IRAQI Academic Scientific Journals
العراقية المجلات الأكاديمية العلمية
مجلة جامعة الكوت
ISSN (E): 2616 - 7808 II ISSN (P): 2414 - 7419
www.kutcollegejournal.alkutcollege.edu.iq
k.u.c.j.sci@alkutcollege.edu.iq
عدد خاص - المؤتمر العلمي الثامن للعلوم الإدارية والاقتصادية - 28-29 يونيو / حزيران 2025

دور حوكمة الشركات في معالجة خروقات الامن السيبراني

م. د. سرى وليد اسماعيل [1] ، د. ايناس حسن كاظم [2] ، د. علي خضير سمير [3]

المستخلص

أدى الإعتماد المتزايد للشركات بنوعيها العام والخاص على تقنيات وشبكات الويب Web لأنظمة الإدارة المالية الخاصة بها إلى زيادة تعرضها للهجمات السيبرانية (الإلكترونية) والتي تعد أحد المخاطر الرئيسية التي يجب على الشركات السيطرة عليها ، وتتعدد أهداف هذه الهجمات فقد تكون بهدف السرقة أو تدمير الأصول المالية أو سرقة الملكية الفكرية أو غيرها من المعلومات الهامة كما أن مجالس الإدارة ليست مستعدة بشكل كافٍ لمعالجة مخاطر الأمن السيبراني بسبب نقص الخبرة في مجال تكنولوجيا المعلومات. ، هدف البحث الى التعرف على مخاطر الامن السيبراني وطرق مواجهتها ودراسة اليات حوكمة الشركات وتعزيزها كوسيلة لمعالجة مخاطر الامن السيبراني ،ولتحقيق هدف الدراسة وفرضيتها سيتم اجراء الدراسة الميدانية على عينة من مسؤولي إدارة الائتمان وادارة خدمة العملاء وادارة تكنولوجيا المعلومات وادارة المخاطر لعينة من المصارف المدرجة في سوق العراق للأوراق المالية وتوصل البحث الى مجموعة من الاستنتاجات أهمها أ، التطور الحادث في المخاطر السيبرانية يحفز المنظمات المالية وخاصة المصارف التجارية على البحث المستمر والمكثف نحو إتخاذ إجراءات وقائية من تلك المخاطر من خلال لوائح تجعل تلك الإجراءات أكثر وضوحاً أمام مجالس إدارات تلك المصارف ، الأمر الذي يؤدي إلى دعم الإستقرار المالي لها.

واوصت الدراسة على المصارف تعيين خبراء التكنولوجيا، وإنشاء لجان التكنولوجيا على مستوى مجلس الإدارة وتفويض المسؤوليات إلى لجنة التدقيق كوسيلة لإدارة مخاطر الأمن السيبراني و فهم الدور الحالي والمستقبلي لآليات الحوكمة في إدارة مخاطر الأمن السيبراني.

الكلمات المفتاحية: حوكمة الشركات، مخاطر الامن السيبراني، ادارة المخاطر

انتساب الباحثين

[1] كلية الادارة والاقتصاد، جامعة، واسط ، العراق، الكوت، 52001

[2، 3] ديوان الرقابة المالية الاتحادي، العراق، بغداد، 10011

[1] sismael@uowasit.edu.iq
[2]Inash0910@gmail.com
[3]Iraq000456@gmail.com

[1] المؤلف المراسل

معلومات البحث
تاريخ النشر: آب 2025

The Role of Corporate Governance in Addressing Cybersecurity Riske

Dr. Sura Waleed Ismael [1] , Dr. Inas Hasan Kazim [2] , Dr. Ali Khader Samir [3]

Abstract

The increasing dependence of companies, both public and private, on Web technologies and networks for their financial management systems has increased their exposure to cyber attacks, which is one of the main risks that companies must control. The goals of these attacks are multiple, as they may be aimed at stealing or destroying financial assets or... Theft of intellectual property or other critical information Boards of directors are also not adequately prepared to address cybersecurity risks due to lack of IT expertise. The aim of the research is to identify cybersecurity risks and ways to confront them, and to study and enhance corporate governance mechanisms as a means of addressing cybersecurity risks. To achieve the goal and hypothesis of the study, the field study will be conducted on a sample of credit management, customer service management, information technology management, and risk management officials for a sample of banks listed on the market. Iraq Securities and the research reached a set of conclusions, the most important of which is: The development occurring in cyber risks motivates financial organizations, especially commercial banks, to continuously and intensively research towards taking preventive measures against those risks through regulations that make those procedures more clear to the boards of directors of those banks, which It supports its financial stability.

The study recommended that banks appoint technology experts, establish technology committees at the board level and delegate responsibilities to the audit committee as a means of managing cybersecurity risks and understanding the current and future role of governance mechanisms in managing cybersecurity risks.

Keywords: corporate governance, cybersecurity risks, risk management

Affiliation of Authors

[1] College of Administration and Economics, University of Wasit, Iraq, Kut, 52001

[3 , 2] Federal Board of Upreme Audit, Iraq , Baghdad, 10011

[1] sismael@uowasit.edu.iq
[2]Inash0910@gmail.com
[3]Iraq000456@gmail.com

[1] Corresponding Author

Paper Info.
Published: Aug. 2025

المقدمة

في عصر تتسارع فيه التطورات التكنولوجية بشكل غير مسبوق، أصبحت البيانات والمعلومات الرقمية من أهم الأصول التي تعتمد عليها المؤسسات والشركات بمختلف أنواعها. ومع هذا الاعتماد المتزايد، برزت تحديات كبيرة تتعلق بالأمن السيبراني، حيث تشكل خروقات البيانات والهجمات الإلكترونية تهديدًا خطيرًا لاستمرارية الأعمال وسمعة المؤسسات ومصالح أصحاب المصلحة. ومن هنا تزايدت الحاجة إلى تطبيق مبادئ حوكمة الشركات بشكل فعّال لتعزيز الاستعداد للأخطار السيبرانية والحد من آثارها.

تلعب حوكمة الشركات دورًا محوريًا في بناء بيئة تنظيمية تضمن حماية الأصول المعلوماتية، من خلال وضع سياسات واضحة للمخاطر، ومراقبة الأداء، وتحميل المسؤوليات، وتعزيز الشفافية والمساءلة. ولا تقتصر أهمية الحوكمة على الوقاية من الهجمات فحسب، بل تمتد أيضًا إلى كيفية الاستجابة لها ومعالجة آثارها بما يحافظ على ثقة المستثمرين والعملاء وأصحاب العلاقة كافة

المبحث الاول

منهجية البحث

أولاً ـ مشكلة البحث

تتمثل مشكلة البحث الحالية في الاجابة عن السؤال الرئيسي التالي: (ماهي الاجراءات اللازمة لحوكمة الشركات للحد من مخاطر الامن السيبراني)

وينبثق عن هذا التساؤل مجموعة من التساؤلات الفرعية وهي:

1- هل هنالك وعي وادراك لعينة الدراسة بمخاطر الامن السيبراني وطرائق مواجهتها؟
2- هل هنالك تأثير لأبعاد حوكمة الشركات في تعزيز امن المعلومات في الوحدات الاقتصادية؟

ثانياً- هدف البحث

التعرف على مخاطر الامن السيبراني وطرق مواجهتها ودراسة اليات حوكمة الشركات وتعزيزها كوسيلة لمعالجة مخاطر الامن السيبراني و استعراض السياسات والممارسات التي تتبعها الوحدات الاقتصادية لحماية بياناتها.

