MJHSS

Volume (41), Number (2), 2026.
ISSN: 1021-6804. On line ISSN: 3006-8665.

Mutah Journal of Humanities and Social Sciences

The Impact of Cyber Risks on Audit Fees: The Moderating Role NIST CSF

Ala' Jaber Almatarneh*

ala.matarneh@wise.edu.jo

Received: 1/1 /2026 **Accepted: 15/4 /2026**

Abstract:

This study aimed to analyze the impact of cyber risks on audit fees and to identify the moderating role of the NIST Cybersecurity Framework (NIST CSF) in this relationship. To achieve its objectives, the study adopted a descriptive-analytical approach. The study population consisted of practicing certified public accountants in Jordan, totaling 688 auditors. Primary data were collected through a questionnaire specifically designed for this purpose, and 280 electronic questionnaires were distributed to the sample members. After data collection, 240 valid questionnaires were retrieved for analysis, while 40 were excluded either due to non-response or invalid data.

The findings revealed that the NIST CSF plays a statistically significant moderating role in the relationship between cyber risks and audit fees. The sub-hypotheses confirmed a significant effect of the framework in mitigating the relationship between cyber risks and certain dimensions of audit fees. Specifically, the framework work was found to reduce the impact of cyber risks on audit efforts, task complexity, audit scope and overall audit-related risks. However, regarding the effect of the framework on the relationship between cyber risks and the use of specialized experts, the results showed no significant effect. In the light of these findings, the study recommended encouraging organizations to adopt and implement the NIST CSF as part of their governance and risk management processes, given its effective role in enhancing responsiveness to cybersecurity threats and reducing their implications for audit tasks.

Key words: Cyber Risks, Cybersecurity, Audit Fees, Certified Public Accountants, NIST CSF Framework.

* Accounting Department, Finance and Business School, World Islamic Sciences and Education University, Jordan.

المجلد(41)، العدد (2)، 2026م.
ISSN: 1021-6804. On line ISSN: 3006-8665.
MJHSS
مجلة مؤتة للدراسات الإنسانية والاجتماعية

أثر المخاطر السيبرانية في أتعاب التدقيق: الدور المعدل إطار NIST CSF

علاء جبر المطارنة*

ala.matarneh@wise.edu.jo

تاريخ الاستلام: 2026 /1/1 **تاريخ القبول: 2026/4/15**

الملخص:

هدفت هذه الدراسة إلى تحليل أثر المخاطر السيبرانية في أتعاب التدقيق، وبيان الدور المعدل لإطار الأمن السيبراني NIST CSF في هذه العلاقة. ولتحقيق أهدافها، اعتمدت الدراسة المنهج الوصفي التحليلي، حيث تمثل مجتمع الدراسة في المحاسبين القانونيين المزاولين للمهنة في الأردن والبالغ عددهم 688 محاسباً قانونياً. وقد تم جمع البيانات الأولية باستخدام استبانة صممت خصيصاً لهذا الغرض، وجرى توزيع 280 استبانة الكترونية على أفراد العينة. وبعد عملية الجمع تم استرداد 240 استبانة صالحة للتحليل بعد استبعاد 40 استبانة إما لعدم استرجاعها او لاحتوائها على بيانات غير صالحة.

أظهرت نتائج الدراسة أن إطار NIST CSF يؤدي دوراً معدلا ذا دلالة إحصائية في العلاقة بين المخاطر السيبرانية وأتعاب التدقيق، إذ أكدت الفرضيات الفرعية وجود تأثير معنوي للإطار في تخفيف العلاقة بين المخاطر السيبرانية وبعض أبعاد أتعاب التدقيق. فقد تبين أن الإطار يسهم في الحد من أثر المخاطر السيبرانية على جهود التدقيق وتعقيد مهامه وتوسع نطاقه والمخاطر الكلية المرتبطة بعمليات التدقيق. أما فيما يتعلق بتأثير الإطار في العلاقة بين المخاطر السيبرانية والاستعانة بالخبراء المختصين، فقد أظهرت النتائج عدم وجود أثر معنوي. وفي ضوء النتائج، توصي الدراسة بضرورة تشجيع المؤسسات على تبني وتطبيق إطار NIST CSF ضمن عمليات الحوكمة وإدارة المخاطر لما له من دور فاعل في رفع كفاءة الاستجابة للتهديدات السيبرانية وتقليل انعكاساتها على مهام التدقيق.

الكلمات المفتاحية: المخاطر السيبرانية، الأمن السيبراني، أتعاب التدقيق، المحاسبون القانونيون، إطار NIST CSF.

* قسم المحاسبة، كلية المال والأعمال، جامعة العلوم الإسلامية العالمية، الأردن.

DOI: https://doi.org/10.35682/y8s1me39

المقدمة:

لم يعد التعامل مع مخاطر الأمن السيبراني مسألة تقنية بحته، بل تحول إلى أولوية استراتيجية جوهرية تتطلب إشرافاً فعالاً من الإدارة العليا ومجالس الإدارة. ففي ظل التحول الرقمي المتسارع، برزت تهديدات سيبرانية متنوعة تشكل مصدر قلق بالغ الأهمية يطال المؤسسات عبر جميع القطاعات، وتؤدي غالبا إلى خسائر مالية فادحة، وتدهور في السمعة وتداعيات قانونية جسيمة. ومع تزايد الخسائر الناتجة عن الهجمات السيبرانية التي سجلت زيادة بلغت 300% منذ جائحة كورونا (Pranggono & Arabo, 2024)، أصبحت حوكمة الأمن السيبراني شرطاً لا غنى عنه لضمان المرونة المؤسسية. هذا الواقع فرض تحولاً جذرياً في نطاق عمليات التدقيق الخارجي، حيث لم يعد دور المدقق يقتصر على فحص القوائم المالية، بل توسع ليشمل تقييم مدى تأثير المخاطر السيبرانية على موثوقية التقارير المالية وفعالية الضوابط الداخلية. وتؤكد الإحصائيات هذا الارتباط، حيث أوضحت أن 28% من حالات التلاعب بالقوائم المالية تنفذ عبر الأنظمة الإلكترونية، بينما ترتبط 25% من عمليات تزوير البيانات بالمستندات الإلكترونية (Kurniawan & Mulyawan, 2023)، وتنعكس هذه التهديدات مباشرة على ملف المخاطر للشركة، ما يؤثر بدوره على نطاق التدقيق وتكلفته. ونتيجة لذلك، استجابت مهنة التدقيق برفع مستوى الأتعاب المفروضة على الشركات ذات المخاطر السيبرانية المرتفعة، وهو ما أظهرته الأدبيات والدراسات التي وجدت علاقة ارتباطية مباشرة بين ارتفاع مخاطر الأمن السيبراني وزيادة أتعاب التدقيق (Zhang & Smith, 2023). هذه الزيادة في الأتعاب تعكس تقدير المدققين للجهد الإضافي والتعقيد المتزايد وارتفاع مخاطر المهمة والحاجة المحتملة لخبراء مختصين.

لمواجهة هذا المشهد التهديدي، تستثمر العديد من المؤسسات في تبني أطر حوكمة معيارية مثل إطار المعهد الوطني للمعايير والتكنولوجيا للأمن السيبراني (National Institute of Standards and Technology – Cybersecurity Framework – NIST CSF)، الذي برز كمرجعية عالمية لإدارة المخاطر السيبرانية. ورغم أن هذه الممارسات الاستباقية تهدف إلى تعزيز المناعة الأمنية، إلا أنه لا يزال هناك فجوة جوهرية في فهم ما إذا كان هذا الالتزام يترجم إلى فوائد مالية ملموسة من منظور تكاليف التدقيق. ويؤكد (Iskandar et al., 2025) حداثة هذا التوجه، مشيرا إلى أن العلاقة بين التدقيق والأمن السيبراني تعد بعداً ناشئاً في مجال إدارة الأمن. وعليه، يبقى السؤال المحوري دون إجابة واضحة: هل يقدر المدققون الخارجيون تبني إطار NIST CSF كعامل مخفف للمخاطر، وهل ينعكس هذا التقدير فعلياً في تخفيض علاوة المخاطر المضافة إلى أتعاب التدقيق؟

بناء على ما سبق، تهدف هذه الدراسة إلى سد الفجوة البحثية من خلال تحقيق هدفين رئيسين: أولاً، بيان أثر المخاطر السيبرانية على الأبعاد المكونة لأتعاب التدقيق (جهود التدقيق وتعقيد المهمة ومخاطر التدقيق ونطاق التدقيق والاستعانة بالخبراء). ثانياً، وهو المساهمة الجوهرية، ببيان ما إذا كان تبني إطار NIST CSF يعمل كمتغير معدل بين المخاطر السيبرانية وهذه الأبعاد. ومن خلال ذلك تسعى الدراسة إلى تقديم رؤى قيمة للمؤسسات حول الجدوى المالية للاستثمار في حوكمة الأمن السيبراني، وتزويد المدققين بأساس لتقييم أثر الأطر المعيارية، وإثراء الأدبيات الأكاديمية بأدلة تجريبية من واقع الممارسة الميدانية.

الأدبيات السابقة:

المخاطر السيبرانية وتأثيرها على الأعمال:

يعد الأمن السيبراني فرعاً متخصصاً من أمن المعلومات، يركز على حماية الأنظمة الرقمية والشبكات والبنية التحتية من التهديدات الإلكترونية، ويهدف إلى ضمان سرية البيانات وسلامتها وتوافرها، إضافة إلى إدارة الحوادث الأمنية والاستجابة لها والتعافي من آثارها (Babiker, 2025; Zaghloul, 2025). تشير التهديدات السيبرانية إلى أنشطة غير قانونية وانتهاكيه مثل سرقة البيانات أو تعطيل الأنظمة، فيما تمثل المخاطر الأثر المحتمل لهذه التهديدات عند استغلال الثغرات، مقاسة بالاحتمالية وحجم التأثير (Hossain et al ., 2024). ويعد التهديد محفزاً للحوادث، بينما تعكس المخاطر حجم الضرر مثل خرق البيانات أو تعطيل الخدمات (AICPA, 2017; Karyani et al., 2023). وتعد الهجمات السيبرانية الصورة الأكثر شيوعا لتلاقي التهديدات مع المخاطر، وقد ازدادت تعقيداً مع التطور التقني (Aderinto & Faforiji, 2025).

وفي ظل التحول الرقمي نحو اقتصاد المعرفة، أصبح الأمن السيبراني تحدياً رئيساً لإدارة المخاطر، ما دفع الحكومات والهيئات الرقابية مثل Public Company Accounting Oversight Board (PCAOB) و Securities and Exchange Commission (SEC) إلى المطالبة بالإفصاح عن التهديدات الإلكترونية في التقارير المالية. كما فرضت الثورة الرقمية والحوسبة السحابية والأجهزة الذكية ضغوطاً إضافية على المؤسسات، حيث انعكس ذلك في ارتفاع وتيرة الحوادث الالكترونية وما يترتب عليها من تكاليف مالية مباشرة وغرامات تنظيمية وإضرار بالسمعة. وقد بلغ متوسط تكلفة خرق البيانات عالميا 4.88 مليون دولار في عام 2024، ووصل إلى 9.36 مليون دولار في الولايات المتحدة، فيما بلغت التكلفة في القطاع الصناعي نحو 830 ألف دولار لكل خرق (IBM, 2024) . كما ارتفعت التكلفة الإجمالية للحوادث السيبرانية من 172 مليار دولار في عام 2017 إلى 8 تريليون في عام 2021، مع توقع بلوغها 10.5 تريليون دولار بحلول عام 2025 بما يعادل 9.1% من الناتج المحلي الإجمالي العالمي (Cobos et al., 2024; Kwon et al., 2023).

