السنة الرابعة والعشرون/ عدد خاص/ تموز 2026
https://doi.org/10.31272/ijes.v24.1541

المجلة العراقية للعلوم الاقتصادية
Iraqi Journal For
Economic Sciences

PISSN : 1812-8742 EISSE : 2791-092X Arcif : 0.375

The relationship between cybersecurity maturity and the quality of external auditing in companies listed on the Iraq Stock Exchange

العلاقة بين نضج الأمن السيبراني وجودة التدقيق الخارجي في الشركات المدرجة في سوق العراق للأوراق المالية

رغد جمال عباس
Raghad Jamal Abbas
raghadsudni86@gmail.com
كلية الإدارة والاقتصاد/ الجامعة العراقية

سما صفاء موسى
sama safaa musa
samaalmourab@gmail.com
كلية العلوم الادارية/ جامعة المستقبل

Abstract

This study analyzes the relationship between cybersecurity maturity and external audit quality in companies listed on the Iraq Stock Exchange from 2020 to 2025. Using a descriptive-analytical approach and panel data, the research utilized SPSS to conduct descriptive statistics and linear regression. The results indicate a statistically significant positive impact, with cybersecurity maturity explaining approximately 49% of the changes in external audit quality. While Iraqi companies show high adoption of basic preventive measures like firewalls, there is a noticeable weakness in advanced analytical systems and cyber training. The findings also highlight a professional gap where external audit procedures remain largely traditional, with limited focus on digital risk assessment. A strong positive correlation was confirmed between the number of cybersecurity programs and the depth of audit procedures. Consequently, the study recommends formally integrating cybersecurity into audit programs and enhancing auditors' digital proficiency.

Keywords: Cybersecurity Maturity, External Audit Quality, Iraq Stock Exchange, Digital Auditing.

المستخلص

يهدف هذا البحث إلى تحليل العلاقة بين نضج الأمن السيبراني وجودة التدقيق الخارجي في الشركات المدرجة بسوق العراق للأوراق المالية للفترة (2020-2025). اعتمدت الدراسة المنهج الوصفي التحليلي باستخدام بيانات "Panel Data"وبرنامج SPSS لاختبار الفرضيات. أظهرت النتائج وجود أثر إيجابي ذو دلالة إحصائية لنضج الأمن السيبراني في جودة التدقيق، حيث يفسر النضج السيبراني نحو 49% من التغيرات في جودة التدقيق. كما كشفت الدراسة عن تركيز الشركات على الجوانب الوقائية التقنية مع ضعف في الأنظمة التحليلية المتقدمة وبرامج التدريب. وفي المقابل، تبيّن أن إجراءات التدقيق الخارجي لا تزال تركز على الجوانب التقليدية مع محدودية في تقييم المخاطر الرقمية. وخلص البحث إلى وجود علاقة ارتباط موجبة قوية بين تطور البنية

السيبرانية وتوسيع نطاق اختبارات التدقيق. وأخيراً، أوصت الدراسة بضرورة دمج الأمن السيبراني رسمياً ضمن برامج التدقيق السنوية وتطوير مهارات المدققين في المجال الرقمي.

الكلمات الرئيسية: نضج الأمن السيبراني، جودة التدقيق الخارجي، سوق العراق للأوراق المالية، التدقيق الرقمي.

1. منهجية البحث

اولاً: مشكلة البحث: في ظل التحول الرقمي المتسارع الذي تشهده بيئة الأعمال، تزايدت المخاطر السيبرانية التي تهدد موثوقية نظم المعلومات المحاسبية وجودة البيانات المالية، ولاسيما في الشركات المدرجة في الأسواق المالية. وعلى الرغم من إدراك أهمية الأمن السيبراني، إلا أن مستوى نضج الأمن السيبراني يختلف بشكل ملحوظ بين الشركات، الأمر الذي قد ينعكس على فاعلية نظم الرقابة الداخلية وقدرة المدقق الخارجي على تنفيذ مهامه بكفاءة. وفي المقابل، تُعد جودة التدقيق الخارجي عنصرًا جوهريًا في تعزيز مصداقية القوائم المالية وحماية مصالح المستثمرين، غير أن الممارسات التدقيقية التقليدية قد لا تكون كافية لمواكبة التعقيد المتزايد لنظم المعلومات والمخاطر السيبرانية المصاحبة لها. كما أن محدودية الإفصاح عن ممارسات الأمن السيبراني قد تُضعف قدرة المدققين على تقييم المخاطر التقنية بشكل دقيق، مما قد يؤثر في جودة عملية التدقيق ونتائجها. وعلى الرغم من تزايد الاهتمام العالمي بدراسة الأمن السيبراني وجودة التدقيق، فإن الأدبيات المحاسبية لا تزال تعاني من نقص في الدراسات التطبيقية التي بحثت العلاقة بين نضج الأمن السيبراني وجودة التدقيق الخارجي باستخدام بيانات فعلية، خاصة في بيئات الأسواق المالية الناشئة. ويبرز هذا النقص بشكل أكثر وضوحًا في سوق العراق للأوراق المالية، في ظل ندرة الدراسات التي تناولت هذا الموضوع خلال فترة التحول الرقمي الأخيرة. وبناءً على ما تقدم، تتمثل مشكلة البحث في غياب الأدلة التطبيقية التي توضح طبيعة العلاقة بين نضج الأمن السيبراني وجودة التدقيق الخارجي في الشركات المدرجة في سوق العراق للأوراق المالية، ومدى انعكاس تطور ممارسات الأمن السيبراني على جودة التدقيق الخارجي.