ثالثاً- أهمية البحث

تنبع أهمية البحث من اهمية المشكلة التي يتناولها والتي تتمثل بتسليط الضوء على أهمية حوكمة الشركات في معالجة التهديدات السيبرانية والاجراءات اللازمة لموجهة المخاطر والحد المنها من خلال وضع استراتيجية متكاملة تقلل من تلك المخاطر وتعزيز قدرة الواحدة الاقتصادية على حماية بياناتها وعملياتها. .

رابعا : الحدود الزمانية والمكانية

الحدود الزمانية: فترة اعداد البحث من 2025/2/10 لغاية 2025/4/12

الحدود المكانية: مصرف بغداد التجاري

خامسا :اسلوب جمع البيانات

(أ) الكتب والمجلات العربية والاجنبية
(ب) الرسائل والاطاريح الجامعية المتوفرة في المكتبات او المنشورة
(ج) البحوث العلمية ذات الصلة بموضوع البحث المنشور على شبكة المعلومات الدولية .
(د) المقابلات الشخصية.

المبحث الثاني

الجانب المفاهيمي

أولاً : مفهوم حوكمة الشركات

تعد الحوكمة من المفاهيم التي زادت أهميتها على صعيد القطاعين العام والخاص لما لها من دور كبير في إدارة الشركة وحماية حقوق المساهمين لارتباطها ارتباطا وثيقا بالأزمات المالية الاقتصادية، فهي تؤثر على مهنة المحاسبة والتي بدورها تؤثر على عدالة القوائم والتقارير المالية التي يتم إعدادها وفقا للمبادئ والمعايير المحاسبية.

ويمكن استعراض بعض التعريفات الدولية وأشهر المنظمات التي تناولت مفهوم حوكمة الشركات كما يلي:

تعريف منظمة التعاون والتنمية الاقتصادية (OECD) "حوكمة الشركات تؤطر مجموعة من العلاقات بين إدارة الشركة ومجلس إدارتها وحملة الأسهم وغيرها من أصحاب المصالح، وهكذا فهي توفر الهيكل الذي من خلاله يتم تحديد الأهداف والوسائل التي تساعد في بلوغها، وتشخيص معايير الأداء اللازم لقياس مدى انجاز الأهداف [1] .

وعرفتها **مؤسسة التمويل الدولية (IFC)** بأنها النظام الذي يتم من خلاله إدارة الشركة والتحكم في أعمالها.

تعريف معهد المدققين الداخليين :هي العمليات التي تتم من خلال الإجراءات المستخدمة من ممثلي أصحاب المصالح، من أجل توفير إشراف على إدارة المخاطر ومراقبة مخاطر الشركة، والتأكيد على كفاية الضوابط لإنجاز الأهداف والمحافظة على قيم الشركة، من خلال أداء التحكم المؤسسي في الشركة .

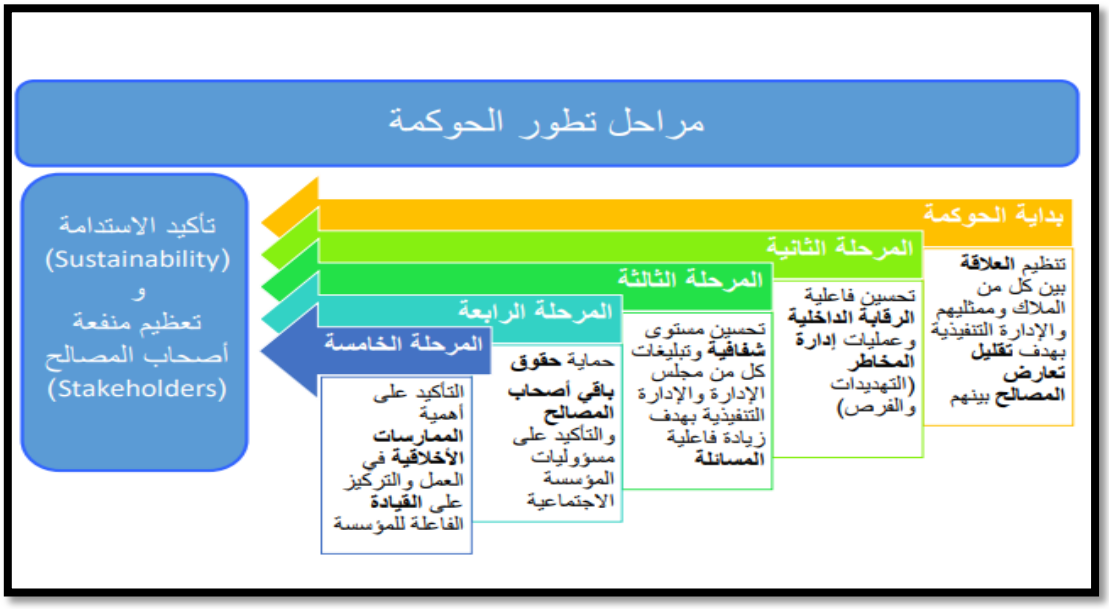
ثانياً : الاسباب التي دعت الى ظهور حوكمة الشركات

ارتباط مفهوم حوكمة الشركات بمفهوم انفصال الملكية عن الادارة في انظمة شركات المساهمة والتي تسمى بنظرية الوكالة ، والتي تعني بتعارض مصالح المدراء التنفيذيين مع طموحات المساهمين وبسبب كبر حجم الشركات وتعقيد عملياتها اصبح هناك الكثير من العلاقات المتعددة في الشركة ، مثل العلاقة بين المستثمرين والمراجع الخارجي وبين المستثمرين والمقرضين والدائنين وغيرهم من اصحاب العلاقات داخل وخارج الشركة ولان كل طرف مصلحة مختلفة عن الطرف الاخر فان كل منهم يسعى الى تعظيم منافعه وتحقيق مصالحة ولو على حساب الفئات الاخرى ، ومن هنا تسعى الحوكمة الى ضمان وجود انضباط سلوكي متوازن لتحقيق المصالح المختلفة لجميع الاطراف وتحقيق كيفية الرقابة الفعالة وادارة المخاطر ، كما ان الاخطاء التي حدثت خلال العقدين الماضيين لا فلاس العديد من الشركات العالمية الكبرى مثل انرون وورلد كوم ،ليست هي فقط التي ابرزت اهمية الحوكمة ، بل كان هنالك فجوة كبيرة بين اداء الشركات وما يحصل عليه المدراء من مكافأة ، اضافة الى اساءة استخدام خيارات الاسهم والتي يقصد بها منح اعضاء الادارة الحق في شراء عدد من اسهم الشركة بسعر محدد مسبقا وعادة ما يزيد عن السعر الذي يتداول به السهم في السوق ، واذا كان الهدف من تلك الخيارات هو حث الادارة على بذل الجهد لتحسين الاداء حتى يرتفع سعر السهم الى مستوى يفوق السعر المحدد في خيار الاسهم ليجني المدراء الارباح الا ان الهدف قد اساء استخدامه ، فقد ركزت الادارة في كثير من الاحيان على الانشطة التي تحقق ارباحا سريعة متجاهلة في ذلك تاثيرها السلبي في المدى الطويل [2] .

