

Received	2026/01/05	تم استلام الورقة العلمية في
Accepted	2026/01/25	تم قبول الورقة العلمية في
Published	2026/01/26	تم نشر الورقة العلمية في

تقييم قدرة المصارف التجارية الليبية على مواجهة التهديدات السيبرانية

في ظل التحول الرقمي

دراسة تطبيقية باستخدام نمذجة المعادلات البنائية

عبد السلام خليفة جبر

عادل العكرمي الاسود

المعهد العالي للعلوم والتقنية سلوك

كلية الاقتصاد العجيلات - جامعة الزاوية

ليبيا

ليبيا

AbdulsalamAswisi@hicps.edu.ly

a.adela.alaswad@zu.edu.ly

عبد السلام بوعجيلة السنوسي

المعهد العالي للعلوم والتقنية سلوك - ليبيا

AbdulsalamAl-Mashaiti@hicps.edu.ly

الملخص

هدفت هذه الدراسة إلى تقييم قدرة المصارف التجارية الليبية على مواجهة للتهديدات السيبرانية في ظل التحول الرقمي المتسارع، وذلك من خلال تحليل الأثر النسبي لمجموعة من المحددات الرئيسية، تمثلت في مستوى تبني التقنيات الرقمية داخل المصارف، وجاهزية الموارد البشرية المتخصصة في مجال الأمن السيبراني، وكفاءة البنية التحتية التكنولوجية، فضلاً عن الإطار التشريعي والسياسات الحكومية ذات الصلة، حيث جرى التعبير عن المتغير التابع بقدرة المصارف التجارية الليبية على مواجهة المخاطر السيبرانية. واعتمدت الدراسة المنهج الوصفي التحليلي، وطُبِّقَت على عينة من المصارف التجارية الليبية، بلغ حجمها (157) مفردة صالحة للتحليل الإحصائي. ولغرض اختبار العلاقات السببية بين متغيرات الدراسة والتحقق من الفروض المطروحة، تم توظيف أسلوب نمذجة المعادلات البنائية باستخدام البرنامج الإحصائي Smart PLS3 وأفضت نتائج التحليل إلى وجود أثر ذي دلالة إحصائية عند مستوى معنوية (0.05) لكل من مستوى تبني التكنولوجيا الرقمية وجاهزية الكوادر البشرية المتخصصة وكذلك التشريعات والسياسات الحكومية. على قدرة المصارف التجارية الليبية في مواجهة المخاطر السيبرانية، في حين كشفت

النتائج عن عدم وجود أثر ذي دلالة إحصائية لكل من كفاءة البنية التحتية التكنولوجية وفي ضوء هذه النتائج، أوصت الدراسة بضرورة إعطاء أولوية استراتيجية لتنمية وتأهيل الكفاءات البشرية المتخصصة في مجال الأمن السيبراني داخل المصارف التجارية الليبية، بالتوازي مع تعزيز مسارات التحول الرقمي المدعومة بإجراءات أمن سيبراني عالية الكفاءة، بما يكفل ترسيخ ممارسات أمنية فعالة، ومواكبة التطورات التكنولوجية المتسارعة، وتحقيق الاستغلال الأمثل للبنية التحتية التكنولوجية في إدارة المخاطر السيبرانية بكفاءة وفعالية. **الكلمات المفتاحية:** التهديدات السيبرانية-التكنولوجيا الرقمية-الكوادر البشرية في مجال الأمن السيبراني-كفاءة البنية التحتية التكنولوجية-المخاطر السيبرانية.

Assessing the Capacity of Libyan Commercial Banks to Confront Cyber Threats in the Context of Digital Transformation: An Applied Study Using Structural Equation Modeling

ADEL AB ALASWAD

Faculty of Economics - Al –
Ajailat- University of Zawia -
Libya

a.adela.alaswad@zu.edu.ly

ABDELSALAM K. GABER

Higher Institute of Science and
Technology – Suluq
Libya

AbdulsalamAswisi@hicps.edu.ly

Abdulsalam AB-Al-Mashaiti

Higher Institute of Science and Technology – Suluq - Libya

AbdulsalamAl-Mashaiti@hicps.edu.ly

Abstract

This study aimed to assess the ability of Libyan commercial banks to confront cyber threats in the context of rapid digital transformation by analyzing the relative impact of a set of key determinants. These determinants included the level of adoption of digital technologies within banks, the readiness of specialized human resources in the field of cybersecurity, the efficiency of technological infrastructure, as well as the relevant legislative framework and government policies. The dependent variable was represented by the ability of Libyan commercial banks to manage and mitigate cyber risks.

The study adopted a descriptive–analytical approach and was applied to a sample of Libyan commercial banks, comprising 157 valid observations suitable for statistical analysis. To test the causal relationships among the study variables and verify the proposed hypotheses, Structural Equation Modeling (SEM) was employed using the SmartPLS3 statistical software.

The results revealed statistically significant effects at the 0.05 significance level for the level of digital technology adoption, the readiness of specialized human resources, and legislative and governmental policies on the ability of Libyan commercial banks to confront cyber risks. In contrast, the findings indicated no statistically significant effect of technological infrastructure efficiency.

In light of these results, the study recommends giving strategic priority to the development and qualification of specialized human competencies in cybersecurity within Libyan commercial banks, alongside strengthening digital transformation pathways supported by highly efficient cybersecurity measures. This would ensure the establishment of effective security practices, keep pace with rapid technological developments, and achieve optimal utilization of technological infrastructure in managing cyber risks efficiently and effectively.

Keywords: Cyber threats; Digital technology; Cybersecurity human resources; Technological infrastructure efficiency; Cyber risks.