يمتد الأثر الاقتصادي للهجمات إلى تقليص رأس المال الإنتاجي والإضرار بالسمعة وتقويض ثقة المستهلكين. فقد أظهرت الدراسات انخفاض رأس المال غير الملموس بنسبة 5%–9% بعد الاختراقات، وتراجع العوائد غير الطبيعية التراكمية بنسبة 1.5%–1.9% خلال 30 يوماً، وانخفاض الأسهم بمعدل 1.09% خلال الثلاثة أيام التالية للإفصاح عن الهجمات، وبنسبة 7.5% بعد خروقات البيانات بخسارة 5.40 مليار دولار من القيمة السوقية. ويعد حادث Equifax عام 2017 مثالاً بارزاً، حيث أدى إلى تسريب بيانات 145 مليون شخص وتكبد غرامات بقيمة 700 مليون دولار (Makridis, 2021; Akey et al., 2024; Kamiya et al., 2021; Kaushik, 2023; Mehmood et al., 2025). على الصعيد الوطني، أظهر تقرير المركز الوطني للأمن السيبراني في الأردن (2025) تسجيل 1297 حادثاً، شكلت البرمجيات الخبيثة 36% منها، واستغلال الحسابات 15%، وعدم الالتزام بالسياسات الأمنية 14%، ومحاولات الاختراق 9%، وهجمات الفدية 2%، وحجب الخدمة 2%، والتصيد الإلكتروني 1%، إضافة إلى خرق البيانات بنسبة 0.002%. كما استهدفت 60% من الحوادث تعطيل الأنظمة، وارتبط 22% بالتجسس السيبراني، و15% بجمع المعلومات، و3% بتحقيق مكاسب مالية. وأظهر التقرير أن 28.6% من الخدمات الشبكية الوطنية ما تزال تستخدم بروتوكولات غير آمنة، وكشف الفحوصات عن 158 ثغرة في المواقع و459 ثغرة في 16276 خادماً حكوميا، 85% منها تعود لعام 2024 فما قبل (NCSC, 2025).

لذلك، يعد الوعي المؤسسي عنصراً محورياً في مواجهة التهديدات، من خلال تدريب الموظفين واعتماد نهج متعدد الطبقات يجمع بين التدابير التقنية والتوعية المستمرة. وتشير الدراسات إلى أن 60% من العملاء المتأثرين بخروقات البيانات يتحولون إلى شركات منافسة أكثر أماناً، ما يجعل ثقافة الأمن السيبراني عاملاً حاسماً في الحفاظ على الثقة والقدرة التنافسية. كما أصبحت إدارة الأمن السيبراني ضرورة حيوية تفرض على المؤسسات اعتماد ضوابط رقابية متقدمة والاستثمار في البحث والتطوير، فيما تؤكد الحوادث مثل هجوم الفدية عام 2017 الذي استهدف 200 ألف شركة حول العالم على أهمية إدماج الأمن السيبراني في الحوكمة المؤسسية واستراتيجيات الاستدامة الرقمية (Waliullah et al., 2025; Babiker, 2025).

العلاقة بين المخاطر السيبرانية وأتعاب التدقيق:

تواجه الشركات المتضررة من الهجمات السيبرانية ضغوطاً تدفعها إلى إخفاء آثارها السلبية حفاظاً على السمعة، ما يزيد من مسؤوليات المدققين الخارجيين في كشف الإخفاقات المحتملة. هذه البيئة تعقد مهام التدقيق وتؤدي غالباً إلى ارتفاع الأتعاب، إذ يدعو المنظمون المدققين إلى تعزيز انتباههم للحوادث السيبرانية لما قد تحمله من آثار على القوائم المالية، سواء عبر اختراق الأنظمة المحاسبية أو كشف ضعف الرقابة الداخلية (Ngo & Tick, 2021). ورغم أن معايير التدقيق لا تعالج خروقات الأمن السيبراني بشكل مباشر، إلا أنها تندرج ضمن مخاطر أعمال العميل التشغيلية، وقد تؤثر على حسابات وبيانات مالية محددة. وتشير الأدبيات إلى أن أتعاب التدقيق تتأثر بثلاث قنوات رئيسة: تكاليف التحقق من سلامة القوائم، والتبعات القضائية، والخسائر غير القضائية مثل الإضرار بالسمعة. كما وجد ارتباط بين الإفصاح عن قضايا الأمن السيبراني وأتعاب التدقيق، ما يعكس إدراك المدققين لتأثير هذه الحوادث على مصداقية البيانات المالية (Calderon & Gao, 2021; Smith et al., 2017). وتتأثر عملية التدقيق بعدة عوامل مثل فعالية الرقابة الداخلية وجودة الحوكمة والمؤشرات التشغيلية، فيما يؤدي ضعف الرقابة إلى تراجع موثوقية القوائم وزيادة احتمالات التلاعب. وقد أظهرت الدراسات ارتفاعاً ملحوظاً في أتعاب التدقيق لدى الشركات المتضررة؛ إذ بينت دراسة تناولت 168 حادثة سيبرانية أن الأتعاب ارتفعت بنسبة 12%، فيما قدرت بعض الدراسات الزيادة بمتوسط 13.5% مقارنة بالشركات غير المتأثرة(Rosati et al., 2019; Xin et al., 2024) .

وتشير التوجيهات المهنية إلى أن فهم أنظمة المعلومات المحاسبية شرط أساسي لتقييم مخاطر الأخطاء الجوهرية الناتجة عن الاختراقات. فالهجمات تمثل تهديداً مزدوجاً لنزاهة البيانات وكفاءة الرقابة الداخلية، مما يفرض على المدققين توسيع نطاق إجراءاتهم. كما تتأثر الأتعاب بعوامل أخرى مثل حجم الشركة وتعقيد العمليات وجودة الأرباح والحوكمة والبيئة التنظيمية، حيث تفرض الأسواق ذات التشريعات الصارمة إجراءات إضافية تزيد الأتعاب، فيما تضيف اختراقات البيانات تكاليف قانونية وغرامات وخسائر في الإيرادات والعملاء (AICPA, 2017; Lai, 2025). أخيراً، ومع تزايد الاعتماد على الأنظمة الرقمية، أصبح من الضروري أن يأخذ المدققون في اعتبارهم مخاطر الأمن السيبراني حتى في حال عدم وقوع حوادث فعلية، لما لها من انعكاسات محتملة على الأداء المستقبلي والعلاقات مع العملاء وبيئة الرقابة الداخلية. وقد عززت لوائح هيئة الأوراق المالية والبورصات (SEC) هذه الاتجاه بإلزام الشركات المدرجة بالإفصاح عن معلومات الحوكمة وإدارة المخاطر المتعلقة بالأمن السيبراني، بما في ذلك دور مجالس الإدارة في الرقابة على هذه المخاطر (Susanto & Soepriyanto, 2024).

وفي ضوء ما تم، تمت صياغة الفرضية الرئيسة الأولى.

الفرضية الرئيسة الاولى H01: لا يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($a \leq 0.05$) للمخاطر السيبرانية على أتعاب التدقيق بأبعاده (جهود التدقيق، تعقيد مهمة التدقيق، مخاطر التدقيق، نطاق التدقيق، الخبراء المتخصصين)

وتؤكد الأدبيات البحثية على وجود محددات متعددة لكل من مخاطر التدقيق وأتعاب التدقيق. حيث تشير إلى أن أتعاب التدقيق ترتبط بعدد من العوامل من أبرزها (Rosati et al., 2019; Frino et al., 2023).

جهود التدقيق:

تشير جهود التدقيق إلى إجمالي الموارد التي يخصصها المدقق لعملية التدقيق والوصول إلى رأي فني محايد حول القوائم المالية. تقاس هذه الجهود عادة بساعات العمل التي يقضيها فريق التدقيق في مختلف مراحل العملية، بدءاً من التخطيط، مروراً بتنفيذ إجراءات التدقيق وجمع الأدلة وانتهاءً بإصدار التقرير (Fang et al., 2025; Lin et al., 2025). وتمثل جهود التدقيق عاملاً محورياً في تحديد أتعاب التدقيق، حيث تتأثر بشكل مباشر بعدم تماثل المعلومات والمخاطر الناشئة. فالشركات التي تعاني من ضعف الشفافية أو فجوات معلوماتية تتطلب موارد تدقيقية إضافية لتقليص المخاطر المرتبطة باكتشاف الأخطاء الجوهرية، مما يزيد من حجم العمل ويرفع الأتعاب (Lai, 2025; Li et al., 2020). وفي سياق متصل، أدت التطورات التكنولوجية المتسارعة وخروقات الأمن السيبراني إلى تعقيد بيئة العمل، مما يفرض على المدققين بذل جهود إضافية لمواكبة المخاطر وتقييم انعكاساتها (Gozman & Willcocks, 2019). فالتعرض للحوادث السيبرانية يدفع المدققين إلى تكثيف جهودهم، الأمر الذي يؤدي إلى زيادة ملموسة في الأتعاب، حيث أظهرت الدراسات أن الخروقات الخارجية وحدها قد تؤدي إلى رفعها بنسبة تتجاوز 8%، مما يعزز دور المدقق كآلية حوكمة خارجية تساهم في ضبط المخاطر السيبرانية (Frino et al., 2023; Smith et al., 2017).

الفرضية الفرعية الاولى($H_{01.1}$): لا يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($a \leq 0.05$) للمخاطر السيبرانية على جهود التدقيق.

تعقيد مهمة التدقيق:

يشير (Fang et al., 2025) إلى أن تعقيد مهمة التدقيق تمثل مستوى الصعوبات والتحديات الفنية التي يواجهها المدقق عند فحص القوائم المالية لشركة معينة. وينشأ التعقيد من عدة مصادر منها: تعقيد العمليات التشغيلية، تعقيد المعاملات المحاسبية، تعقيد بيئة تكنولوجيا المعلومات. وتعد أتعاب التدقيق انعكاساً مباشراً لتعقيد بيئة العميل ومستوى المخاطر المرتبطة بالمهمة، حيث تمثل تعويضاً عن الجهد والخبرة المبذولة. وتعتبر الشركات الأكبر حجماً أو ذات الهياكل التشغيلية المعقدة، مثل الشركات متعددة الفروع، أكثر تطلباً، مما يستدعي جهداً إضافياً من المدققين لفهم طبيعة عملياتها ومخاطرها الكامنة، وهو ما يترجم إلى ارتفاع واضح في الأتعاب (Lai, 2025; Yen et al., 2019). وبالمثل، يسهم التطور المتسارع في أنظمة تكنولوجيا المعلومات في زيادة التعقيد والمخاطر الكامنة، مما يدفع المدققين إلى تكريس وقت وجهد أكبر لتقييم البنية التكنولوجية والرقابية، مما يؤدي بدوره إلى زيادة الأتعاب كاستجابة طبيعية لهذا الجهد الإضافي (Marzuki & Al-Amin , 2021; Smith et al., 2017).

الفرضية الفرعية الثانية($H_{01.2}$): لا يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($a \leq 0.05$) للمخاطر السيبرانية على تعقيد مهمة التدقيق.

مخاطر التدقيق:

تعد مخاطر التدقيق محدداً جوهرياً للأتعاب، حيث تعكس احتمالية وجود تحريفات جوهرية في القوائم المالية وفشل المدقق في اكتشافها. فعندما ترتفع مخاطر العميل، سواء بسبب التدهور الاقتصادي أو التعرض للحوادث السيبرانية، يقوم المدققون بتكثيف إجراءاتهم وتخصيص موارد إضافية، مما يؤدي حتماً إلى زيادة الأتعاب (Frino et al., 2023). وتؤكد الدراسات أن شركات التدقيق تدمج مخاطر العميل المتنوعة، بما في ذلك المخاطر القانونية والتشغيلية والسيبرانية ضمن نماذج التسعير الخاصة بها (Karyani et al., 2023; Li et al., 2020). كما أن تعقيدات أمن المعلومات وضعف الرقابة الداخلية يفرضان إجراءات تقييم أعمق وأكثر شمولية، مما يدفع المدققين إلى فرض علاوات إضافية لتعويض الجهد والمخاطر الإضافية التي يتحملونها (Calderon & Gao, 2021).

الفرضية الفرعية الثالثة($H_{01.3}$): لا يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($a \leq 0.05$) للمخاطر السيبرانية على مخاطر التدقيق.

