مجلة أكاديمية الجبل للعلوم الاجتماعية والإنسانية

Al-Jabal Academy Journal of Social and Humanities
03 (02): 01-29, 2024

eISSN: 2958-5554; pISSN: 2958-5546
https:// lajak.edu.ly/journals/index.php/aajssh :Journal Homepage

تقييم إدارة المخاطر السيبرانية في المصارف الليبية وفق المعايير الدولية

"دراسة استطلاعية على المصرف التجاري الوطني"

خيرالدين عبدربه الحمري
أستاذ مشارك بقسم التمويل والمصارف
كلية الاقتصاد، جامعة عمر المختار / البيضاء

ابتهال فتح الله الهين
معيدة بقسم التمويل والمصارف
كلية الاقتصاد ،جامعة عمر المختار / البيضاء

https://doi.org/10.58309/srzfpg04

المستخلص:

هدفت الدراسة إلى تقييم واقع إدارة المخاطر السيبرانية في المصارف الليبية، وفق بعض المؤشرات المحلية والدولية، من خلال زيارات ميدانية، والاعتماد على المقابلات الشخصية، ثم تقييم واقعها في المصرف التجاري الوطني وفق المعايير والتوصيات الدولية، واختيرت عينة من المسؤولين والمختصين، لاستطلاع أراءهم حول إدارة المخاطر السيبرانية في المصرف، من خلال استبانة، صُممت لتحتوي على أسئلة مصاغة، وفق نقاط مختارة من المعايير والتوصيات الدولية. وقد أظهرت أهم المؤشرات من خلال التقارير المحلية والدولية، أن هناك قصور لدى المصارف الليبية في الالتزام بالمعايير الدولية، ونقص في القدرات المهنية المتخصصة بالمخاطر السيبرانية، بينما أشارت ردود المشاركين في الاستبانة إلى أن المصرف التجاري الوطني، ملتزم إلى حد ما بالتوصيات والمعايير الدولية، برغم ملاحظة الباحثين إلى عدم وجود التزام ببعض التوصيات، مثل وجود لجان مختصة بإدارة المخاطر، وخطة واضح للحوكمة، والافتقار إلى القدرات المهنية المختصة في إدارة هذه المخاطر.

الكلمات المفتاحية:

المخاطر السيبرانية ، الأمن السيبراني ، الحوكمة السيبرانية .

Evaluating the reality of cyber risk management in Libyan banks in accordance with international standards" An Exploratory study on the National Commercial Bank"

Ibtihaal F. Elhai
Faculty of Economics
Omar Al-Mukhtar University

Khiraddeen A. Alhemri
Faculty of Economics
Omar Al-Mukhtar University

KEYWORDS
cyber risks, cyber security, cyber governance.

Abstract:

The study aimed to evaluate the reality of cyber risk management in Libyan banks according to some local and international indicators, through field visits and relying on personal interviews, then evaluating its reality in the National Commercial Bank in accordance with international standards and recommendations. A sample of officials and specialists was chosen to survey their opinions on cyber risk management in the bank, Through a questionnaire, designed to contain questions formulated according to selected points from international standards and recommendations. The most important indicators, through local and international reports, have shown that there is a deficiency in Libyan banks in adhering to international standards, and a lack of professional capabilities specialized in cyber risks. While the responses of the participants in the questionnaire indicated that the National Commercial Bank is somewhat committed to international recommendations and standards, despite the researchers noting the lack of commitment to some recommendations, such as the presence of committees specialized in risk management, a clear plan for governance, and the lack of professional capabilities specialized in managing these risks .

1. إطار وخطة الدراسة

1.1.المقدمة

في ظل استخدام المصارف الواسع والمتزايد لأدوات التقنية الحديثة، في كافة العمليات، واعتمادها على أنظمة وبرامج رقمية لتقديم معظم الخدمات، فإن المصارف أصبحت تواجه في مخاطر جديدة ومتنوعة، مصاحبة لتبنيها لهذه التقنيات، تمثلت في تهديد أمن المعلومات ومدى أمان البرامج والنظم الإلكترونية، والرقمية، والأنترنت، بشأن خصوصية العملاء، أو مخاطر اختراقها أو الإضرار بها، مما يسبب في خسائر توقفها، والتأثير على الخدمات المقدمة للعملاء، والإضرار بسمعة المصارف، هذه المخاطر عُرفت بالمخاطر السيبرانية Cyber Risks([1]) ، (Chen et al.، 2023: 1؛ IMF'Report ، 2024 ؛ McKinsey Global Institute، 2024؛ Institute of International Finance، 2024).

وقد كشفت كثير من التقارير والدراسات الدولية عن ضخامة التهديدات التي تواجه المصارف، من جراء هذه المخاطر، وذلك مع تزايد اعتمادها على الخدمات المالية الرقمية في السنوات الأخيرة، حيث أصبحت المخاطر السيبرانية أهم مصدر تهديد للمصارف وللاستقرار المالي (Elliott and Jenkinson،IMF،2024)، وظلت الجريمة الإلكترونية تشكل حجر الزاوية في مشهد التهديدات للعالم والمؤسسات المختلفة، لعامي 2023، 2024

(CrowdStrike، Global Threat Report، 52:2024). وأصبح مشهد الأمن السيبراني اليوم، أحد أكثر المخاطر التي تهدد البيانات، وينطبق هذا على المؤسسات من جميع الأحجام وفي جميع الصناعات والمجالات، مما يجعل حماية البيانات أكثر أهمية، في ظل بيئة منظمة بشكل متزايد وخصوم أسرع وأكثر ابتكارًا (CrowdStrike BLOG، "Data Protection Day 2024"، 2024).

ونظراً لأن بيانات المصارف الأكثر استهدافًا من قبل مجرمي الإنترنت، فقد أصبح موضوع المخاطر السيبرانية الأكثر شيوعًا وأهمية في الصناعة المصرفية (Rama،2016 ؛ Grobler،2018؛ Kondo et al.، 2018). وقد زاد من أهمية هذه المخاطر، أنها ذات خصوصية من حيث المصدر ووقت حدوثها واستمرارية تطورها، مما يُعقد قياسها أو ضمان الوقاية منها. لذلك، فإن كثير من الدراسات تنبه المصارف إلى ضرورة أن تدرك دائمًا، حقيقة أن طبيعة التهديدات الإلكترونية مستمرة في التطور. وبالتالي، ينبغي التأكد من أن يكون إطار إدارة المخاطر السيبرانية المعتمد لدى المصارف، مقيم بصورة مستمرة، وفقاً للمعايير والتوصيات الدولية، ومواكب للأساليب الحديثة لتطور الجرائم والتهديدات الإلكترونية (Lemieux،2015؛ Deloitte،2023)، خاصة في ظل إشارة دراسات دولية، إلى أنه من المتوقع أن تشهد الخدمات المالية والمصرفية، تغييرات تكنولوجية كبيرة وسريعة خلال الثلاث إلى الخمس سنوات القادمة، يصحبها مخاطر متزايدة ومتغيرة، تتطلب استعدادًا وتأهبًا أكبر للتعامل معها McKinsey Global Institute، 2024)، ويواكب هذه التوقعات، أن هناك اعترافاً متزايداً بأن المخاطر السيبرانية هي مخاطر الأعمال، وجميع القادة بحاجة إلى فهم مشهد المخاطر السيبرانية، حيث أصبحت إدارة المخاطر السيبرانية الآن، أمرًا يخص الجميع (Governance Institute of Australia، Effective Cyber Risk Management،2024: 3).

2.1.مشكلة الدراسة

نظراً لملاحظة الباحثين، لعدم وجود استراتيجيات أو خطط معلنة من قبل المصارف الليبية، لمواجهة المخاطر السيبرانية وكيفية إدارتها، وذلك من خلال زيارات ميدانية لبعض المصارف التجارية، والاستفسار من بعض المسؤولين عن أمن المعلومات وإدارة المخاطر في هذه المصارف، بالإضافة إلى ندرة الدراسات المحلية المهتمة بهذا الجانب من المخاطر، حسب المعلومات المتاحة، فإن هذه الدراسة تأتي لتقييم إدارة

([1]) درج استخدام مصطلح المخاطر السيبرانية في الدراسات والمنظمات الدولية ، للإشارة إلى المخاطر الإلكترونية أو الرقمية، وذلك ما نقصده في هذه الدراسة.

المخاطر السيبرانية في المصارف التجارية الليبية في ظل المعايير والتوصيات الدولية، وذلك من خلال السعي للإجابة عن السؤال الرئيسي التالي: ما هو واقع إدارة المخاطر السيبرانية في المصارف التجارية الليبية، وما مدى التزاماها بالمعايير والتوصيات الدولية؟.

3.1.أهداف الدراسة

1) التعرف على الرؤى الدولية حول تطور المخاطر السيبرانية، ونماذج ومعايير إدارتها في المصارف.
2) بيان مؤشرات محلية ودولية عن واقع إدارة المخاطر السيبرانية في المصارف الليبية.
3) تقييم إدارة المخاطر السيبرانية في المصرف التجاري الوطني، وفق المعايير والتوصيات الدولية.

1.أهمية الدراسة

تكمن أهمية الدراسة في الاتي:

1) تناول موضوع يحظى بأهمية بالغة في الوقت الحالي من كافة المنظمات الدولية، وباهتمام الدراسات الحديثة في مجالات عدة في القطاعات المالية والمصرفية.
2) تأتي الدراسة في وقت دخول المصارف التجارية الليبية في مجال الصيرفة الإلكترونية، مما يستدعي اهتماماً كبيراً بدراسة مخاطر هذه العمليات، والعمل على تشجيع الدراسات النظرية والتجريبية في هذا المجال، والمساهمة في نشر ثقافة الأمن السيبراني لمواجهة هذه المخاطر.

5.1.الدراسات السابقة

يبين الجدول (1) مختصر عن محتوى الدراسات السابقة، التي تم الاعتماد عليها، ويلاحظ تشابهها في الاستناد إلى معايير لجنة بازل في تقييم أثار العمليات المصرفية الإلكترونية ومخاطرها، وفي استخدامها للاستبانة كأداة رئيسية، لكنها تباينت في تركيزها على جوانب أو متغيرات اختلفت في رؤاها، حول تقييم المخاطر أو الأثار الناجمة عن استخدام المصارف للعمليات المصرفية الإلكترونية. حيث ركزت بعض الدراسات على تقييم إدارة المخاطر السيبرانية وفق معايير لجنة بازل، مثل دراسة (فرج ومعيتيق 2024) في ضوء معايير بازل وفق الوثيقة الصادرة عام 1998 ، ودراسة (الحولي 2015) وفق وثيقة بازل (2).

بينما هناك دراسات اهتمت بمزايا هذه العمليات مثل دراسات (Abdou A, et al.، 2015؛ Stanoevska،2021) ، ومنها دراسات هدفت إلى تقييم أثار مخاطر العمليات الناشئة عن الصيرفة الإلكترونية، وكيف تتم إدارتها وفق معايير لجنة بازل بشكل خاص، مثل دراسات Abdou, Hussein. et al.، English, John 2014 ؛ الحولّي 2015؛ Al-Ajmi،2020؛ سمرة 2022)، بينما بحثت دراسة (Abdul-Hussein et al. 2021) في أثر استخدام العمليات الإلكترونية على مخاطر الائتمان ومخاطر السيولة و تقليل التكاليف. فيما ركزت دراسة (Kumar، 2024) استكشاف فحص وتوضيح الجوانب الرئيسية المختلفة لإدارة المخاطر السيبرانية في القطاع المصرفي الهندي.

وتختلف هذه الدراسة، في أنها تهدف إلى تقييم أثر المخاطر السيبرانية أو مخاطر العمليات المصرفية الإلكترونية وإدارتها، وفق المبادئ والتوصيات والمعايير الدولية، بما فيها معايير وتوصيات لجنة بازل (خاصة الوثائق الخاصة بالمبادئ 2011،2003،2001 , الوثائق الخاصة بالمرونة السيبرانية 2018،2021)، مع إضافة بعض التوصيات الصادرة عن أجندة بالي المعدة من قبل صندوق النقد الدولي ومجموعة البنك الدولي 2018، بالإضافة إلى أنها تتضمن موضوع لم يتم تناوله بصورة واسعة في الدراسات المحلية، رغم أنه يحتاج إلى مواكبته باستمرار، نظراً لطبيعته المتغيرة، و تغير طرق تقييمه ومعاييره بصورة مستمرة.

جدول (1) ملخص الدراسات السابقة

عنوان الدراسة	المؤلف ، الناشر	أهداف الدراسة	إداه الدراسة
تقييم إدارة مخاطر العمليات المصرفية الإلكترونية بالمصارف الليبية في ضوء مقررات بازل (دراسة ميدانية على عينة من أفرع المصارف الليبية العاملة بمدينة سرت)	فرج، محمد أبو خزام ومعيتيق، سمية سالم مجلد مجلة جامعة سرت للعلوم الإنسانية	هدفت هذه الدراسة للتعرّف على مستوى التزام المصارف التجارية الليبية بتطبيق تلك المبادئ التي أقرّتها وثيقة لجنة بازل في عام 1998 بشأن إدارة مخاطر الأنشطة المصرفية الإلكترونية.	استبانة
Cyber Risk Management in Indian Banking Sector	(Kumar،2024)	فحص وتوضيح الجوانب الرئيسية المختلفة لإدارة المخاطر السيبرانية في القطاع المصرفي الهندي.	تحليل الوثائق
تأثير إدارة المخاطر الإلكترونية في ضوء مقررات لجنة بازل بالمصارف.	(سمرة، ياسر 2022)	تحديد دور إدارة المخاطر الإلكترونية في ظل مقرات لجنة بازل في المصارف التجارية المصرية الخاصة	استبانة
إدارة مخاطر الخدمات المصرفية الإلكترونية في المصارف الإسلامية.	(الهاشمي، سلطاني . صادق صفيح .2022)	معرفة واقع إدارة مخاطر الخدمات المصرفية الإلكترونية في المصارف الإسلامية، حيث تم الاعتماد على دراسة حالة مصرف الراجحي السعودي	استبانة
Risk Management Principles of E-banking, Challenges of The Macedonia's Banking Sector.	(Stanoevska،2021)	الأثار التي أحدثها تطور التكنولوجيا المالية على المصارف التجارية في مقدونيا	استبانة
Impact of Banking Risks on the Electronic Banking Services.	Abdul-Hussein et al.2021	استكشاف تأثير المخاطر المصرفية على الخدمات المصرفية الإلكترونية في المصارف العراقية	استبانة
A study on Risk Management Practices in Online Banking in Bahrain.	(Al-Ajmi et 2021 al.)	أجرت هذه الدراسة تقييم لإدارة المخاطر للخدمات المصرفية عبر الإنترنت لمصارف مختلفة في البحرين	استبانة ومقابلة
إدارة مخاطر العمليات المصرفية الإلكترونية وفق مقررات لجنة بازل.	(الحولي ، 2015)	الوقوف على عملية إدارة مخاطر الأنشطة المصرفية الإلكترونية في المصارف المحلية العاملة في فلسطين	
E-banking and Risk Management :Evidence from the Cypriot Public Sector Banks.	(Abdou, Hussein 2015)	إبراز مزايا الصيرفة الإلكترونية المخاطر المصاحبة لها في المصارف القبرصية	
An investigation of Risk Management Practices in Electronic Banking: The Case of the UK Banks.	(2014 John et al.)	بحثت هذه الدراسة في ممارسات إدارة المخاطر في الخدمات المصرفية الإلكترونية للمصارف البريطانية	المقابلة

6.1.فرضيات الدراسة

توافقاً مع أهداف الدراسة وأسئلتها، واعتماداً على ما ورد في الدراسات السابقة، من طرق تقييم إدارة المخاطر السيبرانية، من خلال مدى الالتزام بالتوصيات ولمعايير الدولية، فقد صيغت فرضياتها كما يلي:

الفرضية الرئيسية الصفرية :

H0: ليس هناك التزام من المصارف التجارية الليبية بالمعايير بشأن إدارة المخاطر السيبرانية.