وما يلي ملخص أسباب ظهور حوكمة الشركات [3] :

1- حالات الفشل المؤسسي في امريكا وروسيا ودول اسيا .
2- عدم فاعلية اجراءات الرقابة الداخلية التي لا يمكنها اكتشاف ومنع الاخطاء.
3- ضعف مجلس الادارة الذي يمكن ان يؤثر على الادارة التنفيذية والعليا وقد تعاني القصور في قدرتها على القيام بممارسات ادارية ناجحة.
4- عدم توافر الدقة والشفافية في اعداد القوائم المالية .
5- عدم قدرة المستثمرين على تحليل ومقارنة فرص الاستثمار المحتملة .
6- ضعف الاطراف الخارجية في رقابتها للمنشاة كالقائمين على وضع القوانين ومراجعي الحسابات.
7- الممارسات الغير صحيحة من قبل الادارة والادارة التنفيذية والموظفين

الحوكمة مرت بعدة مراحل رئيسية عبر الزمن، بناءً على الحاجة إلى تحسين إدارة المؤسسات والرقابة عليها. بشكل مبسط، يمكننا تلخيص مراحل تطور الحوكمة وكما موضح في الشكل (1) .



الشكل (1) : يوضح مراحل تطور الحوكمة

ثالثاً : مفهوم الأمن السيبراني

يشير الامن السيبراني الى حماية لموجودات الرقمية من المخاطر الموجودة نتيجة استعمال الاتصالات وتكنولوجيا معلومات التي تشكل اساس الفضاء الالكتروني [4] وقد عرف اطار NSIT الامن السيبراني " بانه عملية حماية المعلومات من خلال اكتشاف ومنع والرد على الهجمات السيبرانية ، كما تم تعريف حادثة الامن السيبراني بانه الحادثة التي يكون لها تأثير على الوحدة الاقتصادية مما يستدعي الحاجة للرد والتعافي ، وتتمثل حوادث الامن السيبراني بفشل نظم المعلومات واختراق البيانات وما يترتب عليها من خسائر فادحة في بيانات الوحدة الاقتصادية وممتلكاتها ، واضراراً كبيرة بسمعتها وبنيتها الرئيسة". [5] .

كام تم تعريفه من قبل **[6]** بانه النشاط الذي يؤمن حماية الموارد المالية والبشرية ذات العلاقة بتقنيات المعلومات والاتصالات وامكانية الحد من الاضرار و الخسائر التي تترتب في حال تحقق التهديدات والمخاطر كما يتيح اعادة الوضع الى ماكان عليه بأسرع ما يمكن بحيث لا تتحول الاضرار الى خسائر مادية ولا تتوقف عجلة الانتاج.

وهنالك عدة انواع للهجمات السيبرانية والتي يمكن تصنيفها استناداً إلى المعلومات المطلوبة للمتطفلين و نية المهاجمين ، البرامج الضارة التي يتم تفعيلها عندما ينقر المستعمل على رابط غير مصرح به أو بريد الكتروني مرفق.

ويمكن تصنيف تدابير الامن السيبراني إلى خمسة أنواع رئيسة هي : التدابير التي تركز على أمن الشبكة و وامن السحابة ، أمن التطبيقات ، الامن التشغيلي ،وتدريب المستعملين وامن المعلومات ، وقد تتضمن بعض الاجراءات بروتوكولات كلمة المرور والمصادقة، منهجيات التشفير، وجدران الحماية ، والماسحات الضوئية للبرامج الضارة واستعمال برامج برامج مكافحة الفايروسات [7] .

رابعاً : مخاطر الامن السيبراني

يقصد بمخاطر الامن السيبراني المخاطر التشغيلية على اصول التكنولوجيا والمعلومات التي تؤثر على سلامة وسرية ونظم المعلومات ومقارنة بأنواع المخاطر التي يغطيها التأمين فأن مخاطر الامن السيبراني تتفق من حيث المسؤولية والخصائص مع مخاطر كل من الممتلكات والخصوم والمخاطر الكارثية والتشغيلية ايضاً. ومما لاشك فيه ان تكنولوجيا المعلومات تتيح امكانيات غير مسبوقة وهائلة لانتاجية افضل في القطاعات كافة والتواصل عبر القارات إلا ان البنى التحتية لهذه التقنيات تمثل ارتباطاً بين خدمات مختلفة و مصالح متعددة ودول عدة الامر الذي يجعل من مخاطر الامن السيبراني مخاطر عالمية **[8].**

وبينت دراسة **[9]** ان مخاطر الامن السيبراني تضم ثلاثة انواع وهي كالاتي:

1- مخاطر تتعلق بالسرية : تنشأ عندما يتم الكشف عن البيانات الخاصة داخل الوحدة الاقتصادية إلى اطراف اخرى كما في حال حدوث اختراق للبيانات.
2- مخاطر تتعلق بالنزاهة : تلك التي تنشأ بسبب اساءة استعمال الانظمة كما هو الحال بالنسبة للاحتيال.
3- مخاطر تتعلق باستمرارية الاداء: تلك التي تنشأ بسبب توقف أو تعطيل في ممارسة الأعمال.

وهنالك ثلاث سمات رئيسة للممارسة دفاع الكتروني متوازن وفعال: آمناً ومدركاً ومقاوماً [8]

- آمناً: عن طريق التركيز على توفير الحماية ضد المخاطر ،تتضمن المخاطر على الموجودات الاكثر قيمة للأعمال من وجهة نظر الوحدة الاقتصادية ومنافسيها.
- مدركاً : عن طريق زيادة الوعي في كل مستوى من مستويات الوحدة الاقتصادية وتطوير القدرة على اكتشاف اي سلوك مصاحب بالمخاطر مرتبط بالموجودات قبل حدوث هذا السلوك.
- مقاوماً : أي القدرة على سرعة الاستجابة للضرر بما يضمن عدم تأثيره على العمليات الاخرى ، والقدرة على استعمال الأدوات الضرورية والمتعددة من اجل تخفيض الأضرار التي تنطوي على تكاليف مباشرة ، وفقدان عبء العمل وقيمة العلامة التجارية والإضرار بالسمعة.

