j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, special issue. 2025

The Role of Internal Auditing in Recovering from Cybersecurity Risks in the Iraqi Islamic Banking Sector

Ibtihaj Ismail Yaqoub[1], Zahra Hassan Alawi[2], Tayba Abdulkarim Mohammed[3]

[1,2,3] *College of Administration and Economics, Mustansiriyah University, Baghdad, Iraq.*

hussainalaa10000@uomustansiriyah.edu.iq

Abstract The research aims to identify the role of internal auditing in recovering from cybersecurity risks, reducing cyber violations, and enhancing cyber resilience in the Iraqi Islamic banking sector. It addresses recent developments in the knowledge domain of internal audit practices and the responsibilities of internal auditors, especially in light of global challenges posed by digitalization and the Fifth Technological Revolution. The study is aligned with local requirements issued by the Central Bank of Iraq in 2019 concerning IT governance regulations, as well as international standards set by the General Council for Islamic Banks and Financial Institutions (CIBAFI), and the updated Cybersecurity Framework (CSF 2.0) issued in February 2024, which outlines guidelines for cybersecurity controls . Through the examination of both local and international publications, the research developed specific indicators and concluded with several recommendations. Chief among them is the need to assign a more significant role to internal auditing in evaluating cybersecurity controls. Moreover, the proposed framework by the researchers can serve as a roadmap for defining the evaluative and advisory role that internal auditors can play in Islamic banks to mitigate cyber threats.

Crossref 10.36371/port.2025.special.18

Keywords: *internal audit; cybersecurity risks; cyber resilience; Islamic banking; regulatory framework*

دور التدقيق الداخلي في التعافي من المخاطر السيبرانية في القطاع المصرفي الاسلامي العراقي اعداد

ابتهاج اسماعيل يعقوب & زهره حسن عليوي & طيبة عبد الكريم محمد

قسم المحاسبة / كلية الإدارة والاقتصاد / جامعة المستنصرية ، بغداد ، العراق.

الخلاصة : يهدف البحث الى التعرف على دور التدقيق الداخلي في التعافي من المخاطر الامن السيبراني وفي الحد من الانتهاكات السيبرانية وتعزيز المرونة السيبرانية في القطاع المصرفي الاسلامي العراقي . يتناول البحث المستجدات على الساحة المعرفية في مجال نشاط التدقيق الداخلي والدور الذي يضطلع به المدقق الداخلي ومسؤوليته في ظل التحديات التي تواجه العالم في ظل الرقمنة والثورة التكنولوجية الخامسة، وفق المتطلبات المحلية التي أصدرها البنك المركزي العراقي ذو الصلة بالضوابط الرقابية لتكنولوجيا المعلومات 2019 ودوليا وفق ماصدره المجلس العام للبنوك الاسلامي والموسسات المالية الاسلامية (CIBAFI) .و ألاطار الامن السيبراني (CSF (2.0 الصادر في شباط (2024). من توجيهات بخصوص الضوابط الرقابية للامن السيبراني .ومن خلال استقراء الاصدارات المحلية والدولية تم بناء مؤشرات بهذا الخصوص وتوصل البحث الى جملة من التوصيات من ابرزها منح التدقيق الداخلي دورا اكثر اهمية في تقييم الضوابط الرقابية فضلا عن ان الاطار المقترح من قبل الباحثين يمكن اعتباره خارطة طريق لتحديد الدور التقييمي والاستشاري الذي يمكن ان يؤديه المدقق الداخلي في قطاع المصارف الاسلامية للحد من الانتهاكات السيبرانية .

الكلمات الدالة: *التدقيق الداخلي؛ مخاطر الأمن السيبراني؛ المرونة السيبرانية؛ المصارف الإسلامية؛ الإطار الرقابي*

S. S. Jassim. (2021). Protection of trade names for electronic stores in Iraqi law. *Journal port Science Research,4*(3), pp.158–167. https://doi.org/10.36371/port.2021.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, special issue. 2025

المقدمة

يُعد تقييم الضوابط الرقابية أحد أهم المهام التي يقوم بها نشاط التدقيق الداخلي. ويُعرف التدقيق الداخلي بأنه نشاط مستقل وموضوعي يقدم تأكيداً وخدمات استشارية لإضافة قيمة وتحسين عمليات الوحدة الاقتصادية . ويهدف تقييم الضوابط الرقابية إلى التأكد من أن الضوابط الرقابية في الوحدة الاقتصادية تعمل بشكل فاعل لتحقيق أهدافها. يصاحب تقديم العمليات المصرفية الالكترونية مخاطر متعددة وقد أشارت لجنة بازل للرقابة المصرفية إلى أنه ينبغى قيام البنوك بوضع السياسات والإجراءات التي تتيح لها إدارة هذه المخاطر من خلال تقييمها والرقابة عليها ومتابعتها،

يختص الامن السيبراني بحماية موارد المعلومات لدى الوحدات الاقتصادية ومنها اجهزة الحاسوب واجهزة الشبكة والبرمجيات والبيانات من الوصول غير المصرح به او التعطيل او التدمير، الا انه مع كل تقدم تكنولوجي يجد المخترقون بعض الاساليب المعاصرة لشن هجمات على الامن السيبراني، لذا نرى ما تقدمه الهيئات والمراكز البحثية والجهات المهنية من تحديث مستمر لهذه الضوابط بحكم كون تكاليف الاختراق تكبد الكثير من الخسائر، فضلاً عن انعكاسها على اداء الوحدات الاقتصادية وتوقفها عن العمل احيانا وتعرضها لمخاطر السمعة فضلاً عن مخاطر أخرى.

وللحد من هذه المخاطر سعت الهيئات المهنية والدول على اصدار الارشادات والادلة والقوانين الداعمة لتعزيز الدور الذي يقوم به المدقق الداخلي في تقييم المخاطر واضافة قيمة الى الوحدة الاقتصادية، ومنها ماصدره المجلس العام للبنوك الاسلامي والموسسات المالية الاسلامية (CIBAFI) و اصدارت البنك المركزي العراقي 2019 واخر اصدار في شباط (2024) ويعد هذا الاصدار الاحدث والصادر عن (NIST) المعهد الوطني للمعايير والتكنولوجيا (National institute of standards and technology) يتناول البحث المستجدات على الساحة المعرفية في مجال نشاط التدقيق الداخلي والدور الذي يضطلع به المدقق الداخلي ومسؤوليته في ظل التحديات التي تواجه العالم في ظل الرقمنة والثورة التكنولوجية الخامسة فضلا عما وضعه البنك المركزي العراقي من ضوابط رقابية للمخاطر السيبرانية ، من خلال ثلاث مباحث المبحث الاول منهجية البحث ودراسات سابقة، والمبحث الثاني دور المدقق في ظل المخاطر السيبرانية واهم المرتكزات اطار الامن السيبراني للاصدارات المحلية والدولية ، اما المبحث الثالث يتضمن الجانب التطبيقي اما المبحث الرابع يتضمن الاستنتاجات والتوصيات.

المبحث الاول

منهجية البحث ودراسات سابقة

1. 1: مشكلة البحث

مع تسارع وتيرة الخروقات السيبرانية في مختلف القطاعات ومنها المصارف الاسلامية تُثار العديد من التساؤلات حول قدرة الوحدات الاقتصادية على الصمود من الخروقات السيبرانية بعد إن اصبحت المخاطر السيبرانية في مصاف المخاطر الأكثر تأثيراً ، ومع اهتمام الجهات المختلفة باصدار الارشادات والتعليمات والأطر المنظمة لضوابط رقابية فاعلة ومنها ماصدره البنك المركزي العراقي في اصداره الخاص بالامن السيبراني والصمود السيبراني ودوليا أحدثها اطار (NIST) اطار الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتكنولوجيا الاطار المحدث 2.0 (CSF) الصادر في (شباط 2024) ، وبحكم كون التدقيق الداخلي النشاط الذي يساهم في التقييم يثار التساؤل البحثي التالي:-

(ما هو الدور الذي يضطلع به التدقيق الداخلي في تقيم الضوابط االرقابية في ظل المخاطر السيبرانية الصادرة من الهيئات الرقابية والاشرافية المهنية والمتمثلة بالبنك المركزي العراقي محليا والاصدارت الدولية كاطار الامن السيبراني (2.0) (CFS) – المحدث و ماصدره المجلس العام للبنوك الاسلامي والموسسات المالية الاسلامية (CIBAFI) من الممارسات التي تسهم في وضع ضوابط رقابية فاعلة؟

1. 2: اهمية البحث

تنبع اهمية البحث من اهمية الدور الذي يضطلع به التدقيق الداخلي كنشاط يقيم الضوابط الرقابية للامن السيبراني في الوحدات الاقتصادية في ظل متطلبات البنك المركزي العراقي والاطار الدولي (CSF 2.0) المحدث، ماصدره المجلس العام للبنوك الاسلامي والموسسات المالية الاسلامية (CIBAFI) و دور ومسؤولية المدقق الداخلي في ذلك.

