

إجراءات مقترحة لإمكانية مساهمة مراقب الحسابات في الحد من المخاطر السيبرانية

Proposed actions for the possibility of an auditor contributing to reducing cyber risks

الباحثة: مروة قتيبة محمد الدباغ

أ.د. زياد هاشم السقا

جامعة الموصل/ كلية الإدارة والاقتصاد/ قسم المحاسبة – ديوان الرقابة المالية الاتحادي/ نينوى

E-mail: zyad_hashim@uomosul.edu.iq

تاريخ النشر: 2026/07/22

تاريخ القبول: 2026/05/08

تاريخ الاستلام: 2026/01/15

ملخص

تناول البحث مناقشة مفهوم المخاطر السيبرانية وأهميتها في عمل مراقب الحسابات مع توضيح دور مراقب الحسابات في إمكانية الحد من المخاطر السيبرانية، ومن ثم تحديد مجموعة من الإجراءات اللازمة لذلك والتي يمكن أن يسترشد بها مراقب الحسابات عند عمله في بيئة الأمن السيبراني، حيث اتضح أن المخاطر السيبرانية تُشكّل تحديًا كبيرًا يهدد الأفراد والوحدات على حد سواء وهو يعكس مدى التعقيد الذي ينطوي عليه الأمن السيبراني في العصر الحديث، كما أن تصنيف المخاطر السيبرانية يتركز على الدوافع المختلفة مثل المكاسب المالية، التجسس، أو الإرهاب، مما يعكس تنوع الهجمات السيبرانية واختلاف طبيعتها بناءً على الأهداف، فضلاً عن أن المخاطر السيبرانية لم تعد مجرد تهديدات تقنية محصورة في نطاق نظم المعلومات، بل أصبحت تمثل أحد أبرز محددات الاستقرار المالي والتشغيلي للوحدات الاقتصادية، خاصة مع توسّع الاعتماد على البيئة الرقمية، كما أن آثار هذه المخاطر تتجاوز الخسائر المباشرة لتُهدد بفقدان الثقة المؤسسية والإضرار بالحوكمة الداخلية، مما يستلزم من الوحدات الاقتصادية تعزيز استثماراتها في الأمن السيبراني ليس فقط كإجراء دفاعي، بل كجزء من إستراتيجية إدارة المخاطر الشاملة، لضمان الاستدامة وتعزيز التنافسية في ظل بيئة أعمال تتسم بالتغير السريع والتهديدات المتطورة.

وفي ضوء أطر ومعايير الأمن السيبراني الدولية التي تعد بمثابة أدوات مرجعية تساعد الدول والوحدات في بناء أنظمة متكاملة لحماية بياناتها وبُناها التحتية الحيوية، كما أن هذه الأطر تعمل على توحيد المفاهيم والممارسات وتقديم إرشادات شاملة لتقييم وتحسين الأداء الأمني، بما يضمن حماية الأصول الرقمية والامتثال للمتطلبات القانونية والتنظيمية، فقد تم تحديد مجموعة من الإجراءات العامة والإجراءات العملية التي يمكن أن يقوم بها مراقبو الحسابات ويسترشدون بها في سبيل أداء عملهم في بيئة الأمن السيبراني وبما يمكن أن يسهم في الحد من المخاطر السيبرانية في منظمات الأعمال التي يدققون حساباتها.

الكلمات المفتاحية: تدقيق الحسابات، الأمن السيبراني، المخاطر السيبرانية.

Abstract:

The research addressed the concept of cyber risks and their importance in the work of the auditor, clarifying the auditor's role in mitigating cyber risks. It then identified a set of procedures necessary for auditing cyber risks, which the auditor can use as a guide when working in a cyber-security environment. It became clear that cyber risks pose a significant challenge that threatens both individuals and entities, reflecting the complexity of cybersecurity in the modern era. The classification of cyber risks focuses on different motives such as financial gains, espionage, or terrorism, reflecting the diversity of cyber-attacks and their varying nature based on objectives. Moreover, cyber risks are no longer merely technical threats confined to the scope of information systems, but have become one of the most prominent determinants of the financial and operational

stability of economic units, especially with the increasing reliance on the digital environment. The effects of these risks extend beyond direct losses, threatening institutional trust and undermining internal governance. This necessitates that economic entities enhance their investments in cyber security not only as a defensive measure but also as part of a comprehensive risk management strategy. This is crucial for ensuring sustainability and fostering competitiveness in a rapidly changing business environment characterized by evolving threats.

Given the international cyber security frameworks and standards, which serve as reference tools to assist countries and entities in building integrated systems to protect their data and critical infrastructure, and which unify concepts and practices while providing comprehensive guidance for assessing and improving security performance—thus ensuring the protection of digital assets and compliance with legal and regulatory requirements—a set of general and practical procedures has been identified. These procedures can guide auditors in their work within the cyber security environment and contribute to mitigating cyber risks in the organizations they audit

Keywords: Auditing, Cyber security, Cyber Risks.

* المؤلف المرسل: زياد هاشم السقا، E-mail: zyad_hashim@uomosul.edu.iq

1. مقدمة

في ظل التطورات المتسارعة والمستمرة لاستخدام تقنيات المعلومات في منظمات الأعمال المختلفة فقد ظهرت العديد من التحديات التي تواجه تلك المنظمات في تحقيق أمن المعلومات لديها بصورة عامة والأمن السيبراني بصورة خاصة، حيث أن العمل في بيئة الأمن السيبراني قد أدى إلى زيادة الهجمات الإلكترونية ومحاولات إختراق النظم الالكترونية لتحقيق مآرب عدة قد تسعى إلى منظمات الأعمال، مما أدى إلى ضرورة الاهتمام بدور مراقبي الحسابات في إمكانية مساهمتهم من خلال عملهم في الحد من المخاطر السيبرانية التي تتعرض لها منظمات الأعمال وإبلاغ الجهات ذات المصلحة معها بمدى إلزام منظمات الأعمال بما يحقق الأمن السيبراني بسبب إستخدامها تقنيات المعلومات في أعمالها المختلفة.

واعتمادا على ما سبق فقد تم تحديد مشكلة البحث بتساؤل رئيس هو: ما هي الإجراءات المناسبة التي يمكن من خلالها مساهمة مراقبي الحسابات في الحد من المخاطر السيبرانية التي يمكن أن تتعرض لها منظمات الأعمال المختلفة؟ وتأتي أهمية البحث من حيث:

- زيادة الهجمات الإلكترونية والاختراقات للنظم الالكترونية التي تتعامل معها منظمات الأعمال.
- الحاجة الى الافصاح المحاسبي عن المخاطر السيبرانية.
- ضرورة توفير ما يمكن لمراقبي الحسابات من الاسترشاد به ليكون بإمكانهم القيام بعملهم في ظل التحديات الجديدة.

وعليه يهدف البحث إلى:

- مناقشة مفهوم المخاطر السيبرانية وأهميتها في عمل مراقب الحسابات؛
- تحديد دور مراقب الحسابات في إمكانية الحد من المخاطر السيبرانية؛
- تحديد مجموعة من الإجراءات اللازمة لتدقيق المخاطر السيبرانية.

وللإجابة عن التساؤل المطروح في مشكلة البحث وتحقيق أهدافه، يعتمد البحث على فرضية رئيسة هي: يمكن تحديد مجموعة من الاجراءات التي يسترشد بها مراقبي الحسابات في عملهم في بيئة الأمن السيبراني والحد من المخاطر السيبرانية. ويعتمد البحث على المنهج الاستنباطي من خلال ما تناوله الرسائل والأطاريح والبحوث العلمية ذات العلاقة بموضوع البحث.

وعليه فقد تم تقسيم البحث إلى ثلاثة مباحث هي:

- ❖ مفهوم المخاطر السيبرانية وأهميتها في عمل مراقب الحسابات؛
- ❖ دور مراقب الحسابات في الحد من المخاطر السيبرانية؛
- ❖ إجراءات مقترحة لتدقيق المخاطر السيبرانية.

2. مفهوم المخاطر السيبرانية وأهميتها في عمل مراقب الحسابات

في ظل التوسع المتسارع في تبني تقنيات المعلومات والاتصالات ضمن بيئة الأعمال، أضحت المخاطر السيبرانية من بين التحديات الأكثر إلحاحًا التي تواجه الوحدات الاقتصادية بمختلف أنواعها (Ernst & Young, 2021, 18).

وتؤثر المخاطر السيبرانية بشكل مباشر على السمعة والثقة المالية للوحدات الاقتصادية. فالهجمات الناجمة يمكن أن تؤدي إلى خسائر مالية كبيرة، وتوقف العمليات التجارية، وفقدان البيانات الحساسة للعملاء وهذا يجعل من الضروري للوحدات الاقتصادية أن تستثمر في الأنظمة الأمنية المتقدمة وتحديث سياساتها وإجراءاتها بشكل مستمر.