1. المقدمة

شهد القطاع المصرفي العالمي خلال العقدین الأخيرین تحولاً جذرياً بفعل التقدم المتسارع في تكنولوجيا المعلومات والاتصالات، حيث تبنت المصارف على نطاق واسع تطبيقات التحول الرقمي مثل الحوسبة السحابية، والذكاء الاصطناعي، وإنترنت الأشياء، وسلاسل الكتل (Block- chain)، بهدف تحسين كفاءة العمليات، وتطوير جودة الخدمات، وتعزيز الشمول المالي. وقد أسهم هذا التحول في إعادة تشكيل نماذج الأعمال المصرفية، وتقليل التكاليف التشغيلية، وزيادة سرعة ودقة إنجاز المعاملات المالية (Bank for international settlements, 2018) ورغم ما يوفره التحول الرقمي من فرص استراتيجية للقطاع المصرفي، إلا أنه في المقابل أفرز مجموعة متزايدة

من المخاطر غير التقليدية، وفي مقدمتها المخاطر السيبرانية، التي أصبحت تمثل أحد أخطر التهديدات التي تواجه استقرار المؤسسات المالية عالمياً. وتتمثل هذه المخاطر في الهجمات الإلكترونية، واختراق الأنظمة، وسرقة البيانات، والاحتيال الرقمي، وتعطيل الخدمات المصرفية، وهي مخاطر تتفاقم مع تزايد الاعتماد على القنوات الرقمية في تقديم الخدمات المصرفية (Bouveret, 2018; Von Solms & Van Niekerk, 2013) وتُعد المصارف التجارية من أكثر القطاعات استهدافاً من قبل مجرمي الإنترنت، نظراً لما تمتلكه من بيانات مالية حساسة وأصول رقمية عالية القيمة، الأمر الذي يجعل أي خلل في منظومة الأمن السيبراني سبباً محتملاً لخسائر مالية جسيمة، وتراجع ثقة العملاء، وتهديد الاستقرار المالي والاقتصادي. وقد أكدت تقارير صندوق النقد الدولي وبنك التسويات الدولية أن الهجمات السيبرانية على المؤسسات المالية تشهد تصاعداً ملحوظاً من حيث الحجم والتعقيد، وأن ضعف الجاهزية التقنية والبشرية يزيد من حدة هذه المخاطر (Bank for international settlements, 2018) في ليبيا، وعلى الرغم من الاتجاه المتنامي نحو رقمنة الخدمات المصرفية، خاصة بعد جائحة كوفيد-19 التي عززت الاعتماد على القنوات الإلكترونية، إلا أن موضوع الأمن السيبراني لم يحظَ بالاهتمام الكافي من حيث البحث والتطبيق، مقارنة بسرعة التوسع في استخدام التكنولوجيا المصرفية. كما تعاني المصارف التجارية الليبية من تحديات متعددة، تشمل محدودية الكوادر المتخصصة في الأمن السيبراني، وضعف البنية التحتية التكنولوجية، وغياب الأطر التشريعية والتنظيمية الواضحة، مما يزيد من تعرضها للتهديدات السيبرانية (Oyewole et, 2024) وانطلاقاً من ذلك، تبرز الحاجة إلى دراسة علمية تحليلية تُقيّم مدى قدرة المصارف التجارية الليبية على مواجهة المخاطر السيبرانية في ظل التحول الرقمي، وتبحث في العوامل المؤثرة في هذه القدرة، سواء التقنية أو البشرية أو التنظيمية، بما يساهم في سد فجوة معرفية واضحة في الأدبيات العربية والليبية وتقديم توصيات عملية تعزز من صمود القطاع المصرفي الليبي أمام التهديدات السيبرانية المتزايدة.

2. الدراسات السابقة

نظراً للتطورات المتسارعة في تكنولوجيا المعلومات والاتصالات، وما ترتب عليها من تحول رقمي واسع في القطاع المصرفي، برز الأمن السيبراني كأحد أهم التحديات التي تواجه المؤسسات المالية على مستوى العالم. وقد أولت العديد من الدراسات اهتماماً خاصاً لموضوع المخاطر السيبرانية في البيئة المصرفية، سواء من حيث التعريف بطبيعتها، أو تحليل مصادرها، أو تقييم جاهزية المؤسسات لمواجهتها. وبرز هذا الاهتمام بشكل متزايد مع تزايد وتيرة الهجمات الإلكترونية وتعقيدها، وتوسع المصارف في تقديم خدماتها عبر القنوات الرقمية. وتتوزع الدراسات السابقة في هذا المجال بين دراسات ركزت على الجانب التقني للأمن السيبراني، وأخرى تناولت البعد الإداري والتنظيمي، مثل السياسات والإجراءات، إلى جانب دراسات تناولت دور التشريعات والبنية التحتية المعلوماتية في تعزيز الحماية السيبرانية. كما أن هناك عدداً من الأبحاث التي سلطت الضوء على مدى جاهزية الكوادر البشرية، والتحديات التي تواجه المصارف في توظيف وتأهيل مختصين في أمن المعلومات. وعلى الرغم من هذا الزخم في البحوث على المستوى الدولي والعربي، إلا أن الدراسات التي تناولت موضوع الأمن السيبراني في القطاع المصرفي الليبي تحديداً لا تزال محدودة، خصوصاً من منظور تقييم مدى قدرة المصارف التجارية الليبية على مواجهة هذه المخاطر في ظل بيئة رقمية متغيرة وسياق محلي يتسم بتحديات متعددة على المستويات التقنية والبشرية والتنظيمية. لذلك، تسعى هذه الدراسة إلى سد هذه الفجوة من خلال مراجعة أبرز الدراسات ذات العلاقة، وتحليل نتائجها واستخلاص أوجه التشابه والاختلاف، بما يعزز الإطار النظري للدراسة ويبرز إسهامها العلمي ضمن الحقل المعرفي المتخصص.