وتنقسم هذه الفرضية إلى الفرضيات الفرعية التالية:
H01: ليس هناك نظام إداري واضح لإدارة مخاطر العمليات الإلكترونية.
H02: لا تلتزم السلطات العليا للمصارف التجارية الليبية بالمعايير والتوصيات الدولية الخاصة بالتوجيه والرقابة على المخاطر السيبرانية .
H03: ليس لدى المصارف التجارية الليبية خطة لتنفيذ مراحل تحقيق المرونة السيبرانية .
H04: لا توجد مؤشرات على متابعة المخاطر القانونية ومخاطر السمعة.

الفرضية الرئيسية البديلة:
H1:هناك التزام من المصارف التجارية الليبية بالتوصيات والمعايير الدولية بشأن إدارة المخاطر السيبرانية.
وتنقسم هذه الفرضية إلى الفرضيات الفرعية التالية:
H11: هناك نظام إداري واضح لإدارة مخاطر العمليات الإلكترونية.
H12: تلتزم السلطات العليا للمصارف التجارية الليبية بالمعايير والتوصيات الدولية بالتوجيه والرقابة للمخاطر السيبرانية.
H13: لدى المصارف التجارية الليبية خطة لتنفيذ مراحل تحقيق المرونة السيبرانية.
H14: توجد مؤشرات على متابعة المخاطر القانونية ومخاطر السمعة.

2. مراجعة الأدبيات

1.2.ماهية المخاطر السيبرانية وإدارتها

1.1.2. المخاطر السيبرانية:

يُنظر للمخاطر السيبرانية (Cyber Risk)، وفق سياقات مختلفة، حسب التعميم أو التخصيص، أو الغرض من تعريفها، أو توضيح أثرها. حيث يعرفها المعجم السيبراني لمجلس الاستقرار المالي دون تخصيص، على إنها الجمع بين احتمال وقوع الحوادث السيبرانية وتأثيرها The Financial Stability Board "FSB"، Cyber Lexicon، 10:2023) .

ويراها معهد إدارة المخاطر البريطاني (Institute of Risk Management)، على أنها تعني أي خسارة مالية أو تعطيل أو ضرر يلحق بسمعة منظمة ما، نتيجة فشل ما في أنظمة تكنولوجيا المعلومات الخاصة بها(IRM ، Cyber Risk Resources for Practitioners، 2014 : 10).

وفي القطاع المالي أيضاً، يعرف البنك الدولي المخاطر السيبرانية، على أنها مخاطر الخسارة المالية أو الاضطراب، أو الأضرار بالسمعة، الناجمة عن فشل أنظمة تكنولوجيا المعلومات، بما في ذلك الحوادث السيبرانية الخبيثة، حيث تنوي الجهات التهديدية إلحاق الضرر(World Bank Group، Financial Sector's Cybersecurity: A Regulatory Digest ، 2020: 4).

أما في المصارف بشكل خاص، فيطلق مصطلح المخاطر السيبرانية، على المخاطر المصاحبة للعمليات أو الخدمات المصرفية الإلكترونية، ويُنظر لها، "وفق رؤية لجنة بازل" ولأغراض إدارة المخاطر المالية، كشكل من أشكال المخاطر التشغيلية، التي تمثل الخسارة الناتجة عن العمليات الرقمية، والحوادث الناجمة عن أطراف داخلية أو خارجية أو أطراف ثالثة، بما في ذلك السرقة، والمساس بالنزاهة، والأضرار التي تلحق بالمعلومات وأصول التكنولوجيا، والاحتيال الداخلي والخارجي، وتعطيل الأعمال (Curti Filippo et al.,, 2023: 4).

ويمكن جمع أهم النقاط من هذه التعريفات، لتعريف المخاطر السيبرانية في المصارف، بأنها ذلك الجزء من المخاطر التشغيلية، الناجم عن تعطل البرامج أو الأنظمة الإلكترونية أو الرقمية، وإلحاق الضرر بها، نتيجة أخطاء أو هجوم، بقصد أو بغير قصد، من قبل جهات داخلية أو خارجية.

2.1.2.إدارة المخاطر السيبرانية :

يُحدد إطار إدارة المخاطر السيبرانية بشكل عام، في مجموعة خطوات تتُخذ بشكل دوري لمواجهة التهديدات الإلكترونية، ومعالجتها من خلال رصدها وتحديدها وتقييمها. حيث عرفت الجمعية المهنية

الدولية لحوكمة تكنولوجيا المعلومات آيزاكا (ISACA) إدارة المخاطر السيبرانية على أنها عملية تحديد نقاط الضعف والتهديدات لموارد المعلومات، التي تستخدمها أي جهة أو مؤسسة في تحقيق أهدافها، وتحديد الإجراءات المضادة، التي يجب اتخاذها للحد من المخاطر إلى مستوى مقبول، بناء على قيمة موارد المعلومات للمؤسسة. ولذلك تعتمد إدارة المخاطر السيبرانية على تنسيق لعوامل الخطر، الاستراتيجية والتشغيلية، والسيبرانية، والقانونية والتنظيمية، وسلسلة التوريد والحوكمة، للمنظمات التي تعتمد بشكل متزايد على العمليات الرقمية لإدارة المؤسسة (Sathiyamurthy ، ISACA Journal-، 2019).

وترى شركة (IBM) إدارة المخاطر السيبرانية، على أنها عملية تحديد المخاطر التي تتعرض لها أنظمة المعلومات، وترتيب أولوياتها وإدارتها ومراقبتها. وتؤكد على أنها أصبحت جزءًا حيويًا من جهود إدارة المخاطر المؤسسية الأوسع (What is cyber risk management?، IBM'Home ، 2024).

ومن منظور الحوكمة، فإن إدارة المخاطر السيبرانية ترتكز على استراتيجية شاملة للأمن السيبراني، تتكامل مع العمليات التنظيمية، لمنع توقف الأنشطة بسبب التهديدات أو الهجمات السيبرانية. وتتضمن حوكمة الأمن السيبراني، أطر المسائلة وتسلسلات اتخاذ القرار ،وتحديد المخاطر المتعلقة بأهداف العمل، وخطط واستراتيجيات التخفيف، بالإضافة إلى عمليات وإجراءات الرقابة (America'Cyber Defense Agency-CISA،2024).

وعليه، فأن إدارة المخاطر السيبرانية في المصارف تؤطر عادة، في مجموعة خطوات وإجراءات، يتخذها المصرف بشكل دوري، لمواجهة التهديدات الإلكترونية، ومعالجتها من خلال رصدها وتحديدها وتقييمها، وفق معايير وتوصيات محلية ودولية مقبولة، تُمكن من مواجهة هذه المخاطر وفق نوعها ووقت حدوثها وتطورها.

3.1.2. الأمن السيبراني :

يُعرف الإطار العام للحماية من المخاطر السيبرانية، بالأمن السيبراني (Cyber Security)، ووفق تعريف معجم الاستقرار العالمي، يتمثل الأمن السيبراني في الحفاظ على سرية وسلامة نظم المعلومات من خلال الوسائط السيبرانية، بالإضافة إلى، المساءلة وعدم التنصل والموثوقية FSB's Cyber Lexicon،10:2023).

ولذلك، فالأمن السيبراني في القطاع المصرفي، يتعلق بتأمين البنية الأساسية الرقمية للمصرف بالكامل، من أنظمة الخدمات المصرفية عبر الإنترنت إلى قواعد البيانات الداخلية، ضد الوصول غير المصرح به، وتسريب البيانات، والهجمات الخبيثة. ويشير في مجال الخدمات المصرفية إلى التقنيات والممارسات والعمليات المصممة، لحماية الأنظمة الرقمية والبيانات والشبكات المصرفية من التهديدات الأمنية السيبرانية، وتضمن تدابير الأمن السيبراني حماية هذه البيانات من الخروقات والاحتيال والقرصنة، وغيرها من أشكال الجرائم الإلكترونية.

4.1.2. المرونة السيبرانية:

توصف الممارسات التي تحدد قدرة المصرف على مواجهة الخطر السيبراني، وقدرته على التكيف معه والتعافي منه، بالمرونة السيبرانية (Cyber Resilience). حيث تنبع فكرة المرونة السيبرانية من مفهوم الأمن السيبراني، وتعرف على أنها، قدرة المنظمة على الاستمرار في تنفيذ مهمتها، من خلال التوقع والتكيف مع التهديدات السيبرانية، والتغيرات البيئية الأخرى ذات الصلة، ومن خلال الصمود والاحتواء والتعافي السريع من الحوادث السيبرانية (FSB's Cyber Lexicon، 2023: 10).

وهناك من يعتبر أن المرونة السيبرانية مصطلحًا جديدًا يشير، إلى المفهوم الحالي لإدارة استمرارية الأعمال، ولكن مع التركيز على التهديدات السيبرانية (Wilson, Christopher et al.، IMF ، 2019 : 1) .

3.2. تطور أثر المخاطر السيبرانية

تُبين أغلب المنظمات الدولية المختصة، من خلال دراسات واسعة، تطور المخاطر السيبرانية بشكل مكثف في السنوات القليلة الماضية. حيث يرى صندوق النقد الدولي، أنه برغم أن التكنولوجيا تعزز التطور

المالي والشمول المالي والكفاءة المالية، غير إنها تأتي بمخاطر من شأنها تهديد المستهلك والمستثمر، فضلاً عن مخاطر مرتبطة بالاستقرار المالي والسلامة المالية على نطاق واسع (صندوق النقد الدولي، وثيقة مبدئية :أجندة مؤتمر بالي للتكنولوجيا المالية، 2018 :1). كما يشير الصندوق في تقريره الصادر في أبريل 2024، إلى أن الأحداث السيبرانية قد تنعكس أثارها، بمخاطر على الاستقرار المالي الكلي من خلال فقدان الثقة، وتعطل الخدمات الحيوية، والتأثيرات غير المباشرة على المؤسسات الأخرى، من خلال الروابط التكنولوجية والمالية. كما ينبه التقرير إلى ذلك من المحتمل أن يتسبب في مشكلات تمويلية للشركات، بل وقد تهدد ملاءتها المالية، ويوضح أنه منذ عام 2020، ازداد حجم تلك الخسائر الجسيمة بأكثر من أربعة أضعاف ليصل إلى ثمانية وعشرون مليار دولار، وتتجاوز الخسائر غير المباشرة هذا الرقم بكثير، بما في ذلك أضرار السمعة أو التحديثات الأمنية (IMF، Global Financial Stability Report، 2024).

كما أجرى معهد الاستقرار المالي(FSI) التابع لبنك التسويات الدولية (BIS) في عام 2016 ، مسحًا للمشرفين المصرفيين في ثلاث وسبعون دولة في جميع أنحاء العالم، أظهرت نتائجه أن التكنولوجيا المالية والمخاطر السيبرانية الناتجة عنها هي التحدي الأكبر. ويؤكد ذلك تصنيف موقع مجلة إدارة المخاطر التشغيلية (Risk.net) الذي يبين أن المخاطر السيبرانية هي الأعلى بين أكبر عشر مخاطر تشغيلية لعام 2017 (FSI Insights، 3:2017). كما يبين تقرير مجلة (EdSurge) التابعة للجمعية الدولية للتكنولوجيا في التعليم، الصادر عام 2020، إلى أنه من المتوقع أن تصل الأضرار الناجمة عن جرائم الإنترنت إلى ما يقدر بنحو عشرة ونصف تريليون دولار بحلول عام 2025.

ووفق نتائج مسح إدارة مخاطر المصارف العالمية المنشور في الإصدار الثاني عشر في يناير 2023، لسلسلة دراسات حول إدارة مخاطر المصارف، تُجرى سنوياً مشتركة بواسطة شركة Ernst & Young (EY) ومعهد التمويل الدولي(Institute of International Finance-IIF)، والذي استند إلى بيانات استقصائية من ثمان وثمانون مصرفاً في ثلاثين دولة، يظهر وسط مستويات غير مسبوقة من التقلبات العالمية وعدم اليقين، ارتفاع مخاطر الأمن السيبراني إلى أعلى قائمة المخاطر على المدى القريب للمصارف في جميع أنحاء العالم، حيث حدد استطلاع كبار مسؤولو المخاطر الذين شملهم المسح، أن المخاطر السيبرانية في كل مكان، و في كل خط من خطوط الأعمال، وفي العمليات اليومية وبرامج التحول، وعبر شبكات الشركاء والموردين الواسعة، كما رأى 58٪ من المشاركين في هذا الاستطلاع، أن المخاطر السيبرانية تُعد أكبر المخاطر الاستراتيجية للسنوات الثلاث المقبلة. وأنهم يعتبرون الضوابط السيبرانية هي الأولوية القصوى لتعزيز المرونة التشغيلية(13th annual EY/IIF global bank risk management survey، 2024:8-12).

كذلك بينت دراسة مسحية أعدتها شركة (Deloitte)، حول المستقبل العالمي للفضاء الإلكتروني لعام 2023 "Global Future of Cyber Survey" ،الأثار السلبية للمخاطر السيبرانية، من خلال استقصاء لأكثر من ألف متخذ قرار سيبراني على مستوى المدير أو أعلى، عبر عشرين دولة، من خلال مؤسساتها التي لا يقل عدد موظفيها عن ألف موظف. وقد أظهرت نتائج الدراسة كما هو مبين بالجدول (2) هذه الأثار ومستوى أو رتبة تأثيرها ما بين سنوات الدراسة. وخلصت إلى أن استخدام التقنيات الرقمية يؤدي إلى زيادة التهديدات السيبرانية، وأنه يجب أن توضع إدارة المخاطر السيبرانية كأولوية استراتيجية، لكي تواكب التحول الرقمي بصورة مناسبة.

جدول (2) مقارنة نسب ورتبة الآثار السلبية الناتجة عن الحوادث والانتهاكات السيبرانية وفق دراسات شركة Deloitte، عامي 2021 إلى 2023

العواقب السلبية الناجمة عن المؤشرات والانتهاكات السيبرانية	رتبة 2021	رتبة 2023	نسبة 2023
اضطراب التشغيلية	1	1	%58
الخسارة والعائد	9	2	%56
الخسارة وثقة العملاء / الأثر السلبي على العلامة التجارية	4	3	%56
خسارة السمعة	5	4	%55
وقف تمويل المبادرة الاستراتيجية	-	5	%55

فقدان الثقة في النزاهة التقنية	-	6	%55
التأثير السلبي لتوظيف المواهب والاحتفاظ بها	8	7	%54
سرقة الملكية الفكرية	2	8	%54
انخفاض أ سعار الأسهم	3	9	%52
الغرامات التنظيمية	7	10	%52
التغيير في القيادة	5	-	-

المصدر: (Deloitte Development LLC، Global Future of Cyber Survey، 13:2023).

كما تؤكد شركة ماكنزي (McKinsey & Company) على ضرورة أن تتبنى الشركات المالية إجراءات فورية لحماية نفسها من المخاطر السيبرانية المتنامية ، من خلال عنونة تقريرها الصادر في مارس 2024 ، بـ (الحرب السيبرانية على الأبواب:3-31)، والذي تضمن عرض نتائج دراسة أجراها معهد ماكنزي(McKinsey Global Institute) بالتعاون مع معهد التمويل الدولي (Institute of International Finance) ، بهدف فهم التحديات التي تواجهها الشركات المالية، لإيجاد أفضل الطرق لاستخدام التقنيات التكنولوجية الحالية والمستقبلية وحمايتها، وقد شمل هذا التقرير استطلاعاً، تضمن عينة من المؤسسات المالية في جميع أنحاء العالم. وتشير نتائجه إلى انه برغم الفوائد الهائلة التي توفرها التقنيات الجديدة، إلا أنها تُعرض الشركات إلى مخاطر تتعلق بالأمن السيبراني، حيث يظهر أن القدرات الحالية غالباً ما تكون غير كافية لمواجهتها، مما يستلزم منها الإعداد السريع للتصدي لهذه المخاطر، وإلا فقد تجد أن المخاطر تفوق الفوائد المتوقعة، ومن المتوقع أن يشهد قطاع الخدمات المالية تغييرات تكنولوجية كبيرة وسريعة خلال الثلاث إلى الخمس سنوات القادمة، ومع هذه التطورات السريعة، ستظهر مخاطر متزايدة، تتطلب من الشركات استعدادًا وتأهبًا أكبر للتعامل معها، حيث تشمل هذه المخاطر تحديات تتعلق بالأمن السيبراني، والاستقرار التشغيلي، والحاجة إلى مواكبة التقنيات الجديدة.