تم انشاء خمس وظائف رئيسة لحماية الموجودات الرقمية كاطار عمل من قبل (NIST) المعهد الوطني للمعايير والتكنلوجيا (ENISA) وكالة الاتحاد الأوربي لأمن الشبكات والمعلومات وتتضمن الانشطة التالية: [10]

- التحديد: استعمال الفهم التنظيمي لتقليل المخاطر على الموجودات والأنظمة والبيانات والقدرات.
- الحماية : ضمانات التصميم للحد من تأثير الاحداث المحتمل حدوثها على البنى التحتية والخدمات الحيوية.
- الكشف: تنفيذ الانشطة لتحديد وقوع حدث خطر الامن السيبراني.

- الاستجابة: اتخاذ الاجراءات الملائمة بعد التعرف على الحدث الأمني.
- التعافي: التخطيط للقدرة على اصلاح القدرات والخدمات المعرضة للخطر في الوقت المناسب.

ولرفع درجة الوعي الأمني بالوحدات الاقتصادية ينبغي وضع برنامج تدريبي داخلي متخصص للملاك الفني القائم على أدارة الانظمة التكنولوجية لرفع درجة الوعي بأمن المعلومات ، والتأكد من جاهزيتها لمواجهة الهندسة الاجتماعية وطرق تجنب التصيد الاحتيالي ، وذلك بشكل دوري لمواكبة كل جديد في هذا المجال سريع التغير، وينبغي تثقيف وتدريب الموظفين كافة وارسال رسائل توعية دورية للزبائن في الوقت ذاته لرفع درجة الوعي لديهم اتجاه المحاولات الاختراق والاحتيال الالكتروني.

كما وضع المعهد الامريكي للمحاسبين القانونيين إطار للتقرير عن ادارة مخاطر الأمن السيبراني في عام 2017 لإرشاد الوحدات الاقتصادية ودعمهم في الافصاح عن مخاطر الأمن السيبراني ، ويتضمن الاطار ثلاث عناصر رئيسة وهي :وصف الادارة لبرنامج إدارة مخاطر الأمن السيبراني للوحدة الاقتصادية ،وتأكيدات الادارة بخصوص فاعلية ضوابط الأمن السيبراني، و رأي المدقق الخارجي في إفصاحات الادارة عن وفاعلية ضوابط الوحدة الاقتصادية.

وقد تم وصف برنامج لإدارة مخاطر الأمن السيبراني من خلال العناصر الآتية [11]

1- طبيعة اعمال الوحدة الاقتصادية وعملياتها وتتضمن المنتجات أو الخدمات الرئيسة التي تقدمها والطرق التي يتم بها توزيعها.
2- الانواع الرئيسة من المعلومات المهمة التي يتم إنشاؤها ، تجميعها ، إرسالها ، استعمالها، وتخزينها بواسطة الوحدة الاقتصادية.
3- أهداف برامج إدارة مخاطر الأمن السيبراني وتتضمن الأهداف الرئيسة الخاصة بتوافر البيانات وسريتها وسلامتها وسلامة المعالجة.
4- العوامل التي لها تأثير كبير على مخاطر الأمن السيبراني وتتضمن :انواع الاتصال وخصائص التكنلوجيا ، استعمال مقدمي الخدمات وقنوات التسليم التي تستعملها الوحدة الاقتصادية ، الخصائص التنظيمية وخصائص المستعمل، والتغييرات التكنلوجية والتنظيمية و البيئية وغيرها خلال فترة وصف الوحدة الاقتصادية لبرنامج إدارة مخاطر الأمن السيبراني.
5- هيكل حوكمة إدارة المخاطر ويتضمن عملية إنشاء وصيانة والتقرير عن النزاهة والقيم الاخلاقية لدعم عمل برنامج إدارة مخاطر الأمن السيبراني ، فضلاً عن عملية اشاف مجلس الادارة على برنامج إدارة مخاطر الأمن السيبراني للوحدة الاقتصادية ، واسس المسائلة وخطوط التقرير في مجال الامن السيبراني، فضلاً عن العملية المستعملة لتوظيف وتطوير الأفراد والمتعاقدين الكفء ومحاسبتهم عن مسؤولياتهم المتعلقة بالامن السيبراني.
6- عملية إدارة مخاطر الأمن السيبراني : وتتضمن عملية تحديد مخاطر الأمن السيبراني والتغيرات البيئية والتنظيمية والتكنلوجية التي من المحتمل أن يكون لها تأثير جوهري على برنامج إدارة المخاطر للوحدة الاقتصادية وتقدير المخاطر الخاصة بها ولها تأثير على تحقيق أهداف الامن السيبراني.
7- قنوات اتصال وجودة معلومات الأمن السيبراني .
8- رقابة برنامج ادارة مخاطر الأمن السيبراني وتتضمن عملية اجراء تقييمات مستمرة ودورية للفاعلية التشغيلية لانشطة الرقابة الرئيسة والمكونات الاخرى للرقابة الداخلية ذات العلاقة بالأمن السيبراني.
9- أنشطة مراقبة الأمن السيبراني : وتتضمن عملية تطوير للاستجابة للمخاطر المتوقعة بما في ذلك تصميم وتنفيذ عمليات الرقابة .

خامساً : إطار تحسين البنية الاساسية للأمن السيبراني

صدر هذا الاطار عن NIST حيث بدأ العمل بالمشروع في عام 2013 من خلال دعوتها للأفراد والمنظمات في القطاعين العام والخاص ، وصدرت نسخته الأولى عام 2014 وتم تنقيحه في عامي 2017 و2018 ركز الاطار على النظر في مخاطر الامن السيبراني كجزء من إدارة المخاطر الوحدات الاقتصادية وأنشطة الأمن السيبراني ويتكون من ثلاثة اجزاء هي جوهر الاطار ، مستويات التنفيذ و الملف الشخصي.

ويتمثل جوهر الاطار في مجموعة من الانشطة والنتائج المرغوبة للأمن السيبراني يتم تنظيمها بفئات تتلاءم مع المراجع الاعلامية ، ويحدد خمسة وظائف رئيسة وهي : التحديد ،الحماية ، الاكتشاف ، الرد ، الاستعادة **[12]**

تصف مستويات التنفيذ إلى أي مدى تتلاءم ممارسات إدارة مخاطر الأمن السيبراني في الوحدة الاقتصادية مع الخصائص المحددة لهذا الاطار، ويمثل الملف الشخصي التوافق الفريد بين المتطلبات التنظيمية وأهداف الوحدة الاقتصادية وقابليتها للمخاطر والموارد مقارنة بالنتائج المتوقعة من إطار العمل **[13]**

ويتميز إطار تحسين البنية الاساسية للأمن السيبراني **[13]**

1- قابل للتطبيق على الوحدات الاقتصادية التي تعتمد على التكنلوجيا .
2- في مجال تعزيز الامن السيبراني يمكن أن يكون انموذجاً للتعاون الدولي كونه يشير إلى معايير معترف بها دولياً للأمن السيبراني .
3- يوفر طريقة مرنة لمعالجة الامن السيبراني بما في ذلك تأثيره على الابعاد الالكترونية والمادية والافراد.
4- يوفر هيكل تنظيمي مشترك لمناهج متعددة لتحقيق الامن السيبراني بواسطة تجميع الممارسات والمبادئ الاسترشادية والمعايير التي تعمل بصورة فعالة حالياً

