IRAQI Academic Scientific Journals

University of Kirkuk Journal For Administrative and Economic Science (2025) 15 (4) Part (1): 199-212

UKJAES

University of Kirkuk Journal For Administrative and Economic Science

ISSN:2222-2995 E-ISSN:3079-3521
University of Kirkuk Journal For Administrative and Economic Science

Taama Marwa Jumaa & Al-Shuwaili Safaa Hamid Rashid. The relationship between cyber threats and internal control over financial data in the digital environment. *University of Kirkuk Journal For Administrative and Economic Science* **(2025) 15 (4) Part (1):199-212.**

The relationship between cyber threats and internal control over financial data in the digital environment

Marwa Jumaa Taama [1], Safaa Hamid Rashid Al-Shuwaili [2]

[1,2] *Sumer University, College of Administration and Economics, Thi-Qar, Iraq*

safaa.alshouaily@gmail.com [1]
marwajuma1989@gmail.com [2]

Abstract: This study aimed to analyze the indirect impact of both cyber threats and cybersecurity system readiness on the quality of financial data through the mediating role of internal control over financial information. The research adopted a quantitative methodology using Partial Least Squares Structural Equation Modeling (PLS-SEM), path analysis, and hypothesis testing based on data collected from a targeted sample within a specific organizational setting. The findings revealed significant direct effects of both cyber threats and cybersecurity readiness on internal control, as well as a significant direct effect of internal control on the quality of financial data. Additionally, the study confirmed the presence of significant indirect effects of both cyber threats and system readiness on data quality through internal control, supporting the hypothesis of a mediating role for this variable.

These results highlight the importance of integration between security and control dimensions within organizations, especially in light of the growing cyber threats that can undermine the reliability of financial information. The study further emphasizes the need to invest in cybersecurity systems and enhance the efficiency of internal control mechanisms as a strategic approach to ensuring the quality of financial reporting. This, in turn, supports decision-makers in fostering a trustworthy informational environment that contributes to organizational sustainability and compliance with accounting and regulatory standards.

Keywords: Cybersecurity, Cyber Threats, Cybersecurity System Readiness, Internal Control, Financial Data Quality, Financial Governance.

العلاقة بين التهديدات السيبرانية والرقابة الداخلية على البيانات المالية في البيئة الرقمية

الباحث: صفاء حميد راشد الشويلي [١]، أ.م. مروه جمعه طعمه [٢]

[١،٢] *جامعة سومر-كلية الإدارة والاقتصاد، ذي قار، العراق*

المستخلص: سعى هذا البحث لمعرفة التأثير غير المباشر لكل من التهديدات السيبرانية ومستوى استعداد أنظمة الأمن السيبراني على جودة البيانات المالية، من خلال استجلاء الدور الوسيط الذي تؤديه الرقابة الداخلية على تلك البيانات ضمن هذه العلاقة. وقد اعتمدت الدراسة على منهج كمي، مستخدمة نموذج المعادلات الهيكلية بالحد الأدنى

للمربعات الجزئية (PLS-SEM) لمعة أثر التهديدات السيبرانية ومدى الجاهزية لها على جودة البيانات في ظل رقابة عليها واختبار الفرضية البحثية، من خلال البيانات التي تم جمعها من عينة تنتمي إلى إطار تنظيمي محدد. وأظهرت نتائج التحليل وجود علاقات مباشرة ذات دلالة إحصائية بين التهديدات السيبرانية وجاهزية أنظمة الأمن السيبراني من جهة، والرقابة الداخلية من جهة أخرى، كما أن للرقابة الداخلية وجود تأثير مباشر معنوي على جودة البيانات المالية. وعن وجود مسارات تأثير غير مباشرة وذات دلالة إحصائية لكل من التهديدات السيبرانية وجاهزية الأنظمة على جودة البيانات، عبر الرقابة الداخلية التي تلعب الدور الوسيط، مما يعزز من صحة فرضية الوساطة الجزئية. وتبرز هذه النتائج أهمية التناغم بين البنية الأمنية والرقابية داخل المؤسسات، لاسيما في ظل تصاعد الهجمات الإلكترونية التي قد تقوض موثوقية المعلومات المالية. كما تؤكد الدراسة على ضرورة توجيه الموارد نحو تطوير وتحديث البنية التحتية للأمن السيبراني، بالتوازي مع تعزيز كفاءة أنظمة الرقابة الداخلية، نظراً لما تمثله هذه الجوانب من مرتكزات أساسية لضمان جودة التقارير المالية.
وفي ضوء ما تقدم، تقدم هذه الدراسة توصيات عملية لصانعي القرار بضرورة بناء بيئة معلوماتية آمنة وموثوقة تدعم استدامة الأداء المؤسسي، وتضمن الامتثال للتشريعات والمعايير المحاسبية والرقابية ذات الصلة.

الكلمات المفتاحية: الأمن السيبراني، التهديدات السيبرانية، جاهزية نظم الأمن السيبراني، الرقابة الداخلية، جودة البيانات المالية، الحوكمة المالية.

Corresponding Author: E-mail: safaa.alshouaily@gmail.com

المقدمة

في سياق التوسع المتصاعد للتحول الرقمي الذي تشهدها المؤسسات المالية، برزت حماية البيانات المالية من المخاطر الإلكترونية كقضية جوهرية تشكل محوراً أساسياً في خطط المؤسسات الاستراتيجية، نظراً لما تمثله من أهمية بالغة في الحفاظ على استمرارية العمليات وتحقيق أعلى درجات الوضوح والدقة في إعداد وتقديم البيانات المالية. إن الاعتماد المتزايد على التقنيات الرقمية أدى إلى نشوء تحديات إلكترونية متعددة تهدد سرية وسلامة وإتاحة البيانات المالية، مما يستدعي من المؤسسات إقامة آليات رقابية داخلية قوية وفعالة، تستطيع مواجهة تلك المخاطر والحد من تداعياتها السلبية على جودة المعلومات المالية وصحة القرارات المرتبطة بها (Alghamdi et al., 2022).
تتجلى قيمة الرقابة الداخلية على البيانات المالية في البيئة الرقمية من خلال قدرتها على اكتشاف السلوكيات غير المعتادة، ومنع الاختراقات الإلكترونية المحتملة، والتأكد من الالتزام بالإجراءات والسياسات المالية المعتمدة، إلى جانب الالتزام بالمتطلبات الإشرافية، مما يعزز من مصداقية المعلومات المالية ويقوي ثقة الجهات المعنية بها (Pathak, 2023).
مع ذلك، تشير الدراسات الحديثة إلى أن المخاطر الإلكترونية قادرة على تقويض فعالية أنظمة الرقابة الداخلية، حيث يمكن استغلال نقاط الضعف التكنولوجية لتنفيذ هجمات مدمرة أو تعديل أو حذف البيانات المالية بطرق غير مصرح بها، مما قد يعرض المؤسسات لمخاطر قانونية وتشغيلية متزايدة (Ahn & Chen, 2023). وقد أوضحت دراسة (Chen et al., 2022) أن المؤسسات التي تتعرض لتهديدات رقمية عالية غالباً ما تعاني من نقص في كفاءة أنظمة الرقابة الداخلية المتعلقة بالتقارير المالية (ICFR)، خاصة عند غياب الاستثمار في الحماية الإلكترونية والتأهيل المتخصص للعناصر البشرية، وهو ما يبرز أهمية فحص العلاقة التفاعلية بين الرقابة الداخلية والمخاطر الإلكترونية ضمن السياقات الرقمية. كما أظهرت نتائج بحث (Li et al., 2023) أن كفاءة الرقابة الداخلية تمثل عاملاً وسيطاً أساسياً يساهم في تقليل التأثيرات السلبية للهجمات الإلكترونية على جودة وموثوقية البيانات المالية.
وبناء على ما تقدم، تتجلى أهمية هذا البحث في تناوله للصلة بين التهديدات السيبرانية والرقابة الداخلية على البيانات المالية ضمن البيئة الرقمية، من خلال فحص تأثير الهجمات الإلكترونية على كفاءة الأداء الرقابي، والسعي نحو تحديد السبل الكفيلة بتحسين فعالية هذه الرقابة بما يسهم في تقليص المخاطر السيبرانية، وضمان استمرارية الأداء المؤسسي، وتعزيز ثقة مستخدمي المعلومات المالية في ظل التحول الرقمي المتسارع.

اولاً: إشكالية البحث

على الرغم من التوسع الملحوظ في استخدام الأنظمة الرقمية لإدارة البيانات المالية داخل المؤسسات، إلا أن هذه الأنظمة باتت عرضة لتهديدات سيبرانية متزايدة قد تؤدي إلى التلاعب أو الإتلاف أو السرقة، مما يضعف موثوقية التقارير المالية ويؤثر سلبًا على دقة القرارات الاقتصادية المستندة إليها. ورغم اعتماد المؤسسات على أنظمة الرقابة الداخلية لضمان سلامة ودقة البيانات، إلا أن فعالية هذه الأنظمة قد تتأثر بفعل الطبيعة المستمرة والمتطورة للتهديدات في البيئة الرقمية.
وتُبرز الأدبيات المعاصرة وجود فجوة بحثية تتعلق بفهم العلاقة التفاعلية بين التهديدات السيبرانية وفعالية الرقابة الداخلية على البيانات المالية، لا سيما في ظل التسارع التكنولوجي وصعوبة تحقيق التكامل بين متطلبات الأمن السيبراني وممارسات الرقابة التقليدية.(Ahn & Chen, 2023; Chen et al., 2022)
وعليه، تتمثل إشكالية هذا البحث في دراسة وتحليل طبيعة العلاقة بين التهديدات السيبرانية والرقابة الداخلية على البيانات المالية في البيئة الرقمية، من خلال الإجابة على السؤال الآتي:
ما مدى تأثير التهديدات السيبرانية على فعالية الرقابة الداخلية وجودة البيانات المالية في المؤسسات الرقمية؟

ثانياً: فرضية البحث:

توجد علاقة ذات دلالة إحصائية بين التهديدات السيبرانية وفعالية الرقابة الداخلية على البيانات المالية في البيئة الرقمية.