1. 3: اهداف البحث

1. **التعرف على المرتكزات المحلية والدولية لاطار الامن السيبراني وضوابطه الرقابية .**

S. S. Jassim. (2021). Protection of trade names for electronic stores in Iraqi law. *Journal port Science Research,4*(3), pp.158–167. https://doi.org/10.36371/port.2021.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, special issue. 2025

2. الخوض بغمار مفهوم المخاطر السيبرانية واستعراض التيارات البحثية التي اهتمت بهذا الخصوص.
3. استعراض لبعض الأطر الرقابية المحلية والدولية .

1. 4: فرضية البحث

يرتكز البحث على فرضية رئيسة مفادها:-

(للتدقيق الداخلي دور في تقييم المخاطر السيبرانية من خلال بناء دليل للضوابط الرقابية على وفق تعليمات البنك المركزي العراقي محليا ودوليا على وفق اطار الامن المحدث (CSF 2.0) ومصدره المجلس العام للبنوك الاسلامي والموسسات المالية الاسلامية (CIBAFI)

1. 5: منهج البحث

يعتمد البحث على المنهج التحليلي الاستقرائيوالاستنباطي

الدراسات السابقة واسهامة البحث الحالي

بعنوان اثر مخاطر الامن السيبراني على استخدام البطاقات المصرفية في المصارف الاسلامية العاملة في الاردن .) بواينة ،2023(1 - دراسة تناولت الدراسة الأثر المحتمل لمخاطر الأمن السيبراني (مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية، مخاطر الهجمات السيبرانية) في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن، وذلك باتباع منهج كمي وصفي تحليلي. واستُخدمت الاستبانة لجمع البيانات من الإدارات العليا والوسطى والدنيا في الإدارات والاقسام المستهدفة في البنوك الإسلامية وعددهم (100) فرد. وباستخدام الاستراتيجيات الاحصائية الوصفية والاستدلالية تم التوصل إلى وجود أثر معنوي لمخاطر الأمن السيبراني وأبعاده في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن. وأوصت الدراسة بزيادة اهتمام إدارات البنوك الإسلامية بتطوير وتنفيذ إجراءات الأمن السيبراني اللازمة والمعنية بحماية بيانات العملاء ومنع وقوع أية حوادث وكوارث أمنية

3- (الشورة والشاعر،2020) الامن السيبراني في المصارف الاسلامية الاردنية

تناولت الدراسة البحث في الأمن السيبراني من حيث المقصود به ، حيث أنه مجموعة من الإجراءات والتدابير والوسائل التكنولوجية يتم استخدامها بقصد حماية أمن الشبكات والأجهزة ، بالمختصر (حماية المعلومات الالكترونية من أي اختراقات الكترونية ، والأسباب التي دعت إلى ظهور ما يسمى بالأمن السيبراني ، وتتمثل في الإختراقات والتهديدات السيبرانية (الإلكترونية) ، التي تؤدي إلى أثار كبيرة وسيئة على الدول والمجتمعات ، والمخاطر التي تنجم عن هذه الاختراقات الالكترونية، وما تسببه من خسائر كبيرة ، ويجب مواجهتها من خلال الأمن السيبراني ، وتم التفريق ما بين أمن المعلومات والأمن السيبراني ، وأن الأمن السيبراني جزء من أمن المعلومات ، وبينهما فروق دقيقة من أبرزها ، أن الأمن السيبراني حماية كل شيء الكتروني ، بينما أمن المعلومات حماية كل شيء الكتروني أو مادي ، وفي المبحث الثالث والأخير تم الحديث عن الأمن السيبراني وفاعليته في البنوك الإسلامية الأردنية . وقد خلصت الدراسة إلى عدد من النتائج والتوصيات تمثلت في أن الأمن السيبراني ضرورة لضمان الأمن الوطني ، بسبب ما يقوم به من حماية من أي اختراقات الكترونية ، فهو يعمل على ضمان استمرارية المعلومات، وأن المخاطر السيبراني تتطور نتيجة حيل المخترقين وكشفهم النقاط الضعف والثغرات ، ولا بد من العمل على تطوير الإجراءات السيبرانية ، واتباع برامج الحوكمة السيبرانية ، وإدراك مدى خطورة التعامل بالتكنولوجيا الرقمية.

1. دراسة (متولي واخرون، 2022) بعنوان (دور المدققين الداخليين في مواجهة الاحتيال السيبيراني والمخاطر المتعلقة بالاستعانة بمصادر خارجية: دراسة استكشافية/ بحث منشور)

تهدف هذه الدراسة في كيفية تأثير ظهور جائحة (كوفيد 19) فيما يتعلق الضوابط الداخلية لشركات التأمين ومواجهة الاحتيال حيث ان التحول الرقمي في السنوات الأخيرة، حيث وجدت شركات التأمين تعتمد على الاستعانة بمصادر خارجية كوسيلة للتعامل مع تغييرات نماذج الاعمال ومتطلباته) توصل البحث إلى أن بعد جائحة (كوفيد 19) لابد ان تكون هناك ادلة وارشادات للتغلب على مخاط الانترنيت والاحتيال.

2. دراسة (محمد ،2020) بعنوان (الامن السيبراني في ضوء مقاصد الشريعة الاسلامية بحث منشور

هدف البحث الى دراسة واختبار مكانة الامن السيبراني في الاسلام وبيان مكانته في مقاصد الشريعة الاسلامية واثاره في المقاصد الضرورية مع مناقشة وتحليل ضرورات وجود ضوابط للامنا لسيراني لحماية المجتمع بكافة مفاصله .

S. S. Jassim. (2021). Protection of trade names for electronic stores in Iraqi law. *Journal port Science Research,4*(3), pp.158–167. https://doi.org/10.36371/port.2021.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, special issue. 2025

3. دراسة (Nikola Simics, 2022) بعنوان

(The Internal Auditor's Role in Cybersecurity Governance)

رسالة ماجستير في المحاسبة بتخصص رقابة داخلية

دور المدقق الداخلي فى حركة الأمن السيبراني، دراسة نوعية حول تأثير المدقق الداخلي على الامن السيبراني هدف البحث على كشف ممارسات المدققين الداخليين في السويد ودورهم في الامن السيبراني من خلال المقابلات مع العاملين في التدقيق الداخلي في الشركات السويدية واعضاء معهد المدققين الداخليين السويدي، وتوصل البحث الى اهمية الدور الذي يؤديه المدقق الداخلي في خلال مهارته الشخصية وتقييم المخاطر وخطوط الدفاع الثلاثة في الحد من المخاطر السيبرانية.

4- دراسة (Alina And Others,2017) (Internal Audit Role In Cybersecurity)

بحث منشور (دور التدقيق الداخلي في مخاطر التدقيق الداخلي)

يهدف البحث الى تحديد دور التدقيق الداخلي كخط دفاع اول وخط دفاع ثاني وخط دفاع ثالث فضلاً عن ان الدور الذي يلعبه التدقيق الداخلي الى تقييم المخاطر السيبرانية وضوابط الأمن السيبراني وابلاغ الادارة العليا للوحدة الاقتصادية حول نقاط الضعف والتهديدات ودمج تدابير الأمان السيبراني في خطة التدقيق الداخلي.

مايميز الدراسة الحالية تسليطها الضوء على الاطر الحديثة ذات الصلة بالامن السيبراني وتكاملها مع بعضها للوصول الى دليل مقترح لهذه الضوابط وتحديد الدور الذي يمكن ان يلعبه التدقيق الداخلي في تقييم الضوابط الرقابية .

المبحث الثاني

دور التدقيق الداخلي في الحد من المخاطر السيبرانية في القطاع المصرفي الاسلامي

2. 1: مفهوم المخاطر السيبرانية

تعريف الأمن اصطلاحاً : الأمن عدم توقع المكروه في زمن آت (الجرجاني ،20، 2011).

فالسيبرانية : مأخوذة من كلمة (سيبر) Cyber ، وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي(الربيعة ،11، 2011)

يشير مفهوم مخاطر الأمن السيبراني الى الهجمات الالكترونية التي تسبب الوصول غير المصرح به او تعطيل الانظمة والبرامج والخدمات الالكترونية لشركة ما، وتقصد بها هي المخاطر التي تؤثر على سرية وسلامة المعلومات والتي تحقق خسائر وتهديدات للشركة (Alina et al,2017:511)، ويرى الباحثون ان المخاطر السيبرانية هي أي استراتيجيات مقصودة او غير مقصودة تتعرض لها الاصول الرقمية للشركة من خلال البرمجيات الخبيثة المعروفة او المبتكرة او الوصول غير المصرح به او التاثير على الموارد الرقمية او أي استخدام غير مرغوب به لتقنيات الهندسة الاجتماعية ولا تقتصر المخاطر السيبرانية على المخاطر الخارجية فقد تكون تلك المخاطر داخلية يمكن ان تطلق عليها مخاطر السيبرانية الداخلية او التهديد الداخلي، ويجدر الاشارة الى انه لا يمكن تحديد نوع الخطر السيبراني يحكم الحداثة و التجدد في انواع الهجمات. وعرفتها الاستراتيجية الوطنية للامن السيبراني في العراق بانها احتمال وجود تهديد وهشاشة داخل الفضاء الالكتروني للبلد يضر بأمن نظم المعلومات وهياكل البنى التحتية المعلوماتية الاساسية من خلال التهديدات السيبرانية والثغرات الموجودة في الفضاءات السحابية (استراتيجية الامن السيبراني العراقية، 2019: 66).