4.2. تقييم وإطار عمل المخاطر السيبرانية

يتضمن تقييم المخاطر السيبرانية، عملية منهجية تهدف إلى تحديد نقاط الضعف والتهديدات داخل بيئة تكنولوجيا المعلومات الخاصة بالمؤسسة، وتحديد احتمالية وقوعها، وتحديد أثرها المحتمل وتنفيذ استراتيجيات بشأنها (CrowdStrike،2024؛ Sentinel One, Inc، Cyber Security Risk Assessment، 2024). ولذلك يُعنى تقييم المخاطر السيبرانية في الخدمات المصرفية، بعملية تحديد وتحليل وتقييم التهديدات والثغرات الإلكترونية، التي قد تؤثر على سرية وسلامة وتوافر أنظمة المعلومات، والبيانات الخاصة بالمصارف وعملائها، وذلك بما يساعد على تحديد أولويات وتنفيذ الضوابط والتدابير المناسبة، للتخفيف من المخاطر السيبرانية والامتثال للوائح والمعايير ذات الصلة (Dawodu et al.، 2023 : 220).

وتختلف الآراء حول كيفية تنظيم وإدارة ورقابة المخاطر السيبرانية، فهناك من يرى أن الطبيعة المتطورة للمخاطر السيبرانية، ليست قابلة للتنظيم بشكل محدد، وأنه يمكن معالجتها من خلال اللوائح الحالية المتعلقة بكل من المخاطر التشغيلية والتقنية في القطاع المصرفي، بينما هناك من يشير إلى أن هناك حاجة ملحة لوجود هيكل تنظيمي للتعامل مع الطبيعة الفريدة للمخاطر الإلكترونية، وذلك بالنظر إلى التهديدات المتزايدة الناتجة عن التحول الرقمي الكبير في القطاعات المالية، ورغم ذلك فقد نشأ إجماع قوي على ضرورة وضع أطر فاعلة لإدارة ورقابة هذه المخاطر بصورة خاصة، نظراً للجدل الكبير حول مدى ملائمة الأطر التقليدية لإدارة ورقابة المخاطر السيبرانية، بالنظر إلى الطبيعة المتغيرة لهذه المخاطر(Toronto Center،Supervision of Cyber Risk، 2018). ولذلك هناك من يرى أن قياس وتحليل المخاطر الإلكترونية في المصارف، لم ينضج بعد بالشكل الذي يتيح إدارتها ضمن النظام، ويكون التركيز على التعامل معها وإدارتها بشكل مستقل (Stoyanov, Tongva،2022).

وفي ذات السياق ترى لجنة بازل إن المخاطر السيبرانية فريدة من نوعها، وأنه في ينبغي إدارة المخاطر السيبرانية، كجزء من إطار إدارة المخاطر التشغيلية، فإن بعض خصائص المخاطر السيبرانية، تمثل تحديات أمام أطر إدارة المخاطر التشغيلية التقليدية ومنها (BCBS، OICU-IOSCO، 4 :2016، 5)

أولاً: السمة المميزة للهجمات السيبرانية هي الطبيعة المستمرة المتطورة لاحتمال حدوثها، وعلى عكس معظم مصادر المخاطر الأخرى، فإن الهجمات السيبرانية غالبًا ما يكون من الصعب تحديدها أو القضاء عليها بالكامل، وقد يكون من الصعب تحديد اتساع نطاق تأثيرها .

ثانياً: مصدر المخاطر السيبرانية قد يكون قد يكون من المشارك الرئيسي أو مزود الخدمة، وقد يكون خطر التهديد داخلياً من إهمال الموظفين. ونظراً لأن المصارف تعتمد غالبًا على العديد من مقدمي الخدمات الخارجيين، فإن ذلك يعرضها لمخاطر أمنية إضافية، ويتطلب تقييم وإدارة وضع الأمن السيبراني للأطراف الثالثة، بما في ذلك تقييم التزامهم بالضوابط الأمنية، مما يمثل تحديات في الحفاظ على سلسلة التوريد الآمنة (Dawodu et al.، 2023 : 235) .

ثالثًا: قد تؤدي بعض الهجمات السيبرانية إلى تعطيل إدارة المخاطر والأعمال، وبشكل عام فإن الخطر السيبراني قد يتسبب الهجوم في تعطيل كبير للخدمات في النظام المالي الأوسع.

رابعاً: يمكن أن تكون الهجمات السيبرانية خفية، وتنتشر بسرعة داخل شبكة من الأشخاص والأنظمة، مما يمكنهم من استغلال نقاط الضعف غير المعروفة والروابط الضعيفة في الأنظمة والبروتوكولات، للتسبب في تعطيل أو اختراق الشبكة الداخلية للنظام.

وتتفق مع ذلك المجموعة المصرفية الإلكترونية في لجنة بازل (EBG)، حيث تشير إلى أن الخصائص الأساسية للخدمات المصرفية الإلكترونية، تطرح عددًا من تحديات إدارة المخاطر، منها (Risk Management Principles for Electronic Banking،2003:5):

- سرعة التغيير المتعلقة بالابتكار التكنولوجي .
- مواقع الويب الخاصة بالمعاملات المصرفية الإلكترونية، قد تدمج التطبيقات مع أجهزة الكمبيوتر القديمة، وتسمح بمعالجة مباشرة أكثر للمعاملات الإلكترونية، وتزيد من قابلية التشغيل البيني للنظام والتشغيل.
- قابلية توسع التكنولوجيا تزيد الخدمات المصرفية الإلكترونية من اعتماد المصارف على تكنولوجيا المعلومات.
- قابلية الوصول إلى الشبكات المفتوحة من أي مكان في العالم من قبل أطراف غير معروفة وعبر أجهزة لاسلكية سريعة التطور.

إن إدارة المخاطر السيبرانية عملية مستمرة، وتحتاج المنظمات إلى تقييم برامجها وتعديلها باستمرار، لأن التهديدات الجديدة المحتملة التي يفترض أن تواكبها تحسينات لإدراتها. وعلى الرغم من التغييرات التي قد تنشأ، فإن عملية إدارة المخاطر السيبرانية تتبع عمومًا الخطوات التالية (Thomson Reuters Law Blog، Cybersecurity risk management: An overview،2024).

- **تحديد المخاطر:** هي عملية يتم فيها تحديد المخاطر وتقديرها وتحديد أولوياتها. وهي تشكل الأساس لأي استراتيجية قوية للأمن السيبراني لأنها تساعد أو تسمح للمنظمات بتقدير مجموعة كاملة من التهديدات التي قد تتعرض لها. وتعد الخطوة الأولى في إدارة المخاطر الإلكترونية هي تحديد استخدام الأدوات التحليلية لتحليل التهديدات الإلكترونية والتخفيف من حدتها.McKinsey & Company ، Cybersecurity and Risk & Resilience Practices،2022 :2).
- **تحليل المخاطر:** يعمل تحليل المخاطر على تطوير فحص أكثر تفصيلاً لكل من احتمالية وعواقب التهديدات المعينة، وفي كثير من الأحيان يتم العمل بالطرق الكمية لتقدير أهمية الخسارة المحتملة. وتهدف هذه الخطوة إلى الكشف عن أي تداخل بين الأصول المهمة والثغرات أو التهديدات الموجودة، مما يساعد المؤسسة على تحديد احتمالية وتأثير الهجوم المحتمل. ومن خلال تحليل هذه المعلومات، يمكن للمؤسسة تحديد أولويات الإجراءات للتخفيف من المخاطر (Nagarajan, Janani ، CrowdStrike، 2024).
- **إدارة المخاطر:** لا تستطيع الشركة أو المصرف منع جميع التأثيرات السلبية للمخاطر، ولذلك فإن أحد أهداف إدارة المخاطر السيبرانية هو القضاء على المخاطر ذات الأولوية القصوى أو على الأقل تجنبها، وتعزيز سياسات وبروتوكولات أمن المعلومات، بالشكل الكافي لتجنب أو تقليل المخاطر، وتحتاج المنظمات إلى فهم ما هو معرض للخطر و فهم السياق الذي تعمل فيه المنظمة، والتركيز على أنه مع تطور التكنولوجيا

وتنوع استخدامها ، تتطور أيضًا المخاطر السيبرانية (Governance Institute of Australia، Effective Cyber Risk Management،20:2024).

• **مراجعة المخاطر :** إن مراقبة هذه تهديدات المخاطر السيبرانية ، تتضمن تحديد ما إذا كانت الإجراءات المستخدمة لمنع المخاطر أو تخفيفها، تعمل بالطريقة المخطط لها، مع مراجعة خطة مراقبة المخاطر باستمرار، بما يواكب تغير مصادر المخاطر (Thomson Reuters،Law Blog ، 2024) .

5.2.المعايير والنماذج الدولية لإدارة المخاطر السيبرانية

برغم تباين الآراء حول كيف وضع إطار إدارة المخاطر السيبرانية، ومدى وضع لوائح محددة وملزمة، فإن هناك إجماع دولي على ضرورة وضع معايير إرشاديه وتوصيات، من شأنها مساعدة الإدارة في التعامل مع هذه المخاطر. وتُجمع أغلب التوصيات الدولية بشأن المخاطر السيبرانية، على أن الأهم المتطلبات التنظيمية المحددة للمخاطر السيبرانية (Supervision of Cyber Risk،Toronto Center، 2018). وقد عملت أغلب المنظمات والهيئات الدولية على وضع توصيات ومعايير خاصة وعامة، يمكن أن تشكل أساساً لإدارة المخاطر السيبرانية، وتعد معايير للتعامل معها، نعرض في الجزء التالي أهمها، وأكثرها قبولاً وانتشاراً في القطاع المصرفي بشكل خاص (*).

1.5.2.مبادئ ومعايير لجنة بازل لإدارة المخاطر السيبرانية:

أصدرت لجنة بازل عديد التوصيات والمبادئ الخاصة بإدارة المخاطر السيبرانية في المصارف، التي أصبحت أسساً أو معايير للدراسات الدولية في تقييم إدارة المخاطر في المصارف، حيث نشرت مبادئ إدارة المخاطر الإلكترونية في عام 2003، وتم تعديلها لاحقًا في عام 2011، لتتضمن الدروس المستفادة من الأزمة المالية الكبرى في 2007-2009. وفي عام 2014 ، أجرت اللجنة مراجعة تنفيذ المبادئ، وكان الغرض من هذه المراجعة، تقييم مدى التزام المصارف التي طبقت المبادئ، وتحديد الثغرات الكبيرة في التنفيذ، وتسليط الضوء على ممارسات إدارة المخاطر التشغيلية الناشئة، والجديرة بالملاحظة في المصارف التي واكبت هذه المبادئ لإدارة المخاطر السيبرانية .

وقد تضمنت الوثيقة الصادرة عن اللجنة عام 2003، بعنوان "مبادئ إدارة مخاطر العمليات المصرفية الإلكترونية" والمعدلة في 2011 بعنوان " مبادئ الإدارة السليمة للمخاطر التشغيلية" ، المبادئ العامة كأسس وأدوات أساسية للسلطات الإشرافية، للتحقق من تواجد الممارسات السليمة من قبل المصارف في تعاملها مع قضايا الصيرفة الإلكترونية، وتندرج هذه المبادئ ضمن ثلاثة أجزاء، نوجز أهم ما جاء فيها فيما يلي (BCBS، Risk Management Principles for Electronic Banking، 2003:7-21 ؛ Principles for the Sound Management of Operational Risk، 2011 : 3-18) :

أولاً / المبادئ المتعلقة بمسؤوليات الإدارة العليا للمصارف :

1. إتباع سياسات مراقبة فعالة للإدارة على المخاطر المرتبطة بالأنشطة المصرفية الإلكترونية.
2. مراجعة واعتماد النواحي الرئيسية الخاصة بعمليات التحكيم والمراقبة للنواحي الأمنية .
3. الاهتمام بوضع منهج شامل ومستمر في إدارة ومراقبة علاقات المصرف مع الأطراف الخارجية، ممن يدعمون العمليات المصرفية الإلكترونية للمصرف.

ثانياً/ المبادئ المتعلقة بالتحكم بالأمن :

(*) يوفر منشور للبنك الدولي بعنوان "Financial Sector's Cybersecurity: A regulatory Digest" (2020)، مرجعية مهمة وجامعة، وملخص تنظيمي عبارة عن تجميع شامل للوائح التنظيمية الحديثة لعدة دول ومنظمات دولية، و المبادئ والمعايير التوجيهية العالمية، بشأن الأمن السيبراني للقطاع المالي. ونظرة عالمية للمبادرات التنظيمية والإشرافية. وهي مورد قيم لأي نظام يسعى إلى بناء عملياتها الإشرافية، أو أي دراسة تبحث في إدارة المخاطر السيبرانية، وفق أشهر الممارسات والمعايير الدولية.

متاح على الرابط : https://thedocs.worldbank.org/en/doc/361881595872293851-0130022020/original/CybersecDigestv5Jul2020FINAL.pdf

1. اتخاذ الإجراءات اللازمة والسليمة، للتحقق من صحة وهوية وتفويض العملاء، ممن يقومون بإجراء عمليات مع المصرف عن طريق الأنترنت .
2. استخدام طرق التحقق من صحة التعاملات التي تعزز عدم الإنكار، وتحدد التعاملات المصرفية الإلكترونية.
3. التأكد من تطبيق الإجراءات الملائمة لغايات فصل الواجبات والمهام، ضمن الأنظمة المصرفية الإلكترونية وقواعد المعلومات، والتطبيقات المصرفية الإلكترونية .
4. التأكد من استخدام أدوات مناسبة لمراقبة التفويض، فيما يخص الأنظمة المصرفية الإلكترونية، وقواعد المعلومات، والتطبيقات المصرفية الإلكترونية .
5. اتخاذ الإجراءات اللازمة الهادفة لحماية سلامة المعلومات الخاصة بالتعاملات المصرفية الإلكترونية.
6. ضمان وجود سجلات تدقيق واضحة لجميع المعاملات المصرفية الإلكترونية.
7. اتخاذ الإجراءات اللازمة الكفيلة بالحفاظ على سرية المعلومات المصرفية الإلكترونية الهامة.

ثالثاً / المبادئ المتعلقة بإدارة المخاطر القانونية والمخاطر المرتبطة بالسمعة :

1. التأكد من الإفصاح عن المعلومات الصحيحة على موقع الأنترنت الخاص بالمصرف.
2. اتخاذ الإجراءات المناسبة الكفيلة بالالتزام بالمتطلبات المتعلقة بخصوصية العملاء، في إطار الالتزامات التشريعية والقانونية السائدة في المنطقة التي يقدم فيها المصرف المنتجات والخدمات المصرفية الإلكترونية.
3. ضرورة امتلاك المصرف للقدرة الفعالة على الاستمرارية في تقديم الخدمات المصرفية الإلكترونية، وامتلاكه لخطط وبدائل في حالات الطوارئ، بما يكفل توفر الأنظمة والخدمات المصرفية الإلكترونية في جميع الأوقات.
4. يجب على المصرف وضع خطط مناسبة للاستجابة للحوادث، لإدارة واحتواء وتقليل المشاكل الناشئة عن أحداث غير متوقعة، بما في ذلك الهجمات الداخلية والخارجية، التي قد تُعيق توفير الأنظمة لتوفير الخدمات المصرفية الإلكترونية .

بعد ذلك أقرت اللجنة بأن مبادئ عام 2011، لم تغطي بشكل كاف المصادر الهامة لمخاطر التشغيل، مثل تلك الناشئة عن مخاطر تكنولوجيا المعلومات والاتصالات، مما استدعى إدخال مبدأ محدد بشأن إدارة مخاطر تكنولوجيا المعلومات والاتصالات، وتم إجراء مراجعات أخرى، لضمان الاتساق مع إطار عمل المخاطر التشغيلية الجديد في بازل (3) و إدراك الاحتمال المتزايد لحدوث اضطرابات كبيرة في عمليات المصرف من الأوبئة والكوارث الطبيعية وحوادث الأمن السيبراني المدمرة أو فشل التكنولوجيا، نتج عنها إصدارها في مارس من عام 2021، منشوراً بعنوان " إدارة مبادئ المراجعات السليمة للمخاطر التشغيلية"، وتخصيص المبدأ رقم (10) لتكنولوجيا المعلومات والاتصالات بما في ذلك الأمن السيبراني، الذي أكد أنه يجب أن تضمن المصارف مرونة تكنولوجيا المعلومات والاتصالات، بما في ذلك الأمن السيبراني الخاضع للحماية والكشف وبرامج الاستجابة والتعافي التي يتم اختبارها بانتظام، وتتضمن الوعي المناسب بالموقف ونقل المعلومات ذات الصلة في الوقت المناسب لإدارة المخاطر وعمليات صنع القرار، لتقديم الدعم الكامل وتسهيل تسليم العمليات الحيوية للمصرف (BCBS، Management of Principles for the Sound Revisions to the Operational Risk، 2021: 16-17).

