها بدقة في مرحلة التخطيط، لذا أكد معيار ISA 315 المعدّل على أن يحدد مراقب الحسابات مجالات وخطوات احتمالية التحريفات الجوهرية عبر فهم نشاط العميل وبيئته ونظام رقابته، لأن التطبيق الفعال لنموذج مخاطر المراجعة يساعد المراقب في تخصيص الجهود نحو مناطق المخاطر العالية وضمان تصميم إجراءات مراجعة تستجيب لتلك المخاطر، أي أن مراقب الحسابات يقوم عملياً بوضع تقدير لمخاطر التحريف الجوهري على مستوى القوائم المالية وعلى مستوى التأكيدات المختلفة، ليبني على ذلك نطاق واختيار الاختبارات المناسبة (Elnahass et al., 2024).

كما تعد مخاطر الرقابة من ضمن مخاطر المراجعة أيضاً، والتي تمثل خط الدفاع الأول ضد الأخطاء والتلاعبات، لذا يعد فهم مراقب الحسابات لنظام الرقابة الداخلية لدى العميل ركيزة أساسية لتقييم مخاطر المراجعة، وقد ينشأ مخاطر سوء فهم الرقابة الداخلية عندما يُخطئ مراقب الحسابات في تقييم تصميم أو فعالية الرقابة الداخلية للعميل، مما قد يؤدي إلى تقدير خاطئ لمخاطر التحريفات ودخول إجراءات المراجعة في غير محلها(Esmail and Haque.2022).

تمثل مخاطر الاكتشاف الجانب الثالث من نموذج مخاطر المراجعة، فهي المخاطر المتمثلة في أن يفشل المراجع في اكتشاف التحريفات المادية الموجودة في القوائم المالية على الرغم من تنفيذ إجراءات المراجعة، تُعتبر هذه المخاطر مرتبطة بكفاءة وفعالية إجراءات المراجعة المنفذة وحجم العيّنة المختارة وتقديرات المراجع المهنية أثناء تنفيذ الاختبارات، وبخلاف المخاطر

الكامنة والرقابية التي تخرج عن سيطرة المراجع إلى حد كبير، فإن مخاطر عدم الاكتشاف هي العنصر الذي يستطيع المراجع التحكم فيه وتخفيضه من خلال زيادة حجم الاختبارات أو تحسين نوعيتها (Tavares, et al. 2025)، ولذلك حث معيار المراجعة الدولي (ISA 330) مراقب الحسابات على تصميم طبيعة وتوقيت ومدى إجراءات المراجعة بحيث تنخفض مخاطر عدم الاكتشاف إلى مستوى مقبول بالتناسب مع تقييمه لمخاطر التحريف الجوهري في كل مجال، ويعني ذلك عملياً أنه كلما ارتفع تقييم المراجع لمخاطر التحريف في مجال معين، وجب عليه خفض مستوى مخاطر عدم الاكتشاف المقبول عبر إجراءات أكثر صرامة لضمان كشف أية أخطاء جوهرية محتملة (Elnahass et al., 2024).

ومن ثم تساعد جودة المراجعة في اكتشاف الأخطاء والاحتيال في عملية إعداد التقارير المالية حيث يقوم المراقب ذو الجودة العالية بإجراء تحليلات شاملة لنظام الرقابة الداخلية في الشركة، واختبار مدى كفايته وفعاليته، وتقديم توصيات لمعالجة أي نقاط ضعف تم تحديدها (Mexmonov, 2020)، كما تشمل جودة المراجعة تقييم نظام الرقابة الداخلية في الشركة عن طريق قيام المراقب بإجراء تقييمات للتأكد من وجود رقابة داخلية قوية، وحماية الأصول، وتخفيف مخاطر الاحتيال، وتحسين دقة التقارير المالية، وتحسين استخدام الموارد (Boskou et al., 2019).