سادساً - مساهمة الحوكمة في تعزيز أمن المعلومات:

خلال عامي 2006 و 2008 قام معهد تكنلوجيا المعلومات باصدار نسختين من إطار عمل Val IT فضلاً عن اصدار إطار Risk IT في عام 2009 ' وهذه الاصدارات تناولت المسؤوليات والعمليات ذات العلاقة بتكنلوجيا المعلومات ودورها في إدارة المخاطر و خلق القيمة وتعد هذه الاصدارات اعمال تكميلية لكل من COBIT4 و COBIT4.1 الصادر عام 2007وقد تم دمج هذه الأطر معاً من قبل معهد تكنلوجيا المعلومات خلال عام 2012 واصدار COBIT5 إذ يعد اطار شامل للوحدات الاقتصادية في تحقيق اهدافها لإدارة وحوكمة تكنلوجيا المعلومات ويساعد ها في خلق قيمة مثالية من خلال الحفاظ على التوازن بين تحقيق المنافع وتحسين استعمال الموارد ومستويات المخاطر **[11].**

وقدم COBIT5 خمسة مبادئ تعمل على تمكين الوحدات الاقتصادية من بناء اطار ادارة وحوكمة فعالة وهذه المبادئ هي : تلبية احتياج اصحاب المصلحة ، تطبيق اطار واحد متكامل ، فصل الحوكمة عن الادارة ، تغطية الوحدة الاقتصادية من البداية إلى النهاية ، تمكين المنهج الشمولي.

تم اصدار النسخة الحالية من الاطار تحت مسمى COBIT2019 في نوفمبر 2018 يهدف الى توفير مرونة اعلى في تنفيذ حوكمة تكنولوجيا المعلومات EGIT بالمقارنة مع الاطر السابقة يتميز إطار COBIT2019 بما يلي **[12]**

1- يقدم ثلاث أهداف جديدة للإدارة والحوكمة وكل هدف يرتبط بعملية تتعلق بالمشروعات والبيانات والتأكيد.
2- يحدد مكونات النظام الفعال لحوكمة تكنلوجيا المعلومات.
3- يقدم سلسلة اهداف محدثة.
4- يحدد عوامل التصميم التي ينبغي اخذها في الاعتبار عند تصميم وتنفيذ حوكمة تكنلوجيا المعلومات .
5- يقدم مفهوم مجالات التركيز والذي يركز على مواقف محدد لحل المشاكل.

"وتم تنظيم الاطار في اربعة اقسام رئيسة: مقدمة ، منهجية، أهداف الحوكمة والادارة، دليل التصميم ، دليل التنفيذ، كما قدم الاطار ستة مبادئ تصف المتطلبات الاساسية لحوكمة تكنلوجيا المعلومات وهي : تقديم قيمة لاصحاب المصلحة ، مصممة وفقا لاحتياجات المنظمة ، نظام حوكمة ديناميكي ، فصل الحوكمة عن الادارة ، نظام حوكمة شامل ، تمكين المنهج الشمولي".[14]

كما أن حوكمة الشركات تلعب دوراً حاسماً في تعزيز الأمن السيبراني من خلال وضع وتطبيق سياسات فعالة و تشجيع الإدارة التنفيذية والمجالس الإدارية على فهم التهديدات السيبرانية والتعامل معها يمكن أن يقلل من المخاطر ويحمي بيانات الوحدة الاقتصادية عبر العديد من الطرق، منها [15]

1. إطار سياسات قوي: توفير إطار عمل وسياسات واضحة وشاملة للأمن السيبراني يضمن تحديد المسؤوليات والصلاحيات داخل الشركة بشكل واضح.
2. الرقابة والإشراف: وجود لجان مختصة ضمن هيكل الشركة، مثل لجنة التدقيق ولجنة المخاطر، يعزز الرقابة على تطبيق إجراءات الأمن السيبراني ويضمن التزام كافة الأقسام بها.
3. ثقافة الشركة: تشجيع ثقافة الأمن السيبراني بين الموظفين يساعد في تقليل الأخطاء البشرية التي قد تؤدي إلى حوادث أمنية.
4. التدريب والتوعية: توفير برامج تدريبية مستمرة حول الأمن السيبراني يعزز من قدرة الموظفين على التعرف على التهديدات والتعامل معها بفعالية.
5. التقييم والتحسين المستمر: إجراء تقييمات دورية لمخاطر الأمن السيبراني والتحديث المستمر للسياسات والإجراءات بناءً على هذه التقييمات يضمن جاهزية الشركة لمواجهة التهديدات الجديدة والمتطورة.

6. التكنولوجيا الحديثة: استثمار في تقنيات متقدمة للحماية السيبرانية يعزز من قدرة الشركة على اكتشاف ومنع الهجمات السيبرانية.
7. الاستجابة للحوادث: وجود خطط استجابة فعالة للحوادث السيبرانية يضمن تقليل الأضرار الناجمة عن أي خرق أمني وسرعة التعافي منه.

المبحث الثالث

الجانب العملي

في ظل التحول الرقمي المتسارع الذي يشهده القطاع المصرفي، أصبحت المصارف والمؤسسات المالية أكثر عرضة لمخاطر خروقات الأمن السيبراني، والتي قد تؤدي إلى خسائر مالية جسيمة، وتضر بسمعة المؤسسة، وتؤثر سلباً على ثقة العملاء. ومع تزايد هذه التحديات، برزت أهمية حوكمة الشركات كإطار تنظيمي واستراتيجي يساهم في تعزيز جاهزية المصارف لمواجهة التهديدات السيبرانية، والحد من آثارها، وتحقيق الاستدامة المؤسسية. ، اذ يتم ذلك من خلال استعمال قائمة الفحص (checklist) في تحليل الفجوات والتي تم الاشارة اليها في المستخلص وبعد تشخيص الفجوة لكل متطلب سيتم مناقشة الاسباب التي ادت لظهور هذه الفجوة ومدى امكانية التغلب عليها علماً أنَّ مصرف بغداد التجاري لديه معلومات كافية عن هذه القائمة وله القدرة عن الاجابة عن هذه المعلومات اذ سيعتمد الباحثين هذهِ القائمة لملئها بالمعلومات المطلوبة عن طريق المقابلات الشخصية والمشاهدات الفعلية للتأكد من دقة المعلومات، باستعمال المقياس السباعي والمبين وفقاً للأوزان من (0) اقل وزن الى (6) اعلى وزن كما موضح في الجدول (1)

جدول (1) : يبين المقياس السباعي

التسلسل	فقرات المقياس السباعي	الوزن (الدرجة)
1	مطبق كلياً وموثق كلياً	6
2	مطبق كلياً وموثق جزئياً	5
3	مطبق كلياً وغير موثق	4
4	مطبق جزئياً وموثق كلياً	3
5	مطبق جزئياً وموثق جزئياً	2
6	مطبق جزئياً وغير موثق	1
7	غير مطبق وغير موثق	0