المبحث الاول: الإطار النظري

أولاً: التهديدات السيبرانية ومدى خطورتها

تشكل التهديدات السيبرانية أحد أخطر التحديات التي تواجه المؤسسات في البيئة الرقمية، حيث تتمثل هذه التهديدات في محاولات غير مصرح بها للوصول إلى البيانات أو تعديلها أو تدميرها، باستخدام أساليب تقنية معقدة تشمل الهجمات الخبيثة، وبرمجيات الفدية، والتصيد الإلكتروني، والاختراقات المنظمة (Alghamdi et al., 2022). وتزداد خطورة هذه التهديدات عندما تستهدف البيانات المالية، كون هذه البيانات تمثل الأساس لاتخاذ القرارات الاقتصادية والاستثمارية، وتعد معياراً رئيسياً لثقة أصحاب المصلحة والمستثمرين في المؤسسة. حيث إن تدمير البيانات المالية نتيجة التهديدات السيبرانية قد يؤدي إلى فقدان السجلات التاريخية للمؤسسة وتعطيل العمليات التشغيلية، مما يترتب عليه أيضاً تكاليف مالية عالية لاستعادة البيانات أو دفع فدية للمخترقين، إضافة إلى تعرض المؤسسة لعقوبات تنظيمية وقانونية في حال عدم القدرة على حماية بيانات أصحاب المصلحة (Ahn & Chen, 2023). وتشير دراسة (Li et al., 2023) إلى أن المؤسسات التي تتعرض لهجمات سيبرانية مدمرة للبيانات المالية تواجه تحديات في استعادة البيانات بالشكل الكامل، مما يؤدي إلى انخفاض مستوى جودة البيانات المالية المقدمة للجهات التنظيمية أو المستثمرين

نضيف على ذلك، بأن خطورة التهديدات السيبرانية لا تكمن فقط في الأثر الفوري المتمثل في تدمير البيانات أو سرقتها، وإنما في انعكاساتها طويلة الأجل على مصداقية المؤسسة واستقرارها المالي، إذ قد تؤدي هذه التهديدات إلى زعزعة الثقة بنظم الرقابة الداخلية وقدرتها على كشف التلاعب أو الأخطاء، مما قد يعرض المؤسسة لمخاطر السمعة وتراجع ثقة السوق (Pathak, 2023).

ومن هنا، يصبح الاستثمار في البنية التحتية للأمن السيبراني وتعزيز التكامل بين أنظمة الحماية السيبرانية ونظم الرقابة الداخلية على البيانات المالية أمراً ضرورياً لضمان استمرارية الأعمال وتقليل أثر هذه التهديدات.

كما أظهرت دراسة (Chen et al., 2022) أن الخسائر المالية الناتجة عن التهديدات السيبرانية المدمرة للبيانات لا تقتصر على الخسائر المباشرة، بل تشمل أيضاً التكاليف المرتبطة بعمليات التدقيق اللاحقة ومعالجة نقاط الضعف في نظم الرقابة الداخلية، مما قد يؤثر على قدرة المؤسسات على الالتزام بمتطلبات التقارير المالية في الأوقات المحددة. لذا فإن إدراك حجم هذه المخاطر يمثل خطوة أساسية لتحفيز المؤسسات على تبني استراتيجيات متقدمة للأمن السيبراني ضمن سياق الرقابة الداخلية على البيانات المالية.

ثانياً: فعالية الرقابة الداخلية على البيانات المالية

تشكل الرقابة الداخلية على البيانات المالية نظاماً متكاملاً من السياسات والإجراءات التي تهدف إلى حماية أصول المؤسسة وضمان دقة واكتمال البيانات المالية المقدمة لأصحاب المصلحة، مع الالتزام بالمتطلبات القانونية والتنظيمية ذات الصلة (COSO, 2013). وتعد فعالية الرقابة الداخلية مؤشراً رئيسياً على قدرة المؤسسة في الحد من مخاطر الأخطاء والغش في التقارير المالية، وضمان تقديم معلومات مالية موثوقة تسهم في تحسين جودة اتخاذ القرارات الاقتصادية (Doyle et al., 2022).

وتبرز فعالية الرقابة الداخلية عندما تتمكن المؤسسة من رصد ومعالجة الانحرافات والأخطاء في البيانات المالية بشكل دوري ومنهجي، ومنع عمليات الاحتيال الداخلي التي قد تؤدي إلى تحريف البيانات المالية أو إساءة استخدامها. وقد أشار (Zhang et al., 2023) إلى أن المؤسسات التي تتمتع بنظم رقابة داخلية قوية قادرة على تحقيق مستوى عالٍ من الشفافية في التقارير المالية، تعزز الثقة لدى المستثمرين وتقلل من تكلفة رأس المال.

إلا أن فعالية الرقابة الداخلية على البيانات المالية لا تعتمد فقط على وجود السياسات والإجراءات، بل تعتمد أيضاً على قدرة هذه النظم على التكيف مع المخاطر المستجدة في البيئة الرقمية، بما في ذلك التهديدات السيبرانية، والحاجة إلى دمج تكنولوجيا المعلومات مع إجراءات الرقابة (Ahn & Chen, 2023). وتوضح الأدبيات الحديثة أن الرقابة الداخلية تصبح أكثر فعالية عندما تكون مدعومة بأنظمة رقمنة متقدمة تسمح بالتتبع المستمر للبيانات المالية، والقيام بعمليات تدقيق لحظية للكشف عن أي محاولات غير مشروعة للوصول إلى البيانات أو تعديلها (Li et al., 2023).

بالتالي، فإن فعالية الرقابة الداخلية لم تعد مسألة تقنية أو إجرائية فحسب، بل أصبحت مسألة استراتيجية تتطلب من المؤسسات تعزيز ثقافة الامتثال والمساءلة بين الموظفين، وربط أهداف الرقابة الداخلية بالأهداف التشغيلية والاستراتيجية للمؤسسة. إذ إن تعزيز فعالية الرقابة الداخلية على البيانات المالية في ظل البيئة الرقمية يسهم في تعزيز القدرة على مواجهة الأزمات المالية وتقليل المخاطر النظامية التي قد تؤثر على استدامة المؤسسات في المدى الطويل.

كما أشار (Chen et al., 2022) إلى أن فعالية الرقابة الداخلية تؤدي دوراً حاسماً في التخفيف من أثر التهديدات السيبرانية على البيانات المالية، حيث تسهم الإجراءات الوقائية والرقابية في الكشف المبكر عن محاولات التلاعب أو سرقة البيانات، وتساعد في استعادة البيانات بسرعة في حال حدوث خرق أمني، وهو ما يسهم في استمرارية تقديم تقارير مالية دقيقة وموثوقة حتى في ظل الأزمات الأمنية.

المبحث الثاني: الإطار العملي للبحث

يهدف هذا الفصل إلى استعراض منهجية الدراسة بشكل تفصيلي، بدءاً بتحديد المجتمع الذي تنتمي إليه الدراسة، ثم تقديم لمحة عن العينة المستهدفة، مع التركيز على آلية بناء أداة الدراسة والإجراءات العلمية التي تم اتباعها للتحقق من صدقها وثباتها. كما يتضمن هذا الفصل عرضاً للطرائق الإحصائية المستخدمة في تحليل بيانات الدراسة، بما يوفّر تصوراً شاملاً عن الإطار المنهجي والعملي الذي استندت إليه الدراسة.

أولاً: منهجية الدراسة

اعتمدت هذه الدراسة المنهج الوصفي التحليلي كإطار منهجي لجمع البيانات ذات الصلة بمجال البحث، لا سيما في ضوء سعيها لاستكشاف الدور الوسيط للرقابة الداخلية بالحفاظ على جودة البيانات من التهديدات السيبرانية في البيئة الرقمية. وقد تم اختيار هذا المنهج نظراً لقدرته على وصف الواقع بدقة وتحليله كما هو، مع مراعاة المتغيرات الكمية والكيفية المؤثرة في الظاهرة محل الدراسة، وبهدف الوصول إلى نتائج قابلة للتعميم عبر تحويل البيانات الوصفية والتحليلية إلى مؤشرات علمية قابلة للقياس والاستنتاج.
وقد تم استخدام الاستبانة كأداة رئيسية لجمع البيانات، حيث قام الباحث ببنائها بما يتوافق مع أهداف الدراسة، وبما يمكّنه من التوصل إلى النتائج والتوصيات المرجوة. وتم تحليل البيانات المستخلصة باستخدام برنامج التحليل الإحصائي **SmartPLS 4**، القائم على أسلوب النمذجة بالمعادلات الهيكلية الجزئية(PLS-SEM) ، وذلك بهدف اختبار الفرضيات وتحليل العلاقات بين المتغيرات.

ثانياً: مجتمع الدراسة وعينتها

تمثّل مجتمع الدراسة شركات تحويل الأموال والمصارف العامة والخاصة في العراق. وقد تم اختيار عينة الدراسة باستخدام أسلوب العينة العشوائية البسيطة، حيث تم توزيع الاستبانة على عدد من الخبراء والمدققين الماليين وخبرا الأمن السيبراني من خلال رابط إلكتروني باستخدام أداة Google Forms. وقد بلغ عدد الاستجابات الصالحة للتحليل الإحصائي (١٣٠) مشاهدة.

ثالثاً: أداة الدراسة

استناداً إلى الأدبيات والدراسات السابقة ذات الصلة التي تم تناولها في الإطار النظري، قام الباحث ببناء استبانة وفق مقياس ليكرت الخماسي، كأداة رئيسية لجمع البيانات، وذلك لما يتميز به هذا المقياس من ملاءمة لأهداف الدراسة وفعالية من حيث الوقت والجهد والتكلفة. وقد تضمنت الاستبانة أربعة أقسام رئيسية:

- **القسم الأول** :يتضمن مقدمة توضح عنوان البحث وأهدافه واسم الباحث، مع التأكيد على سرية البيانات وعدم استخدامها إلا لأغراض البحث العلمي.
- **القسم الثاني** :يضم محاور الاستبانة الأساسية، ويتضمن ثلاثة محاور رئيسية:
  - **المحور الأول:** الأمن السيبراني، ويتضمن محورين فرعيين.
  - **المحور الثاني:** الرقابة الداخلية على البيانات المالية.
  - **المحور الثالث:** جودة البيانات المالية.