ثالثاً: انعكاس دور مراقب الحسابات في حوكمة الأمن السيبراني على جودة المراجعة

في ظل تزايد حوادث الأمن السيبراني وآثارها الاقتصادية، يجب على مراقب الحسابات تضمين مخاطر الأمن السيبراني ضمن نموذج مخاطر المراجعة شرطاً لرفع جودة المراجعة، حيث تمثل حوادث الأمن السيبراني عوامل خطر مؤثرة في جودة التقارير المالية كونها تفصح عن ثغرات في نظم الرقابة الداخلية، ولذلك ينبغي أن يقوم مراقب الحسابات بفحص الضوابط التكنولوجية والتأكد من وجود إجراءات رقابة إلكترونية كافية، إذ يمكن أن يؤدي قصورها إلى تلاعب في التقارير المالية أو ضعف في دقة التقارير، بينما يؤدي تحسينها إلي مؤشرات موضوعية مثل تقلّص الاستحقاقات غير العادية وتراجع إعادة إصدار القوائم (Rosati et al., 2023).

ومن ثم يجب على مراقب الحسابات تعديل استراتيجيات المراجعة في مرحلة تخطيط لعملية المراجعة لتشمل اختبارات إضافية تخص الأمن السيبراني، بما في ذلك تقييم مدى تكامل أنظمة المعلومات مع العمليات المالية، حيث يساهم فهم مراقب الحسابات للسياسات والإجراءات الخاصة بحوكمة الأمن السيبراني في الشركة في رفع مستوى التأكد من سلامة المعلومات المالية، وذلك من خلال الآتي:

1- الأهمية النسبية: يتم تقييم الأهمية النسبية للحادث السيبراني من خلال النظر في طبيعته وحجمه ومدى تأثيره المحتمل على عمليات الشركة، بما في ذلك الأضرار غير المالية مثل السمعة وثقة العملاء والغرامات التنظيمية (Grigoryan, and Mirzoyan, 2023)، فإذا تم تصنيف حادثٍ ما على أنه جوهري، يتعيّن الإفصاح عنه بشكل مناسب وفي الوقت الملائم للمساهمين.

2- تقييم المراقب لعوامل الخطر السيبراني والإفصاح عنها: حيث يقوم المراقب في مرحلة تقييم مخاطر المراجعة بدراسة وفهم وتقييم الإفصاحات التي تقدّمها الشركة حول حوكمة الأمن السيبراني والعوامل المساهمة فيها وربطها بمخاطر التحريف، حيث تمثل هذه الإفصاحات لمراقب الحسابات مصدراً مهماً للمعلومات عند تقييمه لمخاطر التحريف في التقارير المالية، ومن ثم تساعد الإفصاحات التفصيلية عن حوكمة الأمن السيبراني المراقب في تحديد المجالات عالية الخطورة التي تتطلب تركيزاً أكبر أثناء المراجعة (Guo, and Fluharty, 2024).

3- تقييم إجراءات الرقابة الداخلية ومراجعة مخاطر الأمن السيبراني: إذ يقوم مراقب الحسابات خلال مرحلة تقييم نظام الرقابة الداخلية وتصميم الاختبارات بدور جوهري في فحص الرقابة المرتبطة بتكنولوجيا المعلومات وأمن المعلومات، وذلك نظراً لتداخلها الوثيق مع مصداقية التقارير المالية، ولذلك طالبت معايير المراجعة الحالية المراقب بأن يفهم تركيبة أنظمة المعلومات لدى العميل وآلية الرقابة المتعلقة بالتقارير المالية (Slapničar et al., 2022)، ومن ثم ينبغي أن يهتم مراقب الحسابات بطبقات البنية التحتية التقنية الأقرب إلى عملية إعداد التقارير المالية، وذلك من خلال اختبار ضوابط صلاحيات الوصول للأنظمة المحاسبية وقواعد البيانات المالية، وضوابط فصل المهام

في إدخال وإقرار العمليات، وكذلك ضوابط التغيرات البرمجية للتأكد من عدم إمكانية إدخال تعديل على البرامج أو البيانات المالية دون موافقات ورقابة، حيث تعتبر هذه الطبقات أقرب ما يكون لمحيط التقارير المالية، وأي خلل فيها قد يسمح بالوصول غير المشروع وتعديل البيانات المالية (Wu et al. 2024).