وفي ضوء ذلك لا بد من بيان المقصود بها ووجهات نظر الكتاب والباحثين بصدد هذا، إذ يمكن تعريف المخاطر السيبرانية على أنها خطر الخسارة المالية و/أو التعطيل أو الضرر الذي يلحق بسمعة الوحدة الاقتصادية من فشل أنظمة تقنية المعلومات الخاصة بها. هناك عدد من الأطر وطرق التقييم لتحديد خطر الإنترنت. ربما تم بالفعل اختيار واحد أو أكثر والموافقة عليه من قبل الوحدة الاقتصادية. إذا لم يكن الأمر كذلك، فمن المهم اختيار واحد والتصديق عليه لاستخدامه في تقييم المخاطر وعملية قياس الأداء. اختيار تقييم المخاطر على مستوى الوحدة ستسهل العملية قبول النتائج من قبل الهيئات الإدارية (Siegel & Sweeney, 2020: 96).

أما الاستراتيجية الوطنية للأمن السيبراني العراقية فقد عرفتها بأنها احتمالية وجود تهديد وهشاشة في الفضاء الإلكتروني الخاص بالعراق يعتمد على إلحاق الضرر بأمن نظم المعلومات وهياكل البنى التحتية المعلوماتية الأساسية من الثغرات والتهديدات الموجودة في الفضاءات السحابية (استراتيجية الأمن السيبراني العراقي، 2019).

وترتبط الهجمات السيبرانية مباشرة بحدثين مهمين يتمثل الأول: باستحداث أجهزة الحاسوب في منتصف الخمسينيات من القرن المنصرم كأداة لمعالجة وحفظ المعلومات رقمياً، وقد تطورت بصورة جذرية في العقود اللاحقة حتى أصبح جهاز الكمبيوتر أساساً في العمل في الكثير من الوحدات الاقتصادية الخاصة والعامة فضلاً عن الحياة اليومية والافراد، أما الحدث الثاني: فهو بظهور الشبكة العنكبوتية والذي أحدث انقلاباً مثيراً من حيث التواصل ونقل المعلومات بسرعة فائقة عن طريق سبل البيانات المرسلة عبر الاثير (فرحات، 2019: 91).

وفقاً للمعهد الوطني للمعايير والتقنية (NIST)، فإن الخطر السيبراني يمثل احتمالية وقوع ظرف أو حدث معين من شأنه أن يؤثر سلباً على الكيان، ويُقاس عادةً بدرجة التهديد الناشئ عن هذا الحدث، والآثار الناتجة عنه عند تحققه (NIST, 2022, 5) ويُبرز هذا التعريف العلاقة التفاعلية بين الاحتمالية والآثار السلبية، مما يستلزم تقييماً مستمراً لطبيعة التهديدات المحيطة بالمنشأة.

وتمثل الهجمات السيبرانية عدداً من المخاطر السيبرانية التي تضم بشكل خاص الآتي (الكرعاوي، 2024: 463):

- مخاطر سيبرانية تتعلق بالسرية: حيث تنشأ عندما يتم الكشف عن المعلومات الخاصة داخل الوحدة الاقتصادية إلى طرف ثالث كما في حالة حدوث اختراق البيانات؛
- مخاطر سيبرانية تتعلق بالنزاهة: التي تتعلق بإساءة استخدام الأنظمة كما هو الحال بالنسبة للاحتيال؛
- مخاطر سيبرانية تتعلق باستمرارية الأداء: تلخص في تعطل أو التوقف عن ممارسة الأعمال.

وهذه الأنواع الثلاثة من المخاطر السيبرانية لها تأثيرات مختلفة ومباشرة على الوحدات، إذ تؤدي لتعطيل الأعمال وتحقيق خسارة وتعطل في تحقيق الأهداف، والتحقيق في تأثيرات اختراق البيانات قد يستغرق وقتاً طويلاً، وهذا ينتج عنه أضرار معنوية تمس السمعة فضلاً عن تكاليف التقاضي، وفي أعقاب الهجمات الالكترونية قد يكون خطر فقدان الثقة عالياً بالنسبة للقطاع المالي وذلك، لاعتماد الوحدات المالية على ثقة زبائنها (البغدادى، 2021، 1464).

كما اتفقت دراستي (شحاته والبردان، 2021، 10) (السواح، 2021، 511) على تصنيف المخاطر السيبرانية إلى ثلاثة أنواع من المخاطر على النحو الآتي:

- **المخاطر المتعلقة بتأمين البيانات والمعلومات:** وهي المخاطر الناشئة من تخزين البيانات والمعلومات للأفراد والوحدات ومن الممكن تعرضها إلى الاختراق أو نقلها للمنافسين؛
- **المخاطر المتعلقة بانتهاك الخصوصية:** وهي المخاطر الناتجة عن مخاطر سرقة البيانات الشخصية؛
- **المخاطر المتعلقة بانتهاك حقوق الملكية الفكرية:** وتتمثل في المخاطر المتعلقة بحقوق الملكية الفكرية نتيجة نسخ الوسائط الرقمية وإعادة إنتاجها وتأخر مستوى التشريعات القانونية.

وعند تصنيف المخاطر السيبرانية التي قد تتعرض لها الوحدات الاقتصادية، يتضح أن المخاطر لا تتوزع بالتساوي بين جميع القطاعات، بل تختلف بحسب طبيعة الصناعة، وحجم البيانات الحساسة المتداولة، ومستوى الاعتماد على التقنية.

وقد أشارت دراسة تابعة للمنتدى الاقتصادي العالمي (WEF World Economic Forum -) إلى أن القطاعات المالية والطبية والحكومية تُعد من أكثر القطاعات تعرضاً للهجمات السيبرانية الموجهة نظراً لقيمتها المعلوماتية العالية، وتتوزع دوافع هذه الهجمات ما بين (الابتزاز المالي كالهجمات باستخدام برامج الفدية، والتجسس، والعبث بالسمعة أو تدمير البيانات، والاستيلاء على الحسابات أو تشويه المواقع، وتعطيل الشبكات أو الاتصالات) (WEF, 2021, 17) كما أن هناك أنواع أخرى من الهجمات السيبرانية تتمثل بالآتي:

- **احتيال المعلومات والبيانات:** وهو التعديل غير المصرح به للبيانات قبل أو أثناء تسجيل الدخول إلى نظام الكمبيوتر واستعادتها بعد اكتمال العملية والقرصنة، وتسمى الوصول غير المصرح به إلى أنظمة الكمبيوتر؛
- **وانتشار الفيروسات:** ويتم إضافة برامج ضارة إلى نظام آخر بغرض تدمير النظام المهاجم، والقنبلة المنطقية، وتعمل هذه البرامج الضارة بشكل مشابه للقنبلة الموقوتة؛
- **مخاطر الأمن الرقمي:** وهي المخاطر التشغيلية والمالية والمتعلقة بالسمعة وأصحاب المصلحة الناتجة عن تهديدات الأمن السيبراني، بما في ذلك مخاطر الانتهاكات الكبيرة للبيانات الناشئة عن الثغرات الداخلية؛
- **ومخاطر الاستراتيجية الرقمية:** المخاطر التشغيلية والمالية والسمعة وأصحاب المصلحة الناتجة عن الانتقال إلى نموذج الأعمال الرقمية يشار إليه أيضاً بالتحول الرقمي وزيادة الاعتماد على البيانات.

وقامت لجنة التقنية في الاتحاد الدولي للمحاسبين (International Federation of Accountants- IFAC) بتصنيفها إلى ثلاث أنواع هي: (مخاطر البنية التحتية لنظم تقنية المعلومات مخاطر تطبيق تقنية المعلومات- مخاطر تقنية المعلومات الخاصة بأعمال المنشأة) (السواح، 2021، 494).

ويشير (سالم، 2023: 981) إلى أنه بسبب نمو تقنية الانترنت حصلت الجرائم السيبرانية على اهتمام كبير مقارنة بالجرائم التقليدية حيث يختلف مفهوم الجريمة السيبرانية اختلافاً كبيراً عن المفهوم التقليدي للجريمة وذلك بسبب وجود العديد من الخصائص المميزة للجرائم السيبرانية ومن أهم هذه الخصائص:

❖ **الأشخاص ذوي المعرفة المتخصصة:** الجرائم السيبرانية هي جرائم يمكن ارتكابها فقط من خلال التقنية لذا من أجل ارتكاب هذا النوع من الجرائم يجب أن يكون لدى الشخص مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب وماهر جدا فيما يتعلق بالإنترنت وأجهزة الكمبيوتر.

❖ **الامتداد العالمي:** في الفضاء السيبراني لا يوجد حدود وان الجريمة السيبرانية هي جريمة ذات بعد دولي أي أنها عابرة للحدود وهذا يعني أن مرتكبي جرائم الأمن السيبراني لديهم القدرة على ارتكاب الجرائم عن بعد والتأثير على الضحايا في أي مكان في العالم ويعتبر هذا أحد الخصائص الرئيسية لجرائم الأمن السيبراني مما يجعلها تختلف عن جميع أنواع الجرائم التقليدية وأيضاً يجعلها معقدة للغاية.

❖ **صعوبة جمع الأدلة:** جزء أساسي من الإفصاح عن الجرائم هو جمع ومعالجة الأدلة الرقمية ولكن من الصعب للغاية جمع الأدلة فيما يتعلق بالجرائم السيبرانية ويرجع ذلك إلى أسباب عديدة على سبيل المثال طبيعة بيانات الكمبيوتر نفسها حيث تعتبر سريعة الزوال كذلك الامتداد الدولي للجرائم السيبرانية واختلاف القوانين بين الدول عليه هناك صعوبة في التحقق فيها وكذلك إثباتها أمام القضاء نظراً لطبيعتها.