اولاً :- تحليل بيانات قائمة الفحص الخاصة بالمتطلبات

اعتمدت البنود الرئيسة والفرعية في بناء قائمة الفحص (Checklist) الخاصة بمتطلبات تطبيق المعايير الدولية للتدقيق الداخلي ومتطلبات ممارسات المحاسبة الابتكارية كما سيجري إيجاد الفجوات في المؤسسة التعليمة الخاصة وحسب المعادلات التالية :

الوسط الحسابي = مجموع (الأوزان × تكراراتها) / مجموع التكرارات **(1)**

النسبة المئوية لمدى المطابقة = (الوسط الحسابي المرجح) ÷ قيمة أعلى وزن في المقياس (6) **(2)**

حجم الفجوة لكل قائمة فحص = 1 – النسبة المئوية لمدى المطابقة **(3)**

1- متطلبات تطبيق حوكمة الشركات

تعد حوكمة الشركات من الركائز الأساسية لتعزيز الشفافية والمساءلة وتحقيق الاستدامة في المصارف ، فإن المصارف تتطلب نماذج حوكمة فعّالة لضمان إدارة المخاطر بشكل سليم، وحماية حقوق المودعين والمساهمين، وتعزيز الثقة في القطاع المصرفي. وتتمثل متطلبات تطبيق الحوكمة في المصارف بمجموعة من المعايير والإجراءات التي تضعها الجهات الرقابية والتنظيمية، وتشمل وجود هيكل تنظيمي واضح، فصل السلطات بين الإدارة التنفيذية ومجلس الإدارة، ضمان استقلالية لجان الرقابة والتدقيق، وتطبيق مبادئ الشفافية والإفصاح. ولهذا فنوضح قائمة الفحص في جدول رقم (4) مستوى التطبيق والتوثيق الفعلي في داخل المصارف الخاصة التي تبين لنا ان معدل التطبيق الفعلي

لمتطلبات تطبيق حوكمة الشركات (**95%**) درجة من اصل (6) درجات وان نسبة التوثيق والتطبيق (**15.8%**) ما يدل على وجود فجوه في التطبيق تصل الى (**84.2%**) ناجمة عن مستوى مطبق كليا وموثق كليا وكما موضح في الجدول (2).

جدول (2) : قائمة فحص متطلبات حوكمة الشركات

ت	متطلبات تطبيق حوكمة الشركات	مستوى التطبيق والتوثيق						
		مطبق كلياً وموثق كلياً	مطبق كلياً وموثق جزئياً	مطبق كلياً وغير موثق	مطبق جزئياً وموثق كلياً	مطبق جزئياً وموثق جزئياً	مطبق جزئياً وغير موثق	غير مطبق وغير موثق
	أولاً: مجلس الإدارة							
1	**هل تم تحديد عدد أعضاء مجلس الإدارة بوضوح؟**	*						
2	**هل يوجد أعضاء مستقلون في المجلس؟**		*					
3	**هل يتم اختيار الأعضاء بناءً على كفاءة وخبرة واضحة؟**	*						
4	**هل تُعقد اجتماعات المجلس بانتظام؟**		*					
5	**هل يتم الاحتفاظ بمحاضر الاجتماعات وتوثيقها؟**		*					
6	**هل تم تحديد مهام وصلاحيات المجلس بدقة؟**	*						
7	**هل توجد لجان متخصصة (مثل لجنة التدقيق، لجنة الترشيحات والمكافآت)؟**	*						
	ثانيًا: الإفصاح والشفافية							
8	**هل تُفصح الشركة عن معلوماتها المالية وغير المالية بانتظام؟**	*						
9	**هل تُعد التقارير السنوية وتتضمن**					*		

	تقرير الحوكمة؟							
10	هل يتم الإفصاح عن مصالح أعضاء المجلس والإدارة التنفيذية؟					*		
11	هل توجد سياسة واضحة للتعامل مع الأطراف ذات العلاقة؟		*					
	ثالثًا: حقوق المساهمين							
12	هل تُحترم حقوق جميع المساهمين بالتساوي؟	*						
13	هل تُتاح للمساهمين المعلومات في الوقت المناسب؟		*					
14	هل يُسمح للمساهمين بالمشاركة والتصويت في الجمعيات العمومية؟		*					
	رابعًا: الرقابة الداخلية وإدارة المخاطر							
15	هل توجد وحدة للرقابة الداخلية مستقلة؟	*						
16	هل تم اعتماد إطار واضح لإدارة المخاطر؟	*						
17	هل يتم تقييم فعالية الرقابة الداخلية بشكل دوري؟			*				
	خامسًا: السلوك المهني والمسؤولية الاجتماعية							
18	هل لدى الشركة مدونة سلوك أو ميثاق أخلاقي؟		*					
19	هل يتم تدريب الموظفين على الالتزام بالقيم المؤسسية؟		*					
2	هل تُطبق مبادئ	*						

0	المسؤولية الاجتماعية والبيئية؟							
	الاوزان	0	1	2	3	4	5	6
	التكرارات	9	8	1	0	1	1	0
	ناتج (الوزن * عدد التكرارات)	0	8	2	0	4	5	0
	المعدل الموزون (الوسط الحسابي المرجح)	%95						
	النسبة المئوية للتطبيق	%15.8						
	حجم الفجوة للمتطلب	%84.2						

المصدر : اعداد الباحثين

من خلال نتائج قائمة الفحص تبين الآتي:

أ- نقاط القوة

- وجود اهتمام مبدئي بتطبيق الحوكمة: مجرد قياس الفجوة ووجود إطار تطبيقي يدل على بدء التحول نحو الحوكمة.
- الإفصاح المنتظم عن المعلومات المالية وغير المالية من أبرز نقاط القوة في المصرف، حيث يُعزّز الشفافية ويُرسّخ الثقة بين المصرف وأصحاب المصلحة، كما يُظهر التزامه بالأنظمة الرقابية ويسهم في دعم قرارات المستثمرين والعملاء بناءً على بيانات دقيقة وواضحة
- إمكانية تحسين الأداء المؤسسي: الفجوة الكبيرة تتيح مساحة واسعة للتحسين، مما يجعل النتائج المترتبة على الإصلاح أكثر وضوحًا وتأثيرًا.
- توفر بعض السياسات والإجراءات ووجود لجان متخصصة مثل لجنة التدقيق ولجنة الترشيحات والمكافآت يعزز من الحوكمة الرشيدة ويُسهم في تحسين الرقابة الداخلية، وضمان الشفافية، واتخاذ قرارات استراتيجية مبنية على كفاءة وخبرة الأعضاء قد تكون هناك بعض اللوائح أو السياسات الجزئية التي يمكن البناء عليها.
- اعتماد إطار واضح لإدارة المخاطر من أبرز نقاط القوة في المصرف، حيث يسهم في تعزيز القدرة على التنبؤ بالمخاطر والتعامل معها بفعالية، مما ينعكس إيجاباً على دقة اتخاذ القرار واستدامة العمليات. كما يضمن هذا الإطار الامتثال للمتطلبات التنظيمية، ويحمي أصول المصرف من الخسائر المحتملة، ويعزز ثقة العملاء والمستثمرين بقدرة المصرف على إدارة التحديات بكفاءة .