ثانياً: أهمية البحث: تنبع أهمية هذا البحث من كونه يعالج أحد الموضوعات المعاصرة التي تفرضها التحولات الرقمية المتسارعة في بيئة الأعمال، والمتمثل في نضج الأمن السيبراني وانعكاسه على جودة التدقيق الخارجي في الشركات المدرجة في الأسواق المالية. وتتجلى أهمية البحث من خلال الجوانب الآتية:

أولًا: الأهمية العلمية: يسهم البحث في إثراء الأدبيات المحاسبية والتدقيقية من خلال ربط مفهوم نضج الأمن السيبراني، الذي غالبًا ما يُتناول في دراسات نظم المعلومات، بمفهوم جودة التدقيق الخارجي، وذلك في إطار تطبيقي واحد. كما يقدم البحث دليلًا تجريبيًا حول هذه العلاقة في بيئة سوق مالية ناشئة، بما يسد فجوة بحثية قائمة في الدراسات العربية والدولية، ولاسيما في السياق العراقي.

ثانيًا: الأهمية التطبيقية: يوفر البحث نتائج كمية قابلة للتطبيق تساعد إدارات الشركات المدرجة في سوق العراق للأوراق المالية على إدراك الدور الذي يؤديه نضج ممارسات الأمن السيبراني في تعزيز جودة التدقيق الخارجي. كما تسهم النتائج في دعم مكاتب التدقيق الخارجي في تحسين إجراءات تقييم مخاطر التدقيق المرتبطة بنظم المعلومات والأمن السيبراني.

ثالثًا: الأهمية التنظيمية والرقابية: يفيد البحث الجهات الرقابية والتنظيمية في سوق العراق للأوراق المالية من خلال تقديم مؤشرات عملية يمكن الاستناد إليها عند تطوير متطلبات الإفصاح والحوكمة السيبرانية، بما يسهم في تعزيز شفافية التقارير المالية ورفع مستوى الثقة في السوق المالي.

ثالثا: اهداف البحث: يهدف هذا البحث إلى تحليل العلاقة بين نضج الأمن السيبراني وجودة التدقيق الخارجي في الشركات المدرجة في سوق العراق للأوراق المالية وذلك من خلال تحقيق الأهداف الآتية:

1. قياس مستوى نضج الأمن السيبراني في الشركات المدرجة في سوق العراق للأوراق المالية بالاعتماد على بيانات فعلية ومؤشرات كمية.
2. قياس مستوى جودة التدقيق الخارجي في الشركات محل الدراسة باستخدام مؤشرات موضوعية مستمدة من تقارير التدقيق الخارجي.
3. اختبار أثر نضج الأمن السيبراني في جودة التدقيق الخارجي باستخدام نماذج تحليل بيانات البانل.
4. تحديد قوة واتجاه العلاقة بين نضج الأمن السيبراني وجودة التدقيق الخارجي في بيئة سوق العراق للأوراق المالية.
5. تقديم مؤشرات عملية يمكن أن تستفيد منها إدارات الشركات ومكاتب التدقيق والجهات الرقابية لتعزيز ممارسات الأمن السيبراني وجودة التدقيق الخارجي.

رابعاً: فرضيات البحث: انطلاقًا من مشكلة البحث وأهدافه، وفي ضوء الإطار النظري والدراسات السابقة، صيغت فرضيات البحث على النحو الآتي:

الفرضية الرئيسة

- H_0: لا يوجد أثر ذو دلالة إحصائية لنضج الأمن السيبراني في جودة التدقيق الخارجي في الشركات المدرجة في سوق العراق للأوراق المالية
- H_1: يوجد أثر ذو دلالة إحصائية لنضج الأمن السيبراني في جودة التدقيق الخارجي في الشركات المدرجة في سوق العراق للأوراق المالية.

خامساً: منهجية البحث: اعتمدت الدراسة على المنهج الوصفي–التحليلي، وذلك لوصف ظاهرة نضج الأمن السيبراني وجودة التدقيق الخارجي، وتحليل العلاقة بينهما باستخدام أساليب إحصائية كمية ملائمة لطبيعة البيانات.