نطاق التدقيق:

يؤثر الإفصاح عن المخاطر السيبرانية بشكل مباشر على نطاق التدقيق، حيث يدفع المدققين إلى توسيع إجراءاتهم للتحقق من موثوقية التقارير المالية وكفاءة الرقابة الداخلية. فالقضايا المرتبطة بالأمن السيبراني ترفع من المخاطر الكامنة ومخاطر الرقابة، مما يفرض على المدققين تبني اختبارات أكثر شمولاً وصرامة لخفض مستوى مخاطر الاكتشاف (Calderon & Gao, 2021; Susanto & Soepriyanto, 2024). ويتأثر مدى اتساع هذه الإجراءات بخصائص مكتب التدقيق وخبرته الصناعية، بالإضافة إلى التعقيد المتزايد للأنظمة المالية الرقمية، والذي قد يضطر المدققين لتوسيع نطاق عملهم لمواجهة الممارسات المحاسبية الملتوية، حتى لو أدى ذلك إلى تأخير إصدار التقرير (Dou et al., 2019; Yen et al., 2019).

الفرضية الفرعية الرابعة($H_{01.4}$): لا يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($a \leq 0.05$) للمخاطر السيبرانية على نطاق التدقيق.

الخبراء المتخصصين:

غالباً ما يترتب على الاستعانة بخبراء من مكاتب التدقيق الكبرى (Big Four) دفع أتعاب أعلى، وذلك لما تمتلكه هذه المكاتب من سمعة وخبرة متخصصة وموارد واسعة تتيح لها تقييم المخاطر المعقدة، بما في ذلك مخاطر أمن المعلومات، بدقة أكبر مقارنة بالمكاتب الأخرى (Li et al., 2020). ويقبل العملاء دفع هذه العلاوة السعرية مقابل ضمان جودة تدقيق عالية، خاصة في ظل الحاجات إلى خبرات تقنية متقدمة للتعامل مع التهديدات السيبرانية (Smith et al., 2017). ويرتبط حجم مكتب التدقيق وخبرته إيجابياً بجودة الخدمات، مما يبرر فرض رسوم أعلى للحفاظ على السمعة وتلبية المسؤوليات القانونية الصارمة (Moreira, 2019).

الفرضية الفرعية الخامسة($H_{01.5}$): لا يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($a \leq 0.05$) للمخاطر السيبرانية على الخبراء المتخصصين.

الدور المعدل لإطار NIST CSF في العلاقة بين المخاطر السيبرانية وأتعاب التدقيق:

يعد تبني إطار المعهد الوطني للمعايير والتكنولوجيا للأمن السيبراني (NIST CSF) أداة محورية تمكن المدققين من تقييم المخاطر المرتبطة بتقنيات المعلومات لدى العملاء. فبفضل طبيعته المرنة والقائمة على النتائج، أصبح الإطار مرجعاً تأسيسياً في مجال أمن المعلومات، حيث يوفر لغة مشتركة ومنهجية شاملة لإدارة المخاطر يمكن تكييفها مع مختلف المؤسسات بغض النظر عن حجمها أو قطاعها. ويساعد الإطار الشركات على تقييم أوضاعها الأمنية وتحديد الفجوات في بنيتها التحتية أو عملياتها من خلال آليات تقييم ذاتي منظمة، كما يتيح لها قياس مستوى نضجها الأمني وتحديد أولويات الاستثمار لتحقيق أعلى عائد من الإنفاق وهو أمر تزداد أهميته في ظل تصاعد تهديدات الحوسبة الطرفية وإنترنت الأشياء (Adebola, 2025; Fadya & Utama, 2025; Kurniawan & Mulyawan, 2023; Ngalim, 2023; NIST, 2024; Reyes-Acosta et al., 2025).

ولتحقيق حماية كاملة، يركز الإطار على ست وظائف رئيسة تبدأ بالحوكمة، التي تدمج السياسات الأمنية في صميم العمليات الإدارية وتوفر أساسا للشفافية والمساءلة. تليها وظيفة التحديد التي توثق التهديدات ونقاط الضعف لدعم اتخاذ قرارات رشيدة. أما وظيفة الحماية، فتوصي بتطبيق ضوابط وقائية متكاملة تشكل أداة ملموسة للمدققين لتقييم متانة الرقابة الداخلية. وتتمثل وظيفة الكشف في المراقبة المستمرة للكشف المبكر عن التهديدات، بينما تركز وظيفة الاستجابة على آليات الإفصاح المنهجي عن الحوادث. وأخيراً، تضمن وظيفة التعافي استمرارية العمليات وترسيخ ثقافة التحسين المستمر. هذه الوظائف المتكاملة توفر مرجعية واضحة يعتمد عليها المدققون في تقييم الجاهزية والشفافية للعميل (IIA, 2025; Nelson et al., 2025; NIST, 2024).

من منظور التدقيق يكتسب الإطار أهمية خاصة عند دمج مخاطر الأمن السيبراني ضمن الملف الشامل للمخاطر المؤسسية، حيث يربط التهديدات الرقمية بالأداء المالي والسمعة، ويسهل على المدققين تقييم شمولية إدارة المخاطر وكفاية الإفصاحات، خاصة مع تزايد الالتزامات القانونية والتنظيمية بالإفصاح عن هذه المخاطر للمستثمرين. كما أن الممارسات المرتبطة بإشراف الإدارة العليا على أنشطة الاستجابة للحوادث، وربط تصنيف المخاطر بالأهداف الاستراتيجية، توفر أدلة موضوعية للمدققين تعزز من ثقتهم في بيئة الرقابة. ويوفر الإطار أيضاً دعما مباشراً للممارسات التدقيق السيبراني من خلال أدوات لتقييم الثغرات واختبارات الاختراق والتحليل الجنائي الرقمي، مع التأكيد على أهمية العنصر البشري كجزء أساسي من الضوابط الأمنية (Al-Matari et al., 2021; Nelson et al., 2025; Ngalim, 2023; Quinn et al., 2025). وفي ضوء تسارع التهديدات السيبرانية، لم يعد الأمن السيبراني مجرد أولوية تنظيمية، بل ضرورة استراتيجية لحماية الأصول الرقمية وضمان استمرارية الأعمال. وعليه، فإن تبني نهج استباقي قائم على التقييمات الدورية للمخاطر والتحديث المستمر للسياسات والضوابط الأمنية، كما يوصي إطار NIST CSF، لا يعزز فقط من مرونة الأنظمة، بل يقدم للمدققين دليلاً قوياً على وجود حوكمة سيبرانية ناضجة، مما قد يؤثر أيجاباً على تقييمهم للمخاطر، وبالتالي تعديل أتعاب التدقيق بشكل يعكس المستوى المتقدم من العناية الواجبة (Reyes-Acosta et al., 2025; Zadorozhnyi et al., 2021).

يستعرض الجدول التالي انعكاس تطبيق الإطار على مكونات المخاطر، وما يترتب على ذلك الأثر من آثار مباشرة على أتعاب التدقيق. إذ يوضح الجدول كيفية إسهام ضوابط الإطار ووظائفه في تحسين بيئة الرقابة وتقليص مستويات المخاطر، الأمر الذي ينعكس بدوره على حجم إجراءات التدقيق المطلوبة، وبالتالي على مستوى الجهد التدقيقي والأتعاب المرتبطة.

Mutah Journal of Humanities and Social Sciences, Volume (41), Number (2), 2026.
DOI: https://doi.org/10.35682/y8s1me39

الجدول (1) انعكاس تطبيق الإطار على مكونات المخاطر

المتغير	تأثير NIST CSF / الارتباط بمكونات المخاطر	الأثر على أتعاب التدقيق
جهود التدقيق	يدعم الإطار تحديد المخاطر السيبرانية بشكل منهجي من خلال التوثيق والتقييمات الدورية وجمع الأدلة، مما يمكن من الكشف المبكر ويقلل الاعتماد على ردود الفعل اللاحقة	يسهم توفر الأدلة الكافية في تقليل حجم الاختبارات المطلوبة والحاجة إلى إجراءات استثنائية او خبراء خارجيين؛ في المقابل يؤدي ضعف التنفيذ إلى الحاجة لعينات أكبر وعمليات تحقق أوسع والاستعانة بالخبراء مما يزيد الجهد والأتعاب
تعقيد عملية التدقيق	يسهم تنظيم بيئة الضوابط السيبرانية وتوحيد السياسات والإجراءات وتعزيز التوثيق والأدلة في توفير لغة مشتركة ورفع كفاءة التقييم	يسهم تقليل التعقيد في تقليص الوقت اللازم لفهم بيئة النظام او جمع الأدلة، مما يعزز كفاءة عمليات التدقيق ويقلل الجهد والأتعاب؛ في المقابل، يرتبط انخفاض مستوى النضج بزيادة التعقيد والوقت المطلوب لإنجاز التدقيق
مخاطر التدقيق	توفير أدوات لتحديد وتصنيف ومعالجة المخاطر. يشمل الحوكمة وتقييم المخاطر وإدارة الهوية؛ حيث تقلل الضوابط الفعالة من المخاطر وتحسن الإدراك المؤسسي للمخاطر	يرتبط ارتفاع نضج ضوابط الأمن السيبراني بانخفاض علاوة المخاطر في أتعاب التدقيق وتقليل الحاجة إلى اختبارات واسعة او إعادة الاختبار، مما يخفض من ساعات التدقيق والتكلفة؛ في المقابل قد يؤدي ضعف النضج إلى ارتفاع المخاطر وزيادة الأتعاب
نطاق التدقيق	يسهم الإطار في تحديد المخاطر الجوهرية ومجالات الأولوية، ويرسل إشارة موثوقة للمستثمرين والمدققين حول فعالية العمليات، مما يقلل من عدم حالات عدم اليقين	يمكن تبني الإطار من تضييق نطاق التدقيق بثقة عبر استبعاد المجالات منخفضة المخاطر، والتقليل من التوسع غير المخطط؛ في المقابل، قد يؤدي غيابه او ضعف تطبيقه إلى توسيع نطاق التدقيق وزيادة الأتعاب
الخبراء المتخصصين	تتطلب بعض وظائف الإطار مثل الكشف والاستجابة والتعافي كفاءات تقنية متخصصة. وتسهم قدرات الاستجابة الفعالة في تقليل الحوادث واحتمالية حدوث اضطرابات ومشاكل مالية	يرتبط النضج العالي بتقليل الاختبار على الخبراء وانخفاض التكلفة؛ في المقابل، يؤدي ضعف النضج او التعامل مع تقنيات معقدة إلى زيادة الاعتماد على خبراء متخصصين مما يرفع الأتعاب

وفي ضوء ما تم، تمت صياغة الفرضية الرئيسة الثانية.

الفرضية الرئيسة الثانية H02: لا يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($a \leq 0.05$) للمخاطر السيبرانية على أتعاب التدقيق بأبعاده (جهود التدقيق، تعقيد مهمة التدقيق، مخاطر التدقيق، نطاق التدقيق، الخبراء المتخصصين) بوجود إطار NIST CSF كمتغير معدل. وانبثق عن هذه الفرضية الفرضيات الفرعية التالية:

DOI: https://doi.org/10.35682/y8s1me39

الفرضية الفرعية الاولى($H_{02.1}$): لا يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($a \leq 0.05$) للمخاطر السيبرانية على جهود التدقيق بوجود إطار NIST CSF كمتغير معدل.