❖ **حجم آثار جرائم الأمن السيبراني لا يمكن تصوره:** تعتبر جرائم الأمن السيبراني أكبر تحديد يواجه المنشآت في الوقت الحالي وواحد من أكبر التحديات التي ستواجه البشرية وذلك على المدى العقدين المقبلين وبالنسبة للمنشآت فإن التكاليف والخسائر المرتبطة بالجرائم السيبرانية ضخمة إلى حد لا يمكن تخيله حيث قد تسبب في تلف البيانات أو سرقتها، سرقة الأموال، الملكية الفكرية، البيانات الشخصية والمالية، تعطيل أعمال الوحدة بعد تعرضها لهجوم سيبراني كالأضرار بسعة الوحدة وفقدان الانتاجية وتغير أرقام البيانات في السجلات المخزنة في ذاكرة الحاسبات وغير ذلك من الآثار ويمكن أن تسبب الجرائم السيبرانية في كل ذلك دون أن يكون لها أي أثر خارجي مرئي.

ووفقاً لما طرح من آراء يمكن أن توصف المخاطر السيبرانية بأنها تهديد أو تحدٍ يستهدف البيانات المخزنة أو المنقولة على الأنظمة الرقمية أو الشبكات أو الأجهزة الإلكترونية أو الإنترنت، وقد يؤدي إلى خسارة مالية أو تعطيل الخدمة أو انتهاك الخصوصية أو الإضرار بسعة الوحدات والتي قد تؤدي إلى انهيارها.

وفي ضوء ما طرح وفي ظل هذه البيئة المتسارعة والمليئة بالمخاطر يتطلب بالفعل إدراج الأمن السيبراني كحجر أساس في أي وحدة لضمان وضع استراتيجية محكمة ضد المخاطر السيبرانية واعتماد ضوابط وعمليات واضحة وقوية مبنية على أساسيات هامة للأمن السيبراني على مستوى الوحدة كلها إذ تحتاج هذه الوحدات إلى هياكل وعمليات فاعلة تمكنها من تحقيق أهدافها.

وعليه فإن **المخاطر السيبرانية** تُشكّل تحدياً كبيراً يهدد الأفراد والوحدات على حد سواء وهو يعكس مدى التعقيد الذي ينطوي عليه الأمن السيبراني في العصر الحديث، كما يتضح أن تصنيف المخاطر السيبرانية يتركز على الدوافع المختلفة مثل المكاسب المالية، التجسس، أو الإرهاب، يعكس تنوع الهجمات السيبرانية واختلاف طبيعتها بناءً على الأهداف.

كما إن تصنيف المخاطر السيبرانية التي تواجهها المنشآت يعتمد على عدة عوامل مثل طبيعة المخاطر وإمكانية حدوث خسائر، إذ تباينت الآراء حول التصنيفات المختلفة للمخاطر السيبرانية في القطاعات إذ يحكم التصنيف لأنواع المخاطر على الدافع إذ يمكن أن يكون البحث عن المكاسب المالية أو التنافسية، وتدمير البيانات، مسح البيانات السيبرانية أو تشفيرها أو منع الوصول إليها، أو الدافع هو الابتزاز، وانقطاع الاتصالات، تعطيل الموقع الإلكتروني أو تعطيل الشبكة تشويه الموقع للاستيلاء على صفحات وسائل التواصل الاجتماعي والدافع هو الابتزاز أو التجسس، حيث يرى (ذياب، 2024: 44) أن أهم الأسباب التي تزيد من وقوع المخاطر السيبرانية نجد أن بعضها يكون بسبب أخطاء تحدث من الأفراد والعاملين في الوحدة الاقتصادية ومشكلات تقنية، وفيما يأتي بعض العوامل التي تزيد من المخاطر السيبرانية:

■ وقوع عطل في الشبكات ينجم عنه فقدان بيانات مهمة.

- استخدام أجهزة الوحدات من أماكن بعيدة؛
- عدم الاطلاع على سياسات الأمن السيبراني؛
- إهمال تحديث كلمة المرور باستمرار؛
- العبث من قبل موظفين غير مختصين في نظام الأمن السيبراني؛
- استخدام أجهزة الوحدة الاقتصادية في إجراء المعاملات البنكية مثل تحويل الأموال؛
- الوصول إلى النظام الإلكتروني للأمن السيبراني من مواقع أخرى من قبل المستخدمين.

وبذلك تعدد مصادر المخاطر السيبرانية التي تهدد استقرار وأمن الوحدات الاقتصادية، ويمكن تصنيفها إلى أربعة محاور رئيسية وهي متداخلة وتؤثر بشكل مباشر على فعالية أنظمة المعلومات وأمنها وهذه المصادر هي:

❖ **المصادر البشرية:** تُعد الأخطاء البشرية وسوء السلوك من أبرز العوامل المسببة للهجمات السيبرانية، سواء كانت ناتجة عن الجهل أو الإهمال أو النية الخبيثة، فوفقاً لتقرير (Verizon Data Breach Investigations Report) هو تقرير سنوي تصدره شركة (Verizon) الأمريكية وهي واحدة من أكبر شركات الاتصالات في العالم إذ يُعد تقريرها من أهم المصادر الموثوقة في تحليل أنماط اختراق البيانات والانتهاكات الأمنية التي تتعرض لها الوحدات في مختلف القطاعات فإن 82% من الخروقات الأمنية تعود إلى العامل البشري، سواء عبر رسائل التصيد الاحتيالي أو استخدام كلمات مرور ضعيفة، كما أن غياب التوعية أو ضعف ثقافة الأمن الرقمي يُفاقم هذه المخاطر (Verizon, 2022, 7).

❖ **المصادر التقنية:** تتمثل في الثغرات البرمجية، وضعف التحديثات الأمنية، وسوء تكوين الشبكات، مما يُتيح للمهاجمين استغلال تلك الفجوات، وتشير دراسة (Grimes, 2019, 153) إلى أن عدم تصحيح الثغرات هو أحد أهم مسببات الهجمات على الأنظمة، إلى جانب استخدام أنظمة قديمة غير مدعومة.

❖ **المصادر التنظيمية والإدارية:** غالباً ما تنشأ المخاطر السيبرانية نتيجة لغياب السياسات الأمنية الواضحة أو عدم تطبيقها بصرامة، ووفقاً لتقرير صادر عن جمعية التدقيق والرقابة على نظم المعلومات (ISACA) فإن العديد من الوحدات تفشل في تطبيق إطار حوكمة فعال للأمن السيبراني، مما يؤدي إلى ضعف في الرقابة الداخلية وسهولة استهدافها (ISACA, 2021, 23).

❖ **المصادر الخارجية:** تشمل هذه الفئة الجهات الخارجية التي تستهدف الأنظمة، مثل المخترقين، ومجموعات الجريمة المنظمة، وأطراف دولية معادية، وأن الهجمات التي تُشن من خارج الوحدة باتت أكثر تعقيداً وتعتمد على أدوات متطورة يصعب اكتشافها بسرعة (IBM, 2023, 12).

وتتفاقم هذه المخاطر عندما تتقاطع تلك المصادر وتغيب الاستجابة الفعالة، ما يستدعي وجود نموذج متكامل لتقييم ومعالجة المخاطر السيبرانية يأخذ في الحسبان الطبيعة الديناميكية لهذه التهديدات.

وتُشكل المخاطر السيبرانية تحدياً متصاعداً على الوحدات الاقتصادية في ظل الاعتماد الواسع على نظم المعلومات الرقمية، مما يجعل هذه الوحدات عرضة لآثار متعددة تمس الجوانب المالية والتشغيلية والسمعية والقانونية. وتُظهر الدراسات أن الهجمات السيبرانية لا تؤدي فقط إلى خسائر مادية مباشرة، بل تسبب أيضاً في اضطرابات مستمرة قد تُقوّض استمرارية الأعمال وتهدد بقاء الكيان الاقتصادي، من أبرز الآثار هذه الآثار ما يأتي:

❖ **الآثار المالية المباشرة:** تمثل في خسائر فورية ناجمة عن سرقة الأموال، أو دفع فديات كما في حالات هجمات، أو تكاليف استعادة البيانات والأنظمة. ووفقاً لتقرير (International Business Machines- IBM)، بلغ متوسط تكلفة اختراق البيانات عالمياً حوالي 4.45 مليون دولار للمنشأة الواحدة (IBM, 2023, 8).