4- تقييم سياسات الإفصاح المتعلقة بحوكمة الأمن السيبراني: يقوم مراقب الحسابات بدراسة تصميم تلك الضوابط الرقابية المتعلقة بالإفصاح والتأكد من تنفيذها، فهو يسأل الإدارة عن الإجراءات المتبعة لرصد الحوادث السيبرانية والإفصاح عنها داخلياً، ويتحقق مما إذا كانت الشركة قد تعرضت لحوادث خلال الفترة وكيف تعاملت معها، وإذا وجد المراقب قصوراً كغياب آلية واضحة للإفصاح عن حوادث الاختراق للإدارة العليا، فإنه يأخذ ذلك بعين الاعتبار كمؤشر على ضعف بيئة الرقابة، وقد يدفعه ذلك إلى توسيع نطاق اختبارات المراجعة بحثاً عن حوادث سيبرانية ربما وقعت ولم يُفصح عنها بسبب خلل في قنوات الإفصاح، بينما إذا تأكد المراقب من وجود بنية قوية للضوابط الإفصاحية مثل وجود لجنة استجابة للحوادث تجتمع فوراً عند أي خرق وتوثّق الوقائع لغايات الإفصاح، فإنه يحصل على درجة أعلى من التأكد بأن الإدارة لن تحجب المعلومات الجوهرية المتعلقة بالأمن السيبراني.

وفي ضوء إرشادات الإفصاح الجديدة الصادرة في 2023 عن SEC سوف يقع على عاتق مراقب الحسابات أيضاً تقييم الإفصاحات المرتبطة بحوكمة المجلس للمخاطر السيبرانية، حيث طالبت هذه الإرشادات الشركات بتضمين معلومات حول مدى خبرة مجلس الإدارة في الأمن السيبراني وكيفية إشرافه على حوكمة الأمن السيبراني، ومن ثم يستطيع مراقب الحسابات تقييم هذه الإفصاحات في التقارير السنوية ويقارنها بواقع الممارسات التي شاهدها خلال عملية المراجعة، وبالتالي يساهم المراقب في تحري صدق الإفصاح المتعلق بدور المجلس إلى جانب تحري صدق الإفصاحات المالية.

وترى الباحثة أن دور مراقب الحسابات في حوكمة الأمن السيبراني يعد أمراً أساسياً لضمان تعزيز جودة المراجعة وتقليل المخاطر المرتبطة بتقارير الشركة المالية، وفي ظل تزايد الهجمات السيبرانية وتأثيراتها المحتملة على التقارير المالية، يُتوقع من مراقب الحسابات أن

يدمج تقييم المخاطر السيبرانية في جميع مراحل عملية المراجعة، ومن خلال التفاعل مع نظام الرقابة الداخلية للشركة، يساهم المراقب في الإفصاح عن نقاط الضعف في حوكمة الأمن السيبراني التي قد تؤدي إلى تحريفات في القوائم المالية، كما يعزز من أهمية استجابة الشركة للحوادث السيبرانية، مما يساعد في تجنب التلاعب المحاسبي، ومن ثم يضمن المراقب أن تكون الإفصاحات المتعلقة بالأمن السيبراني دقيقة وشفافة، مما يساهم في زيادة مصداقية التقارير المالية ورفع مستوى جودة المراجعة.

القسم الثالث: الدراسة التطبيقية

أولاً: مجتمع وعينة الدراسة

يتمثل مجتمع الدراسة في كافة الأفراد العاملين بالشركات المقيدة ببورصة الأوراق المالية بالإضافة إلى الأكاديمين ومراقبي الحسابات بموضوع الدراسة الحالية من ذوي الارتباط بمتغيرات الدراسة، والجدير بالذكر أن مفردات المجتمع في هذه الدراسة يتجاوز 100,000 فرد، فضلاً عن صعوبة الوصول إليهم نظراً لانتشارهم الجغرافي. ومن ثم يمكن للباحثة الاعتماد على أسلوب المعاينة الإحصائية واختيار عينة عشوائية بشرط ألا تقل عن 384 مشاهدة.

وقد تم تقسيم عينة الدراسة من العاملين بالشركات محل الاختبار حسب المسمى الوظيفي إلى (مراقب حسابات– مسئول تكنولوجيا المعلومات– عضو هيئة تدريس بالجامعة– عضو مجلس إدارة) ، وكانت نتيجة الاستجابة كما في الجدول التالي :

جدول رقم (1) استجابة عينة الدراسة

م	المسمى الوظيفي للعينة	القوائم الموزعة	القوائم الصحيحة		القوائم المستبعدة	
			العدد	%	العدد	%
1	مراقب حسابات	160	145	37.96%	15	53.57%
2	مسئول تكنولوجيا المعلومات	80	87	22.77%	3	10.71%
3	عضو هيئة تدريس بالجامعة	90	82	21.47%	8	28.57%
4	عضو مجلس إدارة	70	68	17.80%	2	7.15%
	المجموع	410	382	100%	28	

المصدر : إعداد الباحثة في ضوء النتائج الاحصائية

يتضح مما سبق ارتفاع نسبة استجابة عينة الدراسة على قائمة الاستبيان ، حيث بلغت نسبة استجابة العينة على القائمة (93%) وهي نسبة مرتفعة في العلوم الاجتماعية .