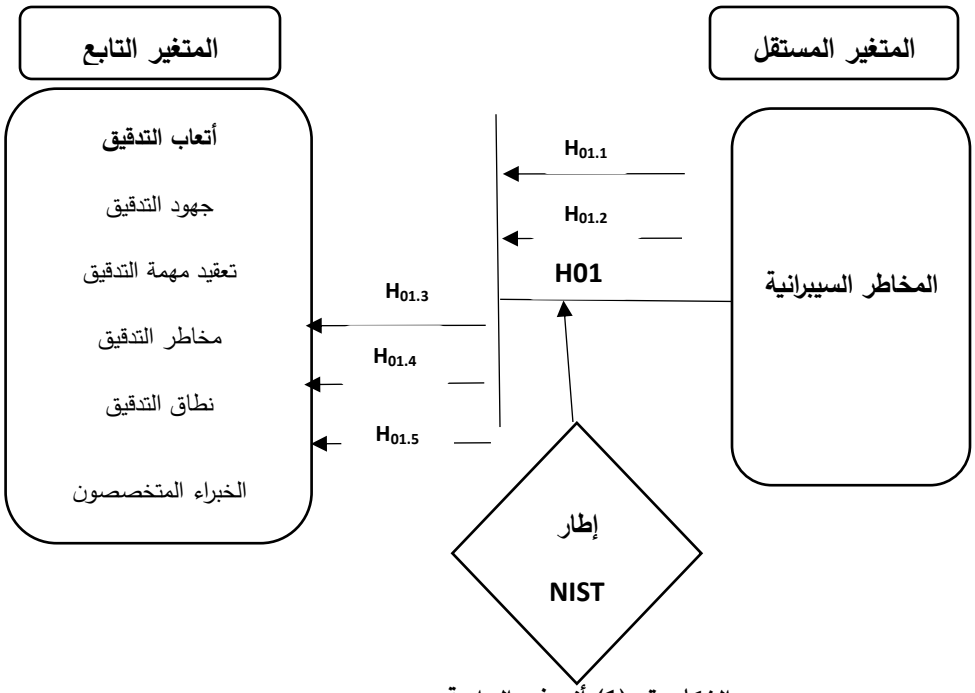
الفرضية الفرعية الثانية($H_{02.2}$): لا يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($a \leq 0.05$) للمخاطر السيبرانية على تعقيد مهمة التدقيق بوجود إطار NIST CSF كمتغير معدل.

الفرضية الفرعية الثالثة($H_{02.3}$): لا يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($a \leq 0.05$) للمخاطر السيبرانية على مخاطر التدقيق بوجود إطار NIST CSF كمتغير معدل.

الفرضية الفرعية الرابعة($H_{02.4}$): لا يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($a \leq 0.05$) للمخاطر السيبرانية على نطاق التدقيق بوجود إطار NIST CSF كمتغير معدل.

الفرضية الفرعية الخامسة($H_{02.5}$): لا يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($a \leq 0.05$) للمخاطر السيبرانية على الخبراء المتخصصين بوجود إطار NIST CSF كمتغير معدل.

استنادا إلى استعراض الأدبيات السابقة التي تناولت الإطار النظري للعلاقات بين متغيرات الدراسة، تم وضع أنموذج الدراسة الموضح في الشكل رقم (1). ويوضح الأنموذج طبيعة التأثير بين المتغير المستقل (المخاطر السيبرانية) والمتغير التابع (أتعاب التدقيق) وذلك في إطار تأثير المتغير المعدل (إطار NIST CSF).



الشكل رقم (1) أنموذج الدراسة

منهجية الدراسة:

منهج الدراسة:

لتحقيق أهداف الدراسة والإجابة عن تساؤلاتها تم الاعتماد على المنهج الوصفي التحليلي الذي يعد أحد المناهج العلمية الرائدة في دراسة الظواهر الاجتماعية والاقتصادية من خلال وصفها تحليليا وتحديد خصائصها ورصد العلاقات السببية والارتباطية بين أبعادها ومتغيراتها المختلفة. وقد تم تطبيق هذا المنهج لدراسة واقع الظاهرة محل البحث، وذلك بالاعتماد على البيانات الأولية التي تم جمعها. يعتمد المنهج الوصفي على رصد الظاهرة وتوثيقها بشكل منهجي، بينما يركز الجانب التحليلي على فحص البيانات إحصائيا واختبار الفرضيات باستخدام أدوات القياس المناسبة، مما يتيح استخلاص استنتاجات علمية دقيقة. وتكمن أهمية هذا المنهج في قدرته على تقديم تفسيرات موضوعية قائمة على الأدلة تمهيدا لصياغة توصيات عملية تسهم في معالجة إشكالية الدراسة.

مجتمع وعينة الدراسة:

تكون مجتمع الدراسة من المحاسبين القانونيين المزاولين للمهنة في المملكة الأردنية الهاشمية والذي يقدر عددهم حوالي (688). ولغايات جمع البيانات، قام الباحث بتوزيع (280) استبانة إلكترونية. وبعد استبعاد (40) استبانة إما لم يتم إرجاعها أو كانت تحتوي على نتائج غير صالحة فقد بلغ عدد الاستبانات الخاضعة للتحليل 240 استبانة وبنسبة (85.7%) من إجمالي العدد الموزع، وهي نسبة تعتبر مرتفعة ومقبولة في الدراسات العلمية. وجدير بالذكر أن هذه النسبة المرتفعة من الاستجابة من مصداقية البيانات وتمثيلها لمجتمع الدراسة، كما تحافظ في تقليل هامش الخطأ في النتائج. وقد تم التحقق من صلاحية جميع الاستبانات المستردة قبل إدخالها للتحليل الإحصائي.

مصادر جمع البيانات:

تهدف الدراسة إلى جمع بياناتها على مصدرين رئيسين: المصادر الثانوية والمصادر الأولية. تتمثل المصادر الثانوية في الأدبيات العلمية من كتب ورسائل جامعية ودوريات محكمة باللغتين العربية والإنجليزية، والتي ساهمت في بناء إطار نظري وتصميم أداة الدراسة. أما المصادر الأولية فتمثلت في الاستبانة، التي تم تطويرها بناءً على مراجعة الأدبيات السابقة واختبارها من قبل خبراء، بهدف قياس اتجاهات عينة الدراسة تجاه متغيرات الدراسة. وقد يسمح هذا التكامل بين المصادر النظرية والميدانية من تحقيق شمولية النتائج وموثوقيتها، حيث توفر المصادر الثانوية الأساس المعرفي بينما توفر المصادر الأولية البيانات الميدانية اللازمة لاختبار فرضيات الدراسة.

أداة الدراسة:

لتحقيق أهداف الدراسة والإجابة عن تساؤلاتها البحثية، قام الباحث بتصميم استبانة لجمع البيانات الأولية من العينة المستهدفة. وقد اعتمد في بناء الأداة على مراجعة شاملة للأدبيات والدراسات السابقة ذات الصلة، ثم تحليل نقدي لمتغيرات الدراسة وأبعادها النظرية، مع أخذ بآراء لجنة من الخبراء والمتخصصين لضمان الصدق الظاهري والمحتوى. وقد روعي في صياغة بنود الاستبانة الدقة العلمية والوضوح اللغوي، مع مراعاة الخصائص المهنية للمستجيبين. وقد تم التحقق من صلاحية أداة الدراسة لقياس متغيرات الدراسة من خلال اختبار صدقها وثباتها، وذلك على النحو الآتي: يهدف اختبار الثبات إلى التحقق من موثوقية أداة الدراسة واتساقها الداخلي، حيث يقيس مدى انسجام قراءات المبحوثين عبر فقرات الأداة المختلفة ودرجة استقرارها الزمني. وقد اعتمدت

DOI: https://doi.org/10.35682/y8s1me39

الدراسة معامل Cronbach's Alpha كمؤشر رئيس للثبات، إذ يعتبر هذا المعامل من أكثر المقاييس استخدامًا في البحوث الاجتماعية لقياس الاتساق. ويشير هذا الاختبار إلى أن أداة الدراسة تتمتع بثبات مقبول عند قيمة ألفا أكبر أو تساوي (0.70)، كما أن اقتراب قيمة ألفا من (100%) يدل على درجات ثبات أعلى لأداة الدراسة(Sekaran & Bougie, 2016) . والجدول الآتي يبين نتائج اختبار ثبات أداة الدراسة، وذلك كما يأتي:

والجدول الآتي يبين توزيع فقرات أداة الدراسة على الأبعاد والمتغيرات ونتائج اختبار ثبات أداة الدراسة، وكما يأتي:

الجدول (2): توزيع فقرات أداة الدراسة على الأبعاد والمتغيرات ونتائج اختبار ثبات أداة الدراسة

المتغيرات	الأبعاد	عدد الاسئلة	قيمة ألفا
المتغير المستقل	المخاطر السيبرانية	10	0.810
المتغير التابع	جهود التدقيق	6	0.790
	تعقيد مهمة التدقيق	6	0.779
	مخاطر التدقيق	6	0.852
	نطاق التدقيق	6	0.782
	الخبراء المختصون	6	0.876
المتغير المعدل	إطار NIST CSF	10	0.741
الأداة ككل			0.958

تؤكد نتائج اختبار الثبات المتمثلة في قيم معامل Cronbach's Alpha التي تتراوح بين (0.741 – 0.876) لمحاور الأداة، وبلغت (0.958) للأداة ككل، تمتع أداة الدراسة بدرجة عالية من الموثوقية تتجاوز الحد الأدنى المقبول (0.70). هذه النتائج تدل على تماسك البناء الداخلي للأداة واتساقها، حيث يتضح انسجاماً واضحاً بين فقراتها وثباتاً في الاستجابات، مما يضمن إمكانية على مقياس متغيرات الدراسة بدقة عالية وموثوقية تامة.

ملاءمة نموذج الدراسة للأساليب الإحصائية المستخدمة:

اختبار الارتباط الخطي المتعدد Multicollinearity:

لضمان موثوقية نتائج الانحدار، تم فحص مشكلة التعدد الخطي التي تؤثر سلبا على استقرار تقديرات النموذج وصعوبة تفسيرها (Sekaran & Bougie, 2016). وباستخدام معامل ارتباط بيرسون كأداة كشف أولية، تبين أن جميع الارتباطات بين المتغيرات المستقلة لم تتجاوز الحد المقبول (0.80)، مما يعد مؤشراً ايجابياً على سلامة البيانات من مشكلات الارتباط الخطي.

الجدول (3): نتائج اختبار مشكلة الارتباط الخطي المتعدد بين أبعاد المتغير المستقل والمتغير المعدل باستخدام معامل الارتباط بيرسون

المتغيرات	المخاطر السيبرانية	إطار NIST CSF	متغير التفاعل (المخاطر السيبرانية * إطار NIST CSF)
المخاطر السيبرانية	1		
إطار NIST CSF	0.675	1	
متغير التفاعل (المخاطر السيبرانية * إطار NIST CSF)	0.667	0.694	1

يتضح مـن الجدول (3) أن قيمـة معـامل ارتباط بيرسون بيـن أبعاد المتغير المستقل والمتغير المعدل تراوحت ما بين (0.667 – 0.694)، وبما أن هذه القيم أقل من الحد الأعلى المسموح به (0.80)، فإن ذلك يدعم سلامة البيانات من مشكلة الارتباط الخطي المتعدد.

ولتأكيد النتيجة الأولية التي أظهرها معامل الارتباط، تم فحص معامل تضخم التباين Variance Inflation Factor (VIF) ومعامل التباين المسموح به (Tolerance). حيث يشير Sekaran & Bougie (2016) إلى أن النموذج يخلو من مشكلة التعدد الخطي أذا كانت قيم عامل تضخم التباين Variance Inflation Factor (VIF) أقل من (10)، وبالتالي قيم ومعامل التباين المسموح به (Tolerance) ما بين (0.1 – 1.0). وفيما يلي نتائج اختبار مشكلة الارتباط الخطي المتعدد

الجدول (4): نتائج اختبار مشكلة الارتباط الخطي المتعدد بين أبعاد المتغير المستقل والمتغير المعدل باستخدام معامل تضخم التباين ومعامل التحمل (التباين المسموح به)

المتغيرات	VIF	Tolerance
المخاطر السيبرانية	3.15	0.320
إطار NIST CSF	3.42	0.290
متغير التفاعل (المخاطر السيبرانية * إطار NIST CSF)	3.28	0.310

يتضح من الجدول (4) أن قيمة معامل تضخم التباين (VIF) تراوحت ما بين (3.42 – 3.15) وهي محصورة بين (1.0 – 10.0)، وتراوحت قيم معامل التباين المسموح به (Tolerance) ما بين (0.290 – 0.320) وهي محصورة بين (0.1 – 1.0)، فإن ذلك يؤكد عدم وجود مشكلة الارتباط الخطي المتعدد.