2.2التأصيل الشرعي للأمن وعلاقة بمقاصد الشريعة

يطلق مصطلح مقاصد الشريعة على الأهداف العامة التي تسعى الشريعة إلى تحقيقها في حياة الناس، ويطلق أيضاً على الأهداف الخاصة التي شرع لتحقيق كل منها حكم خاص، والقصد الأول منها أنها وضعت المصالح العباد في الدارين (1 الشاطي،6، 2011). أما أقسام المقاصد في الشريعة الإسلامية المقصد العام: هو ما فيه صلاح عموم الأمة أو الجمهور ، ويتحقق هذا من خلال أحكام الشريعة الإسلامية.منها حفظ المال فالباحث في مكانة الأمن السيبراني في الشريعة يجده في مرتبة الضروريات وهو من مقومات الحياة إن فقد لم تجر مصالح الدنيا على استقامة، وإصلاح الدنيا بالأمن يترتب عليه صلاح الدين ومعلوم أن الضروريات يراد بها درء المفسدة عن الدين والنفس والعقل والنسب والعرض

S. S. Jassim. (2021). Protection of trade names for electronic stores in Iraqi law. *Journal port Science Research,4*(3), pp.158–167. https://doi.org/10.36371/port.2021.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, special issue. 2025

والمال .فحفظ المال من اهم المقاصد الاسلامية فضلا عن ان الامن السيبراني هدفه حماية المال والحد من الاعتداء عليه عن طريق الاحتيال او الاختراق . فكان لابد ان يكون هناك السياسات والارشادات والتعليمات التي تضع الضوابط الرقابية لتحقيق الامن السيبراني

2. 2: القوانين والادلة الخاصة بالافصاح عن الامن السيراني

يتعلق الامن السيرانى بحماية موارد المعلومات لدى الوحدات الاقتصادية ومنها اجهزة الكمبيوتر واجهزة الشبكة والبرمجيات والبيانات في الوصول غير المصرح به او التعطيل او التدمير، فضلاً عن ان كل تقدم تكنولوجي يحاول المحتالون من خلال طرق جديدة لشن هجمات على الامن السيبراني، مما يجعل المخاطر السيبرانية احد الاعتبارات المهمة لاي وحدة اقتصادية، فقد تكون تكاليف الاختراقات السيبرانية كبيرة جداً، لذا كان للتدقيق الداخلي دوراً في الجهود المبذولة في مجال الامن السيبراني، لذا كان للهيئات المهنية والتشريعية دوراً في وضع القوانين والتشريعات نظراً للتأثير المخاطر السيبرانية وقد كان للحوادث السيبرانية اثرا سلبيا على العديد زن المجالات وكما في الجدول (1) التالي:-

جدول (1) *اثر الحوادث والاختراقات السيبرانية*

الاثر	الترتيب 2021	الترتيب 2022	الترتيب 2023
الاضطراب التشغيلي (بما في ذلك سلسلة التوريد أو النظام البيئي الشريك	1	1	٪58
خسارة الايرادات	9	2	٪56
فقدان ثقة العملاء / تاثير السلبي على العلامة التجارية	4	3	٪56
خسارة السمعة	5	4	٪55
وقف تمويل مبادرة الاستراتيجية	غ/م	5	٪55
فقدان الثقة في السلامة التكنولوجية	غ/م	6	٪55
الاثر السلبي على توظيف المواهب والاحتفاظ بها	8	7	٪54
سرقة الملكية الفكرية	2	8	٪54
انخفاض في سعر الاسهم	2	9	٪52
الغرامات التنظيمية	7	10	٪52
التغيير في القيادة	5	غ/م	غ/م

المصدر : ترنيمة الادارة ,IIA,2023)

على وفق ذلك اصدرت العديد من الجهات القوانين والتشريعات والأدلة بخصوص الافصاحات عن ادارة مخاطر الأمن السيبراني، حيث أصدرت (SEC) هيئة الأوراق المالية والبورصات الامريكية قوانين، تهدف إلى رفع مستوى وتوحيد إفصاحات الأمن السيبراني من الشركات العامة الخاضعة لمتطلبات الإبلاغ المنصوص عليها في قانون الأوراق المالية "(Exchange Act Securities) ووطدت القوانين الجديدة ما يجب على الشركات الإبلاغ عنه فيما يتعلق بإدارة المخاطر واستراتيجيتها وحوكمتها وحوادث الأمن السيبراني التي تعتبر جوهرية، وتتضمن القوانين الجديدة متطلبات على الشركات المسجلة للتداول

1. بيان كيفية تقييمها وتحديدها وإدارتها لتهديدات الأمن السيبراني وهل أثرت أي مخاطر جوهريا أو يوجد احتمال معقول بأنها ستؤثر جوهريا على استراتيجية أعمالها أو نتائج العمليات أو الوضع المالي، ويجب على هذه الشركات أيضا الإفصاح عن حوادث الأمن السيبراني الجوهرية ووصف الجوانب الجوهرية لطبيعة كل حادث ونطاقه وتوقيته.
2. تقديم تفاصيل عن كيفية إشراف مجلس الإدارة على المخاطر السيبرانية ودور الإدارة في تقييم وإدارة المخاطر الجوهرية، إذ قررت هيئة الأوراق المالية والبورصات (SEC) عدم اعتماد متطلب مقترح بشأن الإفصاح عن خبرة مجلس الإدارة في مجال الأمن السيبراني.

S. S. Jassim. (2021). Protection of trade names for electronic stores in Iraqi law. *Journal port Science Research,4*(3), pp.158–167. https://doi.org/10.36371/port.2021.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, special issue. 2025

3. تخضع جهات الإصدار الخاصة الأجنبية للقوانين نفسها ويجب عليها أيضا تقديم معلومات عن حوادث الأمن السيبراني الجوهرية التي تعلن عنها أو يطلب منها الإعلان عنها أو الإفصاح عنها بطريقة أخرى في ولاية قضائية أجنبية أو لأي بورصة أو لحاملي الأوراق المالية.
4. تقديم نموذج "K-8" عموماً في غضون أربعة أيام عمل من تحديد المنشأة أن كان الحادث السيبراني جوهري (قد يُسمح بالتأخير في الإفصاح إذا قرر المدعي العام الأمريكي أن الإفصاح الفوري من شأنه أن يشكل خطرا كبيرا على الأمن القومي أو السلامة العامة وأخطر لجنة الأوراق المالية والبورصات بذلك كتابيا (SEC,2023).

فيما يخص الإفصاح عن الحوادث، أو نماذج K-8، يبدأ سريان القوانين بعد 90 يوما من نشرها في السجل الفيدرالي أو في 18 ديسمبر 2023 أمام الشركات الصغيرة الملزمة بالإبلاغ ما يصل إلى 180 يوما إضافيا للالتزام)، وسيكون موعد الإفصاحات في النموذج K-10 بدءا بالتقارير السنوية للسنوات المالية المنتهية بتاريخ 15 ديسمبر 2023 أو بعده. وذكرت الرابطة الوطنية لأعضاء مجالس الشركات (NACD) أنه على الرغم من أن القوانين الجديدة لا تتناول مؤهلات أعضاء مجلس الإدارة، فإنها ترتقي بدور جميع القيادات ومنها مجلس الإدارة والرؤساء التنفيذيون وكبار مسؤولي أمن المعلومات في إدارة المخاطر، وبينما يتولى أعضاء مجلس الإدارة مسؤولياتهم الجديدة، يمكنهم اللجوء إلى التدقيق الداخلي للحصول على التوكيدات القيمة والرؤية المتعمقة التي سيحتاجون إليها لمعالجة مخاطر الأمن السيبراني في القطاع المصرفي .

2. 3: اطار الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتكنولوجيا (NIST)

أصدر عن المعهد الوطني للمعايير والتكنولوجيا في 26 شباط 2024 اطار الامن السيبراني (National Institute Of Standards And Technology) (CSF 2.0)، حيث تم اعداد الإطار ليتلائم مع القطاعات والاحجام (صغيرة أو متوسطة او كبيرة).