1-دراسة (bank for international settlements, 2018) هدفت الدراسة التي أعدها بنك التسويات الدولية إلى استعراض الممارسات المعتمدة لدى المصارف "Cyberresilience: Range of practices" حول العالم لتعزيز قدرتها على مقاومة التهديدات السيبرانية. حيث ركزت الدراسة على تحليل الأدوات التنظيمية والتقنية المستخدمة في حماية الأنظمة المصرفية من الهجمات الإلكترونية، وذلك من خلال مراجعة تقارير البنوك المركزية والقيام بمقابلات مع عدد من مسؤولي المؤسسات المصرفية الكبرى. وتوصلت النتائج إلى وجود تباين ملحوظ في استعداد المصارف

لمواجهة التهديدات الإلكترونية، وبيّنت أن الدول ذات الأطر التنظيمية الواضحة تحقق نتائج أفضل في هذا المجال. وق أوصت الدراسة بضرورة وضع أطر موحدة على المستوى الدولي لتعزيز الاستجابة الجماعية للهجمات السيبرانية. إلا أن الفجوة بينها وبين الدراسة الحالية تتمثل في أن هذه الدراسة لم تتناول السياق الليبي ولا التحديات المرتبطة بالبنية التحتية الضعيفة والتشريعات الناقصة في بيئات مضطربة مثل ليبيا، مما يجعل من الدراسة الليبية مساهمة مهمة في ملء هذا الفراغ ضمن الأدبيات المتعلقة بالأمن السيبراني في القطاع المصرفي.

2-دراسة (PwC, 2022) يهدف تقرير "Global Digital Trust Insights" الصادر عن مؤسسة PwC (Price water house Coopers) العالمية الى استكشاف مدى جاهزية المؤسسات المالية والشركات الكبرى للتصدي للتهديدات السيبرانية المتزايدة على الصعيد الدولي. شمل التقرير استطلاع رأي أكثر من 3,602 من التنفيذيين في مجالي الأعمال وتكنولوجيا المعلومات، بمن فيهم مشاركون من مختلف أنحاء الشرق الأوسط، حيث سلط الضوء على المشهد السيبراني الحالي والتحديات والفرص التي تواجهها المؤسسات لتبسيط وتحسين أمنها السيبراني في المستقبل . وبين التقرير انه لا تزال الاستثمارات تتدفق في مجال الأمن السيبراني؛ حيث توقّعت 58 % من المؤسسات في الشرق الأوسط زيادة في الإنفاق السيبراني خلال عام 2022، مقارنة بـ 43% في العام السابق له. كما توقّع أكثر من الثلث (31%) زيادات في الإنفاق السيبراني بنسبة 10% أو أكثر، في حين لم تتجاوز هذه النسبة 10% في العام الماضي. وتُدرّك المؤسسات أن المخاطر آخذة في التزايد، إذ يتوقع أكثر من 43% منها ارتفاعاً في الحوادث القابلة للتبليغ عنها خلال العام المقبل مقارنة بعام 2021 . وقد تبيّن أن عام 2021 يُعد من بين الأسوأ على الإطلاق في مجال الأمن السيبراني؛ إذ أصبح المهاجمون أكثر تطوراً، يستغلون الزوايا المظلمة في الانظمة والشبكات بحثاً عن الثغرات ويجدونها. وخلص التقرير إلى إن العديد من الانتهاكات التي نراها لا تزال قابلة للوقاية من خلال ممارسات سيبرانية سليمة وضوابط أمنية قوية.

3-دراسة (Oyewole, Okoye, Ofodile, & Ugochukwu, 2024) من خلال منهجية تجمع بين مراجعة الأدبيات وتحليل الحوادث السيبرانية الحديثة، تتناول هذه

الدراسة تعقيدات التهديدات السيبرانية، والتداعيات المالية للاختراقات، ومدى قوة التدابير الأمنية المتبعة حالياً في القطاع المصرفي. وتشمل نطاق الدراسة فحصاً شاملاً للحوادث السيبرانية الأخيرة، وتقيماً للأثر المالي للهجمات السيبرانية، وتحليلاً لمدى فعالية أطر الأمن السيبراني الحالية، وصياغة توصيات استراتيجية لتعزيز التدابير الوقائية. ومن خلال هذا البحث الأكاديمي، تبرز نتائج رئيسية تؤكد الحاجة الملحة لاعتماد استراتيجيات أمن سيبراني ديناميكية تدمج بين التقنيات المتقدمة، والامتثال التنظيمي، وتعزيز ثقافة الوعي السيبراني. وخلصت الدراسة إلى ضرورة أن يتبنى القطاع المصرفي نهجاً شاملاً وتكيفياً في التعامل مع الأمن السيبراني، مدعوماً باستثمارات استراتيجية في التكنولوجيا والتعليم والتعاون المؤسسي. وتوصي الورقة بدمج تحليلات البيانات الضخمة، والذكاء الاصطناعي، ومنهجيات التقييم المستمر للمخاطر، لمواجهة مشهد التهديدات السيبرانية المتغير بفعالية. وتُعد هذه الورقة بمثابة دعوة جادة للمؤسسات المصرفية لإعادة تأكيد التزامها ببناء مرونة سيبرانية تحمي الأصول المالية وثقة العملاء في ظل التحول الرقمي المتسارع.

4-دراسة (عامر العتوم, 2019) هدفت الدراسة الى فهم طبيعة الخدمات المصرفية الرقمية وتناولت اهم مزاياها والمخاطر المترتبة عليها في المصارف الاسلامية محل الدراسة وبيان الطرق المتاحة لإدارتها وأشارت الدراسة الى ان الخدمات المصرفية الرقمية تتضمن مزايا عديدة يرافقها مخاطر عديدة ايضا. كما تناولت الدراسة دور الهيئات الرقابية في ادارة المخاطر الالكترونية في المصارف الاسلامية وتوصلت الى ان المخاطر الالكترونية لها تأثير قوي على اداء المصرف الاسلامي وان دور الهيئات الرقابية هام جدا في ادارة هذه المخاطر والتقليل من اثارها السلبية على اداء المصارف الاسلامية.