نتائج اختبار فرضيات الدراسة:

يعرض هذا الجزء من الدراسة نتائج اختبار الفرضيات، التي تم التوصل إليها من خلال تطبيق أساليب الإحصاء الاستدلالي الخاصة باختبار الفرضيات. وتهدف هذه الفرضيات إلى التعرف على أثر المخاطر السيبرانية في أتعاب التدقيق بوجود إطار NIST CSF كمتغير معدل. وفيما يأتي نتائج اختبار فرضيات الدراسة.

DOI: https://doi.org/10.35682/y8s1me39

اختبار فرضيات الدراسة:

اشتملت الدراسة على فرضيتين رئيستين، بحثتا في أثر المخاطر السيبرانية في أتعاب التدقيق بوجود إطار NIST CSF كمتغير معدل، وقد تم التحقق من صحة هذه الفرضيات باستخدام تحليل الانحدار الخطي البسيط، وتحليل الانحدار المتعدد، وظهرت النتائج كما يأتي:

نتائج اختبار الفرضية الرئيسة الأولى:

بحثت الفرضية الرئيسة الأولى في أثر المخاطر السيبرانية في أتعاب التدقيق. حيث نصت هذه الفرضية على أنه: "لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) للمخاطر السيبرانية في أتعاب التدقيق بأبعادها (جهود التدقيق، تعقيد مهمة التدقيق، مخاطر التدقيق، نطاق التدقيق، الخبراء المختصين)". وقد ظهرت نتائج اختبارها كما يأتي:

نتائج اختبار الفرضية الفرعية الأولى:

الجدول (5) نتائج تحليل الانحدار الخطي البسيط لأثر المخاطر السيبرانية في جهود التدقيق

المتغير التابع	ملخص النموذج			تحليل التباين ANOVA			
	(R) معامل الارتباط	(R^2) معامل التحديد	(R^2) Adjusted معامل التحديد المعدل	الخطأ المعياري للنموذج	(DF) درجات الحرية	F قيمة المحسوبة	(Sig F*) مستوى الدلالة
جهود التدقيق	0.879	0.772	0.771	0.14152	1	109.102	0.000

* التأثير دال إحصائيا عند مستوى الدلالة ($\alpha \leq 0.05$)

يبين الجدول (5) نتائج اختبار القدرة التفسيرية للنموذج، حيث يتضح وجود علاقة ارتباط موجبة بين كل من المخاطر السيبرانية وأتعاب التدقيق، إذ بلغت قيمة معامل الارتباط ($R=0.879$)، وبلغت قيمة معامل التحديد ($R^2=0.772$)، مما يعني أن متغير المخاطر السيبرانية فسر ما نسبته (77.10%) من التغير الحاصل في جهود التدقيق، مع ثبات العوامل الأخرى. كما يتبين من الجدول وجود الأثر المعنوي للمخاطر السيبرانية في جهود التدقيق، حيث بلغت قيمة F المحسوبة (109.102) وبمستوى الدلالة ($SigF=0.000$) وهي أقل من 0.05.

وبناءً على ذلك فإنه يتم رفض الفرضية العدمية الفرعية الأولى، وقبول الفرضية البديلة، التي تنص على أنه: "يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) للمخاطر السيبرانية في جهود التدقيق".

DOI: https://doi.org/10.35682/y8s1me39

نتائج اختبار الفرضية الفرعية الثانية:

الجدول (6) نتائج تحليل الانحدار الخطي البسيط لأثر المخاطر السيبرانية في تعقيد مهمة التدقيق

المتغير التابع	ملخص النموذج			تحليل التباين ANOVA			
	(R) معامل الارتباط	(R^2) معامل التحديد	(R^2) Adjusted معامل التحديد المعدل	الخطأ المعياري للنموذج	(DF) درجات الحرية	قيمة F المحسوبة	(Sig F*) مستوى الدلالة
تعقيد مهمة التدقيق	0.864	0.747	0.746	0.15094	1	90.820	0.000

* التأثير دال إحصائيا عند مستوى الدلالة ($\alpha \leq 0.05$)

يبين الجدول (6) نتائج اختبار القدرة التفسيرية للنموذج، حيث يتضح وجود علاقة ارتباط موجبة بين كل من المخاطر السيبرانية وتعقيد مهمة التدقيق، إذ بلغت قيمة معامل الارتباط (R=0.864)، وبلغت قيمة معامل التحديد (R^2=0.747)، مما يعني أن متغير المخاطر السيبرانية فسر ما نسبته (74.70%) من التغير الحاصل في جهود التدقيق، مع ثبات العوامل الأخرى. كما يتبين من الجدول وجود الأثر المعنوي للمخاطر السيبرانية في جهود التدقيق، حيث بلغت قيمة F المحسوبة (90.820) وبمستوى الدلالة (SigF=0.000) وهي أقل من 0.05.

وبناءً على ذلك فإنه يتم رفض الفرضية العدمية الفرعية الأولى، وقبول الفرضية البديلة، التي تنص على أنه: "يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) للمخاطر السيبرانية في تعقيد مهمة التدقيق".

نتائج اختبار الفرضية الفرعية الثالثة:

الجدول (7) نتائج تحليل الانحدار الخطي البسيط لأثر المخاطر السيبرانية في مخاطر التدقيق

المتغير التابع	ملخص النموذج			تحليل التباين ANOVA			
	(R) معامل الارتباط	(R^2) معامل التحديد	(R^2) Adjusted معامل التحديد المعدل	الخطأ المعياري للنموذج	(DF) درجات الحرية	قيمة F المحسوبة	(Sig F*) مستوى الدلالة
مخاطر التدقيق	0.947	0.896	0.896	0.07819	1	124.320	0.000

* التأثير دال إحصائيا عند مستوى الدلالة ($\alpha \leq 0.05$)

DOI: https://doi.org/10.35682/y8s1me39

يبين الجدول (7) نتائج اختبار القدرة التفسيرية للنموذج، حيث يتضح وجود علاقة ارتباط موجبة بين كل من المخاطر السيبرانية وتعقيد مخاطر التدقيق، إذ بلغت قيمة معامل الارتباط (R=0.947)، وبلغت قيمة معامل التحديد (R^2=0.896)، مما يعني أن متغير المخاطر السيبرانية فسر ما نسبته (89.60%) من التغير الحاصل في مخاطر التدقيق، مع ثبات العوامل الأخرى. كما يتبين من الجدول وجود الأثر المعنوي للمخاطر السيبرانية في جهود التدقيق، حيث بلغت قيمة F المحسوبة (124.320) وبمستوى الدلالة (SigF=0.000) وهي أقل من 0.05.

وبناءً على ذلك فإنه يتم رفض الفرضية العدمية الفرعية الأولى، وقبول الفرضية البديلة، التي تنص على أنه: "يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) للمخاطر السيبرانية في مخاطر التدقيق".

نتائج اختبار الفرضية الفرعية الرابعة:

الجدول (8) نتائج تحليل الانحدار الخطي البسيط لأثر المخاطر السيبرانية في نطاق التدقيق

	ملخص النموذج			تحليل التباين ANOVA			
المتغير التابع	(R) معامل الارتباط	(R^2) معامل التحديد	(R^2) Adjusted معامل التحديد المعدل	الخطأ المعياري للنموذج	(DF) درجات الحرية	قيمة F المحسوبة	(Sig F*) مستوى الدلالة
نطاق التدقيق	0.829	0.688	0.687	0.17181	1	102.520	0.000

* التأثير دال إحصائيا عند مستوى الدلالة ($\alpha \leq 0.05$)

يبين الجدول (8) نتائج اختبار القدرة التفسيرية للنموذج، حيث يتضح وجود علاقة ارتباط موجبة بين كل من المخاطر السيبرانية وتعقيد مهمة التدقيق، إذ بلغت قيمة معامل الارتباط (R=0.829)، وبلغت قيمة معامل التحديد (R^2=0.688)، مما يعني أن متغير المخاطر السيبرانية فسر ما نسبته (68.80%) من التغير الحاصل في جهود التدقيق، مع ثبات العوامل الأخرى. كما يتبين من الجدول وجود الأثر المعنوي للمخاطر السيبرانية في جهود التدقيق، حيث بلغت قيمة F المحسوبة (102.520) وبمستوى الدلالة (SigF=0.000) وهي أقل من 0.05.

وبناءً على ذلك فإنه يتم رفض الفرضية العدمية الفرعية الأولى، وقبول الفرضية البديلة، التي تنص على أنه: "يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) للمخاطر السيبرانية في نطاق التدقيق".

DOI: https://doi.org/10.35682/y8s1me39

نتائج اختبار الفرضية الفرعية الخامسة:

الجدول (9) نتائج تحليل الانحدار الخطي البسيط لأثر المخاطر السيبرانية في الخبراء المتخصصين

	ملخص النموذج				تحليل التباين ANOVA		
المتغير التابع	(R) معامل الارتباط	(R^2) معامل التحديد	(R^2) Adjusted معامل التحديد المعدل	الخطأ المعياري للنموذج	(DF) درجات الحرية	قيمة F المحسوبة	(Sig F*) مستوى الدلالة
نطاق التدقيق	0.771	0.595	0.593	0.17965	1	82.350	0.000

* التأثير دال إحصائيا عند مستوى الدلالة ($\alpha \leq 0.05$)

يبين الجدول (9) نتائج اختبار القدرة التفسيرية للنموذج، حيث يتضح وجود علاقة ارتباط موجبة بين كل من المخاطر السيبرانية والخبراء المختصين، إذ بلغت قيمة معامل الارتباط (R=0.771)، وبلغت قيمة معامل التحديد (R^2=0.595)، مما يعني أن متغير المخاطر السيبرانية فسر ما نسبته (59.50%) من التغير الحاصل في جهود التدقيق، مع ثبات العوامل الأخرى. كما يتبين من الجدول وجود الأثر المعنوي للمخاطر السيبرانية في جهود التدقيق، حيث بلغت قيمة F المحسوبة (82.350) وبمستوى الدلالة (SigF=0.000) وهي أقل من 0.05.

وبناءً على ذلك فإنه يتم رفض الفرضية العدمية الفرعية الأولى، وقبول الفرضية البديلة، التي تنص على أنه: "يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) للمخاطر السيبرانية في الخبراء المختصين".