رابعاً: تحليل النتائج واختبار الفرضيات

قبل الشروع في اختبار فرضيات الدراسة، كان من الضروري البدء بتقييم كل من النموذجين: النموذج القياسي (القياس) والنموذج الهيكلي، وذلك من خلال الخطوات التالية:

١- تقييم النموذج القياسي (Measurement Model)

يهدف تقييم النموذج القياسي إلى التحقق من جودة أداة القياس وصحتها من حيث الصدق والثبات. ويُقصد بالصدق مدى قدرة الأداة على قياس ما صممت لقياسه، بينما يشير الثبات إلى مدى اتساق النتائج واستقرارها في حال إعادة القياس. ويمكن التحقق من جودة النموذج من خلال الخطوات الآتية:

بناء الموثوقية والصلاحية:

للتأكد من صلاحية أداة جمع البيانات ومدى ملاءمتها لقياس متغيرات الدراسة، اعتمد الباحث على معامل كرونباخ ألفا (Cronbach's Alpha)ومعامل Rho_A لتقييم مدى موثوقية المقياس. يُعد معامل كرونباخ ألفا من المؤشرات التقليدية المستخدمة لقياس الاتساق الداخلي بين فقرات المقياس، في حين يُستخدم معامل Rho_A لتقدير درجة التجانس والثبات الداخلي للمتغيرات الكامنة في النموذج. وقد أظهرت نتائج هذه المؤشرات مستوى مقبولاً من الصدق والثبات، كما يتضح من الجدول الآتي المتعلق بموثوقية وصدق البناء.

جدول (١)

	معامل ألفا كرونباخ	الموثوقية المركبة (rho_a)	الموثوقية المركبة	متوسط التباين المستخرج (AVE)
التهديدات السيبرانية	0.911	0.918	0.926	0.558
الرقابة الداخلية على البيانات المالية	0.932	0.933	0.948	0.786
جاهزية نظم الأمن السيبراني	0.814	0.826	0.869	0.571
جودة البيانات المالية	0.938	0.940	0.946	0.577

أظهرت نتائج معامل ألفا كرونباخ أن جميع المتغيرات تجاوزت الحد الأدنى المقبول البالغ ٠,٧٠، وهو ما يعكس اتساقاً داخلياً مرتفعاً بين فقرات كل محور. فقد بلغ معامل ألفا لمتغير التهديدات السيبرانية (٠,٩١١)، بينما سجل متغير الرقابة الداخلية على البيانات المالية (٠,٩٣٢)، في حين بلغت قيمة معامل ألفا لمتغير جاهزية نظم الأمن السيبراني (٠,٨١٤)، أما متغير جودة البيانات المالية فقد حقق أعلى قيمة بواقع (٠,٩٣٨). وتعكس هذه القيم بشكل عام موثوقية مرتفعة لأداة القياس، وتؤكد تجانس الفقرات المكونة لكل بُعد من أبعاد الدراسة.

أما فيما يتعلق بمعامل Rho_A والموثوقية المركبة، فقد أظهرت النتائج أن جميع القيم تجاوزت الحد الأدنى المقبول (٠,٧٠)، مما يدل على استقرار البنية الداخلية للمتغيرات. إذ بلغت قيمة Rho_A لمتغير التهديدات السيبرانية (٠,٩١٨)، والرقابة الداخلية (٠,٩٣٣)، وجاهزية نظم الأمن السيبراني (٠,٨٢٦)، وجودة البيانات المالية (٠,٩٤٠). أما الموثوقية المركبة، فقد سجلت بدورها قيماً مرتفعة، إذ بلغت (٠,٩٢٦) للتهديدات السيبرانية، و(٠,٩٤٨) للرقابة الداخلية، و(٠,٨٦٩) لجاهزية الأمن السيبراني، و(٠,٩٤٦) لجودة البيانات المالية، مما يؤكد تجانس المؤشرات ومدى تمثيلها للمتغيرات الكامنة.

وفيما يخص متوسط التباين المستخرج(AVE) ، فقد تجاوزت جميع المتغيرات الحد الأدنى المطلوب البالغ ٠,٥٠، مما يشير إلى أن كل مجموعة من الفقرات تفسر نسبة كافية من التباين في المتغير الذي تمثله. حيث بلغ AVE لمتغير التهديدات السيبرانية (٠,٥٥٨)، وللرقابة الداخلية (٠,٧٨٦)، ولجاهزية الأمن السيبراني (٠,٥٧١)، بينما بلغ لمتغير جودة البيانات المالية (٠,٥٧٧). وتعكس هذه النتائج كفاءة أداة القياس في تمثيل البُنى المفاهيمية للمتغيرات محل الدراسة بشكل دقيق.

وبناءً على ما سبق، يمكن التأكيد على أن الأداة المعتمدة في هذه الدراسة تتسم بدرجة عالية من الموثوقية والصدق، مما يجعلها مناسبة للاستخدام في تحليل أثر التهديدات السيبرانية وجاهزية نظم الأمن السيبراني والرقابة الداخلية على جودة البيانات المالية في البيئة الرقمية.

أ- ثبات المؤشرات(Indicator Reliability)

يُقاس ثبات المؤشرات من خلال حساب قيم التحميل الخارجي (Outer Loadings) لكل عبارة. ويتم الاحتفاظ بالعبارات التي تزيد قيمة التحميل لديها عن (٠,٧)، أما العبارات التي تقل عن (٠,٤) فيتم استبعادها مباشرة. وفي حال تراوحت القيم بين (٠,٤) و(٠,٧)، فإنه يتم استبعاد العبارة إذا كان لها تأثير سلبي على الثبات المركب(Composite Reliability) ، وإن لم يكن هناك تأثير سلبي، يفضل الإبقاء عليها (Ringle et al., 2022). ويوضح الجدول أدناه نتائج ثبات المؤشرات الخاصة بمتغيرات الدراسة:

جدول (٢)

	المحاور الفرعية	الفقرات	التشبعات الخارجية
الأمن السيبراني	التهديدات السيبرانية	تتعرض مؤسستنا لمحاولات اختراق إلكترونية بشكل متكرر.	0.673
		توجد محاولات للوصول غير المصرح به إلى البيانات المالية من جهات خارجية.	0.780
		تعاني المؤسسة من رسائل البريد الإلكتروني الاحتيالية المرتبطة بالمخترقين.	0.771
		يوجد تخوف مستمر من استهداف أنظمتنا ببرمجيات الفدية.	0.831
		لدينا وعي بأن التهديدات الخارجية تشكل خطراً على أمن بياناتنا المالية.	0.698
		يوجد احتمال لإساءة استخدام الموظفين لصلاحياتهم التقنية للوصول إلى البيانات المالية.	0.663
		ضعف وعي الموظفين بأمن المعلومات قد يسبب تهديداً سيبرانياً.	0.760
		ضعف إدارة كلمات المرور يعرض بياناتنا المالية لخطر الاختراق الداخلي.	0.769
		قد يقوم بعض الموظفين بتحميل ملفات قد تحتوي على فيروسات تضر بالبيانات المالية.	0.775
		عدم تحديث الأجهزة الداخلية يشكل ثغرة أمام الهجمات السيبرانية.	0.731
	جاهزية نظم الأمن السيبراني	تمتلك المؤسسة نظام كشف التسلل لمواجهة الهجمات السيبرانية.	0.770
		يتم تحديث برامج الحماية في المؤسسة بشكل منتظم.	0.773
		لدى المؤسسة خطة استجابة لحوادث الهجمات السيبرانية.	0.714
		لدينا نظام رقابة داخلية يضمن سلامة إدخال ومعالجة البيانات المالية.	0.861
		يتم اكتشاف الأخطاء والتجاوزات المالية بسرعة من خلال نظام الرقابة.	0.882
	الرقابة الداخلية على البيانات المالية	إجراءات المصادقة والمراجعة تتم وفقاً لسياسات واضحة وفعالة.	0.908
		تخضع جميع العمليات المالية لتوثيق ومراجعة دورية.	0.884
		تدعم الرقابة الداخلية قدرة المؤسسة على الامتثال للمعايير المحاسبية والتقارير.	0.898
		يتم تدريب الموظفين على إجراءات حماية البيانات المالية.	0.806
		لدى المؤسسة سياسات واضحة للتعامل مع التهديدات السيبرانية.	0.712

جودة البيانات المالية	تتميز البيانات المالية بالدقة والموثوقية.	0.823
	تتسم البيانات المالية بالاكتمال وعدم وجود نقص في المعلومات الأساسية.	0.747
	يتم تقديم البيانات المالية في الوقت المناسب دون تأخير.	0.592
	تتسم البيانات المالية بالشفافية وسهولة التحقق منها.	0.747
	يتم حفظ البيانات المالية بنظم آمنة لحمايتها من الضياع.	0.761
	البيانات المالية متاحة عند الحاجة لاتخاذ القرارات.	0.817
	تخضع البيانات المالية لعمليات تحقق مستمرة لضمان جودتها.	0.743
	تتسم البيانات المالية بسهولة المقارنة بين الفترات المالية المختلفة.	0.766
	يتم معالجة الأخطاء في البيانات المالية بشكل فوري ودقيق.	0.737
	توجد بروتوكولات واضحة لحماية سرية البيانات المالية.	0.789
	يمكن استرجاع البيانات المالية المفقودة بسرعة دون تأثير على جودة التقارير.	0.818
	تؤدي البيئة الرقمية إلى تعزيز سرعة إصدار التقارير المالية.	0.719
	تساهم الرقابة الرقمية في تعزيز الشفافية في إعداد التقارير المالية.	0.792

أظهرت نتائج تحليل التشبعات الخارجية لمؤشرات الدراسة اتساقًا وصدقًا مرتفعين في تمثيل المتغيرات الكامنة. فقد تجاوزت جميع فقرات محور التهديدات السيبرانية (بشقيه: التهديدات السيبرانية وجاهزية نظم الأمن السيبراني) الحدود المقبولة علميًا، حيث تراوحت التشبعات بين ٠,٦٦٣ و٠,٨٣١، وسُجلت أعلى القيم في الفقرات المتعلقة ببرمجيات الفدية، مما يعكس وعيًا كبيرًا بالمخاطر السيبرانية. كما أظهرت الفقرات المرتبطة بالتهديدات الداخلية تشبعات مقبولة تدل على تمثيل جيد للمحور، في حين جاءت تشبعات محور جاهزية الأنظمة الأمنية جميعها أعلى من ٠,٧٠، مما يعزز صدقه وارتباطه بالمتغير الكامن.
وفيما يتعلق بمحور الرقابة الداخلية على البيانات المالية، فقد حققت جميع الفقرات تشبعات خارجية مرتفعة (٠,٨٦١–٠,٩٠٨)، وهو ما يدل على صدق مرتفع واتساق داخلي قوي للمؤشر، ويعكس كفاءة أدوات القياس في هذا المجال. أما تشبعات فقرات جودة البيانات المالية، فقد تراوحت بين ٠,٥٩٢ و٠,٨٢٣، وبالرغم من تسجيل بعض الفقرات لقيم أقل من ٠,٧٠، إلا أنها ظلت ضمن الحدود المقبولة، خصوصًا أن استبقاؤها لم يؤثر سلبًا على ثبات المقياس أو صدقه. وسجل بند توقيت تقديم البيانات أدنى تشبع، مما قد يشير إلى تحديات زمنية في إعداد التقارير، في حين أظهرت بقية البنود تشبعات عالية تدل على دقة وتوافر وسهولة استرجاع البيانات.
بناءً عليه، تؤكد نتائج التشبعات الخارجية مبدئيًا صلاحية النموذج القياسي، دون الحاجة إلى حذف أي من الفقرات، مما يتيح الانتقال إلى تقييم الصدق التمييزي والثبات المركب كخطوة تالية لتحليل النموذج الهيكلي واختبار فرضيات الدراسة.