سادساً: متغيرات الدراسة

- المتغير المستقل :نضج الأمن السيبراني.(Cybersecurity Maturity) على أنه درجة تكامل إطار إدارة المخاطر السيبرانية داخل العمليات التنظيمية اليومية، بحيث تصبح ممارسات الأمن جزءًا من الثقافة المؤسسية وليس مجرد إجراءات تقنية.
- المتغير التابع :جودة التدقيق الخارجي.(External Audit Quality) تتمثل في مدى التزام المدقق الخارجي بمعايير التدقيق المتعارف عليها، وتطبيقه لإجراءات تدقيق كافية ومناسبة تمكّنه من تكوين رأي مهني سليم حول عدالة القوائم المالية وخلوها من التحريفات الجوهرية.

المحور الاول: الجانب النظري

المتغير المستقل: نضج الأمن السيبراني

اولاً: مفهوم نضج الأمن السيبراني : نضج الأمن السيبراني يمثل انتقال المنظمة من مرحلة التركيز على الحلول التقنية المنعزلة إلى مرحلة الإدارة الشاملة للأمن السيبراني، والتي تتضمن القيادة، الحوكمة، السلوك التنظيمي، وإدارة المخاطر. (Von Solms, & Van Niekerk, 2013:99). وبحسب (Cybersecurity, 2018:6) ان نضج الأمن السيبراني على أنه درجة تكامل إطار إدارة المخاطر السيبرانية داخل العمليات التنظيمية اليومية، بحيث تصبح ممارسات الأمن جزءًا من الثقافة المؤسسية وليس مجرد إجراءات تقنية. ويُعد نضج الأمن السيبراني من

المفاهيم الحديثة نسبيًا في أدبيات إدارة المخاطر ونظم المعلومات، ويشير إلى مدى تطور وقدرة المنظمة على حماية أصولها المعلوماتية وإدارة المخاطر السيبرانية بصورة منهجية ومتكاملة. ولا يقتصر هذا المفهوم على استخدام التقنيات الأمنية فحسب، بل يشمل السياسات والإجراءات والحوكمة والوعي المؤسسي والاستجابة للحوادث. ويُعرّف نضج الأمن السيبراني بأنه :المستوى الذي تعكس فيه ممارسات الأمن السيبراني في المنظمة قدرتها على التنبؤ بالمخاطر الرقمية، ومنعها، واكتشافها، والاستجابة لها، والتعافي منها بصورة منظمة وقابلة للقياس (Dražček, et al., 2022:2).

ثانياً: أهمية نضج الأمن السيبراني: تنبع أهمية نضج الأمن السيبراني من كونه أحد المرتكزات الأساسية لحماية أصول المنظمة المعلوماتية وضمان استمرارية أعمالها في ظل البيئة الرقمية المعقدة. إذ يسهم ارتفاع مستوى نضج الأمن السيبراني في تقليل المخاطر التشغيلية والمعلوماتية الناتجة عن الهجمات السيبرانية، ويحسن قدرة المنظمة على منع الاختراقات واكتشافها والاستجابة لها في الوقت المناسب(ISACA, 2019:15). وتتجلى أهمية نضج الأمن السيبراني في دعمه لبيئة الرقابة الداخلية، حيث يؤدي تطبيق سياسات وإجراءات أمنية ناضجة إلى تعزيز موثوقية نظم المعلومات المحاسبية، والحد من احتمالات التلاعب أو فقدان البيانات المالية، الأمر الذي ينعكس إيجابًا على جودة التقارير المالية واتخاذ القرارات الإدارية(Cybersecurity, 2018:8). كما يؤكد (Von Solms, & Van Niekerk, 2013:101) أن نضج الأمن السيبراني يسهم في تحويل الأمن من مجرد وظيفة تقنية إلى عنصر استراتيجي داعم للحوكمة المؤسسية، من خلال دمجه في ثقافة المنظمة وسلوك العاملين فيها، بما يعزز الالتزام بالضوابط والسياسات الأمنية. ومن جانب آخر، تشير الدراسات إلى أن المنظمات ذات المستويات المرتفعة من نضج الأمن السيبراني تكون أكثر قدرة على تحقيق الامتثال للمعايير الدولية والقوانين التنظيمية، مما يقلل من المخاطر القانونية والسمعية، ويعزز ثقة أصحاب المصلحة والمستثمرين في مصداقية المعلومات المفصح عنها (KPMG, 2020:22) . وفي سياق التدقيق الخارجي، تزداد أهمية نضج الأمن السيبراني لكونه أحد العوامل المؤثرة في تقييم مخاطر التدقيق، إذ يعتمد المدقق الخارجي على سلامة وأمن نظم المعلومات عند جمع أدلة الإثبات. وبالتالي، فإن ارتفاع مستوى النضج السيبراني يسهم في تحسين كفاءة وفعالية عملية التدقيق وجودتها(Arens et al., 2020:312) .

ثالثاً: مستويات نضج الأمن السيبراني: تشير الأدبيات الحديثة إلى أن نضج الأمن السيبراني لا يتحقق بصورة فجائية، بل يمر عبر مستويات متدرجة تعكس تطور ممارسات الأمن داخل المنظمة من العشوائية إلى التحسين المستمر. وتُعد نماذج النضج، مثل نموذج NIST ونموذج CMMI، من أكثر النماذج استخدامًا في تصنيف مستويات نضج الأمن السيبراني (NIST,2018:10).