- ❖ **انقطاع العمليات التشغيلية:** تؤدي الهجمات السيبرانية إلى توقف الأنظمة الحيوية داخل المنشأة، مما يُعطّل سلسلة التوريد، والمعاملات التجارية، ويؤثر على كفاءة الأداء التشغيلي، وهو ما يُهدد بعجز قصير أو طويل الأجل في تلبية الطلبات.
 - ❖ **الإضرار بالسمعة والثقة:** غالبًا ما تؤدي الحوادث السيبرانية إلى فقدان ثقة الزبائن والمستثمرين، خصوصًا في حالات تسريب البيانات الشخصية أو المالية الحساسة، مما يؤثر على القيمة السوقية للمنشأة (ENISA, 2022, 17).
 - ❖ **التعرض للمساءلة القانونية والتنظيمية:** في حال عدم التزام المنشأة بالضوابط التنظيمية المتعلقة بحماية البيانات (مثل (GDPR - General Data Protection Regulation) أو قوانين الخصوصية المحلية)، فإنها قد تتعرض لغرامات قانونية وعقوبات صارمة، وقد تصل إلى نسب مئوية من الإيرادات السنوية.
 - ❖ **زيادة التكاليف التأمينية والتدقيق:** تؤدي المخاطر السيبرانية إلى ارتفاع في أقساط التأمين على أمن المعلومات، كما تتطلب المنشأة تخصيص موارد أكبر للتدقيق والتقييم الأمني الدوري (PWC, 2022, 11).
 - ❖ **فقدان البيانات:** تتسبب بعض الهجمات في تسريب أو تدمير بيانات ذات طابع استراتيجي أو بحثي، مما يؤدي إلى خسارة ميزة تنافسية أو اختلال في قرارات التخطيط طويلة الأمد.
 - ❖ **ضعف الامتثال والمراجعة الداخلية:** تشير بعض الدراسات إلى أن المخاطر السيبرانية تكشف ثغرات في الرقابة الداخلية ونظم الحوكمة، ما يدفع الوحدات إلى مراجعة سياساتها الأمنية وتحديث بنيتها التحتية التقنية بشكل عاجل (ISACA, 2021, 19).
- نستنتج مما سبق أن المخاطر السيبرانية لم تعد مجرد تهديدات تقنية محصورة في نطاق نظم المعلومات، بل أصبحت تمثل أحد أبرز محددات الاستقرار المالي والتشغيلي للوحدات الاقتصادية، خاصة مع توسع الاعتماد على البيئة الرقمية. كما أن آثار هذه المخاطر تتجاوز الخسائر المباشرة لتهديد بفقدان الثقة المؤسسية والإضرار بالحوكمة الداخلية، مما يستلزم من الوحدات الاقتصادية تعزيز استثماراتها في الأمن السيبراني ليس فقط كإجراء دفاعي، بل كجزء من استراتيجية إدارة المخاطر الشاملة، لضمان الاستدامة وتعزيز التنافسية في ظل بيئة أعمال تتسم بالتغير السريع والتهديدات المتطورة.

3. دور مراقب الحسابات في الحد من المخاطر السيبرانية

من خلال ما تطرق إليه الباحثون يمكن إستنباط مجموعة من الإجراءات التي يتطلب من مراقب الحسابات الأخذ بها وبما يمكن أن يساهم في تعزيز دوره في الحد من المخاطر السيبرانية، يعرضها الباحثان كما يلي:

1.3. فهم التعقيد التقني: وهو يتعلق بكل من: (KPMG, 2024, 3-5).

- ❖ **تنوع الهجمات السيبرانية:** التنوع في طبيعة وتكرار الهجمات السيبرانية يجعل من الصعب على مراقبي الحسابات مواكبة أحدث التهديدات وأساليب الهجوم. يجب على مراقبي الحسابات البقاء على اطلاع دائم بالتهديدات الجديدة والناشئة لتقييم فعالية الضوابط الأمنية الحالية. هذا يتطلب مستوى عالٍ من المعرفة التقنية والخبرة في مجال الأمن السيبراني.
- ❖ **تكامل الضوابط التقنية مع الإجراءات المالية:** يتطلب تقييم الإفصاح عن المخاطر السيبرانية من مراقبي الحسابات فهمًا عميقًا لكيفية تكامل الضوابط التقنية مع الضوابط المالية التقليدية، هذا يشمل فهم كيفية تأثير الثغرات الأمنية على البيانات المالية والإجراءات المحاسبية.

2.3. تقييم الأثر المالي للهجمات السيبرانية: من خلال:

- ❖ **تحديد الأهمية النسبية للهجمات السيبرانية،** حيث يجب على مراقبي الحسابات تقييم مدى تأثير الهجمات السيبرانية على الأداء المالي للوحدة الاقتصادية، ويتضمن تحليل الأثر المالي المباشر للهجمات وكذلك الأثر غير المباشر مثل فقدان الثقة من الزبائن والتأثير على سمعة الوحدة الاقتصادية (KPMG, 2024, 5).

ويعد تقدير الاهمية النسبية للأثار المالية الناجمة عنى الهجمات السيبرانية من القضايا الحديثة التي تزداد أهميتها من مسؤوليات مراقبي الحسابات، إذ ترتب عليها الحكم بشأن الحاجة الى الافصاح عنها؟ التقارير الماليه وفقاً للمعايير المهنية، ولذلك يجب على مراقبي الحسابات أن يقوموا بتحليل شامل لهذه الهجمات لتحديد مدى تأثيرها على الأداء المالي للوحدة الاقتصادية وضمان تقديم تقارير مالية دقيقة وموثوقة فان عليهم:

- يتعين على مراقبي الحسابات تقييم الأثر المالي المباشر للهجمات السيبرانية، هذا يشمل تحديد تكلفة الاستجابة للهجمات، مثل إصلاح الأنظمة المتضررة، واستعادة البيانات، وتوظيف خبراء الأمن السيبراني للتعامل مع التهديدات. بالإضافة إلى ذلك، قد تشمل التكلفة المباشرة فديات المدفوعة للقراصنة في حالة هجمات برامج الفدية، والتي يمكن أن تكون مبالغ كبيرة تؤثر على الربحية المالية للوحدة الاقتصادية (KPMG, 2024, 5)؛
- يجب على مراقبي الحسابات تحليل الأثر غير المباشر للهجمات السيبرانية، والذي يمكن أن يكون أكثر تعقيداً وتنوعاً. هذا يشمل تقييم تأثير فقدان الثقة من الزبائن، والذي يمكن أن يؤدي إلى خسارة الإيرادات نتيجة انتقال الزبائن إلى منافسين آخرين. سمعة الوحدة قد تتضرر بشكل كبير نتيجة للهجمات السيبرانية، مما يؤدي إلى تراجع قيمة العلامة التجارية وفقدان فرص الأعمال الجديدة. تقرير من PwC يشير إلى أن الوحدات الاقتصادية التي تتعرض لهجمات سيبرانية كبيرة يمكن أن تفقد ما يصل إلى 20% من قيمتها السوقية في الأسابيع التالية للهجوم بسبب فقدان الثقة والتأثير السلبي على السمعة (PwC, 2022, 12).
- يتعين على مراقبي الحسابات أخذ العوامل التنظيمية والقانونية في الاعتبار عند تحديد الأهمية النسبية للهجمات السيبرانية، وعليه فان الوحدات الاقتصادية قد تواجه غرامات وعقوبات من الهيئات التنظيمية إذا لم تكن تمثل متطلبات الإفصاح عن الحوادث السيبرانية أو إذا فشلت في حماية بيانات الزبائن بشكل كافٍ. هذه الغرامات يمكن أن تكون كبيرة وتؤثر بشكل ملحوظ على الوضع المالي للوحدة الاقتصادية (Deloitte, 2023, 15)، وأخيراً، يجب على مراقبي الحسابات أن يقوموا بتقييم التأثير على عمليات الوحدة اليومية. الهجمات السيبرانية يمكن أن تعطل الأنظمة والخدمات، مما يؤدي إلى توقف العمليات وفقدان الإنتاجية. هذا يمكن أن يؤثر على الأداء المالي من خلال انخفاض الإيرادات وزيادة التكاليف التشغيلية (EY, 2021, 18).
- الاعتماد على الأطر القائمة: يمكن لمراقبي الحسابات استخدام أطر تقييم الأهمية النسبية الموجودة لتحديد مدى تأثير الهجمات السيبرانية. هذا يشمل استخدام إطار تحليل المخاطر المعلوماتية (FAIR) لتقييم حجم الخسائر وتحديد التكلفة المالية للهجمات السيبرانية (KPMG, 2024, 5).

3.3. التعاون مع الفرق الفنية والتنظيمية

❖ **التعاون بين فرق الأمن السيبراني والمالية:** من المهم أن يتعاون مراقبو الحسابات مع الفرق الفنية والتنظيمية لفهم الإجراءات الأمنية الحالية وكيفية تأثيرها على البيانات المالية، ويجب أن يكون هناك تواصل مستمر بين فرق الأمن السيبراني والفرق المالية لضمان تكامل الإجراءات الأمنية مع الضوابط المالية (KPMG, 2024, 4-5).

❖ **توثيق العمليات الأمنية:** يجب على مراقبي الحسابات التأكد من توثيق جميع العمليات والإجراءات الأمنية بشكل مناسب. هذا يسهل تقييم فعالية الضوابط الأمنية ويضمن استجابة الوحدة بشكل مناسب للهجمات السيبرانية (KPMG, 2024, 6).

4.3. الامتثال للمتطلبات التنظيمية

❖ **فهم المتطلبات التنظيمية:** يتعين على مراقبي الحسابات فهم المتطلبات التنظيمية المتعلقة بالإفصاح عن المخاطر السيبرانية. هذا يشمل متابعة التغييرات في اللوائح والتأكد من أن الوحدات الاقتصادية تلتزم بالمتطلبات الحالية والجديدة (KPMG, 2024, 6).