ب- الصدق التمييزي (Discriminant Validity)

تُعد الصدق التمييزي (Discriminant Validity) أحد المؤشرات الأساسية التي تُستخدم لتقييم مدى تميز المتغير الكامن عن غيره من المتغيرات الكامنة الأخرى ضمن النموذج الهيكلي، كما أوضح ذلك Ringle وآخرون (٢٠٢٢). ويتحقق هذا النوع من الصدق عندما يتمكن المتغير الكامن من التمايز بوضوح عن المتغيرات الأخرى في النموذج، بما يضمن عدم وجود تداخل غير مرغوب فيه في المعاني أو التفسيرات بين المتغيرات المختلفة. وتُجرى اختبارات الصدق التمييزي بصورة منتظمة في الدراسات التي تعتمد على النماذج الهيكلية، وذلك للتأكد من صحة العلاقات المفترضة بين المتغيرات، والتحقق من استقلالية كل متغير كامن عن المتغيرات الأخرى من حيث البناء المفاهيمي والقياس. وتهدف هذه الاختبارات إلى ضمان مساهمة كل متغير كامن في توضيح النموذج الهيكلي بشكل فعّال، دون أن يتأثر أو يُضعف من قبل متغيرات أخرى تشترك معه في بعض الخصائص. ويوضح الجدول التالي نتائج الصدق التمييزي للنموذج المعتمد في هذه الدراسة.

جدول (٣)

الصدق التمييزي نسبة الأحادية وسمة التغاير (HTMT) - مصفوفة	التهديدات السيبرانية	الرقابة الداخلية على البيانات المالية	جاهزية نظم الأمن السيبراني	جودة البيانات المالية
التهديدات السيبرانية				
الرقابة الداخلية على البيانات المالية	0.762			
جاهزية نظم الأمن السيبراني	0.837	0.772		
جودة البيانات المالية	0.799	0.856	0.808	

تشير النتائج أن جميع القيم المحسوبة تقع ضمن الحدود المقبولة علمياً، والتي يجب ألّا تتجاوز ٠,٩٠ في الدراسات ذات السياق الاجتماعي أو الإداري(Henseler et al., 2015) ، مما يعزز من دقة النموذج ويؤكد تحقق الصدق التمييزي بين المتغيرات المدروسة.
وعليه، يمكن القول إن اختبار HTMT قد دعم تحقق الصدق التمييزي في النموذج، الأمر الذي يعزز من موثوقية التحليل البنيوي للبيانات ويمنح الدراسة مصداقية أعلى في تفسير العلاقات السببية بين المتغيرات.

ت- التشبعات المتقاطعة:

يشير مصطلح " التشبعات المتقاطعة (Cross Loading) "، كما هو موضح في الجدول أدناه، إلى أهمية التأكد من أن الفقرات المرتبطة بكل بُعد من أبعاد الدراسة تقيس ذلك البُعد تحديداً، دون أن تتأثر أو تتداخل مع أبعاد أخرى في النموذج. ويتحقق ذلك عندما تكون قيم تحميل الفقرات أعلى على البُعد الذي تنتمي إليه مقارنةً بتحميلها على الأبعاد الأخرى، وهو ما يُعد مؤشراً على التميز البنيوي لكل بُعد ومدى ارتباطه الدقيق بالصفة التي يقيسها.

وتُسهم هذه الآلية في تعزيز وضوح التمايز بين الأبعاد المختلفة، كما تدعم مصداقية البناء المفاهيمي للنموذج، حيث تؤكد أن كل بُعد يقيس سمة فريدة لا تتقاطع بشكل جوهري مع السمات الأخرى. ومن خلال اعتماد هذا الأسلوب، تُمكننا التشبعات المتقاطعة من التأكد من دقة أدوات القياس المستخدمة في الدراسة، وتُعزز موثوقية النموذج الإحصائي البنيوي المعتمد، مما يضفي مزيداً من الثقة على النتائج المستخلصة من التحليل.

جدول (٤)

الفقرات	التهديدات السيبرانية	جاهزية نظم الأمن السيبراني	الرقابة الداخلية على البيانات المالية	جودة البيانات المالية
تتعرض مؤسستنا لمحاولات اختراق إلكترونية بشكل متكرر.	0.673	0.470	0.537	0.540
توجد محاولات للوصول غير المصرح به إلى البيانات المالية من جهات خارجية.	0.780	0.564	0.559	0.558
تعاني المؤسسة من رسائل البريد الإلكتروني الاحتيالية المرتبطة بالمخترقين.	0.771	0.512	0.497	0.533
يوجد تخوف مستمر من استهداف أنظمتنا ببرمجيات الفدية.	0.831	0.719	0.670	0.756
لدينا وعي بأن التهديدات الخارجية تشكل خطراً على أمن بياناتنا المالية.	0.698	0.573	0.572	0.621
يوجد احتمال لإساءة استخدام الموظفين لصلاحياتهم التقنية للوصول إلى البيانات المالية.	0.663	0.547	0.397	0.366
ضعف وعي الموظفين بأمن المعلومات قد يسبب تهديداً سيبرانياً.	0.760	0.548	0.474	0.477
ضعف إدارة كلمات المرور يعرض بياناتنا المالية لخطر الاختراق الداخلي.	0.769	0.533	0.517	0.563
قد يقوم بعض الموظفين بتحميل ملفات قد تحتوي على فيروسات تضر بالبيانات المالية.	0.775	0.540	0.510	0.558
عدم تحديث الأجهزة الداخلية يشكل ثغرة أمام الهجمات السيبرانية.	0.731	0.439	0.517	0.584
تمتلك المؤسسة نظام كشف التسلل لمواجهة الهجمات السيبرانية.	0.653	0.770	0.657	0.644
يتم تحديث برامج الحماية في المؤسسة بشكل منتظم.	0.593	0.773	0.475	0.485
لدى المؤسسة خطة استجابة لحوادث الهجمات السيبرانية.	0.457	0.714	0.312	0.443
لدينا نظام رقابة داخلية يضمن سلامة إدخال ومعالجة البيانات المالية.	0.503	0.806	0.580	0.580
يتم اكتشاف الأخطاء والتجاوزات المالية بسرعة من خلال نظام الرقابة.	0.538	0.712	0.521	0.522
إجراءات المصادقة والمراجعة تتم وفقاً لسياسات واضحة وفعالة.	0.573	0.619	0.861	0.729
تخضع جميع العمليات المالية لتوثيق ومراجعة دورية.	0.566	0.623	0.882	0.689
تدعم الرقابة الداخلية قدرة المؤسسة على الامتثال للمعايير المحاسبية والتقارير.	0.637	0.639	0.908	0.678
يتم تدريب الموظفين على إجراءات حماية البيانات المالية.	0.689	0.569	0.884	0.741
لدى المؤسسة سياسات واضحة للتعامل مع التهديدات السيبرانية.	0.689	0.642	0.898	0.734
تتميز البيانات المالية بالدقة والموثوقية.	0.608	0.625	0.623	0.823
تتسم البيانات المالية بالاكتمال وعدم وجود نقص في المعلومات الأساسية.	0.680	0.514	0.640	0.747
يتم تقديم البيانات المالية في الوقت المناسب دون تأخير.	0.531	0.576	0.515	0.592
تتسم البيانات المالية بالشفافية وسهولة التحقق منها.	0.574	0.523	0.596	0.747
يتم حفظ البيانات المالية بنظم آمنة لحمايتها من الضياع.	0.641	0.557	0.528	0.761
البيانات المالية متاحة عند الحاجة لاتخاذ القرارات.	0.622	0.559	0.658	0.817
تخضع البيانات المالية لعمليات تحقق مستمرة لضمان جودتها.	0.581	0.578	0.699	0.743
تتسم البيانات المالية بسهولة المقارنة بين الفترات المالية المختلفة.	0.677	0.585	0.723	0.766
يتم معالجة الأخطاء في البيانات المالية بشكل فوري ودقيق.	0.475	0.499	0.608	0.737
توجد بروتوكولات واضحة لحماية سرية البيانات المالية.	0.503	0.562	0.527	0.789
يمكن استرجاع البيانات المالية المفقودة بسرعة دون تأثير على جودة التقارير.	0.454	0.479	0.578	0.818
تؤدي البيئة الرقمية إلى تعزيز سرعة إصدار التقارير المالية.	0.516	0.509	0.579	0.719
تساهم الرقابة الرقمية في تعزيز الشفافية في إعداد التقارير المالية.	0.570	0.526	0.623	0.792

يُظهر الجدول السابق أن قيم التحميل الخاصة بالمتغيرات على أبعادها المرتبطة بها تفوق بشكل ملحوظ قيم تحميلها على الأبعاد الأخرى. تؤكد هذه النتائج أهمية وجود ارتباط قوي ودقيق بين المتغيرات والأبعاد التي تمثلها، حيث تعكس القيم العالية للتحميل توافقاً إحصائياً واضحاً يعزز الثقة في صلاحية النموذج الإحصائي المستخدم. كما تدل هذه النتائج على أن القيم المسجلة في الجدول تعد مقبولة إحصائياً، مما يساهم في تعميق فهمنا للعلاقة الفعالة بين المتغيرات وأبعادها ضمن إطار الدراسة.

ث- تحليل الارتباط بين الأبعاد (مؤشر R^2 الخاص بمتوسط التباين المستخرج AVE)

يُستخدم لضمان عدم وجود تداخل أو تقاطع بين الأبعاد المختلفة في النموذج. حيث يشير هذا التحليل إلى أن قيم الارتباط بين البُعد ونفسه يجب أن تكون أعلى من قيم الارتباط بين ذلك البُعد وبقية الأبعاد الأخرى. يوضح الجدول التالي مدى التداخل أو التقارب بين الأبعاد ضمن نموذج الدراسة، مما يعكس وضوح وتميز كل بُعد عن الأبعاد الأخرى.