1. المستوى الأول: البدائي(Initial) في هذا المستوى، تكون ممارسات الأمن السيبراني غير رسمية وتعتمد على ردود الأفعال عند وقوع الحوادث، مع غياب السياسات الموثقة وضعف الوعي الأمني لدى العاملين، مما يجعل المنظمة عرضة للمخاطر السيبرانية(NIST, 2018:10).
2. المستوى الثاني: المتكرر(Repeatable) يتميز هذا المستوى بوجود بعض الإجراءات الأمنية المتكررة، إلا أنها غير موحدة أو مطبقة بشكل شامل على مستوى المنظمة، وغالبًا ما تعتمد على خبرات الأفراد بدلًا من أطر مؤسسية واضحة(ISACA, 2019:18)
3. المستوى الثالث: المعرّف(Defined) في هذا المستوى، تعتمد المنظمة سياسات وإجراءات أمن سيبراني موثقة، ويتم تطبيقها على نطاق واسع، مع تحديد واضح للأدوار والمسؤوليات

وبدء دمج الأمن السيبراني ضمن الهيكل التنظيمي والحوكمة المؤسسية(ENISA, 2021:27) .
4. المستوى الرابع: المُدار(Managed) تنتقل المنظمة في هذا المستوى إلى مرحلة قياس أداء الأمن السيبراني وإدارة المخاطر بشكل منهجي، من خلال مؤشرات أداء واضحة، ومراجعات دورية، وربط الأمن السيبراني بإدارة المخاطر المؤسسية(NIST, 2018:12)
5. المستوى الخامس: المُحسَّن(Optimized) يمثل هذا المستوى أعلى درجات نضج الأمن السيبراني، حيث تعتمد المنظمة على التحسين المستمر والتكيف الاستباقي مع التهديدات السيبرانية، مع استخدام التحليلات المتقدمة، والتعلم من الحوادث، وتعزيز ثقافة الأمن السيبراني على جميع المستويات الإدارية (ISACA, 2019:21) .

رابعاً: أبعاد نضج الأمن السيبراني: يعتمد هذا العرض على إطار المعهد الوطني الأمريكي للمعايير والتكنولوجيا(NIST) ، والذي يُعد من أكثر الأطر استخدامًا عالميًا في قياس نضج الأمن السيبراني داخل المنظمات. ويحدد إطار NIST Cybersecurity Framework خمسة أبعاد (وظائف) رئيسة تمثل جوهر نضج الأمن السيبراني، وتعكس مدى تكامل ممارسات الأمن السيبراني داخل العمليات التنظيمية.(NIST, 2018).

1. بُعد التحديد(Identify):يركز هذا البعد على قدرة المنظمة على فهم بيئتها التشغيلية وتحديد أصولها المعلوماتية والمخاطر السيبرانية المرتبطة بها، بما في ذلك إدارة الأصول، الحوكمة، وتقييم المخاطر. ويُعد هذا البعد الأساس الذي تُبنى عليه باقي أبعاد نضج الأمن السيبراني (NIST, 2018:8)
2. بُعد الحماية(Protect):يتعلق هذا البعد بتطوير وتنفيذ الضوابط والإجراءات اللازمة لحماية الأنظمة والبيانات من الهجمات السيبرانية، ويشمل إدارة الوصول، التوعية والتدريب، حماية البيانات، والصيانة الوقائية. ويعكس هذا البعد مستوى الجاهزية الوقائية للمنظمة (NIST, 2018:9)
3. بُعد الاكتشاف(Detect): يقيس هذا البعد قدرة المنظمة على اكتشاف الحوادث السيبرانية في الوقت المناسب من خلال أنظمة المراقبة المستمرة، وكشف الأنشطة غير الطبيعية. ويعد الاكتشاف المبكر مؤشرًا مهمًا على نضج منظومة الأمن السيبراني(NIST, 2018:10)
4. بُعد الاستجابة(Respond) :يركز هذا البعد على الإجراءات التي تتخذها المنظمة عند وقوع حادث سيبراني، مثل احتواء الهجوم، تحليل آثاره، والتواصل الداخلي والخارجي. ويسهم وجود خطط استجابة واضحة في تقليل الخسائر التشغيلية والمالية(NIST, 2018:11) .
5. بُعد التعافي(Recover) : يتعلق هذا البعد بقدرة المنظمة على استعادة الأنظمة والبيانات المتضررة، وضمان استمرارية الأعمال، وتحسين الإجراءات بناءً على الدروس المستفادة من الحوادث السابقة. ويعكس هذا البعد أعلى مستويات نضج الأمن السيبراني(NIST, 2018:12).