❖ **تقييم مدى امتثال الوحدات الاقتصادية:** يجب على مراقبي الحسابات تقييم مدى امتثال الوحدات الاقتصادية للمتطلبات التنظيمية المتعلقة بالإفصاح عن المخاطر السيبرانية. هذا يشمل فحص السياسات والإجراءات الداخلية والتأكد من أنها تتوافق مع المتطلبات التنظيمية (KPMG, 2024, 7).

5.3. نقص الإرشادات والمعايير المحددة.

من التحديات الرئيسية التي يواجهها مراقبو الحسابات عند تقييم الإفصاح عن المخاطر السيبرانية هو نقص الإرشادات والمعايير المحددة التي يمكن الاعتماد عليها. على الرغم من وجود بعض الإرشادات العامة من الهيئات الرقابية مثل مجلس مراقبة محاسبة الوحدات الاقتصادية العامة (PCAOB) والمجلس الدولي لمعايير المراجعة والتأكد (IAASB)، إلا أن هذه الإرشادات غالبًا ما تكون غير كافية لتغطية كافة جوانب المخاطر السيبرانية وتقييم تأثيرها المالي بشكل دقيق. على سبيل المثال، يشير مجلس PCAOB إلى ضرورة تقييم المخاطر بشكل مستمر وتحديث الإجراءات بناءً على الأدلة الجديدة، لكن هذه الإرشادات قد لا تتطرق بشكل تفصيلي إلى كيفية التعامل مع التهديدات السيبرانية المتطورة (PCAOB, 2021, 33)، وإضافةً إلى ذلك تفتقر العديد من الوحدات الاقتصادية إلى توجيهات واضحة بشأن كيفية الإفصاح عن المخاطر السيبرانية في التقارير المالية، مما يجعل من الصعب على مراقبي الحسابات التأكد من مدى كفاية ودقة هذه الإفصاحات. نقص المعايير المحددة يعني أيضًا أن هناك تباينًا كبيرًا في كيفية الإفصاح عن المخاطر السيبرانية بين الوحدات الاقتصادية المختلفة، مما يزيد من صعوبة تقييم هذه الإفصاحات بشكل موحد ومقارنة فعالة بين الوحدات الاقتصادية (PCAOB, 2008, 34).

6.3. الاعتماد على متخصصين في الأمن السيبراني

نظرًا لتعقيد وتنوع المخاطر السيبرانية، غالبًا ما يحتاج مراقبو الحسابات إلى التعاون مع متخصصين في الأمن السيبراني لفهم وتقييم هذه المخاطر بشكل دقيق. هذا الاعتماد يمكن أن يشكل تحديًا بحد ذاته، حيث يحتاج المراقبون إلى التأكد من أن هؤلاء المتخصصين يمتلكون الكفاءة والخبرة اللازمة، وأن يتمتعوا بالموضوعية والاستقلالية المطلوبة لضمان تقييم موضوعي وشفاف (PCAOB, 2021, 33).

فضلاً عما تقدم، يمكن أن يؤدي الاعتماد على متخصصين خارجيين إلى زيادة التكاليف وتعقيد عمليات التدقيق، خاصةً في الحالات التي تتطلب فحصًا مكثفًا وتقييمًا دقيقًا لأنظمة الأمان السيبراني والبنية التحتية التقنية للوحدات الاقتصادية.

أما مسؤولية مراقب الحسابات فتتعلق بالاطلاع على الأنشطة المتعلقة بالحسابات ومراقبتها من أجل التأكد من سرية وحفظ المعلومات الحساسة في الحسابات، كما ينبغي عليه الحد من تداول معلومات الحسابات الحساسة داخل الوحدات الاقتصادية أو الوحدات التي يعمل بها مراقب الحسابات ومن أجل تنفيذ هذا الدور بشكل فعال، فإن مراقب الحسابات يقوم بتحديد الحسابات الحساسة وتصنيفها بناءً على حساسية المعلومات المخزنة بها، كما يقوم بضبط الأذونات الخاصة بالوصول إلى هذه الحسابات وتحديد من يمكنه الوصول إليها ومن لا يمكنه؛ وفي حال اكتشاف أي انتهاك لسياسة الحسابات أو اكتشاف أي نشاط غير عادي، فإن مراقب الحسابات يجب أن يتخذ الإجراءات اللازمة بسرعة لإجراء التحقيقات اللازمة وتحديد السبب والمسؤول عن ذلك (دليل الاتحاد الدولي للمحاسبين المعايير الدولية للمراجعة، 2005، 274).

ومن الجدير بالذكر أن مراقب الحسابات ليس المسؤول الوحيد عن تحقيق سياسات أمن البيانات أو الوحدة، ولكنه يعتبر جزءاً مهماً من الفريق الذي يعمل على تحقيق هذه السياسات وتحديد المخاطر المحتملة، حيث أشار معيار التدقيق الدولي بالرقم 400 بأنه يجب على مراقب الحسابات القيام بتقييم المخاطر الجوهرية ومخاطر الرقابة للجوانب المادية في البيانات المالية في بيئة نظام المعلومات الالكتروني وذلك لأنها ربما يكون لها تأثير احتمالي عام وخاص على الأخطاء الجوهرية للبيانات المالية (Elifoglu, 2002, 67-71)، كما

أشار نفس المعيار الدولي في الفقرة 33 انه في بيئة نظام معلومات يستخدم الحاسوب فانه لا تتغير أهداف اختبارات الرقابة عنها في البيئة اليدوية ومع ذلك فان بعض إجراءات التدقيق قد تتغير وقد يجد المراقب نفسه مضطراً أو قد يفضل استعمال طرق التدقيق بمساعدة الكمبيوتر (دليل الاتحاد الدولي للمحاسبين المعايير الدولية للمراجعة، 2005، 275)، فضلاً عما أشار إليه معيار التدقيق الدولي رقم 401 في الفقرة 12 بأن: أهداف مراقب الحسابات الخاصة لا تتغير في حالة معالجة المعلومات الحاسوبية يدوياً أو الكترونياً ومع ذلك فان طرق تطبيق إجراءات التدقيق لجمع الأدلة قد تتأثر بطرق معالجة الحاسوب ويستطيع المراقب استعمال الإجراءات اليدوية للتدقيق أو طرق التدقيق بمساعدة الكمبيوتر أو استعمال الطريقتين معا لغرض الحصول على أدلة كافية". ومع: ذلك فإنه قد يكون من الصعب أو المستحيل على المراقب في النظم الحاسوبية التي تستخدم الكمبيوتر لمعالجة تطبيقات مهمة أن نحصل على معلومات معينة لفحصها أو للاستفسار عنها أو للتأكد منها بدون مساعدة الكمبيوتر (دليل الاتحاد الدولي للمحاسبين المعايير الدولية للمراجعة 2005: 287).

وعليه فإنه عندما تقوم الوحدات الاقتصادية بنقل عملية أو تخزين أو الوصول إلى معلومات الكترونياً فانه من غير العملي أو حتى من المستحيل تخفيض المخاطر بمستوى منخفض وبشكل مقبول فقط بواسطة إجراء اختبارات عينية لواحدة أو أكثر من البيانات المالية، كما أن المعيار (80) SAS يستنتج إن اختبارات الرقابة مع الاختبارات العينية يجب أن تكون كافية لتدعيم نتيجة التدقيق دراسة إجراءات التدقيق من قبل المجلس الأمريكي ASB قد وضعت الدليل الالكتروني إن وأمر التقييم المرتبطة به كما لم يجر أي تحديث رغم إن بعض الأحكام الإرشادية قد عاجلت بعض الاعتبارات الحاسوبية في مجال تقنية المعلومات لتقييم الرقابة منذ صدور المعيار (78SAS) إلا أن المعيار الجديد (94SAS) ملا هذه الفجوة لتحقيق أهداف معينة، حيث انه ومع إدراك أهمية تقنية المعلومات جاء المعيار الجديد معدلاً للمعيار (55 SAS) ولكنه لم يغير المبادئ الأساسية له ولم يغير أهميته كنموذج لمخاطر التدقيق ولكنه عالج آثار التقنيات على إجراءات المعايير الفنية (54, 2000 Helms & Lilly).

مما تقدم يتضح:

❖ أن أبرز التهديدات التي تواجه الوحدات الاقتصادية في العصر الحديث، نتيجة الاعتماد المتزايد على التقنية، مما أدى إلى تنوع وتعقيد الهجمات الإلكترونية، كالتجسس الإلكتروني، والبرمجيات الخبيثة، وهجمات الفدية. وقد فرض هذا الواقع تحديات جديدة على مهنة مراقب الحسابات، حيث بات من الضروري أن يشمل الإفصاح المحاسبي المخاطر السيبرانية، نظراً لتأثيرها المباشر وغير المباشر على الأداء المالي وسمعة الوحدات الاقتصادية.

❖ تزايد تعرض الوحدات الاقتصادية للمخاطر السيبرانية في البيئة الرقمية، خاصة مع الانتشار الواسع لتقنيات مثل إنترنت الأشياء (IOT) والعمل عن بُعد. وتُظهر الإحصاءات أن الجرائم السيبرانية تسبب بخسائر مالية ضخمة سنوياً، مما يستوجب من الوحدات الاقتصادية تعزيز أمنها الرقمي واستثماراتها في البنية التحتية السيبرانية.