2.5.2.استراتيجيات صندوق النقد الدولي لتعزيز الأمن السيبراني :

يوضح صندوق النقد الدولي في تقريره الصادر في أبريل 2024، والذي كان عنوان فصله الثالث بـ "المخاطر السيبرانية، نتائج مسح أجراه على المصارف المركزية والسلطات الإشرافية، ويشير فيه أن أطر سياسات الأمن السيبراني، في الأسواق الناشئة والاقتصادات النامية، غالباً ما تظل غير كافية. فعلى سبيل المثال، يبين أن لدى نصف البلدان فقط التي شملها المسح، استراتيجية وطنية للأمن السيبراني، تركز على القطاع المالي أو لوائح مخصصة للأمن السيبراني. ولذلك يورد الصندوق في هذا التقرير عدة توصيات، لتعزيز القدرة على الصمود في القطاع المالي، من ضمنها أنه ينبغي للسلطات أن تضع استراتيجية وطنية مناسبة للأمن السيبراني، مصحوبة بقدرة تنظيمية وإشرافية فعالة، تشمل ما يلي

-94: 2024،Cyber Risk: A Growing concern for macro financial stability،IMF)
:(95

1) تقييم مشهد الأمن السيبراني بشكل دوري، وتحديد المخاطر النظامية المحتملة من الترابط والتركيزات، بما في ذلك مقدمي الخدمات من جهات خارجية.

2) تشجيع النضج السيبراني بين شركات القطاع المالي، بما في ذلك الوصول إلى الخبرة في مجال الأمن السيبراني على مستوى مجلس الإدارة، حيث أن تحسين الحوكمة المتعلقة بالإنترنت، قد يقلل من المخاطر السيبرانية.

3) تحسين أمن الشركات عبر الإنترنت وصحة أنظمتها، مثل مكافحة البرامج الضارة والمصادقة متعددة العوامل، والتدريب والتوعية.

4) إعطاء الأولوية للإبلاغ عن البيانات وجمع الحوادث السيبرانية، وتبادل المعلومات بين المشاركين في القطاع المالي لتعزيز استعدادهم الجماعي.

5) بما أن الهجمات تنشأ في كثير من الأحيان من خارج البلد الأصلي للشركة المالية، ويمكن توجيه العائدات عبر الحدود، فإن التعاون الدولي أمر ضروري لمعالجة المخاطر السيبرانية بنجاح.

6) رغم وقوع حوادث سيبرانية، فإن القطاع المالي يحتاج إلى القدرة على تقديم خدمات الأعمال الحيوية خلال هذه الاضطرابات، ولتحقيق هذه الغاية، يتعين على الشركات المالية تطوير واختبار إجراءات الاستجابة والتعافي، ويتعين على السلطات الوطنية أن تضع بروتوكولات استجابة فعّالة وأطر إدارة الأزمات.

3.5.2. نموذج مجموعة الدول الصناعية السبع G7:

تم وضع نموذج تشغيلي لإدارة المخاطر من قبل مجموعة الدول الصناعية السبع عام 2016، بعنوان "العناصر الأساسية لمجموعة السبع للتقييم الفعال للأمن السيبراني في القطاع المالي"، الذي رأت المجموعة أنه يمكن استخدامه كأداة مرجعية لتصميم وتنفيذ استراتيجية الأمن السيبراني، وإطار العمل التشغيلي للمؤسسات، حيث يساعد في توجيه سياسة المؤسسة العامة وجهودها التنظيمية والإشرافية. ويغطي هذا النموذج الجوانب الرئيسية لحوكمة المخاطر الإلكترونية وتحديد المخاطر والمرونة، ويحتوي على ثمانية عناصر تمثل الأهداف والتوقعات الإشراقية لأي مؤسسة مالية، بما فيها المصارف في إدارة المخاطر السيبرانية، وتتضمن ما يلي(G-7 Fundamental elements for effective assessment of Cybersecurity in the financial sector، 2016 :1-5):

1/ استراتيجية وإطار الأمن السيبراني: إنشاء إطار للأمن السيبراني مصمم خصيصًا للمخاطر السيبرانية، واستراتيجية تكون محددة وواضحة بشكل مناسب، وفق المعايير والمبادئ التوجيهية الوطنية والدولية.

2/ الحوكمة: تحديد وتسهيل أداء الأدوار والمسؤوليات للموظفين، الذين يقومون بالتنفيذ والإدارة والإشراف على فعالية استراتيجية الأمن السيبراني، وإطار العمل لضمان المساءلة، وتوفير الموارد الكافية والسلطة المناسبة والوصول إلى السلطة الحاكمة.

3/ تقييم المخاطر والرقابة: تحديد الوظائف والأنشطة والمنتجات والخدمات، بما في ذلك الترابط والتبعيات والأطراف الثالثة، وإعطاء الأولوية لأهميتها النسبية، وتقييم المخاطر السيبرانية الخاصة لكل منها.

4/ المراقبة: إنشاء عمليات مراقبة منهجية للكشف السريع عن الحوادث السيبرانية، وتقييم فعالية الضوابط المحددة بشكل دوري، من خلال مراقبة الشبكة والاختبار والتدقيق والتمارين .

5/ الاستجابة في الوقت المناسب: وتشمل (أ) تقييم طبيعة ونطاق وتأثير الحادث السيبراني ؛ (ب) احتواء الحادث والتخفيف من أثره؛ (ج) إخطار أصحاب المصلحة الداخليين والخارجيين، مثل سلطات إنفاذ القانون والهيئات التنظيمية والسلطات العامة الأخرى، وكذلك المساهمين ومقدمي الخدمات من الأطراف الثالثة والعملاء، حسب الاقتضاء ؛ (د) تنسيق أنشطة الاستجابة المشتركة حسب الحاجة .

6/ التعافي: استئناف العمليات بشكل مسؤول، مع السماح بمواصلة المعالجة، عن طريق (أ) إزالة المخلفات الضارة للحادث ؛(ب) استعادة الأنظمة والبيانات إلى وضعها الطبيعي؛ (ج) تحديد وتخفيف جميع نقاط

الضعف التي تم استغلالها؛(د) معالجة مواطن الضعف لمنع وقوع حوادث مماثلة؛(هـ) التواصل بشكل مناسب داخلياً وخارجياً.

7/ مشاركة المعلومات: الانخراط في المشاركة في الوقت المناسب لمعلومات موثوقة وقابلة للتنفيذ، بشأن الأمن السيبراني مع أصحاب المصلحة الداخليين والخارجيين، بما في ذلك الكيانات والسلطات العامة داخل القطاع المالي وخارجه، بشأن التهديدات ونقاط الضعف والحوادث والاستجابات، لتعزيز الدفاعات والحد من الضرر وزيادة الموقف الوعي وتوسيع التعلم .

8/ التعلم المستمر: القيام بمراجعة استراتيجية الأمن السيبراني وإطار العمل بانتظام، وعندما تستدعي الأحداث، بما في ذلك مكونات الحوكمة والمخاطر والرقابة والاستجابة والاسترداد ومشاركة المعلومات، لمعالجة التغييرات في المخاطر السيبرانية ، وتخصيص الموارد ، وتحديد الثغرات ومعالجتها ، ودمج الدروس المستفادة.

4.5.2.إرشادات الهيئة المصرفية الأوروبية (European Banking Authority EBA):

أعدت الهيئة المصرفية الأوروبية إرشادات موجهة إلى السلطات المختصة داخل الاتحاد الأوروبي، وتهدف إلى تعزيز إجراءات المراجعة الإشرافية، وعملية التقييم والمنهجيات المشتركة، لتقييم مخاطر تكنولوجيا المعلومات والاتصالات. وتتمحور المبادئ التوجيهية، حول تقييم إدارة واستراتيجية تكنولوجيا المعلومات والاتصالات للمؤسسة المالية، فضلاً عن تقييم مخاطر تكنولوجيا المعلومات والاتصالات والضوابط المعمول بها في سياق المخاطر على رأس المال، حيث تم دمج إرشادات لتكنولوجيا المعلومات بشأن تقييم المخاطر التشغيلية (EBA) الخاصة بـ (SREP) "إرشادات عملية المراجعة والتقييم الإشرافية للبنك المركزي الأوروبي". وبذلك أصبحت تركز هذه المبادئ على تقييم شامل للغاية لعناصر تكنولوجيا المعلومات والاتصالات، بما في ذلك تصنيف (SREP) لمخاطر تكنولوجيا المعلومات والاتصالات، والحوكمة، ومخاطر تكنولوجيا المعلومات والاتصالات، والضوابط، ومخاطر تعهد تكنولوجيا المعلومات، والاتصالات، ومواءمة المخاطر، حيث تتيح منهجيات تصنيف المخاطر وضع المتطلبات لمشرفي المصارف الأوروبية، رسم خريطة لمخاطر تكنولوجيا المعلومات والاتصالات المحددة في فئات المخاطر التالية (EBA، Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process "SREP"، 2016:25-26):

- مخاطر التوافر والاستمرارية: خطر تأثر أداء وتوافر الأنظمة والبيانات سلًبا ، بما في ذلك عدم القدرة على التعافي في الوقت المناسب بسبب فشل الأجهزة أو البرامج ، أو نقاط الضعف في الإدارة ، أو أي حدث آخر.
- مخاطر سالمة البيانات: خطر أن البيانات المخزنة، والمعالجة غير كاملة أو غير دقيقة أو غير متسقة، عبر الأنظمة المختلفة.
- مخاطر التغيير: المخاطر الناشئة عن عدم قدرة المؤسسة على إدارة تغييرات النظام في الوقت المناسب.
- مخاطر الاستعانة بمصادر خارجية: مخاطر إشراك طرف ثالث ، أو كيان مجموعة آخر ، لتوفير أنظمة أو خدمات ذات صلة ، يؤثر سلًبا على أداء المؤسسة وإدارة المخاطر.
- المخاطر الأمنية: خطر الوصول غير المصرح به إلى الأنظمة من داخل المؤسسة أو خارجها.

5.5.2. المبادئ التوجيهية وإرشادات إدارة المخاطر السيبرانية الصادرة عن (CPMI- IOSCO):

أصدرت المنظمة الدولية لهيئات الأوراق المالية، (International Organization of Securities Commissions IOSCO)، و لجنة المدفوعات والبنية التحتية للسوق،(Committee on Payments and Market Infrastructures CPMI)،إطارهما المشترك المعروف اختصاراً بـ (CPMI- IOSCO), وهو إطار عمل شامل يغطي جميع المكونات الوظيفية الرئيسية للمخاطر السيبرانية، بما في ذلك تحديد المخاطر، و حماية أصول المعلومات والتكنولوجيا، والكشف عن نقاط الضعف والاستجابة للحادث والتعافي، ويتضمن في جوهره توقعات الحوكمة الأساسية لمجلس الإدارة والإدارة العليا، وهي أهم المتطلبات التنظيمية المحددة للمخاطر السيبرانية، ويرتكز على أنه يجب البدء، بأن يكون لدى المصارف برنامج أو سياسة أمن إلكتروني موثقة، وتتبع

المتطلبات عادةً إدارة إطار مخاطر العمل، يتضمن الإطار الحوكمة، والتعرف، والحماية، والكشف، والاستجابة، والتعافي. ومن ثم، فإن هذا الإطار يشمل المتطلبات العامة، بشأن الحوكمة والرقابة وملكية المخاطر والمساءلة، وتدابير أمن المعلومات، مثل إجراءات إدارة التصحيح، وضوابط الوصول، والهوية وغيرها، والتقييم الدوري ومراقبة ضوابط الأمن السيبراني، والاستجابة للحوادث، واستمرارية الأعمال وتخطيط التعافي(BIS، OICU-IOSCO، 2016: 5-22) .

6.5.2. برنامج بنك إنجلترا (اختبار التهديدات السيبرانية وفق برنامج CBEST):

منذ عام 2014، أطلقت المملكة المتحدة، عملاً رائداً عالمًيا، لتحليلات التهديدات ونقاط الضعف التي يقودها الذكاء الصناعي، بالإضافة إلى اختبار الاختراق للمؤسسات ذات الأهمية النظامية، وهو برنامج، California Basic Educational Skills Test ، المعروف اختصاراً بـ CBEST، وهو اختبار أمني قائم على التهديدات والمعلومات، ويعتبر الآن الطريقة الأساسية للمصارف في المملكة المتحدة، لاختبار دفاعاتها طوعًا، باستخدام استخبارات التهديدات المتقدمة، ومحاكاة الهجوم الواقعية. واعتبرته الجهات الإشرافية والرقابية في إنجلترا، ومن بينها بنك إنجلترا، جزءاً مهماً من عملها، كونه يتضمن مجموعة أدوات إشرافية جماعية، لتقييم المرونة السيبرانية للشركات والمصارف، ومؤسسات إدارة الأعمال (Bank of England، CBEST Threat Intelligence Led Assessments،2024:6-16)

7.5.2.إرشادات سلطة النقد في سنغافورة لإدارة المخاطر السيبرانية :

صدرت هذه الإرشادات عن السلطة النقدية في سنغافورة، وتسعى إلى معالجة شاملة للمخاطر، من خلال تضمنها توقعات إشرافية، حيث تجمع بين المبادئ التكنولوجية المتزايدة، بما في ذلك المخاطر الإلكترونية التي تواجهها المؤسسات المالية الخاضعة للتنظيم. وتعتبر هذ الإرشادات ملزمة لتحديد الممارسات الجيدة مع المخاطر السيبرانية للمؤسسات المصرفية التي تشرف عليها سلطة النقد السنغافورية، ويمكن الاسترشاد بها دولياً، حيث تحدد إرشادات مبادئ إدارة المخاطر وأفضل الممارسات للقطاع المالي، أهمها ما يلي Management Technology Risk ،MAS "Monetary Authority of Singapore Guidelines،2021: 6-42):

(أ) إنشاء نظام سليم وقوي لإدارة مخاطر التكنولوجيا والإشراف عليها، ويفترض أن يؤدي مجلس الإدارة والإدارة العليا في المصرف دورًا أساسيًا في مراقبة وإدارة مخاطر التكنولوجيا، ويجب على الإدارة العليا ومجلس الإدارة أن تزرع ثقافة مخاطر قوية، وأن تضمن إنشاء إطار سليم وقوي لإدارة مخاطر التكنولوجيا.

(ب) الحفاظ على المرونة السيبرانية، حيث ينبغي على المصارف، أن تتبنى نهجاً دفاعياً متعمقاً، لتعزيز صمود الأمن السيبراني، ومن المهم أيضًا، أن تقوم المصارف بالتحسين بشكل مستمر، لعمليات وضوابط تكنولوجيا المعلومات، للحفاظ على السرية والنزاهة.

8.5.2. توصيات المنظمات العربية بشان إدارة المخاطر السيبرانية:

نشر صندوق النقد العربي عام 2019 خلال الاجتماع الثالث لمجموعة العمل الإقليمية للتقنيات المالية الحديثة، ، دراسة عن الأمن السيبراني في القطاع المصرفي، تضمنت عرض مقارن للمعايير والتجارب الدولية والعربية، تشير إلى التالي:

1) أهمية وجود معايير محددة تنظم المخاطر السيبرانية

البحث المستمر والمكثف نحو اتخاذ إجراءات وقائية من تلك المخاطر، من خلال وضع لوائح تجعل تلك الإجراءات أكثر وضوحاً أمام مجالس إدارات تلك مستمر في تعزيز الأمن السيبراني.

2) الأطر والمعايير الدولية المنظمة للمخاطر السيبرانية:

أهمية وجود استراتيجية للأمن السيبراني، بحيث تضع كل مؤسسة مالية استراتيجية الأمن السيبراني الخاصة بها، وفقًا لممارسات إدارة المخاطر المستندة إلى المبادئ الدولية. وأن تقوم الجهات الرقابية بمراجعة هذه الاستراتيجيات، كجزء من تقييمها للممارسات الشاملة لإدارة المخاطر في المؤسسة.