المتغير التابع: جودة التدقيق الخارجي

اولاً مفهوم جودة التدقيق الخارجي: تُعد جودة التدقيق الخارجي من المفاهيم الأساسية في الفكر المحاسبي والتدقيقي، لما لها من دور محوري في تعزيز مصداقية القوائم المالية وزيادة ثقة مستخدميها. ويشير هذا المفهوم إلى مدى قدرة المدقق الخارجي على اكتشاف الأخطاء الجوهرية والتحريفات المادية في القوائم المالية والإفصاح عنها، مع الالتزام بمعايير التدقيق المهنية والمحافظة على الاستقلالية والموضوعية. ويُعرّف (DeAngelo, 1981:186) ان جودة التدقيق الخارجي بأنها الاحتمال المشترك المتمثل في قدرة المدقق على اكتشاف الأخطاء الجوهرية في النظام المحاسبي للمنشأة، واستعداده للإبلاغ عنها عند اكتشافها، وهو ما يعكس مستوى كفاءة المدقق واستقلاليته المهنية. ويرى(Francis, 2011:125) أن جودة التدقيق

الخارجي مفهوم متعدد الأبعاد، يتأثر بعوامل مرتبطة بالمدقق نفسه مثل الخبرة المهنية وحجم مكتب التدقيق، وبعوامل مرتبطة بالمنشأة محل التدقيق كقوة نظام الرقابة الداخلية ومستوى المخاطر، إضافة إلى تأثير البيئة التنظيمية والتشريعية التي تمارس فيها مهنة التدقيق. كما يشير (Arens, et al., 2017:38)إلى أن جودة التدقيق الخارجي تتمثل في مدى التزام المدقق الخارجي بمعايير التدقيق المتعارف عليها، وتطبيقه لإجراءات تدقيق كافية ومناسبة تمكّنه من تكوين رأي مهني سليم حول عدالة القوائم المالية وخلوها من التحريفات الجوهرية. وبناءً على ما تقدم، يمكن القول إن جودة التدقيق الخارجي تعكس مستوى الكفاءة المهنية والاستقلالية التي يتمتع بها المدقق الخارجي، ومدى فعالية إجراءات التدقيق المطبقة في ضمان موثوقية المعلومات المالية.

ثانياً: أهمية جودة التدقيق الخارجي: تكتسب جودة التدقيق الخارجي أهمية بالغة في بيئة الأعمال المعاصرة، لما لها من دور أساسي في تعزيز مصداقية القوائم المالية وزيادة ثقة مستخدميها، ولاسيما المستثمرين والدائنين وأصحاب المصالح. إذ تسهم جودة التدقيق في الحد من عدم تماثل المعلومات بين إدارة المنشأة والأطراف الخارجية، من خلال توفير تأكيد معقول بشأن عدالة القوائم المالية وخلوها من التحريفات الجوهرية. وفي السياق التنظيمي، تمثل جودة التدقيق الخارجي أحد العوامل الرئيسة في تعزيز الامتثال للأنظمة والتشريعات المحاسبية، ودعم الثقة في مهنة التدقيق، مما يسهم في تحسين سمعة الشركات ومكاتب التدقيق على حد سواء (Arens et al., 2017:41-45). وتبرز أهمية جودة التدقيق الخارجي في دعم كفاءة الأسواق المالية، حيث تؤدي التقارير المالية المدققة بجودة عالية إلى تحسين كفاءة تخصيص الموارد وتقليل مخاطر الاستثمار، مما ينعكس إيجابًا على استقرار الأسواق المالية وجاذبيتها. ومن جانب آخر، تساعد جودة التدقيق الخارجي في تقليل مخاطر الغش والتلاعب المالي، من خلال رفع احتمال اكتشاف الأخطاء الجوهرية والإفصاح عنها، وهو ما يعزز الشفافية والمساءلة ويحد من الممارسات غير السليمة (Francis, 2011:126-130). كما تسهم جودة التدقيق الخارجي في تعزيز فعالية نظم الرقابة الداخلية داخل المنشآت، إذ يعتمد المدقق الخارجي في عمله على تقييم هذه النظم وتحديد نقاط الضعف فيها، الأمر الذي يدفع إدارات الشركات إلى تحسين ضوابطها الداخلية والالتزام بالمعايير المحاسبية والمهنية المعتمدة(DeAngelo, 1981:)187.

ثالثاً: أبعاد جودة التدقيق الخارجي:اعتمدت هذه الدراسة في تحديد أبعاد جودة التدقيق الخارجي على إطار(Francis, 2011:127-131)، والذي يُعد من أكثر الأطر شمولًا وانتشارًا في الأدبيات المحاسبية الحديثة، إذ ينظر إلى جودة التدقيق الخارجي بوصفها مفهومًا متعدد الأبعاد يتأثر بعوامل تتعلق بالمدقق وبيئة التدقيق ونظم الرقابة، وهو ما يتناغم مع طبيعة هذا البحث الذي يربط جودة التدقيق بنضج الأمن السيبراني.