❖ باتت جزءاً أساسياً في مهنة مراقب الحسابات، فقد أصبحت الجهات التنظيمية مثل FASB و PCAOB ومعايير التدقيق الدولية (ISA) تلزم الوحدات الاقتصادية بالإفصاح عن طبيعة المخاطر السيبرانية، وتأثيراتها، والإجراءات المتبعة لإدارتها، كما يتعين على المراقبين تقييم مدى كفاية هذه الإفصاحات ومطابقتها للمعايير.

❖ يواجه المدققون تحديات عدة، من أبرزها التعقيد التقني في فهم أنواع الهجمات، ودمج الضوابط التقنية مع المالية. كما يواجهون صعوبة في تقييم الأثر المالي للهجمات السيبرانية، إذ يتعين عليهم تقدير التكاليف المباشرة (كالاستجابة للحوادث، ودفع الفدية) والتكاليف غير المباشرة (كفقدان الثقة والسمعة السوقية)، إلى جانب تداعيات قانونية محتملة. كذلك، يتطلب التدقيق السيبراني تعاوناً فعالاً مع الفرق التقنية والتنظيمية داخل الوحدة، وتوثيقاً دقيقاً للإجراءات الأمنية المتبعة. ومن التحديات الأخرى التي يواجهها المدققون: نقص الإرشادات والمعايير المتخصصة في الإفصاح السيبراني، والاعتماد المتزايد على خبراء الأمن السيبراني، ما يطرح إشكاليات تتعلق بالكفاءة والاستقلالية والتكلفة.

❖ إن المسؤولية المهنية لمراقب الحسابات في ضوء هذه التحديات، لا سيما في تقييم أنظمة المعلومات، واستخدام الحاسوب في معالجة البيانات، وضمان سلامة الإجراءات المرتبطة بالأمن السيبراني. وقد أكدت معايير مثل ISA 400 و ISA 401 على ضرورة توظيف تقنيات التدقيق بمساعدة الحاسوب في البيئة الرقمية، مع الإشارة إلى أهمية الدليل الإلكتروني وفاعليته في دعم نتائج التدقيق.

4. إجراءات مقترحة لتدقيق المخاطر السيبرانية

تُعد أطر ومعايير الأمن السيبراني الدولية بمثابة أدوات مرجعية تساعد الدول والوحدات في بناء أنظمة متكاملة لحماية بياناتها وبُناها التحتية الحيوية. وتعمل هذه الأطر على توحيد المفاهيم والممارسات وتقديم إرشادات شاملة لتقييم وتحسين الأداء الأمني، بما يضمن حماية الأصول الرقمية والامتثال للمتطلبات القانونية والتنظيمية.

ومن أبرز هذه الأطر إطار المعهد الوطني الأمريكي للمعايير والتقنية والمعروف بـ (National Institute of Standards and Technology)، ويتضمن خمس وظائف رئيسية هي: (التعرف، الحماية، الكشف، الاستجابة، والتعافي) ويمثل هذا الإطار مرجعية معتمدة لتقييم النضج السيبراني في القطاعات الحكومية والخاصة، ويُستخدم على نطاق واسع عالمياً (NIST, 2018, 3). كما يُعد معيار ISO/IEC 27001 من أهم المعايير الدولية لإدارة أمن المعلومات، إذ يُقدّم نظاماً لإدارة أمن المعلومات ويهدف إلى ضمان السرية والتكامل والتوافر للمعلومات من خلال اعتماد ضوابط إدارية وتقنية وتنظيمية (ISO/IEC 27001, 2013, 1).

إلى جانب ذلك، طور مركز بناء القدرات العالمية للأمن السيبراني في جامعة أكسفورد (Global Cyber Security Capacity Centre – GCSCC) بالتعاون مع الاتحاد الدولي للاتصالات (ITU) إطاراً يُعرف باسم نموذج نضج قدرات الأمن السيبراني للدول (Cybersecurity Capacity Maturity Model – CMM)، ويشمل خمسة أبعاد: (السياسة والاستراتيجية، الثقافة والمجتمع، التعليم والتدريب، الأطر القانونية والتنظيمية، والتقنيات والمعايير) (GCSCC, 2016, 10).

وتجدر الإشارة أيضاً إلى اللائحة العامة لحماية البيانات (General Data Protection Regulation – GDPR) المعتمدة من قبل الاتحاد الأوروبي، والتي تُعد من أقوى الأطر التنظيمية لحماية خصوصية البيانات الشخصية، حيث تفرض التزامات صارمة على الوحدات بشأن كيفية جمع ومعالجة وتخزين البيانات (Voigt & Von dem Bussche, 2017, 45). على الرغم من تعدد الأطر والمعايير الدولية، إلا أن لكل منها نطاق تطبيق وأولوية مختلفة بحسب طبيعة الجهة أو الدولة. فعلى سبيل المثال، يُعد إطار (NIST) أكثر مناسبة للقطاعات الصناعية والبنى التحتية الحيوية، إذ يُركز على مراحل إدارة المخاطر بشكل دائري مرّن، مما يساعد الوحدات على تصميم برامج أمنية قابلة للتكيف مع طبيعة التهديدات المتغيرة (NIST, 2018, 7).

أما معيار ISO/IEC 27001، فيُعتبر مناسباً للوحدات الاقتصادية التي تبحث عن نظام شامل لإدارة أمن المعلومات يخضع للتدقيق ويؤهلها للحصول على شهادة اعتماد رسمية، وهو أمر يُعزز من سمعة الوحدة الاقتصادية خاصة في القطاعات الخدمية والمحاسبية التي تتطلب ضمانات عالية لحماية بيانات الزبائن والمستخدمين (ISO/IEC 27001, 2013, 4).

وبالنسبة لنموذج (CMM) الخاص بمركز أكسفورد، فإنه يُستخدم على نطاق واسع من قبل الدول النامية والهيئات الحكومية لتقييم جاهزيتها السيبرانية وتحديد نقاط الضعف في السياسات الوطنية، كما أنه يُعد مرجعاً أساسياً لتطوير استراتيجيات وطنية تتوافق مع قدرات كل دولة (GCSCC, 2016, 15).

من جهة أخرى، يُعالج الإطار القانوني الأوروبي (GDPR) الجوانب المتعلقة بحماية البيانات الشخصية بشكل صارم، ويُلزم الوحدات بتحديد قواعد واضحة للشفافية والموافقة على المعالجة، ما يجعله ذا أهمية كبرى في البيئات المحاسبية والبنكية والتأمينية، حيث

تكون البيانات الحساسة أساس العمليات (Voigt & Von dem Bussche, 2017, 78). وتعتمد إجراءات مراقب الحسابات على المجالات الخاضعة للتدقيق، ينبغي مراعاة المبادئ التالية عند تصميمها: (INTOSAI, 2023, 15)

- ينبغي أن تستند إجراءات التدقيق إلى الإطار والمعايير، سيضمن ذلك دعم أدلة التدقيق للتقييم وفقاً للمتطلبات المعمول بها.
- ينبغي تطوير إجراءات التدقيق بدعم من متخصصي السياسات والعمليات. سيضمن ذلك توافق أساليب التقييم المستخدمة مع أطر العمل مع توقعات متخصصي السياسات والعمليات.
- يجب أن تتوافق إجراءات التدقيق مع منهجية التقييم. إذا كانت النتيجة مبنية على تكوين محدد لضوابط الأمان، فيجب تطوير إجراءات تدقيق لفحص تكوينات الأمان وفقاً للمعيار المطلوب (مثل تكوينات كلمات المرور).
- ينبغي أن تُراعي إجراءات التدقيق استخدام أدوات الأمان، وخاصةً تلك المستخدمة داخل الوحدة الاقتصادية. يُمكن أن يُعزز استخدام هذه الأدوات فعالية وكفاءة إجراءات التدقيق. على سبيل المثال، قد يُقلل استخدام أداة فحص الثغرات الأمنية من الحاجة إلى الحصول على بيانات الأمان من الأنظمة عبر البرامج النصية. تُعد أدوات فحص الثغرات الأمنية وإدارة معلومات الأمان (SIEM) أدوات مفيدة لدمجها في إجراءات التدقيق، إذا كانت أدوات الأمان مُطورة داخلياً أو مُخصصة بشكل كبير، فقد يلزم تنفيذ إجراءات لتقييم سلامة أداة الأمان والتقارير المصدرة.