نتائج اختبار الفرضية الرئيسة الثانية:

بحثت الفرضية الرئيسة الثانية في أثر المخاطر السيبرانية في أتعاب التدقيق بأبعادها (جهود التدقيق، تعقيد مهمة التدقيق، مخاطر التدقيق، نطاق التدقيق، الخبراء المختصين) بوجود إطار NIST CSF كمتغير معدل. حيث نصت هذه الفرضية على أنه: "لا يوجد أثر للمخاطر السيبرانية في أتعاب التدقيق بأبعادها (جهود التدقيق، تعقيد مهمة التدقيق، مخاطر التدقيق، نطاق التدقيق، الخبراء المختصين) بوجود إطار NIST CSF كمتغير معدل. وقد ظهرت نتائج اختبارها كما يأتي:

DOI: https://doi.org/10.35682/y8s1me39

نتائج اختبار الفرضية الفرعية الأولى:

الجدول (10) نتائج تحليل الانحدار الخطي المتعدد لأثر المخاطر السيبرانية في جهود التدقيق بوجود إطار NIST CSF كمتغير معدل

	المتغير المستقل	النموذج الأول			النموذج الثاني			النموذج الثالث		
		B	value t	Sig t*	B	value t	Sig t*	B	value t	Sig t*
	المخاطر السيبرانية	1.034	28.421	0.000	1.109	10.639	0.000	3.730	6.184	0.000
المتغير التابع	إطار NIST CSF				-0.087	-0.769	0.443	2.431	4.179	0.000
	المخاطر السيبرانية * NIST CSF							-0.589	-4.407	0.000
	R^2		0.772		0.773			0.790		
جهود التدقيق	ΔR^2		0.772		0.001			0.017		
	ΔF		109.102		0.592			19.423		
	Sig ΔF		0.000		0.443			0.000		

أظهرت نتائج تحليل الانحدار المتعدد لاختبار الفرضية الفرعية الأولى أن المخاطر السيبرانية تؤثر تأثيرا إيجابيا ومعنويا في جهود التدقيق، حيث بلغت قيمة معامل الانحدار (B=3.730) عند مستوى دلالة (Sig=0.000)، مما يشير إلى أن ارتفاع مستوى المخاطر السيبرانية يؤدي إلى زيادة الجهود التي يبذلها المدققون أثناء تنفيذ مهام التدقيق، وذلك نتيجة الحاجة إلى فحص أعمق لإجراءات من المعلومات وتقييم الضوابط ذات العلاقة بالأنظمة الرقمية. كما أظهرت النتائج أن إطار NIST CSF له تأثير إيجابي ومعنوي على جهود التدقيق حيث بلغت قيمة معامل الانحدار (B=2.431) عند مستوى دلالة (Sig=0.000)، بما يدل على أن تطبيق هذا الإطار يسهم في تحسين جودة العمليات الرقابية وتوسيع نطاق الفحص، الأمر الذي يتطلب من المدققين بذل جهود أكبر في تقييم مدى التزام المؤسسة بمكونات الإطار. أما بالنسبة لمتغير التفاعل (المخاطر السيبرانية * إطار NIST CSF)، فقد كانت قيمة معامل الانحدار سالبة (B=-0.589) وبمستوى دلالة (Sig=0.000)، مما يشير إلى أن الإطار يخفف من الأثر الإيجابي للمخاطر السيبرانية على جهود التدقيق. أي أن تطبيق الإطار يسهم في تقليل حجم الجهود الإضافية المطلوبة من المدققين عند ارتفاع مستوى المخاطر السيبرانية وذلك من خلال تحسين إدارة تلك المخاطر ووضوح المعايير الرقابية المرتبطة بها. كما أوضحت النتائج أن قيمة معامل التحديد (R^2=0.790) أي أن النموذج يفسر ما نسبته 79 % من التغير في جهود التدقيق. كما أن قيمة (Sig F= 0.000) تؤكد معنوية النموذج ككل وملاءمته الإحصائية. وبذلك يمكن القول إن الإطار يؤدي دورا وقائيا وتنظيميا يسهم في تخفيف أثر المخاطر السيبرانية على بيئة التدقيق من خلال تعزيز الضوابط التقنية والحوكمة الأمنية، مما يحد من الحاجة إلى زيادة غير مبررة في جهود المدققين عند مواجهة مستويات مرتفعة من المخاطر.

DOI: https://doi.org/10.35682/y8s1me39

وبناءً على ذلك فإنه يتم رفض الفرضية العدمية الفرعية الأولى، وقبول الفرضية البديلة، التي تنص على أنه: " يوجد أثر للمخاطر السيبرانية في جهود التدقيق بوجود إطار NIST CSF كمتغير معدل ".

نتائج اختبار الفرضية الفرعية الثانية:

الجدول (11) نتائج تحليل الانحدار الخطي المتعدد لأثر المخاطر السيبرانية في تعقيد مهمة التدقيق بوجود إطار NIST CSF كمتغير معدل

	المتغير المستقل	النموذج الأول			النموذج الثاني			النموذج الثالث		
		B	valu e t	Sig t*	B	valu e t	Sig t*	B	valu e t	Sig t*
المتغير التابع	المخاطر السيبرانية	1.029	26.52 0	0.000	0.62 7	5.821	0.00 0	2.430	3.809	0.00 0
	إطار NIST CSF				0.46 6	3.977	0.00 0	2.197	3.572	0.00 0
تعقيد مهمة التدقيق	المخاطر السيبرانية * NIST CSF							– 0.405	- 2.866	0.00 5
	R^2	0.747			0.763			0.771		
	ΔR^2	0.747			0.016			0.008		
	ΔF	90.280			15.813			8.215		
	Sig ΔF	0.000			0.000			0.005		

أظهرت نتائج تحليل الانحدار المتعدد لاختبار الفرضية الفرعية الثانية أن المخاطر السيبرانية تؤثر تأثيرا إيجابيا ومعنويا في مهمة التدقيق، حيث بلغت قيمة معامل الانحدار (B=2.430) عند مستوى دلالة (Sig=0.000)، مما يشير إلى أن ارتفاع مستوى المخاطر السيبرانية يؤدي إلى زيادة درجة تعقيد مهمة التدقيق. ويعزى ذلك إلى أن التهديدات التقنية المتزايدة تتطلب من المدققين فهماً أعمق للأنظمة الالكترونية، بالإضافة إلى مهارات فنية متقدمة لتقييم الضوابط الأمنية وتحليل البيانات الرقمية، مما يزيد من صعوبة إجراءات التدقيق وتعقيدها الفني والإجرائي. كما أظهرت النتائج أن الإطار له تأثير إيجابي ومعنوي على تعقيد مهمة التدقيق، فقد كانت قيمة معامل معامل الانحدار (B=2.197) عند مستوى دلالة (Sig=0.000)، وهو ما يشير إلى أن تطبيق الإطار يزيد من مستوى التعقيد الذي يواجهه المدققون أثناء أداء مهامهم، نتيجة الحاجة إلى التحقق من مدى توافق ممارسات المؤسسة مع مكونات الإطار ومتطلباته التفصيلية، وهو ما يستدعي معرفة متخصصة وإجراءات تدقيق أكثر اتساعا وعمقا. أما بالنسبة لمتغير التفاعل (المخاطر السيبرانية * إطار NIST CSF)، فقد كانت قيمة معامل الانحدار سالبة (B=- 0.405) وبمستوى دلالة (Sig=0.005)، مما يشير إلى أن الإطار يؤدي دورا معدلا يخفف من الأثر الإيجابي للمخاطر السيبرانية على تعقيد مهمة التدقيق. أي أن وجود الإطار يسهم في تقليل حدة التعقيد الناتجة عن ارتفاع مستوى المخاطر

DOI: https://doi.org/10.35682/y8s1me39

السيبرانية، وذلك من خلال توفير إطار منظم لإدارة تلك المخاطر وتوضيح الأدوار والإجراءات الأمنية التي يمكن أن يستند إليها المدقق عن تقييم بيئة تكنولوجيا المعلومات. كما أوضحت النتائج أن قيمة معامل التحديد (R^2=0.771) أي أن النموذج يفسر ما نسبته 77.10% من التغير في تعقيد مهمة التدقيق. كما أن قيمة (Sig F= 0.005) تؤكد معنوية النموذج ككل وملاءمته الإحصائية. وبذلك يمكن القول إن الإطار يؤدي دورا معدلا سلبيا يسهم في الحد من تأثير المخاطر السيبرانية على تعقيد مهمة التدقيق، من خلال تعزيز تنظيم عمليات الأمن السيبراني وتوضيح متطلبات الامتثال مما يسهل على المدققين فهم بيئة الأنظمة وتقييمها بطريقة أكثر كفاءة ووضوحا.

وبناءً على ذلك فإنه يتم رفض الفرضية العدمية الفرعية الثانية، وقبول الفرضية البديلة، التي تنص على أنه: " يوجد أثر للمخاطر السيبرانية في تعقيد مهمة التدقيق بوجود إطار NIST CSF كمتغير معدل ".

نتائج اختبار الفرضية الفرعية الثالثة:

الجدول (12) نتائج تحليل الانحدار الخطي المتعدد لأثر المخاطر السيبرانية في مخاطر التدقيق بوجود إطار NIST CSF كمتغير معدل

	المتغير المستقل	النموذج الأول			النموذج الثاني			النموذج الثالث		
		B	value t	Sig t*	B	value t	Sig t*	B	value t	Sig t*
المتغير التابع	المخاطر السيبرانية	0.912	45.394	0.000	0.881	15.297	0.000	-0.088	-0.258	0.797
	إطار NIST CSF				0.036	0.572	0.568	-0.895	-2.722	0.007
	المخاطر السيبرانية * NIST CSF							0.218	2.882	0.004
مخاطر التدقيق	R^2	0.896			0.897			0.900		
	ΔR^2	0.896			0.000			0.004		
	ΔF	124.320			0.327			8.306		
	Sig ΔF	0.000			0.001			0.004		

DOI: https://doi.org/10.35682/y8s1me39

أظهرت نتائج تحليل الانحدار المتعدد لاختبار الفرضية الفرعية الثالثة أن المخاطر السيبرانية ليس لها تأثير مباشر ومعنوي على مخاطر التدقيق، حيث بلغت قيمة معامل الانحدار (B=-0.088) عند مستوى دلالة (Sig=0.797)، ويشير ذلك إلى أن تأثير المخاطر السيبرانية لا ينعكس بشكل مباشر على مخاطر التدقيق، بل يتأثر بعوامل أخرى ضمن النموذج وهو ما يوضحه متغير التفاعل.

كما أظهرت النتائج أن الإطار له تأثير سالب ومعنوي على مخاطر التدقيق، فقد كانت قيمة معامل معامل الانحدار (B=-0.895) عند مستوى دلالة (Sig=0.007)، ويعزى ذلك إلى أن تطبيق الإطار بحد ذاته يفرض هيكلية وضوابط موثقة، مما يعزز بيئة الرقابة الداخلية بشكل عام. هذا التحسين في الحوكمة والتوثيق يقلل من حالة عدم اليقين لدى المدقق ويخفض تقديره المبدئي للمخاطر، حتى قبل النظر في التهديدات السيبرانية محددة. أما بالنسبة لمتغير التفاعل (المخاطر السيبرانية * إطار NIST CSF)، فقد كانت قيمة معامل الانحدار موجبة (B=0.218) وبمستوى دلالة (Sig=0.004)، مما يشير إلى أن الإطار يؤدي دوراً معدلاً يقوي العلاقة الإيجابية بين المخاطر السيبرانية ومخاطر التدقيق. ويمكن تفسير ذلك بأن الإطار يزيد من شفافية المخاطر ويجعلها قابلة للقياس، مما يرفع من حساسية المدققين تجاهها. فكلما زادت المخاطر السيبرانية المكتشفة ضمن إطار واضح، تطلب ذلك من المدقق توسيع نطاق الفحص بشكل أكبر، والتحقق من سلامة الأنظمة الالكترونية وضوابط أمن المعلومات بعمق أكبر، مما يضمن شمولية التقييم لجميع الجوانب المتأثرة. بعبارة أخرى، الإطار يحول المخاطر من مفهوم غامض إلى بنود فحص واضحة، مما يجعل المدققين يرفعون تقديراتهم للمخاطر بشكل مباشر وقوي استجابة لأي ضعف موثق.

كما أوضحت النتائج أن قيمة معامل التحديد (R^2=0.900) أي أن النموذج يفسر ما نسبته 90 % من التغير في مخاطر التدقيق. كما أن قيمة (Sig F= 0.004) تؤكد معنوية النموذج ككل وملاءمته الإحصائية. وبذلك يمكن القول إن الإطار لا يقلل من تأثير المخاطر السيبرانية على مخاطر التدقيق، بل على العكس يجعله أكثر وضوحاً للمدققين. هذا الوضوح يؤدي إلى تقييم أكثر دقة وحساسية للمخاطر، حيث يرفع المدققون تقديراتهم لمخاطر التدقيق بشكل مبرر عند وجود مخاطر سيبرانية عالية في ظل تطبيق الإطار. وبالتالي، يعد الإطار أداة حوكمة تعزز جودة التدقيق من خلال تحسين قدرة المدققين على اكتشاف المخاطر وتقييمها مهنياً.

وبناءً على ذلك فإنه يتم رفض الفرضية العدمية الفرعية الثالثة، وقبول الفرضية البديلة، التي تنص على أنه: " يوجد أثر للمخاطر السيبرانية في مخاطر التدقيق بوجود إطار NIST CSF كمتغير معدل ".