5-دراسة (Kolesova & Girzheva, 2018) هدفت هذه الدراسة إلى التعرف على تأثير التقنيات المالية الحديثة على القطاع المصرفي. استخدم الباحثان المنهج الوصفي التحليلي من خلال دراسة الوثائق الروسية والأجنبية واستعراض آراء الخبراء المرموقين لتحديد المخاطر المصاحبة لاستخدام التقنيات المالية في البنوك. وأكدت الدراسة أن التقنيات المالية تتطور بسرعة كبيرة، مما يستلزم من المشاركين في السوق التكيف معها. كما أبرزت الدراسة أن التعرف على المخاطر المرتبطة بهذه التقنيات أصبح قضية ملحة

للقطاع المصرفي والاقتصاد ككل، حيث أن الفشل في إدارتها قد يؤدي إلى آثار سلبية على أداء البنوك واستقرار النظام المالي.

6- دراسة (Shulha, Yanenkova, Kuzub, Muda, & Nazarenko, 2022) أجرى الباحثون دراسة بعنوان "نمذجة نظام الأمن السيبراني لموارد المعلومات البنكية"، هدفت إلى تطوير نماذج معرفية غامضة (Fuzzy Cognitive Maps) لتقييم مستوى الحماية الأمنية في المؤسسات المصرفية في ظل تزايد التهديدات السيبرانية. استخدمت الدراسة أسلوب النمذجة المعرفية الغامضة كأداة تحليلية لقياس تأثير التهديدات السيبرانية مثل الهجمات الشبكية، البرمجيات الخبيثة، أخطاء المستخدمين، التأثيرات الفيزيائية، وهجمات حجب الخدمة (DOS) على البنية التحتية للمصارف، وذلك من خلال تطوير نموذج معرفي باستخدام برنامج Mental Modeler. توصلت نتائج الدراسة إلى أن أكثر العوامل تأثيراً على أمن الشبكات البنكية تمثلت في البرمجيات الخبيثة، والأخطاء غير المقصودة من قبل المستخدمين، والتأثيرات الفيزيائية على البنية التحتية. كما بينت النماذج أن اتخاذ تدابير أمنية مناسبة يمكن أن يؤدي إلى رفع مستوى أمن الشبكة بنسبة تصل إلى 65%. وركزت الدراسة كذلك على أهمية الجمع بين الابتكار المفتوح (Open Innovation) وتطوير نظم أمنية متقدمة في مواجهة التهديدات المعاصرة. وفيما يلي جدول رقم (1) الذي يحوي ملخص شامل لكل الدراسات.

جدول 1 ملخص الدراسات السابقة

المؤلف والسنة	المنهجية	المتغيرات	النتائج	الفجوة
Bank for International Settlements (2018)	منهج وصفي تحليلي، ومقابلات مع مسؤولي بنوك مركزية.	النظم، الأدوات التقنية، الجاهزية السيبرانية.	تباين الجاهزية وارتفاع الفاعلية تنظيمياً	لم تتناول الدراسة البيئة الليبي أو البيئات المصرفية ذات البنية التحتية الضعيفة.
PwC (2022)	منهج وصفي مسحي (استبيان دولي).	الإنفاق السيبراني، الجاهزية المؤسسية، الحوادث السيبرانية.	تزايد الاستثمارات السيبرانية مع تصاعد المخاطر السيبرانية.	دراسة عامة غير مصرفية بحثية، ولم تختبر علاقات سببية.

Oyewole et al. (2024)	مراجعة أدبيات وتحليل حوادث سيبرانية	المخاطر السيبرانية، الأثر المالي، التدابير الوقائية	الحاجة لاستراتيجيات سيبرانية تكاملية	لم تطبق نموذجًا إحصائيًا ولم تركز على مصارف دولة نامية بعينها.
عامر العتوم وآخرون (2019)	منهج وصفي تحليلي	الخدمات المصرفية الرقمية، المخاطر الإلكترونية، الدور الرقابي	المخاطر الإلكترونية تؤثر سلبيًا على أداء المصارف الإسلامية ودور الرقابة جوهرية	اقتصرت على المصارف الإسلامية ولم تتناول التحول الرقمي والأمن السيبراني بشكل تكاملي
Kolesova & Girzheva (2018)	منهج وصفي تحليلي، تحليل وثائق وآراء خبراء.	التقنيات المالية، المخاطر المصاحبة، الأداء المصرفي.	التطور السريع للتقنيات المالية يزيد من المخاطر ويتطلب تكيفًا مؤسسيًا.	دراسة نظرية دون تقييم الجاهزية أو النمذجة التطبيقية.
Shulha et al. (2022)	منهج نمذجة تحليلية (Fuzzy Cognitive Maps)	البرمجيات الخبيثة، أخطاء المستخدم، الهجمات الشبكية	إمكانية رفع مستوى الأمن السيبراني بنسبة كبيرة عبر تدابير مناسبة.	ركزت على النمذجة التقنية دون دمج العوامل البشرية والتنظيمية في نموذج شامل.