وفي ضوء ما تم مناقشته يقترح الباحثان مجموعة إجراءات يمكن أن تسهم في تعزيز دور مراقبي الحسابات في تدقيق المخاطر السيبرانية للوحدات المراد تدقيق حساباتها، وكما يلي:

أولاً: إجراءات عامة:

الإجراءات المقترحة	
1.	التأكد من حصر الجهة المسؤولة عن الإفصاح عن المخاطر السيبرانية
2.	تواجد ادارة مستقلة للمخاطر السيبرانية في الجهة الخاضعة للتدقيق وللإفصاح عنها
3.	اختيار افراد مؤهلين لتحديد المخاطر السيبرانية والإفصاح عنها
4.	تدريب مستمر وتطوير للأفراد لتحديد المخاطر السيبرانية وكيفية الإفصاح عنها
5.	أدلة متعلقة بممارسة مهام الفحص والتدقيق للإفصاح عن المخاطر السيبرانية؟
6.	تقويم فاعلية وملائمة نظام الرقابة الداخلية لغرض الإفصاح عن المخاطر السيبرانية
7.	توفر الاستقلالية لدى الافراد ذوي العلاقة بالمخاطر السيبرانية والإفصاح عنها
8.	توفر للأفراد فهم واسع في الامن السيبراني والمخاطر السيبرانية
9.	الإفصاح عن الاجراءات المتخذة والسياسات اللازمة للحفاظ على الامن السيبراني وعدم التعرض للهجمات؟
10.	الإفصاح عن تكاليف ادارة المخاطر السيبرانية؟
11.	الإفصاح عن تكاليف معالجة المخاطر السيبرانية؟
12.	الإفصاح عن مدى استمرارية المخاطر السيبرانية؟
13.	الإفصاح بشكل الكتروني عن المخاطر السيبرانية؟
14.	الإفصاح عن المخاطر السيبرانية ضمن التعليمات والتشريعات والقوانين والإجراءات المتعارف عليها؟
15.	استفسار من قبل الجهات الخاضعة حول وجود المخاطر السيبرانية.

16.	استفسار من قبل الجهات الخاضعة حول الإفصاح عن المخاطر السيبرانية.
17.	استفسار من قبل الجهات الخاضعة حول عدم الإفصاح عن المخاطر السيبرانية وبيان أسباب ذلك.
18.	التعرف على حجم وطبيعة الجهة الخاضعة وجمع المعلومات اللازمة عنها وتحديد الجوانب المهمة للبيئة التي تعمل في محيطها لتحديد المخاطر السيبرانية ومدى الإفصاح عنها.
19.	الإحاطة بالنظام المحاسبي والسياسات والإجراءات المتعلقة بالمخاطر السيبرانية والإفصاح عنها.
20.	جدولة الإجراءات التي سيتم تنفيذها حسب طبيعتها وأوقات تنفيذها وذلك في ضوء أولويات وأسبقيات المهام وتحديد المنهج والأسلوب الأكثر كفاءة للعمل ومدى توفر البنية التحتية لتطبيقها للمخاطر السيبرانية والإفصاح عنها.
21.	تحديد الأهداف والاختبارات الضرورية لتلك الأهداف وتنسيق العمل الذي سيتم تنفيذه من تأهيل القدرات البشرية والفنية للمخاطر السيبرانية والإفصاح عنها.
22.	تحديد عدد افراد الكادر الذين سيكلفون بالعمل ومستوياتهم الوظيفية لتحديد المخاطر السيبرانية والإفصاح عنها.
23.	وضع برنامج لتحديد المخاطر السيبرانية يغطي جميع الأنشطة الرئيسية والفرعية يحدد فيه الإجراءات اللازمة لتنفيذ البرنامج وان يتضمن الأهداف من تنفيذ كل فقرة رئيسيه منه.
24.	توثيق أوراق عمل حول كافة المواضيع وأدلة الإثبات والقرائن التي تؤكد إنجاز فحص المخاطر السيبرانية ومدى الإفصاح عنها.
25.	تحديد مدى تضمن القوائم المالية للمخاطر السيبرانية وتكاليفها وان تكون قد أعدت وفقا للسياسات والقواعد والمعايير المحاسبية.
26.	إيضاح كافة الأمور الهامة الخاصة بالمخاطر السيبرانية والإفصاح عنها ومدى الالتزام بها بشكل مستمر.
27.	إيضاح مدى الالتزام بالإفصاح عن المخاطر السيبرانية بشكل مستمر ام متقطع ضمن التقارير.
28.	بيان التغيرات في الإفصاح عن المخاطر السيبرانية بين السنة الحالية والسنوات السابقة ومدى اتساع أو انحصار الإفصاح.
29.	إبداء الرأي حول مدى تحديد المخاطر السيبرانية والإفصاح عنها.
30.	تحديد مدى إمكانية الاعتماد على التقارير المنشورة حول المخاطر السيبرانية ومدى كفاية الإفصاح عنها.
31.	تحديد درجة الاعتماد على نتائج فحص نظام الرقابة الداخلية وما هي الاجراءات التي تم تنفيذها لتحديد المخاطر السيبرانية والإفصاح عنها.
32.	تضمن التقرير جوانب التحفظ عن عناصر المخاطر السيبرانية ذات التأثير الجوهر التي لم يتم الإفصاح عنها من قبل الجهة الخاضعة.

ثانياً: إجراءات عملية:

أولاً: إجراءات تتعلق بالدخول الى النظام:	
1.	تدقيق سياسات إنشاء الحسابات
2.	اختبار قوة كلمات المرور.

3.	فحص صلاحيات المستخدمين
4.	التأكد من إيقاف حسابات الموظفين المنتهية خدماتهم
5.	تدقيق سجلات الدخول والخروج للمستخدمين
6.	فحص إعدادات التشفير لقاعدة البيانات.
7.	اختبار نظام النسخ الاحتياطي للبيانات
8.	تدقيق إجراءات الحماية من الاختراق
9.	التأكد من أنظمة كشف التسلل IDS/IPS
ثانياً: إجراءات تتعلق بحماية البيانات	
10.	مطابقة سجلات الأنظمة اليدوية والآلية لضمان عدم تغييرها
11.	التأكد من عدم وجود تلاعب
12.	اختبار صلاحيات المستخدمين عبر عينة من الحسابات
13.	التأكد من حفظ النسخ الاحتياطية في موقع مستقل
14.	اختبار استعادة نسخة احتياطية
ثالثاً: إجراءات تتعلق بحماية العمليات	
15.	فحص المعاملات خلال فترات حدوث هجمات أو انقطاع النظام.
16.	التحقق من وجود جدول تحديثات تلقائي للأنظمة والبرامج.
17.	مراجعة سجلات آخر التحديثات
18.	التأكد من وجود سياسة نسخ احتياطية فعالة للبرامج
19.	إعادة تنفيذ عمليات مالية مختارة
20.	تحليل فترات توقف النظام
21.	تقييم ما إذا كان الانقطاع تسبب في فقد بيانات
رابعاً: إجراءات تتعلق بالإفصاح عن المخاطر السيبرانية	
22.	طلب قائمة بالحوادث خلال السنة
23.	تحليل أثر كل حادث على توازن الحسابات
24.	تحليل أثر كل حادث على العمليات المالية
25.	التأكد من الإفصاح عن الحوادث وهل كان لها أثر جوهري
26.	التأكد من أن القوائم المالية تُظهر تكاليف الهجمات السيبرانية
27.	التأكد من أن القوائم المالية تُظهر تكاليف إعادة الهيكلة التقنية

5. الاستنتاجات والتوصيات

- تُشكل المخاطر السيبرانية تحديًا كبيرًا يهدد الأفراد والوحدات على حد سواء وهو يعكس مدى التعقيد الذي ينطوي عليه الأمن السيبراني في العصر الحديث، كما يتضح أن تصنيف المخاطر السيبرانية يتركز على الدوافع المختلفة مثل المكاسب المالية، التجسس، أو الإرهاب، يعكس تنوع الهجمات السيبرانية واختلاف طبيعتها بناءً على الأهداف.
- تؤثر المخاطر السيبرانية بشكل مباشر على السمعة والثقة المالية للوحدات الاقتصادية. فالهجمات الناجحة يمكن أن تؤدي إلى خسائر مالية كبيرة، وتوقف العمليات التجارية، وفقدان البيانات الحساسة للعملاء وهذا يجعل من الضروري للوحدات الاقتصادية أن تستثمر في الأنظمة الأمنية المتقدمة وتحديث سياساتها وإجراءاتها بشكل مستمر.
- توصف المخاطر السيبرانية بأنها تهديد أو تحدٍ يستهدف البيانات المخزنة أو المنقولة على الأنظمة الرقمية أو الشبكات أو الأجهزة الإلكترونية أو الإنترنت، وقد يؤدي إلى خسارة مالية أو تعطيل الخدمة أو انتهاك الخصوصية أو الإضرار بسمعة الوحدات والتي قد تؤدي إلى انهيارها.
- في ضوء ما طرح وفي ظل هذه البيئة المتسارعة والمليئة بالمخاطر يتطلب بالفعل إدراج الأمن السيبراني كحجر أساس في أي وحدة لضمان وضع إستراتيجية محكمة ضد المخاطر السيبرانية واعتماد ضوابط وعمليات واضحة وقوية مبنية على أساسيات هامة للأمن السيبراني على مستوى الوحدة كلها إذ تحتاج هذه الوحدات إلى هياكل وعمليات فاعلة تمكنها من تحقيق أهدافها.
- إن المخاطر السيبرانية لم تعد مجرد تهديدات تقنية محصورة في نطاق نظم المعلومات، بل أصبحت تمثل أحد أبرز محددات الاستقرار المالي والتشغيلي للوحدات الاقتصادية، خاصة مع توسع الاعتماد على البيئة الرقمية. كما أن آثار هذه المخاطر تتجاوز الخسائر المباشرة لتهديد بفقدان الثقة المؤسسية والإضرار بالحوكمة الداخلية، مما يستلزم من الوحدات الاقتصادية تعزيز استثماراتها في الأمن السيبراني ليس فقط كإجراء دفاعي، بل كجزء من إستراتيجية إدارة المخاطر الشاملة، لضمان الاستدامة وتعزيز التنافسية في ظل بيئة أعمال تتسم بالتغير السريع والتهديدات المتطورة.
- إن مراقب الحسابات ليس المسؤول الوحيد عن تحقيق سياسات أمن البيانات أو الوحدة، ولكنه يعتبر جزءاً مهماً من الفريق الذي يعمل على تحقيق هذه السياسات وتحديد المخاطر المحتملة.
- تُعد أطر ومعايير الأمن السيبراني الدولية بمثابة أدوات مرجعية تساعد الدول والوحدات في بناء أنظمة متكاملة لحماية بياناتها وبناءها التحتية الحيوية. وتعمل هذه الأطر على توحيد المفاهيم والممارسات وتقديم إرشادات شاملة لتقييم وتحسين الأداء الأمني، بما يضمن حماية الأصول الرقمية والامتثال للمتطلبات القانونية والتنظيمية.
- هناك مجموعة إجراءات يمكن أن تسهم في تعزيز دور مراقبي الحسابات في تدقيق المخاطر السيبرانية للوحدات المراد تدقيق حساباتها، تشمل مجموعة من الإجراءات العامة والإجراءات العملية التي يمكن أن يسترشد بها مراقبو الحسابات في أداء عملهم في بيئة الأمن السيبراني وبما يمكن أن يسهم في تعزيز دورهم.
- ضرورة الاهتمام بوسائل الأمن السيبراني والتعرف على أهم مجالات المخاطر السيبرانية من قبل مراقبي الحسابات وزيادة معرفتهم التقنية لكي يقوموا بعملهم في بيئة الأمن السيبراني.