تبع ذلك نشر اتحاد المصارف العربية توصيات المشاركون في منتدى رؤساء إدارات المخاطر في المصارف العربية في الغردقة/ مصر، الذي نظمه بالتعاون مع المصرف المركزي المصري واتحاد

المصارف المصرية ، بعض التوصيات، كان أهمها فيما يتعلق بالمخاطر السيبرانية، تأكيده على ضرورة وجود منهجية واضحة لدى المصارف لإدارة المخاطر الرقمية، مع تطوير قدرات العاملين بإدارات أمن المعلومات بالمصارف في إدارة هذه المخاطر، وتضمين الاستراتيجيات والسياسات الخاصة بالمصارف، جزءاً خاصاً بإدارة المخاطر السيبرانية، بالإضافة إلى تعزيز ثقافة الحوكمة الإلكترونية، بحيث تضع كل مؤسسة مالية استراتيجية الأمن السيبراني الخاصة بها، وفقاً لممارسات إدارة المخاطر(نشاط اتحاد المصارف العربية ، العدد 472 ، مارس 2020). وأخيراً أوصى الاتحاد، أثناء إقامته للملتقى السنوي لرؤساء إدارات المخاطر في المصارف العربية للعام 2023 (بدورته الخامسة)، على ضرورة أهمية تزويد إدارة المخاطر بالوسائل والأدوات التي تمكنها من المشاركة في وضع استراتيجيات المصارف في دخول عالم التحول الرقمي.

6.2.المعايير والمبادئ الدولية للمرونة السيبرانية

1.6.2.مبادئ مجلس الإدارة للمرونة السيبرانية (المنتدى الاقتصادي العالمي):

أصدر المنتدى الاقتصادي العالمي في يناير 2017 بالشراكة مع (Boston Consulting Group) و(Hewlett Packard Enterprise) ، منشور بعنوان "تعزيز المرونة السيبرانية - مبادئ وأدوات للمجالس" ، تضمن مبادئ للمرونة السيبرانية، يمكن أن تسترشد بها مجالس الإدارة المصارف، نصت على ما يلي: (World Economic Forum ، "Advancing Cyber Resilience Principles and Tools for Boards"، 2017: 8) :-

المبدأ الأول/ المسؤولية عن المرونة السيبرانية : يتحمل مجلس الإدارة ككل المسؤولية النهائية، للإشراف على المخاطر السيبرانية والقدرة على الصمود، ويجوز لمجلس الإدارة، تفويض نشاط الإشراف الأساسي إلى لجنة قائمة، مثل لجنة المخاطر، أو لجنة جديدة، مثل لجنة المرونة السيبرانية.

المبدأ الثاني / قيادة الموضوع : يتلقى أعضاء مجلس الإدارة توجيهات، تتعلق بالمرونة الإلكترونية عند الانضمام إلى مجلس الإدارة، ويتم تحديثهم بانتظام، بشأن التهديدات والاتجاهات الأخيرة، ويمكن أن يستعينوا بخبراء خارجيين مستقلين.

المبدأ الثالث / موظف مسؤول: يضمن مجلس الإدارة أن يكون أحد موظفي المصرف، مسؤولاً عن الإبلاغ عن قدرة المصرف على إدارة المرونة السيبرانية، والتقدم المحرز في تنفيذ أهدافها، ويجب إن يضمن مجلس الإدارة أن هذا الموظف، يتمتع بإمكانية الوصول المنتظم إلى مجلس الإدارة، والسلطة الكافية ،وقيادة الموضوع، والخبرة والموارد، لإنجاز هذه الواجبات.

المبدأ الرابع/ تكامل المرونة السيبرانية: يضمن مجلس الإدارة، أن تدمج الإدارة المرونة السيبرانية ، وتقييم المخاطر السيبرانية ، في استراتيجية العمل الشاملة وإدارة المخاطر على مستوى المصرف، بالإضافة إلى إعداد الميزانية وتخصيص الموارد.

المبدأ الخامس/ الرغبة في المخاطرة: يقوم مجلس الإدارة سنوًيا، بتحديد وتقدير تحمل مخاطر الأعمال، فيما يتعلق بالمرونة السيبرانية، ويضمن أن هذا يتماشى مع استراتيجية المصرف وقابلية المخاطرة.

المبدأ السادس/ تقييم المخاطر والإبلاغ عنها: يُعد مجلس الإدارة المسؤول عن الإبلاغ عن التقييم الكمي، ومفهوم للمخاطر السيبرانية والتهديدات والأحداث، كبند دائم في جدول الأعمال أثناء اجتماعات مجلس الإدارة، ويقوم بالتحقق من صحة هذه التقييمات، من خلال تقييم المخاطر الاستراتيجي الخاص بها، باستخدام إطار عمل مجلس الإدارة للمخاطر السيبرانية .

المبدأ السابع/ خطط المرونة: يضمن مجلس الإدارة، أن الإدارة تدعم الموظف المسؤول عن المرونة السيبرانية، خلال إنشاء وتنفيذ واختبار وتحسين خطط المرونة السيبرانية، ويتطلب من المسؤول مراقبة الأداء وتقديم تقارير منتظمة إلى مجلس الإدارة.

المبدأ الثامن/ المجتمع: يشجع مجلس الإدارة على التعاون مع أصحاب المصلحة الآخرين، حسب الاقتضاء، من أجل ضمان المرونة السيبرانية الشاملة.

المبدأ التاسع/المراجعة: يضمن مجلس الإدارة، إجراء مراجعة رسمية ومستقلة للمرونة السيبرانية للمصرف سنوياً.

المبدأ العاشر/ الفعالية: يراجع مجلس الإدارة بشكل دوري، أدائه في تنفيذ هذه المبادئ، أو يسعى للحصول على مشورة مستقلة للتحسين المستمر.

2.6.2.مبادئ المرونة التشغيلية (لجنة بازل) :

أصدرت لجنة بازل مبادئ للمرونة التشغيلية في المصارف، في منشورها الصادر في 2021 ، بعنوان مبادئ المرونة التشغيلية، وقد خصص المبدأ السابع للمرونة السيبرانية، ونص على الاتي (BSBC، Principles for Operational Resilience، 2017، 7 : 8):

- على المصارف ضمان مرونة تكنولوجيا المعلومات والاتصالات، بما في ذلك الأمن السيبراني الذي يخضع للحماية والكشف والمراقبة. وتتضمن برامج الاستجابة والتعافي التي يتم اختبارها بانتظام، الوعي المناسب، ونقل المعلومات ذات الصلة في الوقت المناسب، لإدارة المخاطر وعمليات صنع القرار، لتقديم الدعم الكامل، وتسهيل تنفيذ العمليات الحيوية للمصرف.

- أن يكون لدى المصارف سياسة موثقة لتكنولوجيا المعلومات والاتصالات، بما في ذلك الأمن السيبراني، والتي تنص على ذلك متطلبات الحوكمة والرقابة، وخصوصية المخاطر والمساءلة، وتدابير أمن تكنولوجيا المعلومات والاتصالات (مثل ضوابط الوصول ، وحماية أصول المعلومات الهامة ، وإدارة الهوية)، والتقييم الدوري ومراقبة ضوابط الأمن السيبراني، والاستجابة للحوادث، واستمرارية الأعمال.

- على المصارف، تحديد أصول المعلومات الهامة والبنية التحتية التي تعتمد عليها، و إعطاء الأولوية لجهودها في مجال الأمن السيبراني، بناءً على تقييم مخاطر تكنولوجيا المعلومات والاتصالات، وأهمية أصول المعلومات الهامة للعمليات الحيوية للمصرف، مع مراقبة كل المتطلبات القانونية والتنظيمية ذات الصلة المتعلقة بحماية البيانات والسرية، كما يجب على المصارف، وضع الخطط وتنفيذ الضوابط، للحفاظ على سلامة المعلومات الهامة في حالة أي حدث إلكتروني، مثل التخزين الآمن والنسخ الاحتياطي في وضع عدم الاتصال على الوسائط غير القابلة للتغيير للبيانات التي تدعم الحرجة عمليات. كذلك يجب أن تقيم بشكل منتظم ملف تعريف التهديدات لأصول المعلومات الهامة الخاصة بها، واختبارها مواطن الضعف، وضمان قدرتها على الصمود أمام المخاطر المتعلقة بتكنولوجيا المعلومات والاتصالات.

3.منهجية الدراسة وجمع وتحليل البيانات

تعتمد الدراسة على المنهج الاستقرائي والاستنباطي، لتقييم واقع إدارة المخاطر السيبرانية في المصارف التجارية الليبية. من خلال الاعتماد على عرض رؤى المنظمات الدولية لإدارة المخاطر السيبرانية وتطورها، ونماذجها وطرق إدارتها المتبعة أو المقترحة كإرشادات أو توصيات تمثل معايير مقبولة عالمياً، والبحث في التقارير الدولية لاستنباط واقع إدارة المخاطر في المصارف الليبية، وإظهار مؤشرات عنها، ثم تقييم واستقراء واقع إدارة المخاطر في المصارف التجاري الوطني، بالاعتماد على الزيارات الميدانية والملاحظة، وتصميم استمارة استبانة تحتوي على أسئلة مصاغة، وفق المتطلبات والتوصيات المحلية والدولية لإدارة المخاطر السيبرانية، لاستطلاع رؤية المسؤولين والمختصين في المخاطر السيبرانية في مدى التزام المصرف التجاري الوطني بإدارة المخاطر السيبرانية، وفق المعايير الدولية، وتحليلها باستخدام الأدوات الإحصائية المناسبة من برنامج (Stata) .

1.3. واقع المخاطر السيبرانية "المصرفية" في ليبيا

استكمالاً لما عُرض من المفاهيم الدولية للمخاطر السيبرانية، وعرض لتطورها وأثارها، ثم تناول الرؤى الدولية في شكل نماذج أو مبادئ أو توصيات وإرشادات تلقى قبولاً دولياً واسعة تختص بإدارة المخاطر السيبرانية في المصارف، وكيفية التعامل معها ، ومعايير قياس قدرة المصارف على مواجهتها بما يعرف بالمرونة السيبرانية . فإن الدراسة تعتمد بشكل كبير على استكشاف واقع إدارة هذه المخاطر في المصارف الليبية، وإظهار مؤشرات عنها، من خلال تقارير محلية ودولية عن ليبيا، تناولت هذه المخاطر أو واقع إدارتها من قبل المصارف الليبية.

1.1.3. مؤشرات عن واقع وظروف إدارة المخاطر السيبرانية في المصارف الليبية :

نركز في هذا الجزء على عرض لمؤشرات عن واقع الحوكمة في المصارف الليبية، خاصة ما يتعلق بالمخاطر السيبرانية، في مصرف ليبيا المركزي، والمصارف التجارية الليبية. وذلك اعتماداً على مراجعة

الدراسات التي تناولت الحوكمة المصرفية في ليبيا، والاطلاع على بعض نتائج بعض الدراسات والتقارير المحلية، كتقارير ديوان المحاسبة، وتقارير دولية صادرة عن صندوق النقد الدولي خاصة بليبيا، وزيارات ميدانية، لفروع لمصارف التجارية الواقعة في مدينة البيضاء.

1.1.1.3.مؤشرات عن دور مصرف ليبيا المركزي في إرساء معايير الحوكمة في المصارف الليبية:

تشير بعض الدراسات والتقارير الدولية أن دور مصرف المركزي في تطبيق معايير الحوكمة الدولية، كان محصوراً تقريباً في إصدار توجيهات مكتوبة في شكل مناشير، دون القدرة على فرض اتباعها على المصارف التجارية، ربما نتيجة للانقسام الذي شهده القطاع المصرفي خلال السنوات القليلة الماضية، أو عدم قدرته على القيام بالرقابة على تنفيذها. ويمكن توضيح من خلال الآتي :

1/ في 2010/9/27، قام مصرف ليبيا المركزي وفقا لمنشوره رقم (20) لسنة 2010، بإصدار دليل الحوكمة للقطاع المصرفي الليبي، وتعميمه على المصارف التجارية، وقد كانت أهم مضامينه في تكوين لجان للمخاطر ، ولجان للحوكمة، وتحديد مهامها ، وكان ذلك بشكل عام دون تفاصيل فنية محددة، حيث انحصرت في أن تعد هذه اللجان تقارير تتضمن تحديد متطلبات عمل الإدارات، والمسؤوليات وبعض المهام الرقابية.

2/ في 2012/9/8 ، قام مصرف ليبيا المركزي بإصدار منشور رقم (02) لسنة 2021 ، بشأن دليل حوكمة عمل وحدات الامتثال بالمؤسسات المالية. وقد كانت أهم مضامينه، تحديد مهام مجالس الإدارات والإدارات التنفيذية للمصارف ، ومهام وحدات الامتثال. ولم يكن هناك تضمين أي توصيات لاتباع معايير دولية ، كمعايير لجنة بازل الصادرة بالخصوص.

3/ في 2023/7/10، قام مصرف ليبيا المركزي بإصدار منشوره رقم (21) لسنة 2023، بشأن إصدار دليل حوكمة تكنولوجيا المعلومات، الذي تضمن المبادئ التوجيهية المعتمدة من مصرف ليبيا المركزي، كمعايير لتقييم المؤسسة، وأفضل الممارسات لتوجيه المؤسسات المالية فيما يلي:

- إنشاء إطار قوي ومتين لإدارة مخاطر التقنية.
- تعزيز أنظمة الحماية والموثوقية والمرونة والقابلية للاسترداد.
- تطبيق عمليات توثيق مُحكمة لحماية بيانات الزبائن والعمليات والأنظمة.

وقد اعتمد مصرف ليبيا المركزي تقييم مخاطر المصرف وفق درجة التقيد بهذه المبادئ، وطلب من جميع المصارف في ليبيا، الالتزام بهذه الضوابط، بالقدر الذي ينطبق عليها، بجانب التزامها بدليل وسياسات الحوكمة ذات الصلة الصادرة عن مصرف ليبيا المركزي، وأكد على أن أهداف وعمليات دليل حوكمة تكنولوجيا المعلومات ومعطياتها، حد أدنى ويتوجب على إدارة المصرف الامتثال لها وتحقيقها بشكل مستمر.

2.1.1.3. مؤشرات محلية ودولية عن إدارة المخاطر السيبرانية في المصارف الليبية

1.2.1.1.3.(تقرير ديوان المحاسبة الليبي 2020)

يشير تقرير ديوان المحاسبة الليبية الصادر عام 2020 ، إلى ملاحظات تخص المخاطر السيبرانية في المصرف المركزي كان أهمها، عدم تقيد مصرف ليبيا المركزي بأحكام دليل الحوكمة الصادر عنه، خاصة من حيث تكوين اللجان المختصة بالحوكمة والمخاطر السيبرانية.

2.2.1.1.3.(تقرير ديوان المحاسبة 2022)

يؤكد تقرير ديوان المحاسبة الصادر عام 2022، عن ملاحظات التقرير السنوي السابق، حيث يشير إلى مخالفة مجالس إدارات المصارف، لأحكام دليل الحوكمة الصادر عن مصرف ليبيا المركزي في تكوين لجان الحوكمة . كما أشار إلى عدم وجود تقارير جرد لأصول تقنية المعلومات(البرمجيات المعدات التقنية) الأمر الذي ترتب عنه مخاطر جودة نظام المعلومات وبالتالي ضعف مراقبة كافة العمليات بالبنية التقنية للمصارف. وعدم تفعيل نظام مراقبة قواعد البيانات والمنظومة المصرفية، بالرغم من وجوده، الأمر الذي ترتب عنه تكبيد المصارف لخسائر نتيجة عمليات الاختراق التي طالت المنظومة المصرفية.

3.2.1.1.3. تقرير صندق النقد العربي حول الاستقرار المالي في الدول العربية 2024:

يشير صندوق العربي في هذا التقرير إلى دراسة أعدها على إدارة المخاطر السيبرانية في عينة من الدول العربية شملت ليبيا، أن المخاطر السيبرانية جاءت في المرتبة الأولى، كأبرز المخاطر التي تواجه الاستقرار

المالي في هذه الدول، وإن هناك صعوبات تواجهها في تحقيق الأمن السيبراني في المصارف، منها صعوبة التنظيم ونقص القدرات وموثوقية المعلومات، كما أظهر التقرير عن ليبيا بشكل خاص، عدم وجود قياس لتطور الأمن السيبراني على مستوى مصرف ليبيا المركزي (صندوق النقد العربي، الاستقرار المالي في الدول العربية، 2024، 189-191، 212).