3. الفجوة البحثية

على الرغم من توافر دراسات عديدة تناولت المخاطر السيبرانية في القطاع المصرفي على المستويين الدولي والعربي، إلا أن معظمها ركز على بيانات مصرفية مستقرة ومتطورة تقنيًا، في حين لا تزال الدراسات التطبيقية التي تقيّم قدرة المصارف التجارية اللبينة على مواجهة المخاطر السيبرانية في ظل التحول الرقمي محدودة. كما لم تعالج هذه الدراسات بشكل متكامل أثر العوامل التقنية والبشرية والتنظيمية في نموذج واحد قابل للاختبار الإحصائي، مما يبرز فجوة بحثية تسعى هذه الدراسة إلى سدّها من خلال تحليل تطبيقي يعكس واقع البيئة المصرفية اللبينة

4. مشكلة الدراسة

رغم التوسع المتزايد في تبني التقنيات الرقمية داخل المصارف التجارية الليبية وما يرافقه من تحسين في كفاءة الخدمات المصرفية، إلا أن هذا التحول صاحبه تصاعد في المخاطر السيبرانية التي تهدد أمن المعلومات واستقرار العمليات المصرفية، في ظل تحديات تتعلق بضعف الجاهزية التقنية، ونقص الكوادر المتخصصة في الأمن السيبراني، وقصور البنية التحتية التكنولوجية، وغياب الأطر التشريعية والتنظيمية الفعالة. وعلى الرغم من تنامي الاهتمام العالمي بالأمن السيبراني في القطاع المصرفي، لا تزال الدراسات التطبيقية المحلية التي تقيم قدرة المصارف التجارية الليبية على مواجهة هذه المخاطر محدودة، مما يبرز فجوة بحثية تستدعي الدراسة. ومن هنا تتمثل مشكلة البحث في التساؤل حول مدى قدرة المصارف التجارية الليبية، في ظل التحول الرقمي، على مواجهة المخاطر السيبرانية، والعوامل المؤثرة في تعزيز هذه القدرة أو إضعافها.

5. أهداف الدراسة

تهدف هذه الدراسة إلى تقييم قدرة المصارف التجارية الليبية على مواجهة المخاطر السيبرانية في ظل التحول الرقمي، وذلك من خلال تحقيق الأهداف الآتية:

- 1- قياس أثر مستوى تبني التقنيات الرقمية في المصارف التجارية الليبية على قدرتها في مواجهة المخاطر السيبرانية.
- 2- تقييم دور جاهزية الكوادر البشرية المتخصصة في الأمن السيبراني في تعزيز قدرة المصارف التجارية الليبية على التصدي للمخاطر السيبرانية.
- 3- تحليل أثر كفاءة البنية التحتية التكنولوجية للمصارف التجارية الليبية على قدرتها في الحد من المخاطر السيبرانية.
- 4- تقييم أثر التشريعات والسياسات الحكومية المتعلقة بالأمن السيبراني في دعم قدرة المصارف التجارية الليبية على مواجهة المخاطر السيبرانية.

ثانياً: فروض الدراسة

اعتماداً على مشكلة الدراسة وأهدافها، تسعى الدراسة إلى اختبار الفروض الإحصائية الآتية:

H1 : يوجد أثر ذو دلالة إحصائية لمستوى تبني التكنولوجيا الرقمية في المصارف التجارية الليبية على قدرتها على مواجهة المخاطر السيبرانية عند مستوى معنوية $(\alpha \leq 0.05)$.

H2 : يوجد أثر ذو دلالة إحصائية لجاهزية الكوادر البشرية المتخصصة في مجال الأمن السيبراني في المصارف التجارية الليبية على قدرتها على مواجهة المخاطر السيبرانية عند مستوى معنوية $(\alpha \leq 0.05)$.

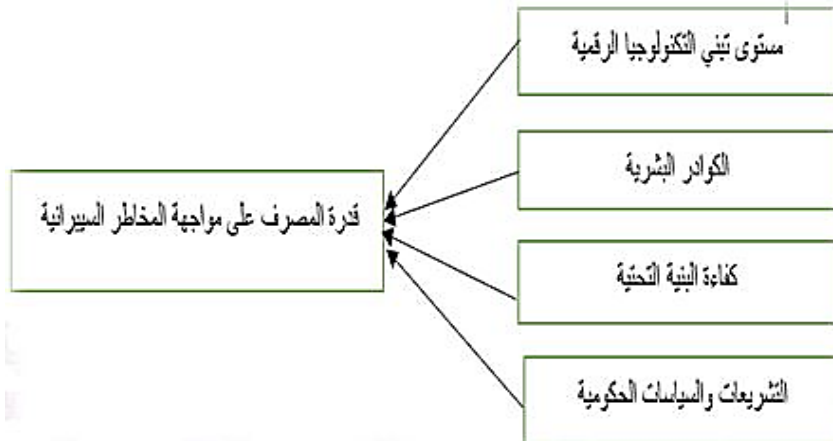
H3 : يوجد أثر ذو دلالة إحصائية لكفاءة البنية التحتية التكنولوجية في المصارف التجارية الليبية على قدرتها على مواجهة المخاطر السيبرانية عند مستوى معنوية $(\alpha \leq 0.05)$.

H4 : يوجد أثر ذو دلالة إحصائية للتشريعات والسياسات الحكومية المتعلقة بالأمن السيبراني على قدرة المصارف التجارية الليبية على مواجهة المخاطر السيبرانية عند مستوى معنوية $(\alpha \leq 0.05)$.

6. متغيرات في الدراسة

يوضح الشكل 1 العلاقة بين متغيرات الدراسة، حيث كانت مستوى تبني التكنولوجيا الرقمية في

المصارف، جاهزية الكوادر البشرية في مجال الأمن السيبراني، كفاءة البنية التحتية التكنولوجية للمصارف والتشريعات والسياسات الحكومية كمتغيرات مستقلة وقدرة المصارف التجارية الليبية على مواجهة المخاطر السيبرانية المتغير التابع.



الشكل 1: متغيرات الدراسة

7. حدود الدراسة

تقتصر الدراسة على المصارف التجارية الليبية فقط حيث تستهدف الموظفين المتخصصين في أقسام تكنولوجيا المعلومات والأمن السيبراني بالمصارف وتركز على تحليل المخاطر السيبرانية وقدرة المصارف على مواجهتها دون التطرق إلى الجوانب المالية الأخرى كالإقراض أو الاستثمار.