1. كفاءة المدقق الخارجي: يشير هذا البعد إلى مستوى المعرفة المهنية والخبرة الفنية التي يمتلكها المدقق الخارجي، وقدرته على فهم نظم المعلومات المحاسبية وتقييم المخاطر المرتبطة بها. وتُعد كفاءة المدقق عنصرًا أساسيًا في اكتشاف الأخطاء الجوهرية والتحريفات، لاسيما في البيئات التي تعتمد على النظم الإلكترونية ونظم المعلومات المتقدمة .

2. استقلالية المدقق الخارجي: تمثل الاستقلالية قدرة المدقق على إصدار رأي مهني محايد دون التأثر بمصالح أو ضغوط من إدارة المنشأة. ويؤكدFrancisأن استقلالية المدقق تعد شرطًا جوهريًا لتحقيق جودة تدقيق مرتفعة، إذ إن ضعف الاستقلالية يؤدي إلى تقليص فعالية إجراءات التدقيق مهما بلغت كفاءة المدقق

3. فعالية إجراءات التدقيق يقيس هذا البعد مدى ملاءمة وكفاية إجراءات التدقيق المطبقة، بما في ذلك تخطيط التدقيق، وتقييم المخاطر، وجمع أدلة الإثبات. ويشيرFrancisإلى أن جودة التدقيق ترتبط ارتباطًا وثيقًا بقدرة المدقق على تصميم إجراءات تدقيق تستجيب لمستوى المخاطر، ومن

ضمنها مخاطر نظم المعلومات والأمن السيبراني.

4. جودة بيئة الرقابة الداخلية يرىFrancisأن جودة التدقيق الخارجي لا تنفصل عن بيئة الرقابة الداخلية للمنشأة، إذ يعتمد المدقق في كثير من الأحيان على هذه البيئة عند تحديد طبيعة وتوقيت ومدى إجراءات التدقيق. وكلما كانت نظم الرقابة – بما فيها الرقابة على نظم المعلومات أكثر قوة ونضجًا، انعكس ذلك إيجابًا على جودة التدقيق

5. موثوقية تقرير المدقق الخارجي يعكس هذا البعد مدى تعبير تقرير المدقق عن الواقع المالي للمنشأة، ووضوح الرأي المهني المقدم، ومدى التزامه بمتطلبات الإفصاح والمعايير المهنية. ويؤكد Francisأن تقرير المدقق يُعد المخرج النهائي لعملية التدقيق ومؤشرًا مباشرًا على جودته.

المحور الثاني: الجانب التطبيقي

المحور الأول: آليات وبرامج نضج الأمن السيبراني في الشركات المدرجة في سوق العراق للأوراق المالية

1 .تحديد آليات وبرامج الأمن السيبراني: تم قياس نضج الأمن السيبراني بالاعتماد على البرامج والأنظمة المطبقة فعليًا داخل الشركات، كما وردت في التقارير السنوية وتقارير إدارة المخاطر.

جدول (1): آليات وبرامج الأمن السيبراني المعتمدة في الشركات المدرجة

ت	الآلية / البرنامج	نسبة الشركات المطبقة (%)	متوسط عدد الأنظمة	مستوى النضج
1	جدران الحماية (Firewalls)	%92	2.4	مرتفع
2	أنظمة كشف ومنع الاختراق (IDS/IPS)	%76	1.6	مرتفع
3	أنظمة مكافحة البرمجيات الخبيثة (EDR/AV)	%88	2.1	مرتفع
4	تشفير قواعد البيانات	%64	1.3	متوسط
5	أنظمة النسخ الاحتياطي والتعافي	%81	1.8	مرتفع
6	أنظمة إدارة الهوية والصلاحيات (IAM)	%59	1.2	متوسط
7	منصات مراقبة الأحداث الأمنية (SIEM)	%47	0.9	منخفض–متوسط
8	برامج التدريب السيبراني للموظفين	%41	1.0	منخفض

المصدر: من اعداد الباحثين وفقا لتقارير سوق العراق للأوراق المالية

تشير نتائج الجدول (1) إلى أن الشركات المدرجة في سوق العراق للأوراق المالية تعتمد بدرجة كبيرة على البرامج الوقائية الأساسية مثل جدران الحماية وأنظمة مكافحة البرمجيات الخبيثة، في حين يظهر ضعف واضح في تبني الأنظمة التحليلية المتقدمة مثل (SIEM) وبرامج التدريب السيبراني. ويعكس ذلك أن نضج الأمن السيبراني لا يزال يتركز في الجانب التقني أكثر من تركّزه في الإدارة الاستباقية للمخاطر السيبرانية.

المحور الثاني: إجراءات جودة التدقيق الخارجي المعتمدة في الشركات المدرجة

1. إجراءات التدقيق الخارجي: تم قياس جودة التدقيق الخارجي من خلال الإجراءات الفعلية المطبقة أثناء عملية التدقيق، وليس من خلال صفات المدقق فقط.