أن الوظائف الاساسية لاطار الامن السيبراني والتي يتضمن ستة وظائف رئيسة (الحوكمة، التحديد، الحماية، الفحص، المسؤولية) وكما في الشكل

ان الوظائف الرئيسة للاطار المفاهيمي للمخاطر السيبرانية كالتالي:- استراتيجية ادارة مخاطر الأمن السيبراني للوحدة الاقتصادية(GN) Govern:- يتم تحديد التوقعات والسياسات والابلاغ عنها ومراقبتها، حيث تم الافصاح عن ما تفعله الوحده الاقتصادية لتحقيق الوظائف الخمس الأخرى وتحديد اولوياتها في سياق مهمتها وتوقعات اصحاب المصلحة. حيث يعتبر إطار عمل الأمن السيبراني NIST أداة لتنظيم وتطوير برامج وسياسات الحماية الخاصة بالوحدات الاقتصادية، ويتضمن الإطار مجموعة من الإرشادات وأفضل الممارسات الوحدات الاقتصادية على بناء مستوى الحماية الخاص بهم، يضع إطار العمل (NIST) مجموعة من التوصيات والمعايير التي تمكن الوحدات الاقتصادية من الاستعداد بشكل أفضل لتحديد الهجمات السيبرانية واكتشافها كما يوفر إرشادات حول كيفية الاستجابة للحوادث الالكترونية ومنعها والتعافي منها.حيث تم صياغة هذه الارشادات والتوصيات من قبل المعهد الوطني للمعايير والتكنولوجيا) (NIST): (National of Standards and Technology) ويعالج إطار العمل هذا الضعف والافتقار للمعايير للأمور المتعلقة بالأمن السيبراني ويوفر مجموعة موحدة من القواعد والمبادئ التوجيهية والمعايير للمؤسسات لاستخدامها عبر الصناعات المجالات المختلفة. حيث تعتبر انشطة الحوكمة ضرورية لدمج الأمن السيبراني في استراتيجية ادارة مخاطر المؤسسة (ERM) ان استراتيجية الأمن السيبراني. تتتضمن الاطار التالي(NIST -2023-33)

1 تحديد الهوية (ID)

يتم فهم مخاطر الأمن السيبراني الحالية للوحدة الاقتصادية، أن فهم أصول الوحدة الاقتصادية (على سبيل المثال، البيانات والأجهزة والبرامج والأنظمة والمرافق والخدمات والأشخاص) والموردين ومخاطر الأمن السيبراني ذات الصلة يمكن للوحدة الاقتصادية من تحديد أولويات جهودها بما يتوافق مع استراتيجية إدارة المخاطر واحتياجات المهمة المحددة في إطار الحوكمة تتضمن هذه

S. S. Jassim. (2021). Protection of trade names for electronic stores in Iraqi law. *Journal port Science Research,4*(3), pp.158–167. https://doi.org/10.36371/port.2021.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, special issue. 2025

الوظيفة أيضا تحديد هوية المستخدمين ، تحسين سياسات الوحدة الاقتصادية، واجراءاتها وممارساتها التي تدعم ادارة مخاطر الامن السيبراني.

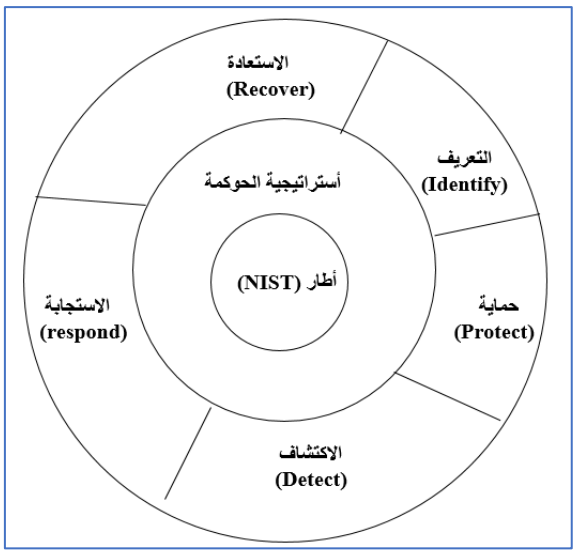
2.: الحماية (protect):- حماية الاصول لمنع او تقليل احتمالية تأثيرات احداث الامن السيراني السلبية، فضلا عن تأمين الاجهزة والخدمات الخاصة بالمنصات المادية والافتراضات، ومرونة البنية التحتية التكنولوجية.

. 3.: الاستجابة (DETECTIDE):- يتم اتخاذ الإجراءات المتعلقة اذا حصل الى حادث سيبراني (اختراق) وقد تم اكتشافه حيث يتم تحليل حالات الاختراق ومؤشرات الاختراق والاسباب التي ادت الى حصول الخلل، ويتم وضع خطط للاستجابة للمخاطر ووضع الانشطة للتعافي من المخاطر.

4-الاستجابة (Rs) (Respond):- يتم اتخاذ الاجراءات المتعلقة بحوادث الأمن السيبراني الذي تم اكتشافه فضلاً عن وضع خطط للاستجابة للمخاطر واعداد تقارير يتم فيها.

5-الاسترداد (R) (Recover):- تتم استعادة (الاسترداد) الاصول والعمليات المتأثرة بحادث الأمن السيبراني، ويمكن توضيح وظائف الامن السيبراني على وفق (NIST) بعجلة، والوظائف تكون مترابطة مع بعضها البعض كلما موضحة بالشكل (1)

الشكل (1) *وظائف (CSF) وفق أطار (NIST 2024)*



Sorce:- Framework National Institute Of Standards And Technology

ان لعديد من المؤسسات تجري تقييمات للثغرات لمعرفة مدى نجاحها في تحديد الأحداث السيبرانية وتحليلها وإدارتها والتعافي منها، ، ينبغي أن تتأكد مجالس الإدارة من أن الإدارة تحدد ما إن كانت عملية التقييم الحالية ستدعم فترة تحول الرقمي ، وعلى الرغم من أن فريق تكنولوجيا المعلومات سيحدد الحوادث، فإن تحديد الأهمية النسبية يجب أن يتضمن إسهامات من مجالات أخرى، مثل الفرق المالية والقانونية والتنظيمية، لاكتساب منظور واسع النطاق. ان (NIST) وفرت الأطر التوجيهيه لفهم وادارة مخاطر الامن السيرانى بفاعلية وقد قدم المعهد الوطني للمعايير والتكنولوجيا النسخة (101) في (16) نيسان عام (2018) (Http//doi.org/10.6028/NIST) والتي حدثت اطار العمل للنسخة (1.0) ويمكن عرض اهم التحديثات التي طرأت على الاطار (101) (NIST) بالجدول (2)

S. S. Jassim. (2021). Protection of trade names for electronic stores in Iraqi law. *Journal port Science Research,4*(3), pp.158–167. https://doi.org/10.36371/port.2021.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, special issue. 2025

الجدول (2) *ملخص عن التغييرات على اطار العمل بين النسخة (1.0) والنسخة (1.1)*

التحديث	وصف التحديث
التوضيح بأن المصطلحات مثل "التقيد" قد تكون مربكة وتحمل معان مختلفة جدا في نظر أصحاب المصلحة المختلفين باطار العمل.	تم إضافة توضيح بأن "الجدوى" هي بنية ولغة إطار العمل من أجل تنظيم التقيد. بمتطلبات الأمن السبراني للمنظمة وللتعبير عن هذا التقيد من خلال متطلبات الأمن السبراني الخاصة بالمنظمة. ومع ذلك، فإن الطرق المختلفة التي يمكن من خلالها استخدام إطار العمل من قبل المنظمة تشير إلى أن عبارات من مثل "التقيد بإطار العمل" قد تكون مربكة.
قسم جديد عن التقييم الذاتي.	إضافة قسم 4.0 التقييم الذاتي لمخاطر الأمن السبراني باستخدام إطار العمل الشرح كيف يمكن استخدام إطار العمل من قبل المنظمات لفهم وتقييم مخاطر الأمن السبراني لديهم، بما في ذلك استخدام المقاييس.
إضافة شرح موسع لاستخدام إطار العمل في مجال إدارة المخاطر السبرانية السلاسل الإمداد.	يساعد القسم الموسع 3.3 إبلاغ متطلبات الأمن السبراني إلى أصحاب المصلحة المستخدمين في فهم إدارة المخاطر السبرانية لسلاسل الإمداد SCRM بشكل أفضل. كما يقوم القسم 3.4 قرارات الشراء بتسليط الضوء على استخدام إطار العمل في فهم المخاطر المتعلقة بالمنتجات والخدمات التجارية الجاهزة. أيضا، تم إضافة معايير سبرانية جديدة تتعلق بإدارة المخاطر السبرانية السلاسل الإمداد إلى مراحل التطبيق. وأخيراً، تم إضافة تصنيف إدارة المخاطر السبرانية لسلاسل الإمداد إلى نواة إطار العمل، ويشمل ذلك عدة تصنيفات فرعية.
تنقيحات لأخذ مسائل المصادقة والتصريح وإثبات الهوية بمزيد من الاعتبار. والتصريح وإثبات الهوية بمزيد من الاعتبار.	تم تنقيح اللغة المستخدمة في تصنيف التحكم في الوصول لأخذ مسائل المصادقة والتصريح واثبات الهوية بمزيد من الاعتبار، وذلك يشمل إضافة تصنيف فرعي لكل من المصادقة وإثبات الهوية. كما تم تغيير اسم التصنيف إلى إدارة الهويات والتحكم في الوصول (PR.AC) من أجل تمثيل نطاق التصنيف والتصانيف الفرعية التابعة له بشكل افضل.
شرح إضافي في القسم التطبيق وبين النماذج شرح أفضل للعلاقة بين مراحل	شرح اضافي في القسم 3.2 تأسيس أو تطوير برنامج أمن سيبراني عن استخدام مراحل إطار العمل في تطبيق إطار العمل. شرح إضافي في مراحل إطار العمل بهدف إبراز اعتبارات إطار العمل في البرامج التنظيمية لإدارة المخاطر. كما تم تنقيح مفاهيم مرحلة إطار العمل. وأيضا، تم تحديث الشكل 2.0 ليحتوي على الإجراءات من مراحل إطار العمل.
نظرة إلى الإفصاح المنسق عن مواطن الضعف	تم إضافة تصنيف فرعي يتعلق بدورة حياة الإفصاح عن مواطن الضعف