ثانياً: الإطار النظري للدراسة

يهدف هذا الجزء إلى بناء الأساس النظري للدراسة من خلال عرض مفاهيم الأمن السيبراني والمخاطر السيبرانية في القطاع المصرفي، وربطها بالنماذج والمعايير الدولية، بما يوضح الأسس التي تستند إليها فروض الدراسة.

• الأمن السيبراني والمخاطر السيبرانية في القطاع المصرفي

أدى التحول الرقمي المتسارع في القطاع المصرفي إلى توسع كبير في استخدام الأنظمة الإلكترونية والقنوات الرقمية، الأمر الذي جعل الأمن السيبراني أحد الركائز الأساسية لحماية الأصول الرقمية وضمان استمرارية الخدمات المالية. ويُعرّف الأمن السيبراني بأنه مجموعة من الإجراءات التقنية والتنظيمية المصممة لحماية الأنظمة والشبكات والمعلومات من الاختراق أو التعطيل أو الاستخدام غير المشروع، مع ضمان السرية والسلامة والتوافر (Stallings, 2018) في المقابل، تُشير المخاطر السيبرانية إلى التهديدات التي قد تلحق أضراراً بالأصول الرقمية للمصارف، سواء كانت ناجمة عن هجمات اختراق أو برمجيات خبيثة أو تصيد إلكتروني أو نتيجة للقصور البشري وضعف الوعي الأمني (Von Solms & Van Niekerk, 2013).

وتُعد المصارف التجارية من أكثر القطاعات تعرضاً للمخاطر السيبرانية نظراً لحجم البيانات المالية الحساسة التي تديرها وأهميتها للنظام المالي، حيث أدى التوسع في رقمنة الخدمات المصرفية إلى زيادة تعقيد الهجمات الإلكترونية واتساع نطاقها (Anderson, Böhme, Clayton, & Moore, 2008; Bouveret, 2018) وقد أكدت تقارير دولية أن نسبة كبيرة من الهجمات السيبرانية العالمية تستهدف المؤسسات المصرفية، مما يستدعي تبني مقاربات شاملة لإدارة هذه المخاطر وتعزيز الصمود السيبراني (Wilson, Gaidosch, Adelman, & Morozova, 2020)

• النماذج المرجعية للأمن السيبراني

يؤكد إطار NIST Cybersecurity Framework أن فعالية إدارة المخاطر السيبرانية تعتمد على التكامل بين التبنّي للأمن للتكنولوجيا الرقمية، والموارد البشرية المؤهلة، والحوكمة المؤسسية، من خلال وظائف التعرف والحماية والكشف والاستجابة والتعافي (Calder, 2018). وفي هذا الصدد، فإن مستوى تبنّي التكنولوجيا الرقمية في المصارف يمثل عاملاً مؤثراً في قدرتها على مواجهة المخاطر السيبرانية، إذ يسهم التبنّي الفعال للتقنيات الرقمية المصحوبة بضوابط أمنية في تعزيز الحماية والكشف المبكر عن المخاطر، بينما يؤدي التبنّي غير المنضبط إلى توسيع نطاق المخاطر. ويشكل هذا الطرح الأساس النظري للفرضية H1.

من جهة أخرى، ينظر معيار ISO/IEC 27001 إلى الأمن السيبراني بوصفه نظاماً إدارياً متكاملًا لإدارة أمن المعلومات، يركز على تقييم المخاطر، وتحديد المسؤوليات، وبناء الوعي الأمني، والتدريب المستمر (Putra, Tistiyan, & Sunaringtyas, 2021). ويبرز هذا المعيار الدور المحوري للعنصر البشري في تقليل المخاطر السيبرانية، خاصة تلك الناتجة عن الخطأ البشري، مما يدعم افتراض وجود علاقة ذات دلالة إحصائية بين جاهزية الكوادر البشرية المتخصصة في الأمن السيبراني وقدره المصارف على مواجهة المخاطر السيبرانية، وهو ما تقوم عليه الفرضية H2.

كما تشير الدراسات إلى أن كفاءة البنية التحتية التكنولوجية تُعد شرطاً أساسياً لتطبيق الضوابط الأمنية وتنفيذ استراتيجيات الأمن السيبراني بفعالية، حيث تسهم البنية التحتية المرنة والمحدثة في تقليل الثغرات التقنية وتعزيز استمرارية الأعمال (Bank for international settlements, 2018). إلا أن هذه الكفاءة تظل مرتبطة بمدى حسن إدارتها وتكاملها مع العنصر البشري و الحوكمة الأمنية، وهو ما يشكل الإطار النظري للفرضية H3.

وفيما يتعلق بالبعد التنظيمي، تؤكد تقارير دولية مثل تلك الصادرة عن بنك التسويات الدولية وصندوق النقد الدولي على أهمية التشريعات والسياسات الحكومية في وضع الحد الأدنى من متطلبات الأمن السيبراني، وتعزيز الامتثال، ودعم الصمود السيبراني في القطاع المصرفي (Bank for international settlements, 2018; Wilson et

(al., 2020)، وعليه فإن وجود تشريعات واضحة وفعالة من شأنه أن يساهم في تعزيز قدرة المصارف على مواجهة المخاطر السيبرانية وهو ما يشكل الأساس النظري للفرضية H4.