جدول (2): إجراءات التدقيق الخارجي المعتمدة داخل الشركات

ت	الآلية / البرنامج	نسبة الشركات المطبقة (%)	متوسط عدد الأنظمة	مستوى النضج
1	التخطيط المبني على المخاطر	%85	1.9	مرتفع
2	اختبار الضوابط الداخلية	%78	2.3	مرتفع
3	تدقيق نظم المعلومات المحاسبية	%69	1.7	متوسط
4	استخدام أدوات التدقيق الإلكتروني (CAATs)	%54	1.2	متوسط
5	تقييم ضوابط الأمن السيبراني	%46	1.1	منخفض–متوسط
6	توثيق مخاطر تكنولوجيا المعلومات	%63	1.5	متوسط
7	إصدار تقارير بدون تحفظ	%71	-	جيد

المصدر: من اعداد الباحثين وفقا لتقارير سوق العراق للأوراق المالية

يبين الجدول (2) أن إجراءات التدقيق التقليدية مثل التخطيط واختبار الضوابط تُطبق بمستويات مرتفعة، في حين أن الإجراءات المرتبطة بتدقيق الأمن السيبراني ونظم المعلومات لا تزال محدودة نسبيًا. ويشير ذلك إلى فجوة مهنية بين تطور المخاطر الرقمية ومستوى استجابة إجراءات التدقيق الخارجي لها في البيئة العراقية.

المحور الثالث: العلاقة بين آليات نضج الأمن السيبراني وإجراءات جودة التدقيق الخارجي

1. اختبار العلاقة باستخدام معامل الارتباط

جدول (3): العلاقة بين برامج الأمن السيبراني وإجراءات التدقيق الخارجي

المتغيرات	معامل الارتباط (r)	مستوى الدلالة	نوع العلاقة
عدد برامج الأمن السيبراني × عدد إجراءات التدقيق	0.71	0.000	موجبة قوية
أنظمة المراقبة السيبرانية × تدقيق نظم المعلومات	0.68	0.001	موجبة قوية
التدريب السيبراني × جودة تقارير التدقيق	0.63	0.002	موجبة متوسطة

المصدر: من اعداد الباحثين

تشير نتائج الجدول(3) إلى وجود علاقة ارتباط موجبة قوية ذات دلالة إحصائية بين مستوى تبني آليات وبرامج الأمن السيبراني وبين عدد وعمق إجراءات التدقيق الخارجي. فكلما زادت الأنظمة السيبرانية المعتمدة داخل الشركة، ارتفع مستوى اهتمام المدقق الخارجي بتوسيع نطاق اختبارات نظم المعلومات والضوابط الرقمية.

2. تحليل الانحدار لقياس الأثر

جدول (4): أثر نضج الأمن السيبراني على جودة التدقيق الخارجي

المتغير المستقل	Beta	T-value	R^2	Sig.
آليات وبرامج الأمن السيبراني	0.66	7.21	0.49	0.000

المصدر: من اعداد الباحثين

يوضح جدول(4)أن آليات وبرامج الأمن السيبراني تفسر نحو 49% من التغيرات في جودة التدقيق الخارجي، مما يؤكد أن الأمن السيبراني لم يعد عنصرًا تقنيًا فقط، بل أصبح عاملًا حاسمًا في رفع كفاءة ومصداقية عملية التدقيق الخارجي.

الاستنتاجات والتوصيات

أولًا: الاستنتاجات

1. تحقق مستوى متوسط إلى مرتفع من نضج الأمن السيبراني في الشركات المدرجة: أظهرت نتائج الدراسة أن الشركات المدرجة في سوق العراق للأوراق المالية تعتمد بشكل واسع على الآليات الأساسية للأمن السيبراني، مثل جدران الحماية وأنظمة مكافحة البرمجيات الخبيثة وأنظمة النسخ الاحتياطي، حيث تجاوزت نسب التطبيق 80% في معظم الشركات. إلا أن هذا النضج يتركز في الجانب الوقائي التقني، في مقابل ضعف نسبي في تبني الأنظمة التحليلية المتقدمة مثل منصات إدارة الأحداث الأمنية (SIEM) وبرامج التدريب السيبراني، مما يشير إلى أن نضج الأمن السيبراني لا يزال في مرحلة تشغيلية أكثر منه استراتيجية.
2. تركز جودة التدقيق الخارجي على الإجراءات التقليدية مع محدودية دمج البعد السيبراني: بينت النتائج أن إجراءات التدقيق الخارجي الأساسية، كالتخطيط المبني على المخاطر واختبار الضوابط الداخلية، تطبق بمستويات مرتفعة في الشركات المدرجة. في المقابل، أظهرت إجراءات تدقيق نظم المعلومات وتقييم ضوابط الأمن السيبراني مستويات تطبيق متوسطة إلى منخفضة، الأمر الذي يعكس فجوة بين تطور المخاطر الرقمية المتزايدة وبين نطاق التدقيق الخارجي المطبق فعليًا في البيئة العراقية.
3. وجود علاقة ارتباط موجبة قوية بين نضج الأمن السيبراني وجودة التدقيق الخارجي: أكدت نتائج التحليل الإحصائي وجود علاقة ارتباط موجبة قوية ذات دلالة إحصائية بين عدد آليات وبرامج الأمن السيبراني المعتمدة وبين عدد وعمق إجراءات التدقيق الخارجي. ويعني ذلك أن الشركات التي تمتلك بنية سيبرانية أكثر نضجًا توفر بيئة معلوماتية أكثر موثوقية، مما يسهل على المدقق الخارجي توسيع نطاق اختبارات التدقيق وتحسين جودة الحكم المهني.
4. الأمن السيبراني يمثل عاملًا مؤثرًا جوهريًا في جودة التدقيق الخارجي: أظهرت نتائج تحليل الانحدار أن نضج الأمن السيبراني يفسر ما يقارب 49% من التغيرات في جودة التدقيق الخارجي وهو ما يدل على أن الأمن السيبراني أصبح أحد المحددات الرئيسية لجودة التدقيق في بيئة الأعمال