https://doi.org/10.6028/nist.cswp.04162018ar

S. S. Jassim. (2021). Protection of trade names for electronic stores in Iraqi law. *Journal port Science Research,4*(3), pp.158–167. https://doi.org/10.36371/port.2021.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, special issue. 2025

وفي نفس السياق أصدر (NIST) مسودة (2.0) من معيار اطار الامن السيبراني في آب / 2023، وان التحديثات ضرورية لمواجهة تحديات الامن السيبراني في الوقت الحالي والمستقبلي، وقد نشرت المسودة للحصول على التعليقات بخصوص ضمان فاعلية (2.0)(NIST) للمستقبل وقادرة على تحقيق الاهداف والغايات من أجل تحفيض الخطر السيبراني فضلاً عن تلقي الحالات التي طرأت في الفترات الأخيرة كخروقات للأمن السيبراني والثغرات واقتراح علاجها (NISTOWN29 Cybersecurity Framwork 2.0, 2023) وفي شباط / 2024 اصدر (NIST) التحديث (2.0) حيث يؤكد الاطار على توسيع نطاق اطار (NIST) السيبراني ويؤكد حوكمة الامن السيبرانى وانه يطبق مع كافة المجالات والقطاعات سواء مصرفية تجاريوة او اسلامية وتؤكد على ادارة مخاطر سلسلة التوريد السيبرانية فضلاً على أن الاطار الجديد اضافة ركيزة جديدة الى الركائز الخمس الاصلية اللازمة لنجاح اطار الأمن السيبراني، وهي (الحكم).

وبعد استقراء الاطار الجديد يمكن أن يحدد الباحثون اهم جوانب التحديث:-

1. **لم يكن اطار (NIST) خروجاً تاماً عما كان موجود في اطار (NIST 1.1) لكنه يتبع نهجاً قائماً على المخاطر في الأمن السيبراني فضلاً عن انه يركز على النتائج ، فالاهم هو النتائج.**
2. **هناك توسع في نطاق تطبيق (CSF.2.0) عن الاطار السابق فهو مخصص لكافة اشكال واحجام الشركات.**
3. **التركيز على الحوكمة وبشكل أكثر اتساعاً فالتغيرات الجوهرية الحاصلة في بيئة الاعمال فرضت التوسع والتركيز على الحوكمة واعتبار المخاطر السيبرانية المخاطر الأهم، والحوكمة على وفق (CSF2.0) تاخذ بعين الاعتبار الطرائق والاساليب التي تتخذها لدعم استراتيجية الأمن السيبراني فضلا عن انها استراتيجية صممت لدعم وأسناد الوظائف الخمس الأخرى.**
4. **ادارة مخاطر سلسلة التوريد (Supply chain Risk Management) وهي العملية التي يتم من خلالها تنفيذ استراتيجيات تهدف للتعرف على التهديدات والمخاطر اليومية والمحتملة التي تتعرض لها سلسلة التوريد فهي الجهود المطلوبة في كيفية التحكم في مخاطر الأمن السيبراني المرتبطة بأطراف خارجية باسم ادارة مخاطر سلسلة التوريد) ، مثلاً الهجمات من برامج خبيثة وان مخاطر سلسلة توريد البرمجيات تشمل المخاطر التي لا يتم اخذها بعين الاعتبار في منتج او تطبيق خلال دورة حياة تطوير البرنامج، فضلاً عن ارشادات اكثر شمولية لادارة مخاطر سلسلة التوريد.**
5. **هناك توافق مع أطر الامن السيبراني الدولية (كمعيار ISO31000) ارشادات ومبادئ للادارة الفاعلة للمخاطر والارشادات الخاصة بالصناعة (COSOERM Framework) 150196009 و (ISO 27001) تأمين اصول المعلومات.**

2. 4: دور التدقيق الداخلي في الحد من مخاطر الأمن السيبراني

تم تحديد أهم المخاطر من قبل (المديرين التنفيذيين للتدقيق الداخلي للاتحاد الأوربي) بمخاطر الامن السيبراني لعام 2023 / من خلال ردود اكثر من 300 من كبار المدققين الداخليين العاملين في المؤسسات في جميع انحاء العالم، احتل الأمن السيبراني المركز الأول في المخاطر وأضحى مصدر قلق لكبار المدققين الداخلين وعد من احد اكبر المخاطر التي تواجهها الوحدات الاقتصادية وبحاجة الى التدقيق الداخلي الذي يقدم المشورة لمجالس الإدارة حول مدى فاعلية ادارة مخاطر الوحدة الاقتصادية في ادارة هذه المخاطر، لقد تم نشر التقرير السنوي للمخاطر بعنوان (المخاطر تحت المجهر) الذي اعدته سبعة معاهد اوربية للمدققيين الداخليين والذي غطى معظم دول الاتحاد الاوربي والذي خرج بنتائج أن أهم المخاطر هي مخاطر الأمن السيبراني حيث مثلت 66 ٪ تليها امن وحماية البيانات 58٪ و الرقمية 36٪.(IIA)

ومع الانتقال إلى عصر الانترنيت أصبحت التكنولوجيا جزءاً كبيراً في حياتنا اليومية وبيئة الاعمال، الا أن المخاطر التي رافقت هذا الانتقال حتمت الحاجة الى مراعاة وجود ضوابط رقابية محكمة، وتفعيل دور التدقيق الداخلي في تقييم الضوابط الرقابية لمخاطر الامن السيبراني بحكم ان الوحدات التي تقع ضحية الهجمات الالكترونية قد تتكبد تكاليف كبيرة واضرار جسيمة، فعلى المدققين فهم طبيعية الحوادث السيبرانية والنظر بعناية أكثر للاستراتيجيات المعتمدة في الحد من هذه المخاطر.

S. S. Jassim. (2021). Protection of trade names for electronic stores in Iraqi law. *Journal port Science Research,4*(3), pp.158–167. https://doi.org/10.36371/port.2021.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, special issue. 2025

ان مسؤولية المدقق تتضمن تصميم اجراءات تستجيب على وجه التحديد للمخاطر ومنها (فهم الادارة للمخاطر وتقييم تاثير سرقة التكنولوجيا والخسائر المباشرة والاضرار المحتملة على ميزتها التنافسية وعلى الارباح المستقبلية، فضلا عن تحليل الحساسية المحتملة في التقديرات التي قد ينتج عنها تأثير جوهري على البيانات المالية وتقسيم وتأثير الهجوم على نفقات التقاضي المحتملة وتكاليف حماية الامن السيبراني واستمرارية الوحدة الاقتصادية (ISCA,2018 ، 15-14) ، ان المسؤولية التي تقع على عاتق المدقق الداخلي تتضمن تقييم للضوابط الرقابية التي وضعتها الادارة المسؤولة، وهل حددت تلك الادارة مخاطر الأمن السيبراني والبيئة السيبرانية كجزء في تقييم المخاطر مع التكنولوجيا التي تقود المخاطر، ودمج فهم البيئة السيبرانية للوحدة الاقتصادية ومتانة تصميم الاعتبارات الرقابية فضلاً عن أن البيئات التي يلاحظ انها شديدة التعقيد فبالأمكان اشتراك خبراء متخصصون في مجال الامن السيبراني (IIA,2024:10) ان مسؤولية المدقق الداخلي يمكن ان تتمحور حول تقسيم مخاطر الامن السيبراني (CSRA) والتي تعني جميع الإجراءات والسياسات والتدابير التي تضعها الوحدات الاقتصادية لتحديد وتصنيف وتقييم وابلاغ الادارة عن المخاطر الى الادارة العليا لتحقيق سلامة البيانات وحمايتها من الهجمات القوى الخبيثة(البرامج الخبيثة) الداخلية والخارجية والدخول غير المصرح به، ورد الهجوم على البنى التحتية الحيوية العامة والخاصة مثل سرقة الهوية والبرامج الضارة وبرامج الفدية والتصيد الاحتيالي عبد البريد الالكتروني لضمان منع المخاطر وتخفيفها ومراقبتها لحماية البنى التحتية الحيوية، بحكم أن الوسائل التقليدية لتدابير الرقابة الداخلية غير ذات فاعلية وكفاءة في حماية تكنولوجيا المعلومات في الوحدات الاقتصادية (Usman and other,2023).