8. منهجية الدراسة

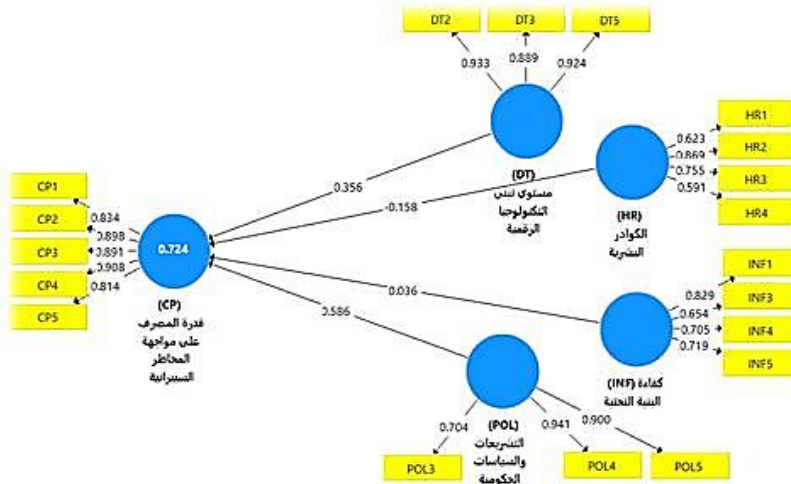
استخدم في هذه الدراسة المنهج الوصفي التحليلي كونه يتلاءم مع أهداف الدراسة فضلاً عن كونه أنسب في وصف الظاهرة محل الدراسة وصفاً دقيقاً ووظفت النمذجة بالمعادلة البنائية من خلال البرنامج الإحصائي (Smart PLS3) باعتباره يحقق أهداف الدراسات التنبؤية وحيث بلغ حجم العينة (157) وبعد بناء النموذج أظهرت مؤشرات التوافق للنموذج ضعفاً في مجمل معدلات التحميل Factor loading لفقرات الأبعاد المكونة لعوامل الدراسة فضلاً عن المؤشرات الأخرى المتمثلة في الموثوقية المركبة Composite Reliability (CR) ومتوسط التباين المستخلص (Average (AVE Variance Extracted وللحصول على مؤشرات تطابق تحقق غايات الدراسة وأهدافها فإن الأمر يتطلب حذف الفقرات التي لا تتمتع بمعدل تحميل يلبي الحد الأدنى لصحة مؤشرات التوافق؛ إذ أن استخدام الفقرات الزائدة عن الحاجة له آثار سلبية على المصادقية وقد يعزز من خطأ القياس (Hair, 2014).

وفي سبيل ذلك قادت عمليات الحذف للفقرات الضعيفة للعوامل المستقلة وكذا التابع على السواء إلى تحسين في المؤشرات وأفضت آلية الحذف إلى حذف عديد الفقرات للعوامل المستقلة تمثلت في الفقرات (DT1.DT4) بالنسبة لعامل مستوى تبنى التكنولوجيا الرقمية. أيضاً الفقرة (HR5) لعامل الكوادر البشرية وكذا الفقرة (INF2) لعامل كفاءة البنية التحتية ناهيك عن الفقرتين (POL1-POL2) لعامل التشريعات والسياسات الحكومية كما أسفرت عملية حذف الفقرات ذات معاملات التحميل المنخفضة آنفة الذكر عن تحسن ملحوظ في قيم مؤشرات التحميل، حيث ظهرت معظمها ضمن مستويات مرتفعة ومقبولة إحصائياً، باستثناء الفقرة (HR4) التابعة لمتغير الكوادر البشرية، إذ بلغ معامل تحميلها (0.591). إلا أن (Hair, 2014) يرى بعدم حذف الفقرات التي لا تقل معاملات تحميلها عن (0.40)، ما لم يؤدي حذفها إلى تحسن جوهري في مؤشرات جودة النموذج، والمتمثلة في معامل الثبات المركب (CR) ومتوسط التباين

المستخلص (AVE). فعند اختبار أثر حذف الفقرة المذكورة، لم يُسفر ذلك عن أي تحسن ملموس في هذه المؤشرات، الأمر الذي يتعين معه الإبقاء عليها ضمن نموذج القياس.

كما أظهرت نتائج تحليل (Bootstrapping) التفاوت في العلاقات بين العوامل المستقلة اتجاه العامل التابع فقد أظهر عامل مستوى تبنى التكنولوجيا الرقمية بدلالة إحصائية قدرها ($P=0.013$) وأن قيمة معامل المسار بينهما بلغت (0.356) أما عامل الكوادر البشرية فظهرت دلالاته الإحصائية مع العامل التابع إذ بلغت ($P=0.034$) وهو مستوى جيد من الدلالة ليعكس أيضا قيمة معامل المسار بينها إذ بلغت (0.158) و يعبر عن قوة العلاقة مع العامل التابع وفي السياق نفسه برز العامل المستقل الآخر التشريعات والسياسات الحكومية بمستوى قوي من الدلالة إحصائية قدرها ($P=0.000$) وأن قيمة معامل المسار بينهما بلغت (0.586) كما هو موضح في الشكل 3 .

كما يبين الجدول 3 مؤشرات حسن جودة مؤشرات التوافق للنموذج وبالتالي يكون النموذج قادر على دراسة الظاهرة محل الدراسة لتحقيق متطلبات القياس في النموذج.



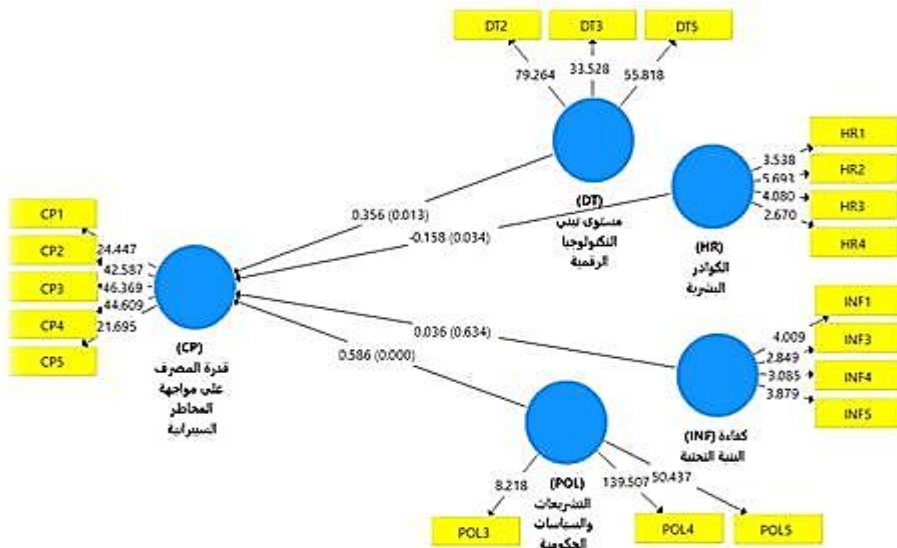
الشكل 2 نموذج الدراسة بعد عملية التحسين في مؤشرات التوافق