ثانياً: اختبار الثبات

يمكن اختبار معاملات الثبات لمحاور قائمة الاستقصاء ، وكذلك للعبارات الخاصة بها كما في الجدول التالي :

جدول رقم (2) معاملات الثبات والصدق لمحاور قائمة الاستقصاء

م	المحور	عدد العبارات	معامل الثبات	معامل الصدق
1	حوكمة مخاطر الأمن السيبراني	10	.868	.932
2	جودة عملية المراجعة	7	.891	.944
3	الدور المقترح لمراقب الحسابات في حوكمة الأمن السيبراني	13	.929	.964

المصدر : إعداد الباحثة وفقاً لنتائج التحليل الإحصائي

يتضح من الجدول السابق وجود مستويات مرتفعة لمعاملات الثبات عبر المحاور الثلاثة، إذ تتراوح بين (868.) و(929.)، حيث كان معامل الثبات أكبر من 50%، هذا يدلّ على اتساق داخلي قوي بين بنود هذه المحاور، ويتّضح أن محور "الدور المقترح لمراقب الحسابات في حوكمة الأمن السيبراني" **حقق أعلى ثبات (929.) وبمعامل صدق (964.)، مما يعكس تجانساً مفاهيمياً قوياً لبنوده (13 بنداً) كما يشير إلى قوة بنوده، يليه محور** "جودة عملية المراجعة"**(891.) وبمعامل صدق (944.) ثم** محور "حوكمة مخاطر الأمن السيبراني" بلغ معامل ثباته **(868.) وبمعامل صدق (932.).**

ثالثاً: الإحصاء الوصفي

قامت الباحثة بإجراء التحليل الوصفي للبيانات باستخدام برنامج الحزم الإحصائية SPSS لمتغيرات الدراسة، وذلك بهدف الوقوف على شكل وطبيعة البيانات والتعرف على قيمة المتوسطات الحسابية والانحرافات المعيارية لمتغيرات الدراسة، ويمكن توضيح ذلك من خلال الجدول التالي:

جدول رقم (3): الإحصاءات الوصفية الإجمالية لمتغيرات الدراسة

المتغير	الوسط الحسابي	الانحراف المعياري	معامل الاختلاف	معامل الالتواء	معامل التفرطح
المحور الأول: حوكمة مخاطر الأمن السيبراني	4.4335	.48073	10.84%	-.745	.226
المحور الثاني: جودة المراجعة	4.4013	.56932	12.94%	-.900	.553
المحور الثالث: الدور المقترح لمراقب الحسابات في حوكمة الأمن السيبراني	4.4613	.50746	11.37%	-1.017	.805

المصدر: إعداد الباحثة وفقاً لنتائج التحليل الإحصائي

يتبين للباحثة من خلال النتائج سالفة العرض بالجدول السابق وجود مستوى اتفاق مرتفع لدى المشاركين عبر المحاور الثلاثة، إذ تقع المتوسطات بين 4.40 و4.46 على مقياس خماسي (المحور الأول = 4.4335 ، الثاني = 4.4013، الثالث = 4.4613)، كما يتضح أن التشتتات محدودة؛ فالانحرافات المعيارية تتراوح بين 480. و569. ومعاملات الاختلاف منخفضة (10.84%– 12.94%)، بما يدل على تجانسٍ مقبول في الاستجابات، كما يتضح أن المحور الثالث ("الدور المقترح لمراقب الحسابات في حوكمة الأمن السيبراني") سجّل أعلى متوسط، بما يعكس قناعة قوية بهذا الدور، بينما أظهر المحور الأول (حوكمة مخاطر الأمن السيبراني) أعلى تجانس نسبيّاً (10.84%)، وفي المقابل، جاء المحور الثاني ("جودة المراجعة") بأعلى تباين نسبي (12.94%)، وهو ما قد يعكس تمايزاً فعلياً بين الشركات في تطبيقات وممارسات الجودة.