ب- نقاط الضعف

- ضعف الالتزام بالمعايير: يشير الرقم إلى عدم الالتزام الكافي بمبادئ الحوكمة مثل الشفافية، المساءلة، والعدالة.
- غياب البنية التنظيمية الفعالة: قد تفتقر المصارف إلى هياكل إدارية واضحة ومسؤولة عن تنفيذ الحوكمة.
- قلة الخبرات والكوادر المؤهلة: نقص الكفاءات القادرة على تنفيذ ومراقبة مبادئ الحوكمة.
- محدودية الوعي والثقافة التنظيمية: الثقافة المؤسسية قد لا تعزز ممارسات الحوكمة.
- عدم استقلالية مجلس الإدارة: من الممكن أن يكون هناك تأثير خارجي على قرارات المجلس.

2- متطلبات تطبيق الامن السيبراني

في ظل التطور المتسارع للتكنولوجيا والتحول الرقمي في القطاع المصرفي، أصبحت المصارف أكثر عرضة للتهديدات السيبرانية والهجمات الإلكترونية. هذه التهديدات قد تؤدي إلى خسائر مالية جسيمة، وانتهاك خصوصية العملاء، وتقويض الثقة في النظام المصرفي ككل. و لتطبيق متطلبات الأمن السيبراني لحماية البنية التحتية الرقمية للمصارف وضمان استمرارية العمل والامتثال للأنظمة والتشريعات المحلية والدولية. تتضمن متطلبات الأمن السيبراني في المصارف مجموعة من السياسات والإجراءات الفنية

والتنظيمية التي تهدف إلى تأمين الأنظمة المصرفية، حماية بيانات العملاء، إدارة المخاطر السيبرانية، وتدريب الكوادر البشرية على أفضل ممارسات الأمن المعلوماتي ، ولهذا فنوضح قائمة الفحص في جدول رقم (5) مستوى التطبيق والتوثيق الفعلي في داخل المصرف التي تبين لنا ان معدل التطبيق الفعلي لمتطلبات ادارة التكلفة الاستراتيجية (491.3%) درجة من اصل (6) درجات وان نسبة التوثيق والتطبيق (81.8%) ما يدل على وجود فجوه في التطبيق تصل الى (18.2%) ناجمة عن مستوى مطبق كليا وموثق جزئي وكما موضح في الجدول (3)

جدول (3) : قائمة فحص الامن السيبراني

ت	متطلبات تطبيق الامن السيبراني	مستوى التطبيق والتوثيق						
		مطبق كلياً وموثق كلياً	مطبق كلياً وموثق جزئياً	مطبق كلياً وغير موثق	مطبق جزئياً وموثق كلياً	مطبق جزئياً وموثق جزئياً	مطبق جزئياً وغير موثق	غير مطبق وغير موثق
	أولاً: الحوكمة والاستراتيجية							
1	هل لدى الشركة سياسة أمن سيبراني معتمدة من مجلس الإدارة؟			*				
2	هل تم دمج الأمن السيبراني ضمن الاستراتيجية العامة للشركة؟						*	
3	هل يتم مناقشة المخاطر السيبرانية في اجتماعات مجلس الإدارة بانتظام؟							*
	ثانياً: الأدوار والمسؤوليات							
4	هل تم تحديد مسؤوليات واضحة للأمن السيبراني ؟			*				
5	هل جميع المستويات الإدارية على دراية بأدوارها في الوقاية والاستجابة للهجمات؟					*		
6	هل هناك نظام تصعيد							*

	Escalation) Protocol) لتبليغ القيادة العليا بالخرق؟							
	ثالثاً: إدارة المخاطر السيبرانية							
7	هل يتم إجراء تقييمات دورية للمخاطر السيبرانية؟					*		
8	هل تم تحديد أصول البيانات الأكثر أهمية وحمايتها؟				*			
9	هل هناك خطة لإدارة الأزمات/الاستجابة للحوادث السيبرانية؟							*
10	هل يتم فحص الطرف الثالث (الموردين/الشركاء) من حيث التهديدات السيبرانية؟							*
	رابعاً: التدقيق والمراجعة							
11	هل يتم تنفيذ مراجعات داخلية وخارجية دورية للأمن السيبراني؟					*		
12	هل تم تنفيذ اختبار اختراق أو تقييم أمني حديث؟							*
13	هل هناك نظام لرصد الامتثال للسياسات السيبرانية؟				*			
	خامساً: الاستجابة والتعافي من الحوادث							
14	هل لدى الشركة خطة استجابة واضحة لحوادث							*

	الأمن السيبراني؟							
15	هل تم اختبار الخطة ميدانيًا (Simulation / Tabletop Exercises)؟							*
16	هل يوجد سجل للحوادث السابقة وتقييمات الاستجابة لها؟							*
17	هل يتم إبلاغ الجهات القانونية والتنظيمية بشكل مناسب عند حدوث خرق؟							*
	سادساً: التدريب والتوعية							
18	هل يتم تدريب الموظفين بانتظام على الأمن السيبراني؟		*					
19	هل تشمل التوعية جميع مستويات الشركة، بما فيها الإدارة العليا؟					*		
20	هل هناك إجراءات محددة للإبلاغ عن التصيد الاحتيالي أو الأنشطة المشبوهة؟						*	
	سابعاً: الشفافية والإفصاح							
21	هل لدى الشركة سياسة إفصاح عن الخروقات السيبرانية؟							*
22	هل يتم إبلاغ أصحاب المصلحة والعملاء في الوقت المناسب؟							*
23	هل تمت مراجعة							*

	مدى التزام الشركة باللوائح المحلية والدولية المتعلقة بالإفصاح السيبراني (مثل GDPR، NCA، إلخ)؟							
	الاوزان	0	1	2	3	4	5	6
	التكرارات	0	1	2	0	4	4	12
	ناتج (الوزن * عدد التكرارات)	0	1	4	0	16	20	72
	المعدل الموزون (الوسط الحسابي المرجح)	%491.3						
	النسبة المئوية للتطبيق	%81.8						
	حجم الفجوة للمتطلب	%18.2						

المصدر : اعداد الباحثين

من خلال نتائج قائمة الفحص تبين الآتي :

أ- نقاط القوة

- عد وجود سياسة أمن سيبراني معتمدة من مجلس الإدارة إحدى نقاط القوة الأساسية في المصرف، حيث يعكس هذا الالتزام المؤسسي العالي أهمية حماية المعلومات والأنظمة، ويعزز القدرة على مواجهة التهديدات السيبرانية بفعالية، مع ضمان الامتثال للمعايير التنظيمية وتعزيز ثقة العملاء والشركاء وجود سياسات أمنية واضحة: توفر سياسات أمن معلومات مكتوبة ومحدثة.
- الاهتمام المستمر بتدريب الموظفين على مفاهيم الأمن السيبراني، مما يُعزز من وعيهم الأمني ويُقلل من مخاطر الهجمات الإلكترونية، ويُساهم في حماية بيانات العملاء والأنظمة المصرفية.
- استخدام تقنيات تشفير قوية لحماية بيانات العملاء والمعاملات.
- فريق متخصص بالأمن السيبراني: وجود قسم داخلي أو شراكة مع شركات أمنية متخصصة لمراقبة الأمن السيبراني بشكل دائم.