– الايوفي والمخاطر السيبرانية للعمليات الرقمية

أيوفي هي إحدى أبرز المنظمات الدولية غير الربحية الداعمة للمؤسسات المالية الإسلامية، تأسست عام 1991م ومقرها الرئيس مملكة البحرين، ولها منجزات مهنية بالغة الأثر على رأسها إصدار 100 معياراً حتى الآن في مجالات المحاسبة والمراجعة وأخلاقيات العمل والحوكمة بالإضافة إلى المعايير الشرعية التي اعتمدتها البنوك المركزية والسلطات المالية في مجموعة من الدول. باعتبارها إلزامية أو إرشادية، كما تحظى الهيئة بدعم عدد من المؤسسات الأعضاء، من بينها المصارف المركزية والسلطات الرقابية والمؤسسات المالية وشركات المحاسبة والتدقيق والمكاتب القانونية من أكثر من 45 دولة، وتطبق معايير الهيئة حالياً المؤسسات المالية الإسلامية الرائدة في مختلف أنحاء العالم، والتي وفرت درجة متقدمة من التجانس للممارسات الإسلامية المالية على مستوى العالم (https://aaoifi.com/about-aaoifi/).ومن الواضح بلا شك أن الأمن السيبراني يمثل تحدياً مشتركاً لكل من المؤسسات المالية الإسلامية ونظيراتها التقليدية. كما تمثل الثروات والبيانات المتداولة داخل النظام المالي الإسلامي هدفا للهجمات الإلكترونية. في المسح العالمي للمصرفيين الإسلاميين الذي أجراه المجلس العام للبنوك الإسلامية (GIBS) لعامي 2020 و 2021، أشارت البنوك الإسلامية إلى مخاطر الأمن السيبراني ومخاطر التكنولوجيا من بين المخاطر الثلاثة الأولى التي تواجهها مؤسساتها.

ومن المنظور الإسلامي، فإن الحفاظ على ممتلكات الأفراد والمنظمات وحمايتها من أي عمل ضار هو أحد مقاصد الشريعة. وتشمل هذه الممتلكات الثروة المالية والملموسة. والموارد الرقمية، والثروة غير الملموسة. يتم تداول هذه الأصول في القطاع المالي وتتعرض للعديد من التهديدات التي تؤثر على أنظمة المعلومات في المؤسسات المالية وتؤدي إلى السرقة والاحتيال والاستغلال الإجرامي / غير المشروع للبيانات العامة والخاصة. وبالتالي، فإن منع مثل هذه التهديدات يتماشى مع مقاصد الشريعة ويرتبط بضمان سلامة الفضاء الإلكتروني واعتماد تدابير لتعزيز المرونة السيبرانية لمؤسسات التمويل الاسلامي. ومن قائمة التدابير، طلب من البنوك الإسلامية أيضاً الإشارة إلى مستوى تنفيذ تدابير الأمن السيبراني. وأظهرت النتائج أن معظم المشاركين في الدراسة هم في مرحلة التنفيذ، إما قيد التنفيذ أو قاموا بتنفيذ جميع التدابير المذكورة بشكل كامل. ويعد استخدام طبقات متعددة من الأمن لفصل شبكة الشركة عن الأنظمة التي تواجه الخارج هو الإجراء الأكثر تنفيذاً، في حين أن إجراء تمارين ربع سنوية لاختبار قدرة المؤسسات على الاستجابة الحوادث الأمن السيبراني هو الإجراء الأكثر عدم تنفيذ من قبل البنوك الإسلامية. من الملاحظ أن البنوك الإسلامية تبذل المزيد من الجهود لتنفيذ تدابير لتأمين أنظمتها وبدرجة أقل في وضع استراتيجيات

S. S. Jassim. (2021). Protection of trade names for electronic stores in Iraqi law. *Journal port Science Research,4*(3), pp.158–167. https://doi.org/10.36371/port.2021.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, special issue. 2025

مصاغة للأمن السيبراني والاختبارات الدورية لضمان المرونة السيبرانية لأنظمتها والتي ينبغي وضعها كأولوية أعلى بما يتماشى مع الهيئات الدولية.

حيث اصدر الايوفي المعيار الشرعي رقم 61 بطاقات الدفع الالكتروني والذي ينظم الامن في عمليات الدفع الالكتروني .(معيار الشرعي 61،2022 ،1155) .فضلا عن قيام (CIBAFI) باصدار الارشادات بخصوص الحد من المخاطر السيبرانية وكالتالي :

https://www.cibafi.org/SurveyPage?ContentId=CI2137

وجود ضوابط مناسبة لتصنيف المعلومات من حيث الأهمية والحساسية

1. اعتماد الأدوات التقنيات للكشف عن البيانات الحساسة ومنعها من مغادرة شبكة الشركة فضلا عن قيام الجهات الرقابية في المصرف بتقييم القدرات الأمنية وإدارة المخاطر السيبرانية من قبل مقدمي الخدمات .
2. دمج الأمن السيبراني في عمليات التصميم للنظم والبرامج ،
3. توظيف طبقات متعددة من الأمان لفصل شبكة الشركة عن الأنظمة المواجهة للخارج
4. تدريب الموظفين على الأمن السيبراني مرة واحدة على الأقل سنوياً
4. مراقبة واكتشاف الأنشطة و / أو الأحداث الشاذة
5. بتسجيل محاولات الوصول عن بعد مع تنبيهات بشأن الأنشطة الضارة المحتملة
6. مراقبة الأفراد الذين يعملون على شبكة الشركة، بما في ذلك الاتصالات أو الأجهزة غير المصرح بها

إجراء اختبارات الاختراق لتحديد نقاط الضعف التي قد تؤثر على أنظمة أو الشبكات أو الأشخاص.

وقدر اصدر البنك المركزي العراقي على حد سواء للمصارف التجارية والاسلامية – ضوابط حوكمة تقنية المعلومات والاتصالات والتي تتعلق بأحكام دليل حوكمة تقنية المعلومات الصادرة عن البنك المركزي العراقي في عام 2019. -- مراجعة وتطوير استخدامات تقنية المعلومات والاتصالات وضمان أمن المعلومات والاتصالات توفير بنية تحتية كافية وفعالة من الناحية التشغيلية لتقنية المعلومات وأنظمة تقنية المعلومات والاتصالات والشبكات الإلكترونية والبرمجيات المستخدمة في المصرف توفير إجراءات كافية وفعالة من الناحية التشغيلية المتخذة للاحتفاظ بنسخ احتياطية محدثة من المعلومات لمواجهة الأزمات المحتملة وفقدان قواعد البيانات. توفير التقنيات الكافية للخدمات الإلكترونية للزبائن وضمان التشغيل الفعال لتقنيات زبائن المصرف.