رابعاً: نتائج اختبارات الفروض الإحصائية:

يمكن للباحثة اختبار فرض الدراسة في ضوء الأساليب الإحصائية التي تتناسب مع طبيعة الفروض، حيث أن محاور الدراسة تعبر عن طبيعة العلاقة بين كل متغير وآخر ومدى إيجابيتها في تأثير المتغيرات على بعضها البعض، ومن ثم فإن الباحثة في هذه الحالة سيقوم باختبار الفرض الإحصائية من خلال الاعتماد على الاختبارات القائمة على أساس قياس الفروق

الجوهرية والتعرف على مدى اتفاق عينة الدراسة عن إيجابية العلاقة ومن ثم التوصل إلى النتيجة النهائية لاختبار الفرض الإحصائي، وذلك من خلال العرض التالي:

ينص هذا الفرض الثاني على أنه " لا يوجد تأثير ذو دلالة إحصائية للدور المقترح لمراقب الحسابات في حوكمة مخاطر الأمن السيبراني علي جودة المراجعة."، ولاختبار صحة الفرض قامت الباحثة باستخدام تحليل الانحدار البسيط وبرنامج Smart PLS4، والذي يستخدم في التنبؤ بالتغيرات في المتغير التابع نتيجة التأثر بالمتغير المستقل، ولقد تم اختبار هذا الفرض من خلال الجدول رقم (4) والشكل رقم (1):

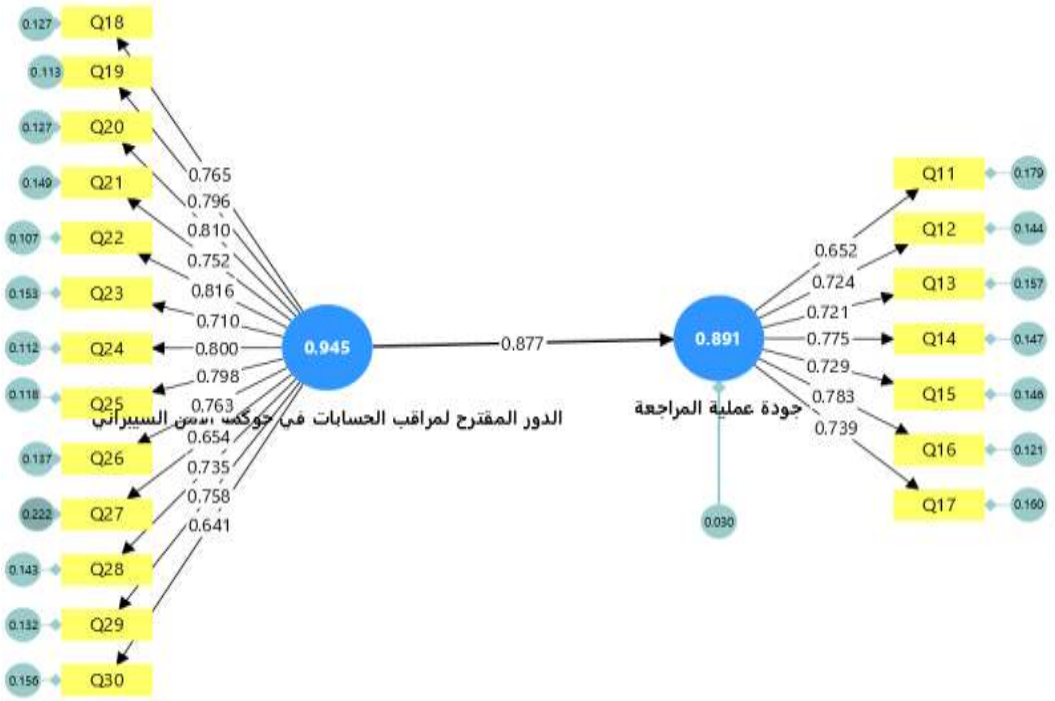
جدول رقم (4): نتائج اختبار أثر الدور المقترح لمراقب الحسابات في حوكمة الأمن السيبراني على جودة المراجعة

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.116	.157		.741	.459
	الدور المقترح لمراقب الحسابات في حوكمة الأمن السيبراني	.967	.035	.816	27.535	.000