DOI: https://doi.org/10.35682/y8s1me39

نتائج اختبار الفرضية الفرعية الرابعة:

الجدول (13) نتائج تحليل الانحدار الخطي المتعدد لأثر المخاطر السيبرانية في نطاق التدقيق بوجود إطار NIST CSF كمتغير معدل

المتغير التابع	المتغير المستقل	النموذج الأول			النموذج الثاني			النموذج الثالث		
		B	value t	Sig t*	B	value t	Sig t*	B	value t	Sig t*
نطاق التدقيق	المخاطر السيبرانية	1.011	22.910	0.000	0.829	6.576	0.000	3.682	5.009	0.000
	إطار NIST CSF				0.212	1.547	0.123	2.953	4.165	0.000
	المخاطر السيبرانية * NIST CSF							-0.641	-3.936	0.000
	R^2	0.688			0.691			0.710		
	ΔR^2	0.688			0.003			0.019		
	ΔF	102.520			2.393			15.494		
	Sig ΔF	0.000			0.123			0.000		

أظهرت نتائج تحليل الانحدار المتعدد لاختبار الفرضية الفرعية الرابعة أن المخاطر السيبرانية تؤثر تأثيرا إيجابيا ومعنويا في نطاق التدقيق، حيث بلغت قيمة معامل الانحدار (B=3.682) عند مستوى دلالة (Sig=0.000)، مما يشير إلى أن ارتفاع مستوى المخاطر السيبرانية يؤدي إلى توسع نطاق التدقيق الذي يقوم به المدققون. ويعزى ذلك إلى أن زيادة التهديدات والهجمات التقنية تتطلب تغطية أوسع لإجراءات الفحص، والتحقق من سلامة الأنظمة الالكترونية وضوابط امن المعلومات بما يضمن شمولية التقييم لجميع الجوانب المتأثرة بالمخاطر التقنية.

كما أظهرت النتائج أن الإطار له تأثير إيجابي ومعنوي على نطاق التدقيق، حيث بلغت قيمة معامل الانحدار (B=2.953) عند مستوى دلالة (Sig=0.000)، وهو ما يشير إلى أن تطبيق الإطار يسهم في زيادة نطاق التدقيق من خلال تعزيز المتطلبات الرقابية وتوسيع مجالات الفحص لتشمل تقييم التوافق مع مكونات الإطار. وهذا يستدعي من المدققين تغطية أكبر للضوابط السيبرانية عند تنفيذ مهامهم. أما بالنسبة لمتغير التفاعل (المخاطر السيبرانية * إطار NIST CSF)، فقد كانت قيمة معامل

DOI: https://doi.org/10.35682/y8s1me39

الانحدار سالبة (B=-0.641) وبمستوى دلالة (Sig=0.000)، وهو ما يشير إلى أن الإطار يؤدي دورا معدلا يخفف من الأثر الايجابي للمخاطر السيبرانية على نطاق التدقيق. أي أن وجود الإطار يسهم في تقليل الحاجة إلى توسيع نطاق التدقيق الناتج عن ارتفاع مستوى المخاطر السيبرانية، من خلال تنظيم إدارة تلك المخاطر ووضوح آليات الرقابة المتعلقة بها، مما يحد من الحاجة إلى فحص مفرط أو مكرر من قبل المدققين. كما أوضحت النتائج ان قيمة معامل التحديد (R^2=0.710) أي أن النموذج يفسر ما نسبته 71 % من التغير في نطاق التدقيق. كما أن قيمة (Sig F= 0.000) تؤكد معنوية النموذج ككل وملاءمته الإحصائية. وبذلك يمكن القول إن الإطار يؤدي دورا معدلا سلبيا، حيث يسهم في تقليص أثر المخاطر السيبرانية على توسع نطاق التدقيق، من خلال تعزيز الضوابط الرقابية وتنظيم إجراءات الأمن السيبراني بما يتيح للمدقق العمل ضمن نطاق أكثر تركيزا وكفاءة دون الحاجة إلى توسع غير ضروري في إجراءات التدقيق عند مواجهة مستويات مرتفعة من المخاطر التقنية.

وبناءً على ذلك فإنه يتم رفض الفرضية العدمية الفرعية الرابعة، وقبول الفرضية البديلة، التي تنص على أنه: " يوجد أثر للمخاطر السيبرانية في نطاق التدقيق بوجود إطار NIST CSF كمتغير معدل ".

نتائج اختبار الفرضية الفرعية الخامسة

الجدول (14) نتائج تحليل الانحدار الخطي المتعدد لأثر المخاطر السيبرانية في الخبراء المختصين بوجود إطار NIST CSF كمتغير معدل

	المتغير المستقل	النموذج الأول			النموذج الثاني			النموذج الثالث		
		B	value t	Sig t*	B	value t	Sig t*	B	value t	Sig t*
المتغير التابع	المخاطر السيبرانية	0.862	18.682	0.000	0.468	3.612	0.000	1.272	1.634	0.104
	إطار NIST CSF				0.457	3.247	0.001	1.230	1.638	0.103
	المخاطر السيبرانية * NIST CSF							-0.181	-1.047	0.296
خبراء التدقيق	R^2	0.595			0.612			0.614		
	ΔR^2	0.595			0.017			0.002		
	ΔF	82.350			10.546			1.097		
	Sig ΔF	0.000			0.001			0.296		

أظهرت نتائج تحليل الانحدار المتعدد لاختبار الفرضية الفرعية الخامسة أن المخاطر السيبرانية لا تؤثر تأثيرا معنويا في الاستعانة بالخبراء المختصين، حيث بلغت قيمة معامل الانحدار (B=1.272) عند مستوى دلالة (Sig=0.104) وهي غير

معنوية إحصائيا. وهذا يشير إلى أن زيادة أو انخفاض مستوى المخاطر السيبرانية لا ينعكس بشكل واضح على درجة اعتماد المدققين على الخبراء الفنيين او المتخصصين في المجالات التقنية. وقد يعزى ذلك إلى أن قرار الاستعانة بالخبراء غالبا ما يتأثر بعوامل أخرى، مثل سياسات المؤسسة او طبيعة المهمة أو توافر الموارد البشرية، أكثر من تأثره بمستوى المخاطر السيبرانية بحد ذاتها. كما أظهرت النتائج أن الإطار لا يؤثر معنويا في الاعتماد على الخبراء المختصين، حيث بلغت قيمة معامل الانحدار (B=1.23) عند مستوى دلالة (Sig=0.103)، مما يشير إلى أن تطبيق الإطار لا يؤدي بالضرورة إلى زيادة أو تقليل الحاجة إلى الخبراء الخارجيين. ويحتمل أن تطبيق الإطار يعتمد بدرجة أكبر على كفاءة فرق العمل الداخلية وخبراتهم بدلا من الاعتماد على استشارات خارجية. أما بالنسبة لمتغير التفاعل (المخاطر السيبرانية * إطار NIST CSF)، فقد كانت قيمة معامل الانحدار سالبة (B=-0.181) وبمستوى دلالة (Sig=0.296)، مما يدل على أن الإطار لا يؤدي دورا معدلا في العلاقة بين المخاطر السيبرانية والاعتماد على الخبراء المختصين. أي أن وجود الإطار لا يغير طبيعة العلاقة بين هذين المتغيرين. كما أوضحت النتائج أن قيمة معامل التحديد (R^2=0.614) أي ان النموذج يفسر ما نسبته 61.40% من التغير في الاعتماد على الخبراء المختصين. وبذلك يمكن القول إن قرار الاستعانة بالخبراء في مهام التدقيق لا يتأثر مباشرة بارتفاع او انخفاض المخاطر السيبرانية أو بتطبيق الإطار، وإنما يعتمد على عوامل تنظيمية ومؤسسية أخرى مثل حجم المهمة وطبيعة الأنظمة محل التدقيق ومدى توافر الكفاءات الفنية داخل فريق التدقيق.

وبناءً على ذلك فإنه يتم قبول الفرضية العدمية الفرعية الخامسة، التي تنص على أنه: " لا يوجد أثر للمخاطر السيبرانية في الخبراء المختصين بوجود إطار NIST CSF كمتغير معدل ".

التوصيات:

1- ضرورة تشجيع المؤسسات على تطبيق الإطار ضمن عمليات الحوكمة وإدارة المخاطر، بهدف رفع كفاءة الاستجابة للتهديدات وتقليل تأثيرها على مهام التدقيق.

2- يوصى مدققو الحسابات الخارجيون والداخليون بدمج تقييم الضوابط السيبرانية ضمن مراحل التخطيط والتنفيذ للتدقيق، خاصة في القطاعات ذات الاعتماد العالي على الأنظمة الرقمية، بما يعزز دقة تقدير جهود التدقيق في ظل المخاطر السيبرانية المتنامية.

3- قيام الهيئات المهنية والرقابية بإصدار أدلة مهنية أو نماذج تقييم توضح كيفية التعامل مع المخاطر السيبرانية وفق الإطار، لتكون مرجعا موحدا للمدققين في تحليل تأثير تلك المخاطر على مكونات التدقيق المختلفة.

4- أهمية الاستثمار في برامج تدريبية متقدمة لتمكين المدققين من فهم المخاطر السيبرانية وتقييمها وتقليص الاعتماد المفرط على خبراء خارجيين، مما يعزز استقلالية المدقق وكفاءته.

5- تعزيز التنسيق بين إدارات الأمن السيبراني والتدقيق الداخلي لتبادل المعلومات حول الثغرات والتهديدات بما يضمن شمولية تقييم المخاطر وتكامل الضوابط.

6- التوسع في الدراسات المستقبلية لتشمل متغيرات معدلة جديدة، كأثر حوكمة تكنولوجيا المعلومات أو الخبرة التخصصية للمدقق في الأمن السيبراني. إضافة إلى ذلك، يمكن تعميق التحليل عبر دراسة تأثير هذه العوامل على جودة عملية التدقيق ذاتها، وليس فقط أتعابها، وإجراء مقارنات بين فعالية أطر عمل مختلفة مثل (ISO 27001, CIS Controls, COBIT 2019) أو بين قطاعات صناعية مختلفة.

References

Adebola, K. N., "The Role of NIST Cybersecurity Framework in The Adoption of Cloud-Native Technologies in The Financial Service Sector", *International Journal of Computer Engineering and Technology (IJCET)*, 16(3), 2025, 490-512. Retrieved from https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_16_ISSUE_3/IJCET_16_03_031.pdf

Aderinto, A. A., & Faforiji, A. C., "Cybersecurity Threats and Financial Performance of Listed Commercial Banks in Nigeria", *Asian Journal of Advanced Research and Reports*, 19(4), 2025, 381-394. Retrieved from https://journalajarr.com/index.php/AJARR/article/view/990

AICPA., "*Reporting on an Entity's Cybersecurity Risk Management Program and Controls"*, New York, NY: American Institute of Certified Public Accountants, 2017. Retrieved from https://www.aicpa-cima.com/cpe-learning/publication/reporting-on-an-entitys-cybersecurity-risk-management-program-and-controls-attestation-guide-OPL

Akey, P., Lewellen, S., Liskovich, I., & Schiller, C. M., *"Hacking Corporate Reputations"*, Toronto: Rotman School of Management - University of Toronto, 2024. Retrieved from https://www.ecgi.global/sites/default/files/working_papers/documents/hackingcorporatereputations_0.pdf

Al-Matari, O. M., Helal, I. M., Mazen, S. A., & Elhennawy, S., "Integrated Framework for Cybersecurity Auditing", *Information Security Journal*, 30(4), 2021, 189-204. Retrieved from https://www.tandfonline.com/doi/full/10.1080/19393555.2020.1834649

Babiker, I., "The Role of Internal Audit in Enhancing Cyber Security from The Auditors' Point of View", *Journal of Business and Environmental Sciences*, 4(1), 2025, 127-146. Retrieved from https://jcese.journals.ekb.eg/article_386443.html

Calderon, T. G., & Gao, L., "Cybersecurity Risks Disclosure and Implied Audit Risks: Evidence from Audit Fees", *International Journal of Auditing*, 25(1), 2021, 24-39. Retrieved from https://onlinelibrary.wiley.com/doi/epdf/10.1111/ijau.12209