- ضرورة الأخذ بمجموعة الإجراءات التي تم اقتراحها (في ضوء مجموعة من الأطر والمفاهيم والمعايير الصادرة عن مجموعة من المنظمات والجهات المعنية) كخطة عمل لمراقبي الحسابات لكي يكون عملهم مستنداً إلى مجموعة من المعايير ذات العلاقة بعملهم في بيئة الأمن السيبراني ومساهماتهم في الحد من المخاطر السيبرانية.

❖ قائمة المراجع

- الاتحاد الدولي للمحاسبين IFAC، 2005، دليل المعايير الدولية للمراجعة والفحص والتأكدات الأخرى والخدمات ذات العلاقة، نيويورك: الاتحاد الدولي للمحاسبين (الترجمة العربية الرسمية، إصدار 2005).
- جمهورية العراق، هيئة المستشارين، 2019، الاستراتيجية الوطنية للأمن السيبراني 2019-2023، الأمانة العامة لمجلس الوزراء، العراق.
- ذياب، فاطمة عبد الحسين، 2024، دور حوكمة تقنية المعلومات في تعزيز فاعلية التدقيق السيبراني: دراسة ميدانية على عينة من الوحدات الاقتصادية العراقية، جامعة البصرة، كلية الإدارة والاقتصاد، رسالة ماجستير غير منشورة.
- ذياب، مشتاق علي، 2024، تدقيق مخاطر الأمن السيبراني وانعكاسه على اجراءات التدقيق والمسؤولية المهنية لمراقب الحسابات، جامعة بغداد، المعهد العالي للدراسات المحاسبية والمالية، أطروحة دكتوراه.
- سالم، عبد الحكيم محمود، 2023، تأثير المخاطر السيبرانية على ممارسات التدقيق المالي في بيئة الأعمال الرقمية، المجلة العراقية للعلوم المحاسبية والمالية، المجلد 18، العدد 3.
- السواح، حسام عبد الله، 2021، دور التدقيق الداخلي في إدارة مخاطر الأمن السيبراني: دراسة تحليلية تطبيقية، مجلة البحوث المحاسبية، جامعة الإسكندرية، المجلد 22، العدد 4.
- شحاته، أحمد عبد المنعم، البردان، حسين، 2021، أثر تطبيق معايير الإفصاح عن المخاطر على جودة التقارير المالية في ظل التهديدات السيبرانية، مجلة البحوث المالية والتجارية، جامعة الأزهر، العدد 2، مصر.
- علي، سهى يونس والسقا، زياد هاشم، 2023، متطلبات التدقيق الداخلي لتعزيز الأمن السيبراني في ضوء إرشادات معهد المراقبين الداخليين (IIA): دراسة تطبيقية في جامعة الموصل، مجلة تكريت للعلوم الاقتصادية والإدارية، المجلد 63، العدد 19.
- فرحات، عبد الرزاق. 2019، الأمن السيبراني ودوره في حماية المعلومات في البيئة الرقمية، دار صفاء للنشر والتوزيع، الأردن.
- الكرعاوي، أحمد جاسم محمد، 2024، الإفصاح المحاسبي عن مخاطر الأمن السيبراني في ضوء المعايير الدولية للتقارير المالية: دراسة تطبيقية، جامعة الكوفة، كلية الإدارة والاقتصاد، رسالة ماجستير غير منشورة، العراق.
- Deloitte. 2023. Cyber Risk Frameworks and Regulatory Compliance. .Deloitte Insights
- Elifoglu, Halil, Aykut Abel, and Joseph J. Hazen. 2002. "Cybercrime: A New and Growing Problem for Businesses." Review of Business Information Systems 6, no. 1.
- EY (Ernst & Young). 2019. IFRS Challenges and Auditor Responsibility. .EY
- EY (Ernst & Young). 2021. Cybersecurity and Financial Integrity. EY Global.
- .CERT. 2020-GCCCybersecurity in the GCC Region: Challenges and Policy Responses, p. 11.
- GCSCC (Global Cyber Security Capacity Centre). 2016. Cybersecurity Capacity Maturity Model for Nations (CMM). University of Oxford.
- Grimes, Roger A. 2019. Cybersecurity Program Development for Business. .Wiley
- Helms, Marilyn M., and Bryan Lilly. 2000. "Electronic Audit Evidence: SAS 80 and Beyond." Journal of Accountancy

- https://www3.weforum.org/docs/WEF_Annual_Report_2021_22.pdf
- IBM X-Force. 2023. Threat Intelligence Index 2023.
- IBM. 2023. Cost of a Data Breach Report 2023.
- INTOSAI Working Group on Information Technology Audit,(2023), Cybersecurity and Data Protection Audit Guideline.
 - ISACA. 2015. Cybersecurity Nexus Glossary. <https://www.isaca.org/resources/glossary>.
 - ISO/IEC. 2012. 27032: Guidelines for Cybersecurity. Geneva: International Organization for Standardization.
 - ISO/IEC. 2013. 27001: Information Security Management Systems – Requirements. .Organization for Standardization Geneva: International
 - ITU (International Telecommunication Union). 2021. Global Cybersecurity Index Report.
 - ITU. 2021. GCI 2020 Report: Country Profiles.
 - KPMG. 2021. Leases and IFRS 16 Implementation. KPMG Publications.
 - KPMG. 2024. Cybersecurity Risk and Audit Challenges. .KPMG Insights
 - McAfee. 2021. Cloud Adoption and Risk Report. McAfee Corp.
 - NIST (National Institute of Standards and Technology). 2018. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: NIST, p. 3.
 - NIST (National Institute of Standards and Technology). 2020. Cybersecurity Framework Version 1.1. Gaithersburg, MD: NIST.
 - NIST (National Institute of Standards and Technology). 2020. Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). Gaithersburg, MD: NIST.
 - NIST (National Institute of Standards and Technology). 2022. Risk Management Framework for Information Systems and Organizations, Special Publication 800-37 Rev. 2, p. 5.
 - OECD (Organisation for Economic Co-operation and Development). 2019. Digital Security Risk Management for Economic and Social Prosperity. Paris: OECD Publishing.
 - Public Company Accounting Oversight Board (PCAOB). 2022. Cybersecurity and the External Audit. .PCAOB
 - PwC (PricewaterhouseCoopers). 2022. Global Digital Trust Insights. PwC Global.
 - PwC (PricewaterhouseCoopers). 2023. Trust in Reporting: The Role of Cyber Risk Disclosures. PwC Global.
 - PwC. Managing Cyber Risk in an Interconnected World. .PwC Global, 2022
 - SEC (U.S. Securities and Exchange Commission). Commission Guidance on Public Company Cybersecurity Disclosures. .2018
 - Siegel, Carol A., and Mark Sweeney. 2020. Cyber Strategy: Risk-Driven Security and Resiliency. .Boca Raton, FL: CRC Press, Taylor & Francis Group
 - UNESCWA. Cybersecurity in the Arab Region: Assessment and the Way Forward. United Nations Economic and Social Commission for Western Asia, 2022
 - Verizon. (2022). 2022 Data Breach Investigations Report.
 - Voigt, P., & Von dem Bussche, A. 2017. The EU General Data Protection Regulation (GDPR): A Practical Guide. .Springer