R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson	F	Sig.
.816	.666	.665	.32939	1.859	758.156	.000[b]

a. Dependent Variable: جودة المراجعة

المصدر: إعداد الباحثة وفقاً لنتائج التحليل الإحصائي



شكل رقم (1): نتيجة اختبار الفرض

ولقد أظهرت نتائج تحليل الانحدار مدعومةً بمخرجات النموذج البنائي(PLS-SEM) ، إذ تبيّن وجود أثر إيجابي ومعنوي قوي **للدور المقترح لمراقب الحسابات في حوكمة مخاطر الأمن السيبراني على جودة المراجعة، فقد جاء معامل الانحدار غير المعياري** (B = 0.967)، **وهذا دالاً وبدرجة عالية** (t = 27.535)، (Sig. = 0.000)، **إلى جانب معامل معياري كبير** (β = 0.816)، **وهو ما يعكس أهمية عملية واضحة للأثر وقدرته على تحسين جودة المراجعة مع تعاظم الدور المقترح، ويُعزز هذا الاستنتاج بقوة ملاءمة النموذج الإجمالية حيث جاءت قيمة** F (758.156) ، **ومعنويته** (Sig. = 0.000).

كما أظهر معامل التحديد (R^2 = 0.666; adj R= .665) **أن الدور المقترح لمراقب الحسابات** يفسر نحو 66.5% **من التباين في جودة المراجعة ، وهو ما يؤكد مكانته كعامل رئيس في زيادة جودة مخرجات المراجعة، وعلى مستوى النموذج البنائي(Smart PLS4) ، جاءت المسارات المباشرة من الدور المقترح إلى جودة المراجعة** موجبة ودالة، **بما يتسق تماماً مع نتائج الانحدار ويُعزّز متانة الاستدلال.**

واستناداً إلى ما سبق، يمكن للباحثة رفض الفرض العدمي **وقبول الفرض البديل: *"يوجد أثر ذو دلالة إحصائية للدور المقترح لمراقب الحسابات في حوكمة مخاطر الأمن السيبراني على جودة المراجعة".***

النتائج والتوصيات والمقترحات البحثية

تمثل الهدف للدراسة في قياس أثر الدور المقترح لمراقب الحسابات في حوكمة مخاطر الأمن السيبراني علي جودة المراجعة، ونص الفرض الثاني للدراسة على أنه إحصائية للدور المقترح لمراقب الحسابات في حوكمة مخاطر الأمن السيبراني على جودة المراجعة، وقد قامت الباحثة لاختبار صحة الفرض من خلال استخدام تحليل الانحدار البسيط وبرنامج Smart PLS4، ولقد أظهرت نتائج تحليل الانحدار وجود أثر إيجابي ومعنوي قوي للدور المقترح لمراقب الحسابات في حوكمة مخاطر الأمن السيبراني على جودة المراجعة، فقد جاء معامل الانحدار غير المعياري (B = 0.967)، **وهذا دالاً وبدرجة عالية** (t = 27.535)، (Sig. = 0.000)، **إلى جانب معامل معياري كبير** (β = 0.816)، **وهو ما يعكس أهمية عملية واضحة للأثر وقدرته على تحسين جودة المراجعة مع تعاظم الدور المقترح، ويُعزز هذا الاستنتاج بقوة ملاءمة النموذج الإجمالية حيث جاءت قيمة F** (758.156)، **ومعنويته** (Sig. = 0.000). **كما أظهر معامل التحديد** (R^2 = 0.666; adj R= .665) **أن الدور المقترح لمراقب الحسابات** يفسر نحو 66.5% **من التباين في جودة المراجعة ، وهو ما يؤكد مكانته كعامل رئيس في زيادة جودة مخرجات المراجعة.**

ويتضح مما سبق، يمكن للباحثة قبول الفرض الإحصائي للدراسة على الشكل البديل: ***"يوجد أثر ذو دلالة إحصائية للدور المقترح لمراقب الحسابات في حوكمة مخاطر الأمن السيبراني على جودة المراجعة".***

وفي ضوء النتائج التي توصلت لها الدراسة توصي الباحثة بالآتي:

1- **يجب إدماج تقييم مخاطر الأمن السيبراني في تخطيط المراجعة كعامل مؤثر في مخاطر التحريف الجوهري.**
2- **ينبغي توسيع اختبارات ضوابط تكنولوجيا المعلومات (ITGCs) لتشمل: إدارة الهوية والصلاحيات، النسخ الاحتياطي والاستعادة، إدارة الثغرات، وضوابط الأطراف الثالثة.**
3- **يجب إنشاء قسم واضح في تقرير مجلس الإدارة يشرح الحوكمة والسياسات، نتيجة اختبارات التعافي، وأي حادثة جوهرية وتأثيرها المالي وإجراءات المعالجة.**
4- **ينبغي مواءمة إفصاحات الشركات المصرية المدرجة مع أطر معترف بها (مثل NIST CSF/ISO 27001) لإتاحة مقارنة أفضل بين الشركات.**
5- **ضرورة تصميم برامج تدريب تفاضلية حسب مستويات الخبرة لمراقبي الحسابات، تجمع بين وحدات تقنية وحوكمة وتقييم مخاطر.**
6- **توصي الباحثة بإجراء دراسات مستقبلية في دراسة أثر الدور الوسيط للجنة المراجعة على العلاقة بين دور مراقب الحسابات في حوكمة الأمن السيبراني وجودة التقارير المالية.**

قائمة مراجع البحث

أولاً: المراجع العربية

القاضي، كريم محمد حافظ توفيق. (2024). أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني علي قرارات الاستثمار في الشركات الصغيرة والمتوسط الحجم – دراسة تجريبية علي الشركات المقيدة بالبورصة المصرية. *مجلة الإسكندرية للبحوث المحاسبية*، كلية التجارة، جامعة الإسكندرية ، مجلد 8، عدد 1، ص ص: 323-374.

ثانياً: المراجع الأجنبية

Ali, O. A. M., et al. (2020). The impact of cyber governance in reducing the risk of cloud accounting in Jordanian commercial banks-from the perspective of Jordanian auditing firms. *Modern Applied Science*, *14*(3), 75-89.

Boskou, G., Kirkos, E., & Spathis, C. (2019). Classifying internal audit quality using textual analysis: the case of auditor selection. *Managerial Auditing Journal*, *34*(8), 924-950.

Elnahass, M., Jia, X., & Crawford, L. (2024). Disruptive technology and audit risks: Evidence from FTSE 100 companies. *Emerging Markets Review*, *63*, 101218.1-26.

Eltweri, A. (2021). The Impact of Cyber-Security on Audit Quality.

Esmail, Z. M., & Haque, S. I. (2022). The Influence of the Business Risk-Based Auditing Application on the Audit Process: An Empirical Investigation in the Yemeni Context. *Journal of Business Strategy Finance and Management*, *4*(2), 214- 228.

Guo, X., & Fluharty, A. (2024). Mandatory Disclosure of Negative Events and Auditor Behavior: Evidence from a Natural Experiment. *Journal of risk and financial management*, *17*(11), 497. 1-25.

Hossain, M. S., Belina, H., Hasan, M. M., & Kim, M. M. (2025). The Effects of Auditor-level Cybersecurity Breaches on Auditor-Client Relationships. *European Accounting Review*, 1-28.

Mexmonov, S. (2020). The role of the internal audit based international internal audit standards in Uzbekistan. ***Архив научных исследований*****, 33(1).1-5.**

Mijwil, M., Filali, Y., Aljanabi, M., Bounabi, M., & Al-Shahwani, H. (2023). The purpose of cybersecurity governance in the digital transformation of public services and protecting the digital environment. ***Mesopotamian journal of cybersecurity, 2023,*** **1-6.**

Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-security incidents and audit quality. ***European Accounting Review, 31*****(3), 701-728.**

Sebastian, G. (2022). Could incorporating cybersecurity reporting into SOX have prevented most data breaches at US publicly traded companies? An exploratory study. ***International Cybersecurity Law Review,*** **3(2), p:367-383.**

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. ***International Journal of Accounting Information Systems, 44,*** **100548. 1-21.**

Tavares, M. C., Almeida, M. F., Vale, J., & Kapo, A. (2025). Audit 5.0 in Risk and Materiality Assessment: An Ethnographic Approach. ***Journal of Risk and Financial Management, 18*****(8), 419. 1-25.**

Wu, T. H., Huang, S. Y., Chiu, A. A., & Yen, D. C. (2024). IT governance and IT controls: Analysis from an internal auditing perspective. ***International Journal of Accounting Information Systems,*** **52, 100663.1-16.**