Cobos, E. V., Cakir, S., Mei-Zahav, H., & Barakcin, B. B., "The Role of Cybersecurity in Economic Performance", *Washington, DC: World Bank*, 2024. Retrieved from https://documents1.worldbank.org/curated/en/099092324164526526/pdf/P178769189c7360111ac1f1185e04824dec.pdf

Dou, C., Yuan, M., & Chen, X., "Government-Background Customers, Audit Risk and Audit Fee", *China Journal of Accounting Studies*, 7(3), 2019, 385–406. Retrieved from https://www.tandfonline.com/doi/full/10.1080/21697213.2019.1703391

Fadya, M., & Utama, D. N., "Towards Secure Information Systems: Developing and Implementing an Information Security Evaluation Model Using NIST CSF and COBIT 2019", *TEM Journal*, 14(1), 2025, 182-191. Retrieved from https://www.temjournal.com/content/141/TEMJournalFebruary2025_182_191.pdf

Fang, Q., Wang, Z., & Dang, L., "Audit effort in the digital Era: Uncovering the dynamic interplay of business strategy and digital transformation", *International Journal of Accounting Information Systems*, 56, 2025, 1-16. Retrieved from https://www.sciencedirect.com/science/article/pii/S1467089525000235

Frino, A., Palumbo, R., & Rosati, P., "Does Information Asymmetry Predict Audit Fees?", *Accounting & Finance*, 63(2), 2023, 2597-2619. Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1111/acfi.12985

Gozman, D., & Willcocks, L., "The emerging Cloud Dilemma: Balancing Innovation with Cross-Border Privacy and Outsourcing Regulations", *Journal of Business Research*, 97, 2019, 235-256. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0148296318302935

Hossain, M. S., Belina, H., Hasan, M., & Kim, M. M., "The Effects of Auditor-level Cybersecurity Breaches on Auditor-Client Relationships", *European Accounting Review*, 34(5), 2024, 1-28. Retrieved from https://www.tandfonline.com/doi/full/10.1080/09638180.2024.2435389

IBM., Cost of a Data Breach Report 2024. IBM and Ponemon Institute, 2024. Retrieved from https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

IIA., "Auditing Cybersecurity Operations: Prevention and Detection", *Lake Mary, FL: The Institute of Internal Auditors*, 2025. Retrieved from https://www.theiia.org/en/content/guidance/recommended/supplemental/gtags/gtag-auditing-cybersecurity-operations-prevention-and-detection/

Iskandar, N. Z., William, & Deniswara, K., "Toward Secure Auditing: A Study On Auditor Readiness in Cybersecurity Implementation Using Extended Utaut Frameworks", Journal *of Theoretical and Applied Information Technology*, 103(4), 2025, 1179-1188. Retrieved from https://www.jatit.org/volumes/Vol103No4/4Vol103No4.pdf

Kamiya, S., Jun-Koo, K., Jungmin, K., Milidonis, A., & Stulz , R. M., "Risk Management, Firm Reputation, and The Impact of Successful Cyberattacks on Target Firms", *Journal of Financial Economics*, 139(3), 2021, 719-749. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0304405X20300143

Karyani, E., Noveria, A., Faturohman, T., & Rahadi, R. A.,"Disclosures of Cyber Exposure and Audit Fees: Evidence from Asean-4 Banking", *Corporate Governance and Organizational Behavior Review*, 7(4), 2023, 299-312. Retrieved from https://virtusinterpress.org/Disclosures-of-cyber-exposure-and-audit-fees-Evidence-from-ASEAN-4-banking.html

Kaushik, D., "The Impacts of Cybersecurity and AI on Businesses and Individuals", Journal *of Student Research*, 12(4), 2023, 1-10. Retrieved from

https://www.researchgate.net/publication/377351935_The_Impacts_of_Cybersecurity_and_AI_on_Businesses_and_Individuals#:~:text=This%20paper%20revealed%20that%20cybersecurity,inconvenience%2C%20constant%20new%20threats%2C%20and

Kurniawan, Y., & Mulyawan, A. N., "The Role of External Auditors in Improving Cybersecurity of the Companies through Internal Control in Financial Reporting", *Journal of System and Management Sciences*, 13(1), 2023, 485-510. Retrieved from https://www.aasmr.org/jsms/Vol13/No.1/Vol.13.No.1.26.pdf

Kwon, Y., Lee, J.-D., & Owens, J., "Managing Fintech Risks: Policy and Regulatory Implications", *Philippines: Asian Development Bank*, 2023. Retrieved from https://www.adb.org/publications/managing-fintech-risks-policy-regulatory-implications

Lai, J., "Artificial Intelligence Applications and Audit Fees: An Empirical Study", *International Review of Economics and Finance*, 103, 2025, 1-14. Retrieved from https://www.sciencedirect.com/science/article/pii/S1059056025005842

Li, H., No, W. G., & Boritz, J. E., "Are External Auditors Concerned about Cyber Incidents? Evidence from Audit Fees", *AUDITING: A Journal of Practice & Theory*, 39(1), 2020, 151-171. Retrieved from https://publications.aaahq.org/ajpt/article-abstract/39/1/151/6129/Are-External-Auditors-Concerned-about-Cyber?redirectedFrom=fulltext

Lin, W., Li, L. Z., Li, L. L., & Hay, D., "Repetitive key audit matters and audit effort", *Pacific Accounting Review*, 37(2), 2025, 209–242. Retrieved from https://www.emerald.com/par/article-abstract/37/2/209/1242623/Repetitive-key-audit-matters-and-audit-effort?redirectedFrom=fulltext

Makridis, C. A., "Do Data Breaches Damage Reputation? Evidence from 45 Companies Between 2002 and 2018", *Journal of Cybersecurity*, 7(1), 2021, 1-8. Retrieved from https://academic.oup.com/cybersecurity/article/7/1/tyab021/6362163

Marzuki, M. M., & Al-Amin , M. S., "The Effect of Audit Fees, Audit Quality and Board Ownership on Tax Aggressiveness: Evidence from Thailand", *Asian Review of Accounting*, 29(5), 2021, 617-636. Retrieved from https://www.sciencedirect.com/org/science/article/abs/pii/S1321734821000212

Mehmood, K. T., Ashraf, Z., Iqbal, R., Rafique, A. A., Gul, H., & Ali, M., "Cyber security Governance as a Pillar of Enterprise Risk Management: Designing a Compliance-Driven Framework for Operational Resilience, Policy Enforcement, and Regulatory Alignment", *Annual Methodological Archive Research Review (AMARR*), 3(5), 2025, 59-77. Retrieved from https://amresearchreview.com/index.php/Journal/article/view/110

Moreira, G. P., "Cybersecurity and External Audit. The Disclosure of Risk Factors in Annual Reports", *Lisbon: Universidade Católica Portuguesa*, 2019. Retrieved from https://core.ac.uk/download/237231002.pdf

NCSC., "Cyber Threat Situational Report", *Amman: National Cyber Security Center*, 2025. Retrieved from https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/q1_2025_report.pdf

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K.,"NIST Special Publication 800.NIST SP 800-61r3. Incident Response Recommendations and Considerations for Cybersecurity Risk Management", *A CSF 2.0 Community Profile, U.S. Department of Commerce & National Institute of Standards and Technology*, 2025. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

Ngalim, B.,"Integrating NIST and ISO Cybersecurity Audit and Risk Assessment Frameworks into Cameroonian Law", *Journal of Cybersecurity Education, Research and Practice*, 2024(1), 2023, 1-11. Retrieved from https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/4/

Ngo, T. N., & Tick, A., "Cyber-Security Risks Assessment by External Auditors", *Interdisciplinary Description of Complex Systems*, 19(3), 2021, 375-390. Retrieved from https://www.researchgate.net/publication/355150443_Cyber-security_Risks_Assessments_by_External_Auditors

NIST., "The NIST Cybersecurity Framework (CSF) 2.0. RESOURCE & Overview Guide. Maryland", *United States: National Institute of Standards and Technology*, 2024, Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Pranggono, B., & Arabo, A., "COVID-19 Pandemic Cybersecurity Issues", *Internet Technology Letters*, 4(2), 2024, 1-6. Retrieved from https://pmc.ncbi.nlm.nih.gov/articles/PMC7675576/

Quinn, S., Ivy, N., Barrett, M., Gardner, R., Smith, M. C., & Witte, G., "NIST Interagency Report NIST IR 8286Cr1 ipd. Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight. U.S.", *Department of Commerce & National Institute of Standards and Technology*, 2025, Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8286Cr1.ipd.pdf

Reyes-Acosta, R. E., Mendoza-González, R., Diaz, E. O., Martin, M. V., Rosas, F. J., Romo, J. C., & Mendoza-González, A., "Cybersecurity Conceptual Framework Applied to Edge Computing and Internet of Things Environments", *Electronics*, 14(11), 2025, 1-40. Retrieved from https://www.mdpi.com/2079-9292/14/11/2109

Rosati, P., Gogolin, F., & Lynn, T., "Audit Firm Assessments of Cyber-Security Risk: Evidence from Audit Fees and SEC Comment Letters", *The International Journal of Accounting*, 54(3), 2019, 1-56. Retrieved from https://www.worldscientific.com/doi/10.1142/s1094406019500136?srsltid=AfmBOoqnslOqI6VVNAD-8H4Dz7cCG8Ed-dlJMHCuVz5XM-YVTw3cIbUg

Sekaran, U., & Bougie, R., "Research Methods for Business: A Skill-Building Approach (7 ed.)" *West Sussex: Wiley & Sons*, 2016.

Smith, T., Higgs, J., & Pinsker, R., "Do Auditors Price Breach Risk in Their Audit Fees?", *University of South Florida*, 2017, Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3234312

Susanto, & Soepriyanto, G., "Cybersecurity Disclosure and Audit Fees: An Empirical Study of Listed Companies On the Indonesia Stock Exchange", *Edelweiss Applied Science and Technology*, 8(6), 2024, 6090-6104. Retrieved from https://learning-gate.com/index.php/2576-8484/article/view/3328

Waliullah, M., George, M. Z., Hasan, M. T., Alam, M. K., Munira, M. S., & Siddiqui, N. A., "Assessing The Influence of Cybersecurity Threats and Risks on the Adoption and Growth of Digital Banking: A Systematic Literature Review", *American Journal of Advanced Technology and Engineering Solutions*, 1(1), 2025, 226-257. Retrieved from https://arxiv.org/abs/2503.22710

Xin, J., Du, K., & Xia, Y., "The Impact of Enterprise Digital Transformation on Audit Fees—An Intermediary Role Based on Information Asymmetry", *Sustainability*, 16(22), 2024, 1-21. Retrieved from https://www.mdpi.com/2071-1050/16/22/9970

Yen, J.-C., Lim, J.-H., Wang, T., & Hsu, C., "The Impact of Audit Firms' Characteristics on Audit Fees Following Information Security Breaches", *Journal of Accounting and Public Policy*, 37(6), 2019, 489-507. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0278425418302369

Zadorozhnyi, Z.-M., Muravskyi, V., Shevchuk, O., & Bryk, M., "Innovative Accounting Methodology of Ensuring the Interaction of Economic and Cybersecurity of Enterprises", *Marketing and Management of Innovations*, (4), 2021, 36-46. Retrieved from https://mmi.sumdu.edu.ua/wp-content/uploads/mmi/volume-12-issue-4/529-2021-03_Zadorozhnyi_0.pdf

Zaghloul, S. A., "Information Systems and CyberSecurity Audit", *The 14th ARABOSAI Scientific Research Competition*, 2025, pp. 1-132. Jeddah - KSA: ARABOSAI. Retrieved from https://www.arabosai.org/fileadmin/Contenu/Documents_to_download/FINAL_ENGLISH_-_Dr._Samy_Zaghloul.pdf

Zhang, Y., & Smith, T.,"The Impact of Customer Firm Data Breaches on the Audit Fees of their Suppliers", *International Journal of Accounting Information Systems*, 50, 2023, 1-51. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S1467089523000209