جدول (٥)

محك فورنيل- لاركر	التهديدات السيبرانية	الرقابة الداخلية على البيانات المالية	جاهزية نظم الأمن السيبراني	جودة البيانات المالية
التهديدات السيبرانية	0.747			
الرقابة الداخلية على البيانات المالية	0.713	0.887		
جاهزية نظم الأمن السيبراني	0.734	0.697	0.756	
جودة البيانات المالية	0.760	0.806	0.721	0.760

ح- عامل تضخم التباين(VIF) :

هو مقياس يُستخدم لتقييم درجة التداخل الخطي المتعدد بين مؤشرات الدراسة. تُعتبر القيم المقبولة إحصائياً هي القيم التي تقل عن ٥، مما يدل على عدم وجود تداخل جوهري بين المتغيرات. أما في حال تجاوز قيم VIF هذا الحد، فإن ذلك يشير إلى وجود ارتباط عالٍ بين المتغير محل الفحص وباقي المتغيرات في الدراسة. يعرض الجدول التالي قيم عامل تضخم التباين لمتغيرات الدراسة، مما يتيح فهماً أفضل لاحتمالية وجود تداخل خطي متعدد داخل النموذج.

جدول (٦)

الفقرات	معامل تضخم التباين VIF
تتعرض مؤسستنا لمحاولات اختراق إلكترونية بشكل متكرر.	1.778
توجد محاولات للوصول غير المصرح به إلى البيانات المالية من جهات خارجية.	2.362
تعاني المؤسسة من رسائل البريد الإلكتروني الاحتيالية المرتبطة بالمخترقين.	2.197
يوجد تخوف مستمر من استهداف أنظمتنا ببرمجيات الفدية.	2.834
لدينا وعي بأن التهديدات الخارجية تشكل خطراً على أمن بياناتنا المالية.	2.024
يوجد احتمال لإساءة استخدام الموظفين لصلاحياتهم التقنية للوصول إلى البيانات المالية.	2.494
ضعف وعي الموظفين بأمن المعلومات قد يسبب تهديداً سيبرانياً.	3.644
ضعف إدارة كلمات المرور يعرض بياناتنا المالية لخطر الاختراق الداخلي.	2.875
قد يقوم بعض الموظفين بتحميل ملفات قد تحتوي على فيروسات تضر بالبيانات المالية.	2.938
عدم تحديث الأجهزة الداخلية يشكل ثغرة أمام الهجمات السيبرانية.	1.955
تمتلك المؤسسة نظام كشف التسلل لمواجهة الهجمات السيبرانية.	1.651
يتم تحديث برامج الحماية في المؤسسة بشكل منتظم.	1.851
لدى المؤسسة خطة استجابة لحوادث الهجمات السيبرانية.	1.750
لدينا نظام رقابة داخلية يضمن سلامة إدخال ومعالجة البيانات المالية.	1.934
يتم اكتشاف الأخطاء والتجاوزات المالية بسرعة من خلال نظام الرقابة.	1.463
إجراءات المصادقة والمراجعة تتم وفقاً لسياسات واضحة وفعالة.	2.539
تخضع جميع العمليات المالية لتوثيق ومراجعة دورية.	1.366
تدعم الرقابة الداخلية قدرة المؤسسة على الامتثال للمعايير المحاسبية والتقارير.	3.526
يتم تدريب الموظفين على إجراءات حماية البيانات المالية.	3.073
لدى المؤسسة سياسات واضحة للتعامل مع التهديدات السيبرانية.	3.259
تتميز البيانات المالية بالدقة والموثوقية.	3.397
تتسم البيانات المالية بالاكتمال وعدم وجود نقص في المعلومات الأساسية.	3.143
يتم تقديم البيانات المالية في الوقت المناسب دون تأخير.	1.832
تتسم البيانات المالية بالشفافية وسهولة التحقق منها.	2.582

يتم حفظ البيانات المالية بنظم آمنة لحمايتها من الضياع.	2.601
البيانات المالية متاحة عند الحاجة لاتخاذ القرارات.	3.306
تخضع البيانات المالية لعمليات تحقق مستمرة لضمان جودتها.	3.839
تتسم البيانات المالية بسهولة المقارنة بين الفترات المالية المختلفة.	2.407
يتم معالجة الأخطاء في البيانات المالية بشكل فوري ودقيق.	2.654
توجد بروتوكولات واضحة لحماية سرية البيانات المالية.	3.778
يمكن استرجاع البيانات المالية المفقودة بسرعة دون تأثير على جودة التقارير.	3.153
تؤدي البيئة الرقمية إلى تعزيز سرعة إصدار التقارير المالية.	3.422
تساهم الرقابة الرقمية في تعزيز الشفافية في إعداد التقارير المالية.	3.682

يوضح الجدول السابق أن جميع قيم عامل تضخم التباين (VIF) للمتغيرات أقل من ٥، مما يشير إلى ملاءمة النموذج لقياس العلاقات بين متغيرات الدراسة. وهذا يدل على عدم وجود مشكلة التداخل الخطي المتعدد (Multicollinearity)، مما يعزز من صحة النموذج ودقته في تقييم التفاعلات بين المتغيرات.

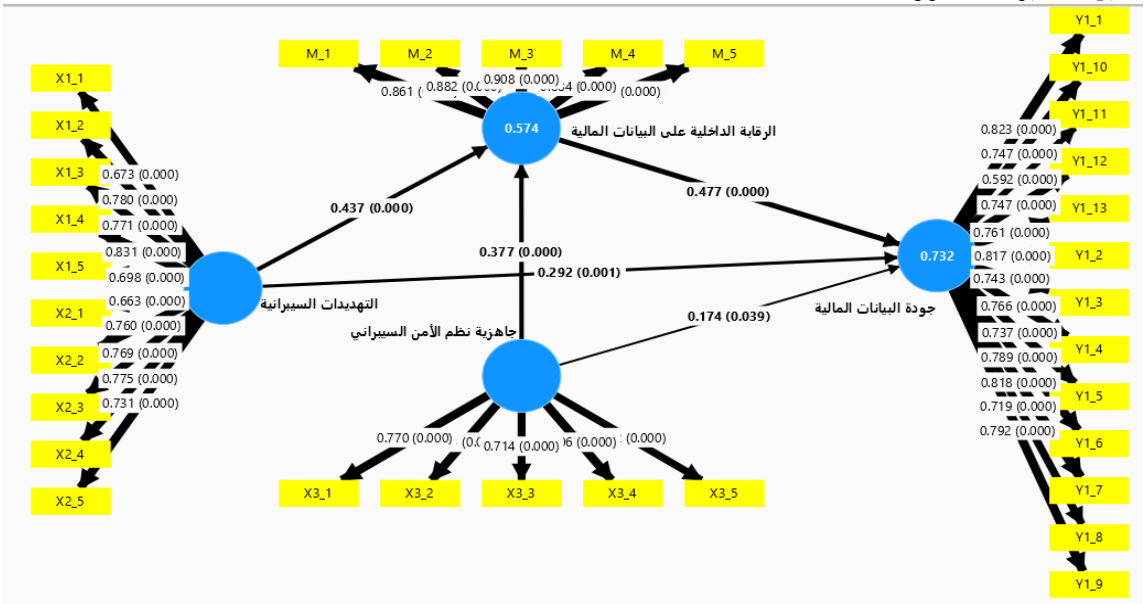
خ- عامل تضخم التباين (VIF):

تشير إحصائيات التداخل الخطي، والمتمثلة في عامل تضخم التباين(VIF) ، إلى مدى وجود مشاكل محتملة للتعدد الخطي في النموذج الداخلي للدراسة. يحدث التعدد الخطي عندما تكون المتغيرات المستقلة مرتبطة ارتباطاً عالياً ببعضها البعض، مما قد يؤثر سلباً على دقة تقديرات النموذج. تُعتبر قيمة VIF أقل من ٥ مقبولة عموماً، إذ تدل على أن التعدد الخطي ليس مشكلة جوهرية. تظهر النتائج أن جميع قيم VIF تقع تحت هذا الحد، مما يشير إلى أن التعدد الخطي لا يشكل إشكالية كبيرة في النموذج، وفقاً لما أشار إليه Ringle وآخرون.(2022)

جدول (٧)

	معامل تضخم التباين VIF
التهديدات السيبرانية -> الرقابة الداخلية على البيانات المالية	2.171
التهديدات السيبرانية -> جودة البيانات المالية	2.619
الرقابة الداخلية على البيانات المالية -> جودة البيانات المالية	2.349
جاهزية نظم الأمن السيبراني -> الرقابة الداخلية على البيانات المالية	2.171
جاهزية نظم الأمن السيبراني -> جودة البيانات المالية	2.504

تظهر النتائج أن قيم VIF لجميع العلاقات بين المتغيرات تتراوح بين ٢,١٧١ و٢,٦١٩، وهي قيم تقع ضمن النطاق المقبول إحصائياً (أقل من ٥)، مما يدل على عدم وجود مشاكل ملحوظة في التعدد الخطي بين المتغيرات.. وبناءً على هذه القيم، يمكن الاستنتاج بأن النموذج خالٍ من مشاكل التعدد الخطي الجوهرية، مما يعزز من موثوقية النتائج واستقرار تقديرات النموذج في قياس العلاقات بين المتغيرات المدروسة.



شكل (١)

د- تقييم النموذج الهيكلي:

تُعَدُّ عملية تقييم النموذج الهيكلي خطوةً أساسيةً تسبق اختبار الفرضيات، حيث تهدف إلى التأكد من جودة النموذج من خلال عدة معايير رئيسية تتمثل في معامل التحديد(R^2) ، وحجم التأثير(F^2) ، ومؤشر ملاءمة النموذج .(GOF) يركز هذا التقييم على قياس مدى قدرة النموذج على تفسير العلاقات بين المتغيرات، وتوضيح قوة هذه العلاقات.