ب- نقاط الضعف

- ضعف التحديثات والصيانة الدورية اذ ان التأخر في تحديث الأنظمة والتطبيقات قد يخلق ثغرات أمنية.
- الهندسة الاجتماعية وضعف وعي بعض الموظفين: إمكانية استغلال الموظفين غير المدرّبين في هجمات التصيّد أو الابتزاز الإلكتروني.
- يفتقر المصرف إلى خطة واضحة ومحدثة لإدارة الأزمات المتعلقة بالحوادث السيبرانية، مثل الهجمات الإلكترونية، اختراق البيانات، أو الأعطال التقنية الكبيرة. وهذا يشمل غياب الإجراءات الموثقة، فرق الاستجابة، قنوات الاتصال، وتحديد الأدوار والمسؤوليات خلال الطوارئ
- غياب سياسة إفصاح واضحة عن الخروقات السيبرانية في المصرف يُعد من نقاط الضعف في إطار الشفافية وإدارة الحوادث الأمنية، مما قد يؤدي إلى تأخير في التنبيه للمخاطر المحتملة ويُضعف من ثقة أصحاب المصلحة. نقص الاستثمار في الأمن السيبراني: قيود الميزانية قد تؤثر على القدرة على تطبيق حلول أمنية متطورة.

- الاعتماد الزائد على الطرف الثالث في التعامل مع مزودي خدمات خارجيين قد يفتح باباً لتهديدات أمنية إن لم يتم التدقيق عليهم.

المبحث الرابع

الاستنتاجات والتوصيات

اولاً : الاستنتاجات

1. أظهرت نتائج البحث أن وجود إطار قوي لحوكمة الشركات يسهم بشكل فعّال في الوقاية من خروقات الأمن السيبراني، ويعزز قدرة المصارف على التصدي لها عند وقوعها.
2. تبين أن العديد من المصارف تعاني من ضعف في دمج مبادئ الحوكمة ضمن استراتيجيات الأمن السيبراني، مما يفاقم من تأثير الخروقات عند حدوثها.
3. أظهر البحث أن مشاركة مجلس الإدارة في مناقشة قضايا الأمن السيبراني كانت محدودة في المصرف، مما يضعف من فاعلية الاستجابة للمخاطر السيبرانية.
4. نقص في وجود سياسات داخلية واضحة تتعلق بالأمن السيبراني ضمن أنظمة الحوكمة، وغياب المعايير والإجراءات الموحدة للتعامل مع الحوادث السيبرانية.
5. ان الامتثال للتشريعات والمعايير الدولية المتعلقة بالأمن السيبراني (مثل ISO 27001 أو NIST) لا يزال غير كافٍ في كثير من الشركات، رغم أهميته في تعزيز فعالية الحوكمة.

ثانياً: التوصيات

1. ضرورة أن تعتمد المصارف استراتيجيات واضحة للتحول الرقمي تتكامل مع أهدافها الاستراتيجية وخاصة في مجال إدارة التكلفة.
2. تشجيع المصارف على الاستثمار المستمر في تقنيات مثل الذكاء الاصطناعي، تحليل البيانات الضخمة، والحوسبة السحابية لدعم عملياتها بكفاءة أعلى.
3. تنظيم برامج تدريبية وتطويرية لتنمية المهارات الرقمية للعاملين في القطاع المصرفي لضمان فعالية تطبيق التحول الرقمي.
4. تعيين خبراء التكنولوجيا، وإنشاء لجان التكنولوجيا على مستوى مجلس الإدارة وتفويض المسؤوليات إلى لجنة التدقيق كوسيلة لإدارة مخاطر الأمن السيبراني و فهم الدور الحالي والمستقبلي لآليات الحوكمة في إدارة مخاطر الأمن السيبراني.
5. يجب أن يحصل التحول الرقمي على دعم إداري وتنفيذي من الإدارة العليا لضمان تنفيذ المشاريع الرقمية بسلاسة وتكامل.
6. اعتماد أدوات قياس فعالة لمتابعة أثر التحول الرقمي على إدارة التكلفة وقيمة المصرف بشكل دوري لتحسين الأداء باستمرار.

المصادر

[1] https://www.oecd.org/corporate/principles-corporate-governance.htm

[2] Anderson ,Uorton L& Ramamoort ,Sridhar& Head ,Michal et al , Internal Auditing ,Assurance &Advisory Service ,4th edition 2017.

[3] Moeller R. Robert, “Executive's Guide to COSO Internal Controls Understanding and Implementing the New Framework”, John Wiley & Sons, 2014.

[4] Salin, H. and Lundgren, M. (2022). Towards Agile Cybersecurity Risk Management for Autonomous Software Engineering Teams. J. Cybersecurity. Priv., 2, 276–291.

[5] محروس، رمضان عارف رمضان2022 ،" استخدام المنهجية الرشيقة في تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني"، **مجلة البحوث المالية والتجارية**، العدد الثالث، 142 -491.

[6] Alina , C. M., Cerasela S.E., and Gabriela G**, (2017)** ,Internal audit role in cybersecurity ovidius university Annals Economic Sciences Series 17 (2) Pp. 510 – 513 .

[7] Krishnasamy, V., andVenkatachalam, S. (2021),"An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using Index-level Boundary Pattern Convergent Encryptionalgorithm",Materials Today: Proceedings.

[8] Hartmann C.C. and J. Carmenate, **(2021)** ,Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches Implications for Practice Policy and Research, American Accounting Association, 15 (2) Pp. 9 - 23 .

[9] Shahimi S. and N. Mahzan, **(2018)** ,Building a research model and hypotheses development and findings of Exploratory Interviews International Journal of Management Excellence 10 (2) Pp. 1257 – 1283**.**

[10] Al-Alawi, A. I., and Al-Bassam, S. A. (2019),"Assessing the Factors of Cybersecurity Awareness in the Banking Sector", **Arab Gulf Journal of Scientific Research**, Vol. 37, No. 4, 17-32.

[11] American Institute of Certified Public Accountants (AICPA). 2017a. SOC for Cybersecurity: A Backgrounder. New York, NY: AICPA.

[12] Morin, P. (2020). NIST Cybersecurity Framework- Assessing the Maturity of your Cybersecurity Program.

[13] National Institute of Standards and Technology "NIST" (2018). Framework for Improving Critical Infrastructure Cybersecurity. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

[14]https://www.ifc.org/wps/wcm/connect/industry_ext_content/ifc_external_corporate_site/financial+markets/our+approach/corporate+governance

[15] https://www.theiia.org/The Institute of Internal Auditors (IIA) (https://www.theiia.org/)