4.2.1.1.3. تقرير صندوق النقد الدولي عن ليبيا (مراجعة القطاع المالي،2020)

صدر عن صندوق النقد الدولي عام 2020، تقرير عن زيارة خبراء الصندوق لليبيا، بعنوان مراجعة القطاع المالي، أشار في تناوله للمخاطر السيبرانية ، إلى ارتفاع المخاطر التشغيلية، بسبب ضعف هيكل المعلومات وإدارة المخاطر بجميع أنواعها، وأن هناك نقص في القدرات الرقمية، سواء لدى المصارف التجارية أو مصرف ليبيا المركزي.

4. استطلاع واقع إدارة المخاطر في المصرف التجاري الوطني

عملت الدراسة على استطلاع يشمل المسؤولين والمختصين بإدارة المخاطر السيبرانية بالمصرف التجاري الوطني، اعتمد على زيارات ميدانية ومقابلات مع بعضهم، بغرض جمع بعض المعلومات اللازمة، وتصميم استبانة بهدف تقييم واقع إدارة المخاطر السيبرانية بالمصرف، ومدى التزامه بمعايير حوكمتها، قُدمت لعينة من مسؤولي المصرف في الإدارة العليا، ومختصين من إدارة المخاطر، ومكتب المعلومات.

1.4. تصميم الاستبانة

تم صياغة أسئلة الاستبانة وتقسيمها إلى محاور، بما يتوافق مع أهداف الدراسة، وإمكانية اختبار فرضياتها، ولذلك صممت إلى محاور تتضمن أهم النقاط التي تعد أساس التقييم وفق توصيات المنظمات الدولية (خاصة توصيات اتفاقية بالي للتكنلوجيا المالية، والمعدة بإشراف صندوق النقد والبنك الدوليين، توصيات لجنة بازل، فيما يخص إدارة المخاطر السيبرانية (وفق منشور 2021). وعليه تضمنت الاستبانة خمس محاور كما يلي :

المحور الأول :خصص للمعلومات الشخصية والعامة .

المحور الثاني: إدارة المخاطر العمليات الإلكترونية (السيبرانية).

المحور الثالث : مراحل تحقيق المرونة السيبرانية.

المحور الرابع: إشراف مجلس الإدارة والإدارة العليا.

المحور الخامس: السمعة والمخاطر القانونية.

وقد وضعت اختيارات الإجابة على أسئلة الاستبانة، لتكون إجابة واحدة لكل سؤال من بين خمس اختيارات، وذلك وفقاً لمقياس ليكرت الخماسي (Likert scale)، واعتمدت درجات المقياس وفق اختيارات الإجابة، كما هو مبين بالجدول (3) .

جدول (3) درجات مقياس ليكرت وفق اختيارات الإجابة

مستوى المقياس	رافض بشدة	رافض	محايد	موافق	موافق بشدة
الدرجة	1	2	3	4	5

وبذلك، فإن المتوسط الحسابي لخيارات الإجابة ثلاث درجات، وهذا يعني انه كلما زاد المتوسط الحسابي عن ثلاث درجات، كما دل ذلك على تطبيق أكثر لتوصيات لجنة بازل بخصوص إدارة المخاطر السيبرانية في المصارف التجارية، والعكس صحيح، فكلما قل المتوسط الحسابي عن 3 درجات، كلما دل ذلك على تطبيق أقل التوصيات لجنة بازل، بخصوص إدارة المخاطر السيبرانية.

ولغرض تحليل البيانات المتحصل عليها من استمارات الاستبانة بطريقة سهلة وبسيطة، فقد اعتبرت الإجابة موافق بشدة أو موافق على أنها إيجاب (أي تطبيق توصيات لجنة بازل بشأن إدارة المخاطر السيبرانية)، والإجابة أرفض أو أرفض بشدة على أنها (عدم تطبيق توصيات لجنة بازل بشأن إدارة المخاطر السيبرانية) ، أما الإجابة بمحايد فقد تم استبعادهما من التحليل.

2.4. صدق وثبات الاستبانة:

تم تقييم صدق وثبات الاستبانة، باستخدام حساب معامل الفاكروباخ (Cronbach's alpha coefficient)، حيث بلغ للأسئلة من (1) إلى (34) حوالي 0.9576، وهو معامل مرتفع يدل على مصداقية الاستبيان.

3.4. تحليل إجابات المشاركين

وزعت (50) استمارة، أُسترجع منها 37 استمارة، صالحة للتحليل. وكانت الردود على كل محور كما يلي :

1.3.4.المحور الأول/ معلومات شخصية عن المشاركين في الاستبيان

يوضح الجدول رقم (5) معلومات شخصية عن المشاركين في الاستبيان ، وفق إجاباتهم عن أسئلة المحور الأول، فيما ما عدا احد الاستمارات المرجعة لم يجب فيها المشارك عن هذه الأسئلة . حيث بلغ عدد الموظفين من المشاركين النسبة الأعلى التي بلغت تقريباً 67 % ، ثم نسبة رؤساء الأقسام بنحو 14 % ثم مساعدو مدراء الإدارات ومدراء الوحدات والمهندسون التقنيون بنفس النسبة لكل منهم والتي كانت حوالي 6 % .

وظهر أن مؤهلات المشاركين كانت جيدة، حيث بلغت نسبة من يحمل درجة البكالوريوس نحو 64%، فيما نسبة 6 % تقريباً لكل من حملة الماجستير و 5% الدكتوراه ، والبقية من حملة الدبلوم المتوسط . وذلك يشير إلى أن أغلب المشاركين يحملون مؤهلات عليا، يفترض أن تساعدهم على فهم محتوى أسئلة الاستبانة، وإمكانية الإجابة عليها. بينما يتضح أن المشاركين الذين تلقوا دورات في العمل المصرفي بلغت نسبتهم75%، بينما بلغت نسبة الذين لم يتلقوا دورات في هذا المجال حوالي 25%. وبلغ المتوسط الحسابي لسنوات الخبرة للمشاركين في مجال العمل المصرفي بنحو 17.33 سنة .

جدول (5) معلومات شخصية عن المشاركين في الاستبيان

وظائف المشاركين في المصرف		
الوظيفة	العدد	النسبة المئوية
موظف	52	%67
مساعد مدير إدارة	2	%5
مدير وحدة	2	%5
رئيس قسم	5	%14
مراقب تقني	1	%3
مهندس	2	%6
الإجمالي	37	%100
التأهيل العلمي		
المؤهل العلمي	العدد	النسبة المئوية
دبلوم متوسط	9	%25
بكالوريوس	42	%64
ماجستير	2	%6
دكتوراه	2	%5
الإجمالي	37	%100
التدريب		
الحاصلين على دورات تدريبية في العمل المصرفي	العدد	النسبة المئوية
نعم	27	75%
لا	10	%25
الإجمالي	37	%100
بينما بلغ متوسط سنوات الخبرة للمشاركين 17.33 سنة		

2.3.4.المحور الثاني/ إشراف مجلس الإدارة والإدارة العليا (التنظيم والإشراف):

تضمن هذا المحور ستة عشر سؤالاً، ويهدف إلى تقييم إشراف مجلس الإدارة والإدارة التنفيذية العليا على إدارة المخاطر، فيما يتعلق بالتنظيم والإشراف على المخاطر السيبرانية، ونورد ما أظهرته إجابات المشاركين على أسئلة المحور، متسلسلة وفق ترتيبها الوارد في الجدول رقم (6) كما يلي :

1) نسبة 51% من المشاركين، يوافقون على أن للمصرف إدارة مخاطر فاعلة لجميع الأنشطة المصرفية الإلكترونية، مبين لها الضوابط المحددة للعمل والمساءلة، بينما يرفض ما مجموعه أكثر من 8% ذلك، وتقريباً نسبة 21 % كانوا محايدين.

2) أن ما نسبته 47% من المشاركين محايدين ، ونسبة 31% موافقين، على أن إدارة المخاطر تتابع العمليات الإلكترونية بكفاءة وفاعلية، وأن 8% موافقين بشدة ، في حين أن حوالي 14% رافضين.

3) أن حوالي 24% من أفراد العينة موافقين على أن أعمال إدارة المخاطر الإلكترونية تخضع لتدقيق داخل فعال، وأن 11% موافقين بشدة، في حين أن 54% من المشاركين محايدين ، ونسبة 11% رافضين

4) يظهر أن نسبة 38% من المشاركين موافقين، ونسبة 8% موافقين بشدة، على وجود استراتيجية وسياسة معتمدة من مجلس الإدارة لمخاطر العمليات الإلكترونية ، وأن حوالي 35.14% كانوا محايدين، في حين بلغت نسبة الرافضين بشدة 16%، وأن 3% رافضين ذلك.

5) عند الاستفسار عن وجود سياسة وإجراءات واضحة لدى المصرف في تقييم مخاطر العمليات الإلكترونية. ظهر ما نسبته 42% موافقين على انه يوجد لدى المصرف سياسة وإجراءات واضحة في تقييم مخاطر العمليات الإلكترونية ، وأن 14% من المشاركين موافقين بشدة، في حين بلغت نسبة المحايدين حوالي 36%، وأن5 % رافضين، و2% رافضين بشدة.

جدول(6) يبين إجابات المشاركين حول إشراف مجلس الإدارة والإدارة العليا (التنظيم والإشراف)

ت	الإجابة (التكرار ، والنسبة المئوية) / السؤال	ارفض بشدة	ارفض	محايد	موافق بشدة	موافق
1	يوجد بالمصرف إدارة مخاطر فعالة لجميع الأنشطة المصرفية الإلكترونية، مبين لها الضوابط المحددة للعمل والمساءلة.	1	2	8	19	7
		%3	%5	%22	%51	%19
2	تمارس إدارة المخاطر متابعة العمليات الإلكترونية بكفاءة وفاعلية.	0	5	17	11	3
		%0	%14	%47	%31	%8
3	تخضع أعمال إدارة المخاطر الإلكترونية لتدقيق داخلي فعال ومستقل.	0	4	20	9	4
		%0	%11	%54	%24	%11
4	يوجد في المصرف استراتيجية وسياسة معتمدة من مجلس الإدارة لإدارة مخاطر العمليات الإلكترونية.	6	1	13	14	3
		%16	%3	%35	%38	%8
5	يوجد لدى المصرف سياسة و إجراءات واضحة في تقييم مخاطر العمليات الإلكترونية	1	2	13	15	5
		%2	%5	%37	%42	%14
6	يصنف المصرف المخاطر السيبرانية عن العمليات المصرفية الإلكترونية من ضمن مخاطر التشغيل.	0	1	12	20	4
		%0	%3	%32	%54	%11
7	يعمل مجلس الإدارة والإدارة العليا للمصرف على المراجعة المستمرة وإجراء الموافقات اللازمة لعمليات الرقابة الأمنية للمصرف.	1	4	11	14	6
		%3	%11	31%	39%	%16
8	يضع المصرف جدول محدد لمراجعة ورقابة المخاطر الإلكترونية	1	5	19	9	3
		%3	%13	%52	%24	%8
9	يعمل المصرف باستمرار على دراسة المخاطر السيبرانية وتقييمها ووضع الخطط اللازمة لمواجهتها.	2	3	18	10	4
		%5	%8	%49	%27	%11
10	يضع المصرف المعايير والسياسات والإجراءات الخاصة بالأمن السيبراني، ويعمل على مراجعتها وتحديثها باستمرار.	2	2	9	21	3
		%5	%5	%25	%57	%8
11	يهتم المصرف بوضع نموذج أو اطار واضح للهجمات السيبرانية المتوقع مواجهتها.	2	2	18	11	4
		%5	%5	%49	%30	%11
12	يعمل المصرف من فترة لأخرى على اتخاذ إجراءات لتحسين رقابة	2	1	16	15	3

	المخاطر الإلكترونية .	%5	%3	%43	%41	%8
13	يحدد المصرف البيانات التي يجب حمايتها من الاختراق وفق المعايير الدولية لإدارة المخاطر السيبرانية	0	2	16	11	8
		%0	%5	%43	%30	%22
14	يتبع المصرف في إجراءات شاملة للعناية الواجبة والرقابة الإدارية للاستعانة بمصادر خارجية	1	0	10	20	5
		%3	0	%28	%56	%13
15	يراعي المصرف ضمان استمرار الأعمال وسرية المعلومات ونزاهتها عند التعامل مع الطرف الثالث.	1	1	8	22	5
		%3	%3	%22	%60	%12
16	تتوافق كيفية التعامل المصرف مع الأطراف الثالثة مع احتياجات وسياسات المصرف، فيما يخص متطلبات الحماية، ومتطلبات الأمان لمعلومات المصرف والعملاء.	1	2	8	20	6
		%3	%5	%22	%54	%16

6) أن حوالي 54% من أفراد العينة موافقين على أن المخاطر الناتجة عن العمليات المصرفية الإلكترونية يصنفها المصرف من ضمن مخاطر التشغيل، وأن 11% موافقين بشدة، في حين أن 32% بلغت نسبة المشاركين محايدين، وأن 2.70% رافضين .

7) تبين أُن ما نسبته 39% موافقين على أن مجلس الإدارة والإدارة العليا بالمصرف تقوم بالمراجعة المستمرة، وإجراء الموافقات لعلميات الرقابة الأمنية، وأن 17% من المشاركين موافقين بشدة، في حين بلغت نسبة المحايدين 31% وبلغت نسبة الرافضين 11% وأن ما نسبته 2.78% رافضين بشدة .

8) يتضح أن ما نسبته 51% محايدين وهي أعلى نسبة، وأن 24% من أفراد العينة موافقين على أن المصرف يضع جدول محدد لمراجعة ورقابة المخاطر الإلكترونية، وأن 8% موافقين بشدة، في حين بلغت نسبة الرافضين لهذا السؤال 14%، وأن ما نسبته 3% رافضين بشدة .

9) يظهر أن حوالي 49% من المشاركين محايدين وهي أعلى نسبة، وأن ما نسبته 27% موافقين على أن المصرف يقوم باستمرار بدراسة المخاطر السيبرانية، ويضع الخطط اللازمة لمواجهتها، وأن 11% موافقين بشدة ، في حين بلغت نسبة الرافضين 8.11%، بينما نسبة 5.41% من المشاركين كانوا رافضين بشدة.

10) ظهر أن 57% موافقين على أن المصرف يضع المعايير والسياسات الخاصة بالأمن السيبراني ويعمل على مراجعتها باستمرار، وأن.11% موافقين بشدة، في حين أن 24% من المشاركين محايدين، وأن ما نسبته 5.4% رافضين ، كذلك ما نسبته 5.41% رافضين بشدة .

11) يتضح أن حوالي 49% من المشاركين بالدراسة كانوا محايدين، وأن 30% موافقين، على أن المصرف يهتم بوضع نموذج أو إطار واضح للهجمات السيبرانية المتوقع مواجهتها، وأن ما نسبته 11% موافقين بشدة، وبلغت نسبة 10% مجموع الرافضين.

12) إن نسبة 43% كانوا محايدين، ونسبة 41% وافقوا بشدة 8% وافقوا، على أن المصرف يعمل من فترة لأخرى على اتخاذ إجراءات لتحسين رقابة المخاطر الإلكترونية، والنسبة الباقية رفضوا ذلك.

13) إن حوالي 43% من المشاركين كانوا محايدين، وأن 30% موافقين على أن يحدد المصرف البيانات التي يجب حمايتها من الاختراق، وفقاً المعايير الدولية لإدارة المخاطر السيبرانية، وأن ما نسبته 22% موافقين بشدة، وكانت نسبة الرافضين نحو 5%.

14) ظهرت نسبة الموافقين 56% ونسبة 13% موافقين بشدة، على أن المصرف يتبع في إجراءات شاملة للعناية الواجبة والرقابة الإدارية للاستعانة بمصادر خارجية للعلاقات وتعهدات الطرف الثالث، في حين أن بلغت نسبة المحايدين 28% ، والبقية كانوا رافضين بشدة.