التحديات التي تواجه المدقق الداخلي في تقييم المخاطر السيبرانية:

يمكن تحديد بعض التحديات التي تواجه المدقق الداخلي في تقييم المخاطر السيبرانية (Erin et al,2020, Ojeka et al.2023) ،(Usman et al,2023) ان غياب تدابير رقابية عالية الجودة لحوكمة الشركات ولحوكمة تقنيات المعلومات يجعل تجديد المخاطر ورصدها ومراقبتها غاية في الصعوبة وخاصة في الخدمات المالية ويكاد يكون الاهم ألاخلاقيات المهنية للمدققين الداخليين فهي تعزز من تقييم مخاطر الأمن السيبراني فضلا عن كفاءتهم ومهاراتهم فهي تعزز من اداءهم لمهامهم في التقييم حيث ربطت بعض الادبيات والنتائج الميدانية التي توصلت اليها الى ان الافراد عندما يفتقرون إلى الوعي بالأمن يجعل موقف الادارة الضعيف ينعكس سلباً تجاه الاستجابة لمخاطر الأمن السيبراني (Stein bart & Rasch Ke 2018, 3)) ،(Baseda Pama Ki & Sihvonen,2010) ويمكن القول ان مقاييس كفاءة التدقيق الداخلي يمكن قياسها بمدى الاستجابة لاحتياجات الجهات الخاضعة للتدقيق ومدى رضاها على مستوى اداء نشاط التدقيق الداخلي، فضلاً عن المدى الذي يمكن ان يقاس به فاعلية اداء التدقيق مرتبط بتلبية توقعات مجلس الادارة (IIA,2020:7) وان الادارات عليها ان تدرك أن

S. S. Jassim. (2021). Protection of trade names for electronic stores in Iraqi law. *Journal port Science Research,4*(3), pp.158–167. https://doi.org/10.36371/port.2021.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, special issue. 2025

هناك تدابير ينبغي ان تاخذها بعين الاعتبار للتخفيف من مخاطر وهجمات الامن السيبراني واعتبار التدقيق الداخلي احد خطوط الدفاع الثلاث ولكنه ليس خط الدفاع الوحيد في الوحدة الاقتصادية، وانه يسهم في وضع المخاطر السيبرانية ضمن انموذج ادارة مخاطر الوحدة الاقتصادية (Usman et al.2023:1-23) فضلا عن ان البيئة التي تعمل بها الوحدة الاقتصادية لها دوراً كبيراً ففي بيئة التهديدات المتلاحقة وسريعة التطور فان تقييم كفاءة الامن السيبراني يتضمن الامتثال للوائح والتعليمات المتاحة واختيار افضل الممارسات واحدث الاساليب القائمة على المخاطر المستقبلية والاهتمام بالتدابير الاستباقية والتي تتعامل مع توظيف احدث الاساليب والتقنيات المتاحة للتقييم الفاعل لمخاطر الأمن السيبراني (Kahydoglu, 2020,11).

المبحث الثالث : دليل مقترح لتقييم دور التدقيق الداخلي في الحد من مخاطر الامن السيبراني وفق اطار (CSF) 2.0

لغرض اختيار دور نشاط التدقيق الداخلي في مواجهة مخاطر الأمن السينراني (في قطاع المصارف) وتم أختيار هذا القطاع تحكم الخروقات المستمرة التي يتعرض لها ووضع دليل يرتكز الى اطار مخاطر الامن السيبراني المحدث (2024) والاطر المحلية والدولية

الوظيفة	نعم	لا
1. الحوكمة - حوكمة الأمن السيبراني أ. يضم مجلس الادارة عضواً من التدقيق الداخلي يتمتع بالمهارات التقنية والتعامل مع الخروقات السيبرانية. ب. لدينا برنامج لفحص الامتثال لتعليمات مخاطر الأمن السيبراني وضعها المصرف. ج. لدينا تعليمات وادلة لتطبيق سياسة الأمن السيبراني. د. لدينا سجل شامل خاص بالمخاطر السيبرانية وضمان تحديثه باستمرار ويكون ضمن عمل ادارة المخاطر في الشركة ويقوم قسم التدقيق لتحديثة. هـ- يراقب قسم التدقيق الداخلي مستوى المخاطر السيبرانية في المصرف. و- لقسم التدقيق الداخلي صلاحية التعامل مع تقييم الضوابط الخاصة بالأمن السيبراني والرقابة عليها وتحسينها. ز- يشارك التدقيق الداخلي في تحديد الهجمات الداخلية والخارجية التي قد يتعرف لها المصرف. ح- الاستعانة بالتدقيق الداخلي لاتخاذ الاجراءات التصحيحية حال حدوث الخروقات.		
2. تحديد الهوية (identify) أ- يتم الاستعانة بنشاط التدقيق الداخلي في تحديد وتعريف المخاطر المالية للامن السيراني للمصرف. ب - يتم الاستعانة بنشاط التدقيق الداخلي في تحديد المخاطر والاحتياجات الفريدة للمصرف. جـ- يتم الاستعانة بنشاط التدقيق الداخلي في تحديد العمليات التجارية الهامة والأصول في المصرف. د - اشتراك نشاط التدقيق الداخلي في وضع وضع شروط التعهيد الخارجي عند التعاون مع جهات خارجية في تصميم (موقع ويب) للمصرف او البرامج المحدثة. هـ - اخذ بعين الاعتبار المقترحات المقدمة من قيل نشاط التدقيق الداخلي في تحديد الجهة التي سيتعاقد معه المصرف عند تحديث او شراء الي برنامج. و- يقوم نشاط التدقيق الداخلي بإعداد تقرير لاحق للحوادث السيبرانية يوثق فيه الحادث والاستجابة واجراءات التعافي والدروس المستفادة ميها		
3- الحماية (protect)		

S. S. Jassim. (2021). Protection of trade names for electronic stores in Iraqi law. *Journal port Science Research,4*(3), pp.158–167. https://doi.org/10.36371/port.2021.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, special issue. 2025

أ- يساهم نشاط التدقيق الداخلي في وضع الخطط الاستراتيجية مع الادارة العليا لضمان ادارة مخاطر فاعلة في المصرف. ب- الاستعانة بنشاط التدقيق الداخلي في وضع السياسات لحماية الأصول المادية والبرمجية. ج - يساهم نشاط التدقيق الداخلي في تحديد الادوار وفصل الوظائف والمسؤوليات وتحديد الوصول المصرح به. د- لدينا ضوابط تم وضعها باستشارة نشاط التدقيق الداخلي (الضوابط حماية) للحد من والسيطرة على المخاطر السيبرانية. ها - يساهم نشاط التدقيق الداخيل في وضع ضوابط الامن المادي والبيئي والرقمي والشبكي. و- لنشاط التدقيق الداخلي دوراً في اقتراح التحديثات التلقائية للبرامج وادارة وصيانة البرامج. ح- يحتفظ نشاط التدقيق بنسخ احتياطية للبرامج وتحديثاتها. ي- يقدم نشاط التدقيق الداخلي تقريرا يستعرض به اهم الاحداث والخروقات السيبرانية التي تعرض لها المصرف نتيجة ضعف الاهتمام بجانب الوصول المادي والبرمجي والشبكي.		
4- الاكتشاف (Detect) أ- يعمل نشاط التدقيق الداخلي في المصرف على تطور وأختبار العمليات والاجراءات للكشف عن مؤشرات حوادث الأمن السيبراني المحتملة. ب- يبلغ نشاط التدقيق الداخلي الادارة العليا بأي خروقات واسبابها وكيفية علاجها.		
ج- تقديم المشورة للموظفين عن الخروقات السلبية التي حدثت فوراً لضمان اتخاذ اجراءات الاستجابة المناسبة للحادث.		
5- الاستجابة (Respond) أ - يساهم التدقيق الداخلي في تنفيذ خطة الاستجابة للحوادث السيبرانية بمجرد اكتشافها. ب- تحديد المسؤوليات بشكل واضح للاستجابة الفورية في حاله حدوث الخروقات. ج - للتدقيق الداخلي دليل يصنف فيه الحوادث السيرانية (عالية الخطورة ، متوسطة الخطورة ، منخفضة الخطورة، غير خطرة) بناءاً على دراسات مسبقة. د- يقوم التدقيق الداخلي يتحديد السبب الجذري لحصول الخروقات باعادة تقييم الضوابط الرقابية باستمرار. ه- للتدقيق الداخلي خطة طوارئ يجمع بها كل المعلومات التي تتعلق بالثغرات التي ادت للاختراق. و- يقوم التدقيق الداخلي يتقييم خطط الاستجابة للحوادث بشكل مستمر. ح- لدينا مصفوفة الخطر السيبراني يسهم نشاط التدقيق الداخلي في وضعها والمتمثلة باحتمالية الحدث السيبراني وحجم الأثر ومستوى الخطر المقبول.		
6- الاستعادة او التعافي (Recover) أ- لنشاط التدقيق الداخلي دورا في استعادة الاصول والعمليات التي تضررت من حوادث الامن السيبراني. ب- لنشاط التدقيق الداخلي خطة تضمن التشغيل للاميرة والبرمجيات في حالات الطوارئ او الكوارث. ج- لنشاط الترقيق الداخلي تعليمات تحدد به الادوار والسؤوليات داخل وخارج المصرف عند تعرض المصرف للاختراق والاستجابة الفورية للتعافي. د. يساهم التدقيق الداخلي في التأكد من صلاحية النسخ الاحتياطية يفترات متلاحقة. هـ - للتدقيق الداخلي تقييم مستمر لنوعية المعلومات التي يتم ابلاغ اصحاب المصالح (الخارجيين) عنها مع الاحتفاظ بدليل السرية المعلومات.		

S. S. Jassim. (2021). Protection of trade names for electronic stores in Iraqi law. *Journal port Science Research,4*(3), pp.158–167. https://doi.org/10.36371/port.2021.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, special issue. 2025

و- يساهم التدقيق الداخلي في بعض الاحيان بالاستعانة بطرف ثالث (خارجي) لتقيم المخاطر السيبرانية للتعاني السريح من الخروقات.		