ذ- معامل التحديد:(R^2)

يُستخدم معامل التحديد (R^2) لتقدير دقة معاملات الانحدار، ويُحسب بتربيع معامل الارتباط البسيط بين المتغيرات، حيث تتراوح قيمته بين ٠ و١، وتشير القيم القريبة من الواحد إلى دقة أعلى في التنبؤات الانحدارية وقلة الخطأ العشوائي. يعكس معامل التحديد قدرة النموذج على تفسير التغيرات في المتغير التابع بناءً على المتغيرات المستقلة. يتم تفسير قيم (R^2) عادةً وفقاً للمعايير التالية: إذا كانت القيمة أقل من ٠,١٩ يُعتبر النموذج غير مقبول، وإذا كانت بين ٠,١٩ و٠,٣٣ يُعتبر ضعيفاً، أما القيم بين ٠,٣٣ و٠,٦٧ فتُعد متوسطة، في حين أن القيم الأعلى من ٠,٦٧ تدل على قوة عالية في تفسير النموذج. يوضح الجدول التالي قيم معامل التحديد (R^2)للمتغيرات المستخدمة في الدراسة.

جدول (٨)

	مربع الارتباط	مربع الارتباط المعدل
الرقابة الداخلية على البيانات المالية	0.574	0.567
جودة البيانات المالية	0.732	0.725

تشير نتائج مربع الارتباط ومربع الارتباط المعدل إلى مدى تفسير المتغيرات المستقلة للتغيرات في المتغيرات التابعة ضمن النموذج المدروس. ففيما يتعلق بالرقابة الداخلية على البيانات المالية، يظهر مربع الارتباط قيمة ٠,٥٧٤، في حين بلغ مربع الارتباط المعدل ٠,٥٦٧، مما يعكس قدرة معتدلة للنموذج على تفسير التباين في هذا المتغير مع تعديل بسيط يأخذ في الاعتبار عدد المتغيرات المستخدمة. أما جودة البيانات المالية فقد سجلت قيماً أعلى، حيث بلغ مربع الارتباط ٠,٧٣٢ ومربع الارتباط المعدل ٠,٧٢٥، مما يشير إلى قدرة قوية للنموذج في تفسير التغيرات المتعلقة بجودة البيانات المالية. تعكس هذه القيم بشكل عام دقة ملحوظة للنموذج في تفسير العلاقة بين المتغيرات، مع إشارة إلى تفوق قدرة النموذج في تفسير جودة البيانات المالية مقارنة بالرقابة الداخلية على البيانات المالية.

ر- حجم التأثير(F^2) :

يُعتبر حجم التأثير (F^2) من المؤشرات المهمة التي تعكس مدى تأثير المتغيرات المستقلة على المتغيرات التابعة في النموذج. وقد قدم كوهين (١٩٨٨) دليلاً لتفسير قيم F^2 وفقاً لمستويات التأثير المختلفة، حيث تدل القيمة الأقل من ٠,٠٢ على عدم وجود تأثير يذكر. بينما تشير القيمة التي تقع بين ٠,٠٢ وأقل من ٠,١٥ إلى تأثير صغير، وتُعبر القيمة التي تتراوح بين ٠,١٥ وأقل من ٠,٣٥ عن تأثير متوسط، أما القيم التي تتجاوز ٠,٣٥ فتدل على تأثير كبير. يعرض الجدول التالي قيم F^2 للمتغيرات المدروسة في هذه الدراسة.

جدول (٩)

	مربع ف
التهديدات السيبرانية -> الرقابة الداخلية على البيانات المالية	0.206
التهديدات السيبرانية -> جودة البيانات المالية	0.121
الرقابة الداخلية على البيانات المالية -> جودة البيانات المالية	0.360
جاهزية نظم الأمن السيبراني -> الرقابة الداخلية على البيانات المالية	0.153
جاهزية نظم الأمن السيبراني -> جودة البيانات المالية	0.045

تشير نتائج تحليل حجم التأثير (مربع ف) إلى تفاوت في قوة التأثير بين المتغيرات المستقلة على المتغيرات التابعة في النموذج. حيث يظهر أن العلاقة بين التهديدات السيبرانية والرقابة الداخلية على البيانات المالية تتمتع بتأثير متوسط بقيمة ٠,٢٠٦، مما يعكس أهمية التهديدات السيبرانية في تشكيل وتحسين آليات الرقابة الداخلية ضمن المؤسسة. أما التأثير بين التهديدات السيبرانية وجودة البيانات المالية فهو صغير نسبياً بقيمة ٠,١٢١، مما يدل على وجود تأثير لكنه أقل قوة مقارنةً بالعلاقة السابقة. كما يبرز التأثير الكبير للرقابة الداخلية على جودة البيانات المالية، حيث بلغت قيمة مربع ف ٠,٣٦٠، مما يؤكد الدور الحاسم للرقابة الداخلية في ضمان دقة وكفاءة جودة البيانات المالية. فيما يتعلق بجاهزية نظم الأمن السيبراني، يظهر تأثير متوسط على الرقابة الداخلية بقيمة ٠,١٥٣، وهو ما يشير إلى أن استعداد المؤسسة من حيث نظم الأمن السيبراني يسهم بشكل ملحوظ في دعم الرقابة الداخلية. بينما كان التأثير بين جاهزية نظم الأمن السيبراني وجودة البيانات المالية ضعيفاً نسبياً بقيمة ٠,٠٤٥، مما يعكس تأثيراً محدوداً لهذا المتغير على جودة البيانات المالية مباشرة. هذه النتائج توضح تباين درجات التأثير بين المتغيرات المختلفة، مما يعكس الأهمية النسبية لكل منها في إطار النموذج المدروس.

ز- مؤشر جودة المطابقة:(GOF)

يُعد مؤشر جودة المطابقة (GOF) من المقاييس الأساسية في تقييم مدى ملاءمة النموذج الإحصائي للبيانات الفعلية. ويُستخدم هذا المؤشر، الذي يُعرف أيضاً بمؤشر جودة المطابقة، لتقدير كفاءة النموذج في تفسير العلاقات بين المتغيرات المستقلة والتابعة. ويُعتبر مؤشر GOF أداة فعّالة لقياس جودة النموذج، إذ يُعبر عن الفجوة بين القيم الفعلية والقيم المتوقعة التي ينتجها النموذج.
يُحسب هذا المؤشر من خلال الجذر التربيعي لحاصل ضرب متوسط التباين المستخرج (AVE) ومعامل التحديد (R^2) الخاص بنموذج المعادلات الهيكلية. وبحسب Wetzels وآخرين (٢٠٠٩)، فإن قيمة GOF التي تتجاوز ٠,٣٦ تُعد مقبولة ومؤشراً على جودة مناسبة للنموذج. وفي إطار هذه الدراسة، تم احتساب قيمة GOF من خلال استخراج الجذر التربيعي لحاصل ضرب قيم AVEوR^2، وهو ما يوفر مؤشراً يعكس مدى تطابق النموذج مع البيانات الفعلية. ويعرض الجدول التالي قيمة GOF لنموذج الدراسة، مما يدل على مستوى جودة المطابقة العامة للنموذج.

جدول (١٠)

المحور	مربع الارتباط	متوسط التباين المستخرج (AVE)
التهديدات السيبرانية		0.558
جاهزية نظم الأمن السيبراني		0.571
الرقابة الداخلية على البيانات المالية	0.574	0.786
جودة البيانات المالية	0.732	0.577
المتوسط الحسابي	0.653	0.623

تم حساب مؤشر ملاءمة النموذج باستخدام الصيغة التالية:

$$\sqrt{0.623 \times 0.653} = 0.637823$$

ويلاحظ أن قيمة المؤشر الناتجة تشير إلى جودة عالية لملاءمة النموذج، حيث أنها تتجاوز عتبة ٠,٣٥، والتي تستخدم عادة كمعيار لتحديد مدى ملاءمة النموذج.

س- تقييم معاملات المسار في النموذج الهيكلي:

تُعنى عملية تقييم معاملات المسار في النموذج الهيكلي بدراسة وتحليل العلاقات بين مكونات النموذج المختلفة، حيث يتم التحقق من القيم الفعلية لمعاملات المسار التي تربط بين المتغيرات ضمن النموذج. تهدف هذه العملية إلى الكشف عن مدى توفر الأدلة الإحصائية التي تؤيد أو ترفض تأثير إدارة المعرفة كوسيط في تعزيز أداء الموارد البشرية من خلال تطبيقات الذكاء الاصطناعي داخل المنظمة محل الدراسة. يشمل التحليل مجموعة من المؤشرات الإحصائية المهمة مثل متوسط العينة، وفترة الثقة، ومستوى الدلالة الإحصائية المستخلصة من تحليل التمهيد (Bootstrapping) للنموذج بأكمله. وقد أسفر تحليل معاملات المسار الخاصة بهذه الفرضية عن النتائج المبينة في الجدول التالي.

جدول (١١)

المحاور	العينة الأصلية (O)	متوسط العينة (M)	الانحراف المعياري (STDEV)	إحصاءات قيمة ت (|O/STDEV|)	فترات الثقة 2.5%	فترات الثقة 97.5%	التحيز المصحح لفترات الثقة التحيز	التحيز المصحح لفترات الثقة 2.5%	التحيز المصحح لفترات الثقة 97.5%	الدلالة أو قيمة P
التهديدات السيبرانية -> الرقابة الداخلية على البيانات المالية	0.437	0.443	0.075	5.801	0.293	0.590	0.006	0.274	0.575	0.000
التهديدات السيبرانية -> جودة البيانات المالية	0.292	0.301	0.084	3.475	0.141	0.471	0.009	0.130	0.459	0.001
الرقابة الداخلية على البيانات المالية -> جودة البيانات المالية	0.477	0.468	0.102	4.695	0.260	0.655	-0.009	0.272	0.666	0.000
جاهزية نظم الأمن السيبراني -> الرقابة الداخلية على البيانات المالية	0.377	0.368	0.083	4.532	0.196	0.523	-0.008	0.216	0.537	0.000
جاهزية نظم الأمن السيبراني -> جودة البيانات المالية	0.174	0.169	0.084	2.070	0.005	0.335	-0.005	0.014	0.345	0.039

تشير مخرجات تحليل معاملات المسار ضمن النموذج الهيكلي إلى وجود علاقات سببية ذات دلالة إحصائية قوية بين متغيرات الدراسة، مما يدل على مناسبة الإطار النظري المقترح وتوافقه مع البيانات التجريبية. فقد بيّنت النتائج أن للتهديدات السيبرانية تأثيرًا مباشراً وإيجابيًا على فعالية الرقابة الداخلية على البيانات المالية، حيث بلغ معامل التأثير ٠,٤٣٧، بقيمة إحصائية (T) تعادل ٥,٨٠١، وهو ما يشير إلى أن تصاعد التهديدات الرقمية يدفع المؤسسات نحو تعزيز ضوابطها الداخلية، لحماية بياناتها من المخاطر السيبرانية، بما يتماشى مع ما طرحه Nguyen وآخرون (٢٠٢١) من ضرورة تحديث أنظمة الرقابة في ظل تصاعد التهديدات التقنية.
كما كشفت النتائج أن للتهديدات السيبرانية تأثيراً معنوياً على جودة البيانات المالية، وإن كان بدرجة أدنى، حيث بلغ معامل التأثير ٠,٢٩٢، بقيمة (T) بلغت ٣,٤٧٥، ما يعكس احتمال تراجع دقة ومصداقية التقارير المالية عند غياب وسائل الحماية المناسبة،

وهي نتيجة تنسجم مع ما أورده Vasarhelyi و Alles (2019) حول الآثار السلبية للهجمات السيبرانية على جودة الإفصاح المالي.