15) يتضح أن حوالي نسبة 60% موافقين، 12% موافقين بشدة، على أن المصرف يراعي ضمان استمرار الأعمال وسرية المعلومات وتزامنها عند التعامل مع الطرف الثالث في حين بلغت نسبة المحايدين حوالي 22% ، وأن نسبة 6% لمجموع الرافضين والرافضين بشدة.

16) يتضح أن حوالي 54% من المشاركين موافقين، ونسبة 16% موافقين بشدة، على كيفية تعامل المصرف مع الأطراف الثالثة، وتوافقها مع احتياجات وسياسات المصرف، فيها فيما يخص متطلبات العملية ومتطلبات الأمان ، بينما كانت نسبة المحايدين22%، وما نسبته 5% رافضين، ونسبة 3% رافضين بشدة.

3.3.4. المحور الثالث/إدارة مخاطر العمليات الإلكترونية (الضوابط الأمنية):

خصصت أسئلة هذا المحور، لتقييم الضوابط الأمنية التي يضعها المصرف لإدارة مخاطر العمليات الإلكترونية، وقد كانت ردود المشاركين كما هي مبينة بالجدول(7) ظاهرة متتالية كالآتي :

1) ظهر أن النسبة الأعلى وهي 54% موافقين أن لدى المصرف إجراءات للمصادقة على عملاء الخدمات المصرفية الإلكترونية، وأن 21% موافقين بشدة، ونسبة المحايدين بلغت 23%، 3% رافضين لذلك.

2) يتضح أن النسبة الأعلى 44% من المشاركين موافقين على أن لدى المصرف أساليب تضبط توثيق المعاملات وتمنع التنصل وتعدد المساءلة عن العمليات المصرفية الإلكترونية ، وأن 17% موافقين بشدة، في حين بلغت نسبة المحايدين39%.

جدول (7) يبين ردود المشاركين على أسئلة إدارة مخاطر العمليات الإلكترونية

ت	الإجابة (التكرار والنسبة المئوية) / السؤال	ارفض بشدة	ارفض	محايد	موافق بشدة	موافق
1	لدى المصرف إجراءات للمصادقة على عملاء الخدمات الإلكترونية.	0	1	8	19	7
		%0	%2	%23	%54	%21
2	لدى المصرف أساليب تضبط توثيق المعاملات ،وتمنع التنصل، وتحدد المساءلة، عن العمليات المصرفية الإلكترونية.	0	0	14	16	6
		%0	%0	%39	%44	%17
3	يستخدم المصرف الإجراءات المناسبة لضمان الفصل بين المهام بين التخطيط والتنفيذ والمراقبة، ضمن أنظمة وقواعد البيانات والتطبيقات للعمليات الإلكترونية.	0	1	17	14	4
		0	%3	%47	%39	%11
4	يستخدم المصرف الضوابط المناسبة الخاصة بالترخيص وامتيازات الوصول داخل أنظمة وقواعد البيانات والخدمات المصرفية الإلكترونية.	1	3	10	18	4
		%2	%8	%28	%49	%11
5	يضمن المصرف سلامة البيانات الخاصة بالمعاملات والسجلات المصرفية الإلكترونية.	0	1	10	22	3
		%0	%3	%28	%61	%8
6	يتبع المصرف إجراءات تدقيق واضحة للعمليات الإلكترونية.	0	1	12	18	4
		0%	%4	%34	%51	%11
7	يتخذ المصرف كافة الإجراءات لضمان سرية المعلومات المصرفية	0	0	10	21	5
		%0	%0	%28	%58	%14

3) يظهر أن النسبة الأعلى 47% من المشاركين محايدين، وأن ما نسبته 39% موافقين على أن المصرف يستخدم الإجراءات المناسبة لضمان الفصل بين المهام ضمن أنظمة وقواعد البيانات للعمليات الإلكترونية، وأن11% موافقين بشدة ، وحوالي 3% رافضين لذلك وهي النسبة الأقل.

4) يتبين أن النسبة الأعلى التي بلغت 49% كانت للموافقين ، على أن المصرف يستخدم الضوابط والإجراءات المناسبة الخاصة بالترخيص وامتيازات الوصول داخل انظمة وقواعد البيانات والخدمات المصرفية الإلكترونية وأن ما نسبته 11% موافقين بشدة، وبلغت نسبة المحايدين 28%، وان نسبة8% رافضين لذلك، وان 3% رافضين بشدة.

5) يتضح أن نسبة 11% من المشاركين موافقين على أن المصرف يضمن سلامة البيانات الخاصة بالمعلومات المصرفية الإلكترونية، وأن 61% موافقين بشدة، وأن نسبة المحايدين بلغت 28%، وما نسبته 3% رافضين.

6) وافق ما نسبته 51% على أن المصرف يتبع إجراءات تدقيق واضحة للعمليات الإلكترونية ، ونسبة 11% وافقوا بشدة ، بينما بلغت نسبة المحايدين 34% ، وأن 4% موافقين .

7) ظهر أن نسبة 58% موافقين على أن المصرف يتخذ كافة الإجراءات لضمان سرية المعلومات المصرفية، وأن نسبة 14% موافقين بشدة، وبلغت نسبة المحايدين حوالي 28%.

4.3.4. المحور الرابع/ مراحل تحقيق المرونة السيبرانية:

تهدف أسئلة هذا المحور إلى تقييم إجراءات وأساليب المصرف لتحقيق مستوى المرونة السيبرانية المناسب، ويبين الجدول رقم (8) إجابات المشاركين والتي يمكن ملاحظة أهم ما ورد فيها، وما تعكسه من مؤشرات فيما يلي:

1) فيما يخص مدى اتباع المصرف لاستراتيجية تتضمن توقع للمخاطر السيبرانية، فإن أغلب المشاركين يرون أن المصرف يضع استراتيجية لتوقع المخاطر السيبرانية، حيث بلغت نسبة الموافقين بشدة والموافقين 68%، 14% على التوالي، بينما كانت نسبة المحايدين 14 % ، والبقية يرون أن المصرف ليس لديه هذه الاستراتيجية.

2) زادت نسبة الموافقين على أن لدى المصرف إطار دفاعي مرن يحافظ على المهام وكافي للتصدي للتهديدات التي يتعرض لها عن 68%، بينما لم يرى ذلك ما نسبتهم نحو 14% ، والبقية كانوا محايدين. وهذا يشير إلى المشاركين وفق ما يرون أن المصرف لديه إطار للأمن السيبراني مرن، يناسب العمل التقني ويكفي لمواجهة أي مخاطر قد تعترض هذه العمليات.

جدول (8) يبين إجابات المشاركين حول مراحل تحقيق المرونة السيبرانية

ت	الإجابة (التكرار ،النسبة المئوية) / السؤال	أرفض بشدة	أرفض	محايد	موافق	موافق بشدة
1	يضع المصرف استراتيجية واضحة لتوقع مخاطر الأحداث السيبرانية ومعالجتها.	2	1	4	19	11
		%5	%3	%11	%51	%30
2	لدى المصرف إطار دفاعي مرن يحافظ على المهام وكافي للتصدي للتهديدات التي يتعرض لها.	0	2	5	25	5
		%0	%5	%14	%68	%14
3	لدى المصرف نظام دفاع الكرتوني قوي ونشط دائماً ضد الأحداث السيبرانية	1	4	7	17	7
		%3	%11	%19	%47	%19
4	يعمل المصرف على مراقبة الشبكات الإلكترونية والإنترنت للكشف عن التهديدات السيبرانية في الوقت المناسب.	0	2	7	21	7
		%0	%5	%19	%57	%19
5	يعتمد المصرف على الأتمتة والتعلم الآلي لمواجهة التهديدات السيبرانية المستقبلية.	5	3	18	6	4
		%14	%8	%50	%17	%11
6	لدى المصرف نظام التكيف واستعادة الأنظمة والمنصات الرقمية بسرعة عند وقوع أحداث سيبرانية.	1	1	17	11	7
		%3	%3	%46	%30	%19
7	يعمل المصرف على التقييم الذاتي والمستمر وقياس أداء إدارة المخاطر السيبرانية.	2	1	11	16	7
		%5	%3	%30	%43	%19

3) كذلك عند سؤال المشاركين على نظام الأمن السيبراني بصيغة أخرى، فقد أكد نحو 47% ، و19 % وفق نسب الموافقة ، على أن لدى المصرف نظام دفاع إلكتروني قوي ونشط دائماً ضد الأحداث السيبرانية، بينما ما نسبته 11% , 3% ، لم يروا ذلك ، وباقي المشاركين كانوا محايدين.

4) من خلال سؤال المشاركين على عمل المصرف على مراقبة الشبكات الإلكترونية والإنترنت للكشف عن التهديدات السيبرانية في الوقت المناسب، فقد أكد أكثر من 75% وفق إجابات الموافقين والموافقين بشدة، بينما نسبة 19 % كانوا محايدين ، ولم يرفض ذلك إلا ما نسبته 5% من إجمالي المشاركين.

5) عند محاولة معرفة أراء المشاركين في مدى اعتماد المصرف على الأتمتة والتعلم الآلي لمواجهة التهديدات السيبرانية المستقبلية، فإن نسبة 50% منهم كانوا محايدين، ونسبتي الرافضين مجتمعة نحو 28%، ولم يوافق ويوافق بشدة على ذلك إلا ما نسبته 22% .

6) لأجل تقييم المرونة السيبرانية للمصرف فقد تم سؤال المشاركين عن مدى وجود نظام بالمصرف للتكيف واستعادة الأنظمة والمنصات الرقمية بسرعة عند وقوع أحداث سيبرانية، ويبدو أن أغلب المشاركين لا يروا وجوداً لهذا النظام ، حيث كان محايداً ما نسبته 46% ونحو 48% لنسب الرفضين ، وفقط 5.4% لنسب الموافقين .

7) تضمن السؤال الأخير في هذا المحور، الاستفسار عن مدى عمل المصرف على التقييم الذاتي والمستمر وقياس أداء إدارة المخاطر السيبرانية، ورأى ما يزيد عن 62%، وفق إجابات الرافضين بأن المصرف لا يعمل على ذلك، ونسبة 28 % كانوا محايدون، ولم يوافق سوى نسبة 8%، في كلا نسبتي الموافقة.

5.3.4. المحور الخامس/ السمعة والمخاطر القانونية:

خُصص هذا المحور لمعرفة مدى التزام المصرف بالتوصيات الدولية ، فيما يخص مخاطر السمعة والمخاطر القانونية، التي قد تنشأ عن العمليات الإلكترونية، ويبين الجدول رقم (9) ما يلي :

1) يتبين أن حوالي 47% من المشاركين موافقين بشدة على أنه لدى المصرف إفصاح مناسب ومعلومات كافية للخدمات المصرفية الإلكترونية، ونسبة 14% كانوا موافقين بشدة ، بينما بلغت نسبة المحايدين حوالي 36%، ونسبة 3% رافضين.

2) يتضح أن نسبة 50% من المشاركين، كانوا موافقين أن المصرف يوفر كافة المتطلبات ويتخذ كافة الإجراءات الضامنة لخصوصية معلومات العميل، وأن 22% موافقين بشدة، بينما بلغت نسبة المحايدين 28%.

3) يظهر أن حوالي 41% موافقين على أن المصرف يضع الخطط، ويوفر الاحتياطات اللازمة لاستمرارية الأعمال، والتخطيط للطوارئ، وضمان إعادة تفعيل الأنظمة والخدمات المصرفية، كذلك وافق بشدة ما نسبته 6% ، بينما كانت نسبة المحايدين 50% ، ونسبة 3% رافضين لذلك .

4) يتبين أن حوالي 28% موافقين على أن المصرف لديه تخطيط للاستجابة للحوادث وتقليل المشاكل الناتجة عنها التي قد تعيق استمرار الخدمات الإلكترونية ،وأن 11% موافقين بشدة، بينما بلغت نسبة المحايدين 55% وهي أعلى نسبة، وأن 3% كانوا رافضين لذلك.

جدول(9) يبين إجابات المشاركين حول محور السمعة أو المخاطر القانونية

ت	الإجابة (التكرار والنسبة المئوية) / السؤال	ارفض بشدة	ارفض	محايد	موافق	موافق بشدة
1	لدى التصرف إفصاح مناسب ومعلومات كافية للخدمات المصرفية الإلكترونية.	0	1	13	17	5
		%0	%3	%36	%47	%14
2	يوفر المصرف كافة المتطلبات ويتخذ كافة الإجراءات الضامنة الخصوصية معلومات العميل.	0	0	10	18	8
		%0	%0	%28	%50	%22
3	يضع المصرف الخطط ويوفر الاحتياطات اللازمة لاستمرارية الأعمال والتخطيط للطوارئ وضمان إعادة تفعيل الأنظمة والخدمات المصرفية بالسرعة اللازمة.	0	1	18	15	2
		%0	%3	%50	%41	%6
4	لدى المصرف تخطيط للاستجابة للحوادث وتقليل المشاكل الناتجة عنها التي قد تعيق استمرار الخدمات الإلكترونية.	1	1	20	10	4
		%3	%3	%55	%28	%11

4.4. اختبار توافق ردود المشاركين على محاور الاستبانة :

بغرض اختبار مدى توافق ردود المشاركين حول محاور الاستبانة، فقد تم حساب المتوسط الحسابي والانحراف المعياري والحد لأدنى والحد الأقصى لكل محور من المحاور الأربعة كما في الجدول (4) . الذي يبين أن هناك توافق على كل محاور الاستبانة، بلغ المتوسط الحسابي لمحور محددات مجلس الإدارة والرقابة 3.49، و 3.74 لمحور إدارة مخاطر العمليات الإلكترونية، و3.69 لمحور مراحل تحقيق المرونة السيبرانية، بينما بلغ 3.64 لمحور محددات المخاطر القانونية ومخاطر السمعة . وكلها كان أكبر من 3 ، هناك توافق بين ردود المشاركين على كل محاور الاستبانة.

جدول (4) المتوسط الحسابي والانحراف المعياري لمحاور الاستبيان

المحور	عدد المشاهدات	المتوسط الحسابي	الانحراف المعياري	أقل قيمة	أكبر قيمة
إشراف مجلس الإدارة والإدارة العليا	35	3.49	0.62	1.88	4.75
إدارة المخاطر العمليات الإلكترونية	35	3.74	0.57	2.71	5.00
مراحل تحقيق المرونة السيبرانية	36	3.69	0.70	1.86	4.86
السمعة والمخاطر القانونية	36	3.65	0.53	2.75	5.00

المصدر : وفق النتائج الظاهرة من برنامج Stata.

5. اختبار فرضيات الدراسة

كما عُرض سابقاً ، فقد صيغت فرضيات الدراسة الرئيسية، إلى فرضية رئيسية في صورتيها العدم والبديلة، هناك/ أو ليس هناك التزام من المصارف التجارية الليبية بالتوصيات والمعايير الدولية بشأن إدارة المخاطر السيبرانية. حيث اختُبرت هذه الفرضية وفق الفرضيات الفرعية الممثلة لها، باستخدام اختبار T، لقبولها أو رفضها كلاً على حده. حيث كانت النتائج كما هي ظاهرة بالجدول (10) مبنية للآتي:

جدول يبين نتائج اختبار T للفرضيات الفرعية (وفق محاور الاستبانة)

المتغير	إحصائية اختبار T	درجة الحرية	الاحتمال	الانحراف المعياري	فترة الثقة
الفرضية الفرعية الأولى مراحل تحقيق المرونة السيبرانية	5.937	35	0.000	0.116	3.93- 3.45
الفرضية الفرعية الثانية إشراف مجلس الإدارة والإدارة العليا	4.716	34	0.000	0.104	3.70 – 3.28
الفرضية الفرعية الثالثة إدارة مخاطر العمليات الإلكترونية	7.751	34	0.000	0.096	3.94 – 3.55
الفرضية الفرعية الرابعة السمعة والمخاطر القانونية	7.324	35	0.000	0.088	3.82 – 3.47

إعداد الباحثين وفق للنتائج الإحصائية لكل متغير (محدد) .

1.5. الفرضية الفرعية الأولى :

درجة الحرية (N-1) هي 35، وأن قيمة T= 5.9373، وبما أن قيمة T المحسوبة أكبر من 3، فإننا نرفض فرض العدم، أي أن لدى المصارف التجارية الليبية، خطة لتنفيذ مراحل تحقيق المرونة السيبرانية.