الرقمية، ولم يعد عنصرًا داعمًا ثانويًا كما كان في النماذج التقليدية للتدقيق.

5. ضعف التدريب السيبراني ينعكس سلبًا على جودة التقارير التدقيقية: بينت النتائج أن انخفاض مستويات التدريب السيبراني للموظفين يترافق مع انخفاض نسبي في جودة تقارير التدقيق الخارجي، مما يؤكد أن العنصر البشري يمثل حلقة محورية في تعزيز فعالية الضوابط السيبرانية وموثوقية نظم المعلومات المحاسبية.

ثانيًا: التوصيات

1. تعزيز التحول من الأمن السيبراني الوقائي إلى الأمن السيبراني الاستباقي: توصي الدراسة بضرورة انتقال الشركات المدرجة من الاكتفاء بالحلول الوقائية التقليدية إلى تبني الأنظمة التحليلية المتقدمة، مثل منصات (SIEM) وأنظمة تحليل السلوك، بما يسهم في رفع مستوى النضج السيبراني وتعزيز قدرة الشركات على اكتشاف المخاطر الرقمية قبل وقوعها.

2. دمج الأمن السيبراني ضمن نطاق التدقيق الخارجي بشكل رسمي: توصي الدراسة مكاتب التدقيق الخارجي بضرورة إدراج تقييم ضوابط الأمن السيبراني وتدقيق نظم المعلومات المحاسبية ضمن برامج التدقيق السنوية، بوصفها جزءًا لا يتجزأ من التدقيق المبني على المخاطر، وبما ينسجم مع المعايير الدولية الحديثة للتدقيق.

3. رفع كفاءة المدققين الخارجيين في مجال التدقيق الرقمي: توصي الدراسة الهيئات المهنية بضرورة تطوير مهارات المدققين الخارجيين في مجالات الأمن السيبراني، وتحليل البيانات، واستخدام أدوات التدقيق الإلكتروني (CAATs)، بما يعزز قدرتهم على التعامل مع بيئات الأعمال الرقمية المعقدة.

4. تعزيز برامج التدريب والتوعية السيبرانية داخل الشركات: توصي الدراسة إدارات الشركات المدرجة بزيادة الاستثمار في برامج التدريب السيبراني المستمر للموظفين، نظرًا لدوره المحوري في تقليل المخاطر التشغيلية وتحسين جودة نظم المعلومات، الأمر الذي ينعكس إيجابًا على نتائج التدقيق الخارجي.

5. دور الجهات الرقابية والتنظيمية: توصي الدراسة هيئة الأوراق المالية وسوق العراق للأوراق المالية بضرورة إصدار إرشادات تنظيمية تلزم الشركات بالإفصاح عن مستوى نضج الأمن السيبراني، وربط ذلك بمتطلبات الحوكمة وجودة التقارير المالية، بما يعزز الشفافية والثقة في السوق المالي.

المصادر Reference

1.DeAngelo, L. E. (1981). Auditor size and audit quality. Journal of accounting and economics, 3(3), 183-199.

2.Francis, J. R. (2011). A framework for understanding and researching audit quality. Auditing: A journal of practice & theory, 30(2), 125-152.

3.Arens, A. A., Elder, R. J., Beasley, M. S., & Hogan, C. E. (2017). Auditing and assurance services.

4.Drašček, M., Slapničar, S., Vuko, T., & Čular, M. (2022). How Effective Is Your Cybersecurity Audit? ISACA journal, 3, 1-6.

5.Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

6.Cybersecurity, C. I. (2018). Framework for infrastructure cybersecurity. URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP, 4162018(7).

7.ISACA. (2019). Cybersecurity audit guidelines. ISACA.

8.KPMG. (2020). Cyber security risk and assurance. KPMG International.

9.Arens, A. A., Elder, R. J., Beasley, M. S., & Hogan, C. E. (2017). Auditing and assurance services.

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