وفيما يخص العلاقة بين الرقابة الداخلية وجودة البيانات المالية، فقد كانت هذه العلاقة الأبرز في النموذج، حيث سجلت أعلى معامل تأثير بواقع ٠,٤٧٧، وقيمة (T) وصلت إلى ٤,٦٩٥، مما يدل على أن وجود آليات رقابية داخلية قوية يسهم في رفع مستوى جودة البيانات من خلال الحد من الأخطاء والكشف المبكر عن الانحرافات، وهي نتيجة تتسق مع ما توصل إليه Bedard وآخرون (٢٠١٢) بشأن دور الرقابة في تحسين مصداقية التقارير المالية.

أما جاهزية أنظمة الأمن السيبراني، فقد أظهرت تأثيراً إيجابياً على الرقابة الداخلية بمعامل بلغ ٠,٣٧٧ وقيمة (T) تساوي ٤,٥٣٢، ما يعكس الدور الداعم للبنية التحتية السيبرانية في تعزيز كفاءة أنظمة الضبط الداخلي، وهو ما يتوافق مع ما ذكره Al-Dmour وآخرون (٢٠٢١) حول العلاقة التكميلية بين الاستثمار في الأمن السيبراني وفعالية الرقابة المؤسسية.

وأظهرت النتائج أيضًا وجود علاقة إيجابية ضعيفة لكنها معنوية بين جاهزية نظم الأمن السيبراني وجودة البيانات المالية، حيث بلغ معامل التأثير ٠,١٧٤ وقيمة2.070 (T) ، ما يشير إلى مساهمة غير مباشرة لجاهزية تلك النظم في تحسين جودة البيانات، وهي نتيجة تتفق مع ما أشار إليه Cao وآخرون (٢٠٢٠) بأن أثر الأمن السيبراني يظل محدودًا ما لم يُدعَم بسياسات حوكمة فعالة للبيانات.

وعليه، يمكن الاستنتاج أن الرقابة الداخلية تمثل العنصر الوسيط الأكثر تأثيراً في العلاقة بين التهديدات السيبرانية وجودة البيانات المالية، بينما تمثل جاهزية نظم الأمن السيبراني عنصراً داعماً يعزز من كفاءة هذا الدور، بما يؤكد ضرورة تبني إطار تكاملي يجمع بين الأمن السيبراني والرقابة الداخلية لضمان جودة المعلومات المالية في بيئة الأعمال الرقمية المعاصرة.

جدول (١٢)

المحاور	العينة الأصلية (O)	متوسط العينة (M)	الانحراف المعياري (STDEV)	إحصاءات قيمة ت (|O/STDEV|)	فترات الثقة		التحيز المصحح لفترات الثقة			الدلالة أو قيمة P
					2.5%	97.5%	التحيز	2.5%	97.5%	
التهديدات السيبرانية -> جودة البيانات المالية	0.208	0.207	0.055	3.790	0.105	0.316	-0.002	0.110	0.326	0.000
جاهزية نظم الأمن السيبراني -> جودة البيانات المالية	0.179	0.175	0.062	2.878	0.064	0.307	-0.004	0.077	0.333	0.004

تُبرز نتائج التحليل الإحصائي للتأثيرات الكلية غير المباشرة في النموذج الهيكلي وجود علاقات سببية معنوية بين المتغيرات المستقلة والتابعة عبر متغير وسيط، مما يعكس فاعلية المسارات غير المباشرة في تفسير ديناميكيات النموذج المفاهيمي. فقد أظهرت النتائج أن للتهديدات السيبرانية أثراً غير مباشر موجباً وذو دلالة إحصائية على جودة البيانات المالية من خلال دور الرقابة الداخلية، حيث بلغ معامل التأثير غير المباشر ٠,٢٠٨، بمتوسط عينة قدره ٠,٢٠٧، وانحراف معياري بلغ ٠,٠٥٥، فيما سجّلت قيمة T نحو ٣,٧٩٠، متجاوزة بذلك القيمة الحرجة المعتمدة عند مستوى الدلالة ٠,٠٥، ما يدل على وجود دلالة إحصائية قوية. كما أن فترة الثقة بنسبة ٩٥٪ تراوحت بين ٠,١٠٥ و٠,٣١٦، دون أن تتضمن الصفر، الأمر الذي يعزز من موثوقية هذا التأثير الإحصائي. وتدعم هذه النتيجة ما خلصت إليه دراسات سابقة، من بينها دراسة Nguyen وآخرون (٢٠٢١)، التي أوضحت أن تصاعد المخاطر السيبرانية يُحفّز المؤسسات على تعزيز منظومة الرقابة الداخلية، وهو ما ينعكس بشكل إيجابي على دقة وموثوقية التقارير المالية.

كما بيّنت النتائج أن جاهزية نظم الأمن السيبراني تؤثر كذلك بصورة غير مباشرة وبشكل معنوي وإيجابي على جودة البيانات المالية من خلال الرقابة الداخلية، إذ بلغ معامل هذا التأثير ٠,١٧٩، بمتوسط عينة مقداره ٠,١٧٥ وانحراف معياري بلغ ٠,٠٦٢، فيما سجّلت قيمة T نحو ٢,٨٧٨، وهي قيمة دالة إحصائياً عند مستوى دلالة بلغت P = 0.004. أما فترة الثقة البالغة ٩٥٪ فقد تراوحت بين ٠,٠٦٤ و٠,٣٠٧ دون أن تشمل الصفر، مما يعزّز من مصداقية هذا التأثير غير المباشر. وتتسق هذه النتيجة مع ما توصل إليه Al-Dmour وآخرون (٢٠٢١)، الذين أكدوا أن الاستثمار في تعزيز جاهزية النظم السيبرانية يساهم بشكل غير مباشر في تحسين جودة المعلومات المالية، من خلال رفع كفاءة نظام الرقابة الداخلية.

وبالتالي، تبرز هذه النتائج أهمية الدور الوسيط الذي تؤديه الرقابة الداخلية في تمرير تأثير كل من التهديدات السيبرانية ومستوى جاهزية الأمن السيبراني إلى جودة البيانات المالية. وهو ما يؤكد ضرورة تبني منظور تكاملي لتحليل العلاقات السببية، يأخذ بعين الاعتبار الأثر غير المباشر باعتباره مساراً حيوياً لفهم تفاعل مكونات النموذج النظري في بيئة الأعمال الرقمية.

نتائج البحث

أبرزت نتائج التحليل الإحصائي للنموذج الهيكلي وجود روابط ذات دلالة إحصائية بين متغيرات الدراسة، سواء فيما يتعلق بالتأثيرات المباشرة أو غير المباشرة. فقد أظهرت البيانات أن التهديدات السيبرانية تُحدث أثراً مباشراً موجباً ومعنوياً على الرقابة الداخلية للبيانات المالية، حيث بلغ معامل التأثير ٠,٤٣٧، مع قيمة T بلغت ٥,٨٠١، وهي قيمة تفوق المستوى المقبول إحصائيًا (P < 0.001)، مما يشير إلى أن تصاعد الهجمات السيبرانية يدفع المؤسسات إلى تطوير وتعزيز أنظمتها الرقابية الداخلية. وتتوافق هذه النتيجة مع ما توصلت إليه دراسات سابقة، مثل دراسة Nguyen وآخرين (٢٠٢١)، التي بيّنت أن تزايد التهديدات الإلكترونية يُحفز المؤسسات على تبنّي نظم رقابة أكثر صرامة.

وفي السياق ذاته، أوضحت النتائج وجود تأثير إيجابي مباشر للرقابة الداخلية على جودة البيانات المالية، بوزن معياري بلغ ٠,٤٧٧ وقيمة T وصلت إلى ٤,٦٩٥، وهي دلالة إحصائية قوية($P < 0.001$) ، ما يعكس الدور الحيوي للرقابة الداخلية في رفع مستوى دقة ومصداقية البيانات المحاسبية، وهو ما أشارت إليه دراسات مثل Al-Dmour وآخرين (٢٠٢١).

أما فيما يخص جاهزية أنظمة الأمن السيبراني، فقد تبين أنها تمارس أثراً مباشراً موجباً ومعنوياً على الرقابة الداخلية، حيث بلغ معامل التأثير ٠,٣٧٧ وقيمة T نحو ٤,٥٣٢، كما أظهرت النتائج وجود أثر مباشر، وإن كان أقل نسبياً، على جودة البيانات المالية بوزن معياري قدره ٠,١٧٤ وقيمة T بلغت ٢,٠٧٠($P = 0.039$) ، مما يعكس أن تعزيز البنية التحتية السيبرانية يسهم بشكل فعّال في تحسين كفاءة أنظمة الرقابة، ومن ثم تحسين جودة البيانات.

أما على صعيد التأثيرات غير المباشرة، فقد اتضح أن التهديدات السيبرانية تؤثر بشكل غير مباشر ودال إحصائيًا على جودة البيانات المالية من خلال الرقابة الداخلية، بوزن معياري بلغ ٠,٢٠٨ وقيمة T وصلت إلى ٣,٧٩٠. كما أن لجاهزية أنظمة الأمن السيبراني أثراً غير مباشر على جودة البيانات بلغ ٠,١٧٩، مع قيمة T تساوي ٢,٨٧٨($P = 0.004$) ، وقد دعمت فترات الثقة لهذه العلاقات دلالتها الإحصائية بعدم احتوائها على الصفر، مما يؤكد قوة هذه المسارات غير المباشرة.