2.5. الفرضية الفرعية الثانية :

درجة الحرية (N-1) هي 34، وأن قيمة T = 4.7166، وبما أن قيمة T المحسوبة أكبر من 3، فإننا نرفض فرض العدم، أي أن السلطات العليا للمصارف التجارية الليبية، تلتزم بالتوصيات والمعايير الدولية الخاصة بالتوجيه والرقابة على المخاطر السيبرانية.

3.5. الفرضية الفرعية الثالثة :

درجة الحرية (N-1) هي 34 ، وأن قيمة T= 7.7510، وبما أن قيمة T المحسوبة أكبر من3، فإننا نرفض فرض العدم، أي أن هناك نظام واضح لإدارة مخاطر العمليات الإلكترونية، وفق بالتوصيات والمعايير الدولية.

4.5. الفرضية الفرعية الرابعة :

درجة الحرية (N-1) هي 35 ، وان قيمة T = 7.324 2 وبما أن قيمة T اكبر من 3 فإننا نرفض الفرض العدم، إي انه توجد مؤشرات على متابعة المخاطر القانونية ومخاطر السمعة وفق التوصيات والمعايير الدولية.

ومن خلال قبول الفرض البديل في الفرضيات الفرعية الأربعة، فإننا نقبل الفرض الرئيسي لهذه الدراسة، وهو أن هناك التزام من المصارف التجارية الليبية بالتوصيات والمعايير الدولية ،بشأن إدارة المخاطر السيبرانية.

ورغم ذلك فإن ملاحظة الباحثين، لعدم توافق هذه النتيجة مع واقع الحال في بعض الحالات، إلا أن ذلك قد يشير إلى أن ذلك يخضع لروى المشاركين، التي قد لا تكون دقيقة بالصورة الكافية، حال أن هناك قصور في إدراك بعضهم لمضامين الأسئلة بصورة كاملة، أو في معرفتهم بما نعنيه من المعايير والتوصيات الدولية، والذي يعتقد الباحثين أنه احتمال قائم، ويحتاج إلى التحقق منه بصورة أوسع في دراسات لاحقة.

6. الخاتمة

اعتمدت الدراسة على عرض لرؤى المنظمات والهيئات الدولية المختصة، بداية من نظرتها إلى ماهية وإدارة المخاطر السيبرانية، ثم بما توصي به من معايير، وما تتبعه من نماذج في هذه الإدارة. كذلك المبادئ التي وضعتها هذه الهيئات كركائز يمكن أن تمثل إطاراً لإدارة المخاطر السيبرانية. ثم عُرضت مؤشرات عن واقع إدارة المخاطر السيبرانية في المصارف الليبية، وفق تقارير محلية ودولية، وأُجري استطلاع لآراء بعض المسؤولين والمختصين بالمصرف التجاري الوطني بمدينة البيضاء بوصفه عينة الدراسة، حول واقع إدارة المخاطر السيبرانية بالمصرف ومدى التزامه بالمعايير والتوصيات الدولية . وقد كانت أهم النتائج التي توصلت إليها الدراسة ما يلي:

أولاً / نتائج خاصة برؤى الأدبيات والمنظمات الدولية للمخاطر السيبرانية في المصارف الليبية:

1) تُجمع الدراسات وتقارير المنظمات الدولية، على تنامي المخاطر السيبرانية المصرفية، وتطورها وتغير مصادرها وأوقات حدوثها، وبالتالي، توصي بتحديث إدارة هذه المخاطر وسبل مواجهتها، حسب تغيرات هذه المخاطر.

2) ليس هناك اتفاق دولي على أنظمة أو نماذج موحدة لإدارة المخاطر السيبرانية المصرفية، غير أن هناك ركائز أساسية متشابهة ، تتمثل في تحديد وتحليل ومراجعة المخاطر السيبرانية، وفق المعايير والتوصيات الدولية، لإدارة هذه المخاطر ،وسبل مراقبتها، والإشراف عليها.

ثانياً/ نتائج خاصة بمؤشرات محلية ودولية عن واقع إدارة المخاطر السيبرانية في المصارف الليبية:

1) ترى الجهات الرقابية في ليبيا ممثلة في ديوان المحاسبة الليبي، من خلال ما ظهر من تقاريره السنوية، أن هناك قصور في الالتزام بمعايير حوكمة المخاطر بالمصارف الليبية، ومخالفة مجالس إداراته، لأحكام دليل الحوكمة الصادر عن مصرف ليبيا المركزي، الذي اكتفى بإصداره ولم يلتزم هو كذلك بما جاء فيه.

2) أظهر تقرير صندوق النقد العربي(2024)، عدم وجود قياس لتطور الأمن السيبراني على مستوى مصرف ليبيا المركزي.

3) يشير تقرير البنك الدولي (2020) إلى ارتفاع المخاطر التشغيلية في المصارف الليبية، بسبب ضعف هيكل المعلومات وإدارة المخاطر بجميع أنواعها، وأن هناك نقص في القدرات الرقمية، سواء لدى المصارف التجارية أو مصرف ليبيا المركزي.

ثالثاً / نتائج خاصة بملاحظات الباحثين، ورؤية المسؤولين والمختصين، حول مدى التزام المصرف التجاري الوطني بالمعايير الدولية :

1) لاحظ الباحثين عدم الالتزام ببعض التوصيات الدولية من قبل المصرف التجاري الوطني، مثل تكوين لجان أو مكاتب مختصة بحوكمة وإدارة المخاطر السيبرانية، أو وجود خطط واضحة ومعلنة للتعامل مع هذه المخاطر وكيفية مواجهتها، أو إطار حماية محدد الإجراءات والأدوات، أو إعداد تقارير دورية وتفصيلية، حول تطورها واحتمالات حدوثها. مع ملاحظة أن مكتب أمن المعلومات بالمصرف التجاري الوطني، هو الوحيد المختص والمتابع بشكل مباشر للمخاطر السيبرانية، وأن لديه عناصر فنية مدركة لأبعاد المخاطر السيبرانية، وتبذل جهوداً ملاحظة في الاستعداد لها، وتوعية الموظفين والإدارة العليا بهذه المخاطر، من خلال تعميم مناشير توعوية حول هذه المخاطر معدة من المكتب.

2) بين تحليل رؤى المشاركين المسؤولين والمختصين بالمصرف التجاري الوطني، أن هناك التزام من المصرف، بالمعايير والتوصيات الدولية. رغم ملاحظة الباحثين من خلال مقابلة البعض منهم، بان هناك قصور في معرفتهم بشكل مفصل للمعايير والتوصيات الدولية حول المخاطر السيبرانية، مما جعل الباحثين لا يثقون بصورة كاملة بالردود الواردة على كل الأسئلة.

ووفق ما توصلت إليه الدراسة من مؤشرات ونتائج، وملاحظه الباحثين أثناء إعداد الدراسة، فإننا نورد بعض **التوصيات فيما يلي:**

1) على الجهات الإشرافية والرقابية على المصارف، بما فيها الداخلية ومصرف ليبيا المركزي والإدارات العليا، الاهتمام بالتوعية بالمخاطر السيبرانية، ورسم الخطط الواضحة لمواجهتها، وفق ما ورد من توصيات ومعايير محلية، والالتزام بدليل التكنولوجيا ودليل حوكمة المصارف الواردة عن مصرف ليبيا المركزي، وبوما يتوافق مع المعايير والتوصيات الدولية.

2) يفترض أن يكون اهتمام المصارف بالمعايير والتوصيات بشأن إدارة المخاطر السيبرانية، واضحاً من خلال تبني المعايير والتوصيات المحلية والدولية، ووضع إطار للأمن السيبراني، وخطة وإجراءات معلنة لإدارة المخاطر السيبرانية، وتشكيل لجان خاصة بمراقبة تنفيذها واعتبارها من المخاطر التشغيلية، واعتبار متابعتها جزءاً رئيسياً، من مسؤوليات الإدارات المختصة بالرقابة والإشراف، مثل مكاتب الامتثال.

3) على المصرف المركزي والمصارف الليبية توظيف وتأهيل العناصر ذات المهارة والمعرفة والقدرة، الفنية والإدارية بالمخاطر السيبرانية، والتخفيف قدر المستطاع من خدمات الطرف الثالث " الأطراف الخارجية"، أو موردي الأنظمة والبرامج التقنية.

3) ترى الدراسة أن هناك مجالاً كبيراً لإعداد دراسات لاحقة تتبني موضوع إدارة المخاطر السيبرانية، خاصة من خلال تقييم الرقابة الإشرافية والتنظيمية عليها، أو تقييم الحوكمة السيبرانية في المصارف الليبية، بهدف المساهمة في التنبيه إليها، ودعم الوعي المصرفي بشأنها للمصارف والعملاء.

قائمة المراجع

إسماعيل ، محمد (2019)، " الأمن السيبراني في القطاع المصرفي" ، صندوق النقد العربي ، موجز سياسات : العدد الرابع، أبو ظبي- الإمارات العربية المتحدة .

الحولي، شادي سلامة. (2015). إدارة مخاطر العمليات المصرفية الإلكترونية وفق مقررات لجنة بازل : دراسة تطبيقية على البنوك المحلية العاملة في فلسطين. (أطروحة ماجستير). الجامعة الإسلامية، فلسطين (قطاع غزة).

البنك الدولي (2020) ،" مراجعة القطاع المالي في ليبيا".

الهاشمي، سلطاني و صادق، صفيح " إدارة مخاطر الخدمات المصرفية الإلكترونية في المصارف الإسلامية: دراسة حالة مصرف الراجحي السعودي"، مجلة الاقتصاد و التنمية البشرية، 13 (1) 91-104.

ديوان المحاسبة الليبي ، التقرير السنوي العام 2022.

ديوان المحاسبة الليبي ، التقرير السنوي العام 2020.

سمرة، ياسر وأخرون (2022) " تأثير إدارة المخاطر الإلكترونية في ضوء مقررات لجنة بازل بالبنوك ، مجلة البحوث والدراسات البيئية، معهد الدراسات والبحوث البيئية - جامعة مدينة السادات، مصر.

صندوق النقد الدولي (2019) ، " أجندة مؤتمر بالي للتكنولوجيا المالية ــ وثيقة مبدئية".

فرج، محمد أبو خزام و معيتيق، سمية سالم (2024)،" تقييم مخاطر العمليات المصرفية الإلكترونية بالمصارف الليبية في ضوء مقررات بازل (دراسة ميدانية على عينة من أفرع المصارف الليبية العاملة بمدينة سرت)، مجل جامعة سرت للعلوم الإنسانية، العدد 14 ، المجلد 1 ، سرت .

معاد، سهى (2022) " المرونة السيبرانية وفق بازل" مجلة اتحاد المصارف العربية، عدد 494، لبنان. 48-51.

المراجع الأجنبية:

Al-Ajmi, Aysha Saud(2021)," A Study on Risk Management Practices in Online Banking in Bahrain", Conference paper: Advanced Machine Learning Technologies and Applications, AISC,volume 1141,pp.589-598.

Abdou, Hussein et al.(2015)," E-banking and risk management: Evidence from the Cypriot public sector banks", Banks and Bank Systems, 10(3), 17-27.

Abdou, Hussein et al.(2014) ," An investigation of risk management practices in electronic banking: the case of the UK banks ", , Banks and Bank Systems, 9 (3).

Al-Ajmi, Aysha Saud(2021)," A Study on Risk Management Practices in Online Banking in Bahrain", Conference paper: Advanced Machine Learning Technologies and Applications, AISC,volume 1141, 589-598.

Abdou, Hussein et al.(2015)," A E-banking and risk management: Evidence from the Cypriot public sector banks", Banks and Bank Systems, 10(3),17-27.

Abdou, Hussein et al.(2014) ," An investigation of risk management practices in electronic banking: the case of the UK banks ", , Banks and Bank Systems, 9 (3).

- Basel Committee on Banking Supervision(2018), "Cyber-resilience Range of practices"., Bank for International Settlements.
- Basel Committee on Banking Supervision (2021)," Principles for Operational Resilience"., Bank for International Settlements.
Basel Committee on Banking Supervision (2001),"Risk Management Principles for Electronic Banking", Bank for International Settlements.
Basel Committee on Banking Supervision (2003),"Risk Management Principles for Electronic Banking", Bank for International Settlements.
Basel Committee on Banking Supervision (2021)," Revisions to the Principles for the Sound Management of Operational Risk"., Bank for International Settlements.
Basel Committee on Banking Supervision (2018),"Sound Practices :Implications of fintech developments for banks and bank supervisors"., Bank for International Settlements.
Basel Committee on Banking Supervision (1998)"Risk Management for lectronic
Banking and Electronic Money Activities"., Bank for International Settlements.
Basel Committee on Banking Supervision (2011)" Principles for the Sound Management of Operational Risk"., Bank for International Settlements.
Basel Committee on Banking Supervision (2023)"Basel III Monitoring Report".,Bank for International Settlements.
Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions,(2016)" Guidance on cyber resilience for financial market infrastructures OICU-IOSCO ", Bank of International Settlements(BIS).
Crisanto, Juan Carlos and Prenio, Jermy (2017) "Insights on policy implementation No 2 : Regulatory approaches to enhance banks' cyber-security frameworks", Financial Stability Institute FSI,BIS, 3-14.
CrowdStrike(2024)," Global Threats Report ", 52-53.
Dawodu et al.(2023), Cyber Security Risk Assessment in Banking : Methodologies and Best Practices", Computer Science & IT Research Journal 4(3):220-243
European Central Bank –ECB-,(2016) "G-7 Fundamental elements for effective assessment of Cybersecurity in the financial sector .
European Banking Authority -EBA(2016)," Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)", Consultation Paper, pp25-26.
Ernst & Young(EY) , Institute of International Finance-IIF(2024)," Managing through persistent volatility: the evolving role of the CRO and the need for organizational agility",13th annual EY/IIF global bank risk management survey, 8-12.
Financial Stability Board," Cyber Lexicon :Updated in 2023".
- Governance Institute of Australia(2024)," Effective Cyber Risk Management: A best practice governance guide: A best practice governance guide for digitally secure and resilient organisations".
Global Future of Cyber Survey:",(2023)Deloitte Development LLC
Building long-term value by putting cyber at the heart of the business",12-13.
IBM' Home ,(2024), " What is cyber risk management".
International Monetary Fund (2024) Global Financial Stability Report , Chapter 3:" Cyber Risk: A Growing Concern for Macro financial Stability".
International Monetary Fund (2024)." Global Financial Stability Report : Steadying the Course: Uncertainty, Artificial Intelligence, and Financial Stability".
International Monetary Fund-IMF(2024) Cyber Risk: a Growing concern for macrofinancial stability", Global Financial Stability Report, Chapter (3).

Jennifer Elliott, Nigel Jenkinson(2020)," Cyber Risk is the New Threat to Financial Stability", IMF BLOG.
Jing Chen et al.(2023) ,"Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach"., Journal of Business Ethics , 187.pp.199–224.
Kumar(2024)," Cyber Risk Management In Indian Banking Sector", Educational Administration: Theory and Practice, 30(4), pp.477–486
Mohammed, Abdul-Hussein Jasim et al.,(2021) " Impact of Banking Risks on the Electronic Banking Services: A Comparative Study" , TEM Journal, 10(2) ,663-672.
Monetary Authority of Singapore-MAS(2021)," Technology Risk Management Guidelines".
Nye, Andrew (2024) ," CBEST Threat Intelligence-Led Assessments: Implementation Guide for CBEST participants", Bank of England
Sentinel One, Inc(2024)," Cyber Security Risk Assessment: Step-by-Step Process" sentinel One, Inc' blog.9/9/2024.
Stanoevska, Elena Parnardzieva(2021)," KNOWLEDGE –International Journal 44(1)
Sudhakar , Sathiyamurthy (2019) , "Bulletproof Risk Management to Thrive in the Digital Economy", ISACA Journal,V3,1 May 2019.
Sunil Kumar(2024)," Cyber Risk Management In Indian Banking Sector", Educational Administration: Theory and Practice, 30(4),477–486
Toronto Center(2018)، "Supervision of Cyber Risk".
World Bank Group: Financial Sector Advisory Center -Fin SAC, (2019,2020) "Financial Sector's Cybersecurity: A Regulatory Digest".