المبحث الرابع

الاستنتاجات والتوصيات

اولاً:- الاستنتاجات

خرج البحث بحملة من الاستنتاجات من أبرزها:-

1. يعد اطار عمل الأمن السيبراني (NIST) نهجاً لإدارة مخاطر الامن السيبراني وقد اجري عليه تحديثات من (CSF 1.0) و (CSF 1.1) واخيراً التحديث الذي صدر في شباط / 2024 (CSF 2.0) حيث ركز على الادارة الفاعلة للمخاطر كاساس لاضافة قيمة للوحدة الاقتصادية.
2. المرتكزات الرئيسة الاطار الأمن السيراني (CSF2.0) تتضمن ست فئات (الحوكمة (Govern)، والتعرف (Identify)، والحماية (Protect) والكشف (Detect)، والاستجابة (Respond) والتعاقي (Recover) الغرض من إصداره هو الاسهام في تقليل مخاطر الامن السيبراني وزيادة قدرة التكيف مع التغيرات التي تطرأ على بيئة الأعمال المتغيرة، وانعكاس ذلك على زيادة الثقة في الوحدات الاقتصادية.
3. تعد المخاطر السيبرانية من أبرز المخاطر واكثرها اهمية على وفق اصدارات الهيئات المهنية ومنها نشرة اعتماد المدققين الداخليين في الاتحاد الاوربي.
4. تشكل المخاطر السيبرانية تهديداً متزايداً للوحدات الاقتصادية، وللتدقيق الداخلي الدور الحيوي في ادارة هذه المخاطر ومحاولة تحجيمها والتخفيض من خطورتها.
5. يعد تقسيم الضوابط الرقابية المتعلقة بالوصول المادي الى الضوابط البيئية الى أمن الشبكات وأمن النسخ الاحتياطية والتوثيق من الادوار التي يقوم بها التدقيق الداخلي في هذا المجال.
6. يمكن ان يساهم هم التدقيق الداخلي على الانتقال في مخاطر الامن السيبراتى من مجال المعقد والمتطور إلى المجال الأمن والقادر على التعافي اذا ما تم مؤامة إطار الامن السيبراتي العالمي (CSF2.0) مع مسؤوليات المرفق الداخلي.
7. الاطار المقترح من قبل الباحثين يمكن اعتباره خارطة طريق لتحديد الدور التقييمي والاستشاري الذي يمكن ان يؤديه المدقق الداخلي في قطاع المصارف.

التوصيات

خرج البحث بجملة من التوصيات من ابرزها:-

1. تطوير المواهب الوطنية القادرة على التعامل مع الثغرات وتقليصها، وخصوصاً في الجانب الرقابي ورفع الوعي السيبراني ومخاطره.
2. التحسين والتطوير بالدفاعات السيبرانية لواجهة تحديات أمن المعلومات وفق مسارات دولية محددة.
3. توفير دورات متطورة للكوادر العاملة في المجال المحاسبي والتدقيقي من خلال برامج متكاملة ويتم منح الشهادات ذات الصلة المعتمدة دوليا تتعلق بالاختراق الاخلاقي المعتمد والتكاء الاصطناعي وتحيزه، والتدقيق الالكتروني الداخلي.
4. قيام نقابة المحاسبين ومعهد المدققين الداخليين المعتمد فى العراق بدوره ياعلان مبادرة التدقيق الداخلي في ظل الامن السيبراني والذي يتضمن الاعلان عن مسابقة تنافسية بخصوص ابتكار او تطوير نظم تدقيق في ظل اعتماد الذكاء الاصطناعي، فضلاً عن تعزيز التعاون والتكامل مع الجهات الدولية ذات الصلة بالامن السيبراني.

S. S. Jassim. (2021). Protection of trade names for electronic stores in Iraqi law. *Journal port Science Research,4*(3), pp.158–167. https://doi.org/10.36371/port.2021.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, special issue. 2025

5. انشاء مرصد (الامن السيرانى/ في العراق لتعزيز مؤشر جاهزية الامن السيراني لدولة العراق وبناء تجربة رقمية في مجالات التكنولوجيا حلول الذكاء الاصطناعي.
6. التوجه البحثي من قبل الباحثين والمهتمين بمجال التدقيق الداخلي باعتماد مفهوم التدقيق الداخلي للامن السيبراتي كأحد المتغيرات البحثية المهمة والذي يتضمن عملية فحص الضوابط الرقابية الامنية المطبقة في الوحدات الاقتصادية للتأكد من توفر الضوابط التي تضمن سلامة وحماية المعلومات.
7. تعزيز المناهج في معهد المتفقين الداخليين والبرامج التطبيقية في الامن السيبراتي والتدقيق الداخلي على أن المعهد شهد تطور بهذا الخصوص في ادخال التكنولوجيا والضوابط الرقابية ضمن برنامج المدقق الداخلي المعتمد في المرحلة الثانية بمادة نظم محاسبة وتقنيات.
8. العمل على حصول المؤسسات المالية والمصارف في البيئة العراقية على احدث التقنيات فيما يتعلق بالبرامجيات لمواجهة القرصنة الالكترونية مع تحديث التعليمات الصادرة عن البنك المركزي العراقي على وفق مستجدات البيئة الرقمية.
9. اعتماد الدليل المقدم من قبل الباحثين في تفعيل دور التدقيق الداخلي كنشاط يسهم في الحد من المخاطر السيبرانية.

المصادر

[1] متولي / عبد المنعم وعبد العظيم ، سمر والمرجي محمد، "دور المدقق الداخلي في مواجه خطر الامن السيراني وخطر الغش في الاستعانة بمصادر خارجية في عمليات التأمين دراسة استكشافية، مجلة الاسكندرية للبحوث المحاسبية، المجلد 6، العدد 3 ، سيتمبر 2022 ، الصفحة (1- 31).

[2] اميرهم، جيهان عادل، (اثر جودة المراجعة الداخلية في الحد من مخاطر الامن السيبراني وانعكاسه على ترشيد قرارات المستثمرين)، مجلة البحوث المالية والتجارية، المجلد (23) العدد الثالث، يونيو (2022).

[3] ISCA, Cybersecurity Risk Considerations in a Financial Statements Audit, (2018), Global Mindset Insights".

[4] Zwilling, D. ( ), Trendsand challenges Regarding Cyber Risk Mitigation by CISOS - A Systematic Literature and Experts (opinion Review Basd on Tex Anlytics, Journal Accounting and Electronic Risk Management.

[5] Steinbart.p. & Raschkes R. (2018), (The RelastienShip between Internal Audit and Information Security: An Expoloratory Investigation) Journal of Accounting and Economics, (2 May).

[6] Kahyaoglu, K. (2020) (Personality of interr Auditors; an exploratory study in the Wetherland Relevance to practice Keywords), Research Article personality → http://doi.org 110-5-mab.

[7] All, (2020), Measuring Internal Audit Effective and Efficiency.

[8] Nist Cswp2g (Initial Public Draft Jung-2023), http:// Cyberframworkpnast@nist.gov.

[9] Alina, Cara tas and Cerasela, Spatariu and Gabriela, Gheorghiu, 2017, (Internal Audit Role in Cybersecurity, ovidlus University Annals, Economic Sciences Series, 2/2017.

[10] Doron, Rosenblum, 2023, (Cyber risk management: the role of internal audit), KEREston global, Kreston. Com/managing Cyber-risks-internal-audit.

[11] ERMA, (the Role of Internal Audit in Strengthening Cyber Security) .(2023).

[12] Cybersecurity tops risk list for audit cherifs) 2023 http:// www.Ila.org.uk.riskn Focus. Charterd Institute of Internal Auditors (CIIA).

[13] Simić, Nikola, 2022, (The Internal Auditor. Role in cybersecurity Governance) Master's Thesis, UPPSALA University.

S. S. Jassim. (2021). Protection of trade names for electronic stores in Iraqi law. *Journal port Science Research,4*(3), pp.158–167. https://doi.org/10.36371/port.2021.3.2

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, special issue. 2025

[14] Usma, Alih, che-Ayoiband olarinoye, Salau, (2023) (The Role of Wternal Auditors Characteristics. In CYBRSECRITY Risk ASSESSMENT IN FINANCIAL-BASED BUSINESS organisation CONCEPTUAL REVIEW, Journal JPB, V. 8 : 2922, Doi:http://doi.org/10.26668/businessreview

[15] شركة (SSL Com)، (2022) "اطار عمل الأمن السيراني (NIST) نظرة عامة معمقة (http://ww.ssl.com).

[16] ستراتيجية الامن السيراني العراقي (2019) ، مستشار الامن الوطني امانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات حتى (١-١٥)

S. S. Jassim. (2021). Protection of trade names for electronic stores in Iraqi law. *Journal port Science Research,4*(3), pp.158–167. https://doi.org/10.36371/port.2021.3.2