وفيما يتعلق بجودة النموذج التفسيري، فقد بين معامل التحديد (R^2) أن الرقابة الداخلية تفسر ما نسبته ٥٧,٤٪ من التباين، بينما تفسر مجموعة المتغيرات المستقلة (الرقابة الداخلية، التهديدات السيبرانية، جاهزية الأمن السيبراني) ما نسبته ٧٣,٢٪ من التباين في جودة البيانات المالية، وهو ما يشير إلى قوة تفسيرية معتدلة إلى مرتفعة للنموذج. كما كشفت نتائج تحليل حجم الأثر (F^2) عن وجود تأثيرات تتراوح بين المتوسطة والقوية، خصوصاً في العلاقة بين الرقابة الداخلية وجودة البيانات المالية، والتي بلغ حجم الأثر فيها ٠,٣٦٠، مما يعكس فعالية المتغير الوسيط في نقل التأثير.

وبناء على ما سبق، يمكن الاستنتاج أن الرقابة الداخلية للبيانات المالية تشكل متغيراً وسيطاً فاعلاً في تفسير العلاقة بين كل من التهديدات السيبرانية وجاهزية الأمن السيبراني من جهة، وجودة البيانات المالية من جهة أخرى، وهو ما يتماشى مع الاتجاهات المعاصرة في إدارة أمن المعلومات وتحسين جودة التقارير المالية.

التوصيات

استناداً إلى النتائج التي توصل إليها البحث، والتي أظهرت وجود تأثيرات مباشرة وغير مباشرة معنوية للتهديدات السيبرانية وجاهزية نظم الأمن السيبراني على جودة البيانات المالية من خلال الرقابة الداخلية، يوصي الباحث بما يلي:

١. **تعزيز استراتيجيات الحماية من التهديدات السيبرانية** :يتوجب على المؤسسات، لا سيما تلك المعنية بإعداد التقارير المالية، تطوير سياسات أمنية شاملة لمواجهة التهديدات السيبرانية، بما في ذلك تحديث الأنظمة باستمرار، وتنفيذ اختبارات اختراق دورية، وبناء ثقافة مؤسسية واعية بالمخاطر الرقمية.
٢. **رفع جاهزية نظم الأمن السيبراني** :توصي الدراسة بزيادة الاستثمار في البنية التحتية السيبرانية، من خلال تحديث البرامج والمعدات الأمنية، وتبني تقنيات متقدمة مثل الذكاء الاصطناعي للكشف المبكر عن الاختراقات، بما يعزز من فاعلية الرقابة الداخلية.
٣. **تفعيل دور الرقابة الداخلية كوسيط تنظيمي** :بالنظر إلى الأثر الوسيط المهم للرقابة الداخلية في تحسين جودة البيانات المالية، توصي الدراسة بتقوية نظم الرقابة الداخلية من خلال إعداد كوادر متخصصة، وتبني منهجيات قائمة على تقييم المخاطر، مع مراجعة دورية لمدى كفاءة وفعالية الضوابط والإجراءات.
٤. **إدماج الأمن السيبراني ضمن إطار الحوكمة المؤسسية** :توصي الدراسة بدمج اعتبارات الأمن السيبراني ضمن سياسات الحوكمة الداخلية للمؤسسة، بحيث يتم النظر إليه كعنصر جوهري في إدارة المخاطر المؤسسية، خصوصاً في ما يتعلق بجودة البيانات المالية والمساءلة.

الخاتمة

استناداً إلى ما تقدم، خلصت هذه الدراسة إلى مجموعة من النتائج المحورية التي تبرز الدور الحاسم لكل من التهديدات السيبرانية ومستوى جاهزية أنظمة الأمن السيبراني في التأثير على جودة البيانات المالية، وذلك من خلال الدور الوسيط الذي تؤديه الرقابة الداخلية. وقد أظهرت النتائج أن التهديدات السيبرانية تشكّل عاملاً ضاغطاً وسلبياً على جودة المعلومات المالية، غير أن توافر نظام رقابة داخلية فعال يسهم في احتواء هذا التأثير السلبي ويعزز من استقرار النظام المحاسبي والمالي داخل المؤسسة. كما أوضحت الدراسة أن مستوى الجاهزية السيبرانية يسهم بدور إيجابي مباشر في دعم البنية الرقابية، الأمر الذي ينعكس بشكل غير مباشر على تحسين جودة البيانات المالية.

وتتسق هذه النتائج مع ما أوردته أدبيات سابقة تناولت تأثير الأمن السيبراني في كفاءة النظم المالية، إلا أن هذه الدراسة تسهم بإضافة نوعية من خلال تسليط الضوء على المسارات غير المباشرة لذلك التأثير، عبر وسيط الرقابة الداخلية، وفي إطار بيئة تنظيمية محددة. وتبرز هذه الإضافة أهمية التفاعل بين الأبعاد التقنية والإدارية في معالجة إشكالية جودة البيانات المالية، لا سيما في ظل التوسع المتسارع في تطبيقات التحول الرقمي الذي يشهده قطاع الأعمال المعاصر.

وعليه، فإن تبني رؤية متكاملة تربط بين تقوية منظومة الأمن السيبراني وتفعيل أدوات الرقابة الداخلية يُعد توجهاً ضرورياً لتعزيز دقة البيانات المالية وموثوقيتها، وهي مقومات أساسية لاتخاذ قرارات اقتصادية ورقابية رشيدة. كما تفتح هذه النتائج المجال أمام دراسات مستقبلية يمكن أن تتناول متغيرات وسيطة أو معدّلة إضافية، مثل ثقافة المؤسسة أو درجة نضجها الرقمي، وذلك بهدف تطوير نماذج تحليلية أكثر شمولاً لفهم العلاقة المعقدة بين الأمن السيبراني وجودة التقارير المالية في بيئات الأعمال الحديثة.

References

1- Ahn, H., & Chen, Y. (2023). Cybersecurity risk and internal control over financial reporting. *Journal of Accounting and Public Policy*, 42(1), 106960. https://doi.org/10.1016/j.jaccpubpol.2022.106960
2- Ahn, H., & Chen, Y. (2023). Cybersecurity risk and internal control over financial reporting. *Journal of Accounting and Public Policy*, 42(1), 106960. https://doi.org/10.1016/j.jaccpubpol.2022.106960
3- Ahn, H., & Chen, Y. (2023). Cybersecurity risk and internal control over financial reporting. *Journal of Accounting and Public Policy*, 42(1), 106960. https://doi.org/10.1016/j.jaccpubpol.2022.106960
4- Al-Dmour, R. H., Masa'deh, R., & Tarhini, A. (2021). The effect of cybersecurity readiness on accounting information systems effectiveness. *Information and Computer Security*, 29(4), 594–614.
5- Alghamdi, I. A., Al-Rahmi, W. M., & Alzahrani, A. I. (2022). Cybersecurity in the digital transformation era: challenges and solutions in financial data protection. *Journal of Information Security and Applications*, 66, 103162. https://doi.org/10.1016/j.jisa.2022.103162
6- Alghamdi, I. A., Al-Rahmi, W. M., & Alzahrani, A. I. (2022). Cybersecurity in the digital transformation era: challenges and solutions in financial data protection. *Journal of Information Security and Applications*, 66, 103162. https://doi.org/10.1016/j.jisa.2022.103162
7- Bedard, J. C., Hoitash, R., & Hoitash, U. (2012). Evidence on the association between internal control reporting and auditor reporting on internal control. *Accounting Review*, 87(4), 1155–1184.
8- Cao, M., Toyasaki, F., & Van Wassenhove, L. N. (2020). Managing Information Quality in the Age of Cyber Risk: A Financial Perspective. *European Journal of Operational Research*, 280(2), 499–514.
9- Chen, C., Lee, C. C., & Lin, C. (2022). Does cybersecurity risk affect internal control quality? Evidence from the U.S. banking industry. *Journal of Banking & Finance*, 141, 106662. https://doi.org/10.1016/j.jbankfin.2022.106662
10- Chen, C., Lee, C. C., & Lin, C. (2022). Does cybersecurity risk affect internal control quality? Evidence from the U.S. banking industry. *Journal of Banking & Finance*, 141, 106662. https://doi.org/10.1016/j.jbankfin.2022.106662
11- Chen, C., Lee, C. C., & Lin, C. (2022). Does cybersecurity risk affect internal control quality? Evidence from the U.S. banking industry. *Journal of Banking & Finance*, 141, 106662. https://doi.org/10.1016/j.jbankfin.2022.106662
12- COSO. (2013). *Internal Control—Integrated Framework: Executive Summary*. Committee of Sponsoring Organizations of the Treadway Commission.
13- Doyle, J., Ge, W., & McVay, S. (2022). Determinants of weaknesses in internal control over financial reporting and the implications for earnings quality. *Contemporary Accounting Research*, 39(2), 1123–1154. https://doi.org/10.1111/1911-3846.12735
14- Li, S., Zhang, Y., & Zhou, J. (2023). Cybersecurity incidents and financial reporting: The role of internal control systems. *Accounting Horizons*, 37(2), 73-93. https://doi.org/10.2308/HORIZONS-2022-0070
15- Li, S., Zhang, Y., & Zhou, J. (2023). Cybersecurity incidents and financial reporting: The role of internal control systems. *Accounting Horizons*, 37(2), 73-93. https://doi.org/10.2308/HORIZONS-2022-0070
16- Li, S., Zhang, Y., & Zhou, J. (2023). Cybersecurity incidents and financial reporting: The role of internal control systems. *Accounting Horizons*, 37(2), 73-93. https://doi.org/10.2308/HORIZONS-2022-0070
17- Nguyen, T., Ngo, L. V., Ruël, H., & Doan, T. (2021). Cybersecurity threats and internal control systems: The moderating role of digital transformation. *Journal of Business Research*, 134, 761–772.
18- Pathak, J. (2023). *Cybersecurity in Accounting and Financial Systems: Protecting Data Integrity and Confidentiality*. Springer.
19- Pathak, J. (2023). *Cybersecurity in Accounting and Financial Systems: Protecting Data Integrity and Confidentiality*. Springer.
20- Vasarhelyi, M. A., & Alles, M. G. (2019). The Impact of Artificial Intelligence on the Audit Profession. *Journal of Emerging Technologies in Accounting*, 16(1), 1–20.
21- Zhang, Y., Li, S., & Zhou, J. (2023). Internal control quality and financial reporting reliability: Evidence from cybersecurity incidents. *Journal of Accounting Research*, 61(3), 675-709. https://doi.org/10.1111/1475-679X.12466