ولما كانت قيمة معامل التحديد (R^2 Coefficients of determination) تتأثر بعدد الأسهم الواقعة عليها إذ بلغت قيمتها (0.724) وعلى النحو المبين بالشكل 2 أعلاه إلا

أن ظهور العلاقة غير ذي دلالة إحصائية لإحدى العوامل المستقلة والمتمثلة في عامل كفاءة البنية التحتية (INF) البالغة قيمتها ($P=0.634$) مع التابع وعلى النحو المبين بالشكل 3؛ تظهر التأثير غير الحقيقي في قيمة R^2 المتحصل عليها نتيجة لطبيعة العوامل التي لا ترتبط بعلاقة ذات دلالة إحصائية مع المتغير التابع ؛ كونها لا تعبر عن قيمة التباين المفسر بدقة وأنه ينتج تحيزا جوهريا وان تلك القيمة يتعين تصفيتها من خلال الحصول على قيمتها المعدلة والمتمثلة في (R^2 Square Adjusted) (Hair,) (2014) وعلى النحو المبين بالجدول 2 .

جدول (2): معامل التحديد المعدل (R^2 Adjusted) لنموذج الدراسة

Adjusted R Square	R Square	المتغير التابع
0.724	0.731	قدرة المصرف على مواجهة المخاطر السيبرانية (CP)



الشكل 3 يبين الدلالة الإحصائية لمتغيرات الدراسة من خلال تقنية (Bootstrapping)

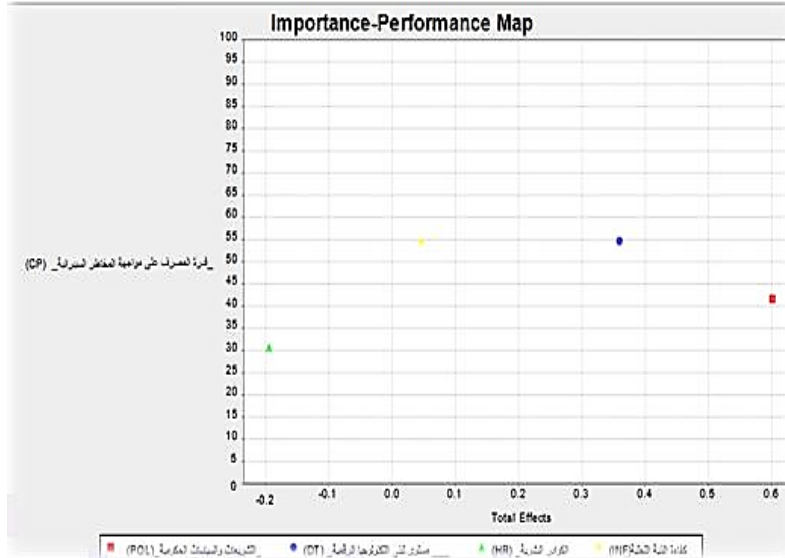
الجدول 3 قيم الثبات ومعاملات التحميل ومتوسط التباين المستخلص لعوامل الدراسة

P-Value	Average Variance	Composite Reliability	rho_A	Cronbach's Alpha	Loadings	الفقرات	
-	0.757	0.939	0.936	0.920	0.834	CP1	قدرة المصرف على مواجهة المخاطر السيبرانية
					0.898	CP2	
					0.891	CP3	
					0.908	CP4	
					0.814	CP5	
Sig (0.013)	0.835	0.953	0.938	0.934	0.933	DT2	مستوى تبني التكنولوجيا الرقمية (DT)
					0.889	DT3	
					0.924	DT5	
Sig (0.034)	0.516	0.806	0.765	0.701	0.623	HR1	الكوادر البشرية (HR)
					0.869	HR2	
					0.755	HR3	
					0.591	HR4	
Non- Sig (0.634)	0.533	0.819	0.790	0.727	0.829	INF1	كفاءة البنية التحتية (INF)
					0.654	INF3	
					0.705	INF4	
					0.719	INF5	
Sig (0.000)	0.731	0.889	0.884	0.812	0.704	POL3	التشريعات والسياسات الحكومية (POL)
					0.941	POL4	
					0.900	POL5	

9. الأهمية والأداء

عندما تكون معاملات المسار في النموذج ذات دلالة إحصائية إلا أن حجم تأثيرها محدود جدا فإن تحليل الأهمية النسبية في مثل هذه الحالات يعد من الأهمية بمكان في مثل هذه الحالات (Hair, 2014) إذ تعمل منهجية خريطة الأهمية والأداء على توسيع نتائج البرنامج الإحصائي (Smart-pls3) والاستنتاجات وتستند على معاملات المسار غير المعيارية إذ يعبر المحور السيني على الأهمية في حين يشكل المحور الرأسي الأداء

ويعكس متوسط الدرجات الموحدة غير المعيارية ويبين الجدول 3 ملخصاً لبيانات خريطة الأداء - الأهمية.



الشكل 4 : عوامل الدراسة لمخطط الأهمية والأداء IPMA

يظهر تحليل مخطط الأهمية والأداء بأن مستوى تبني التكنولوجيا الرقمية تشكل المستوى الأعلى من الأهمية إذ بلغت (0.359) كما هو مبين بالجدول 4 الأمر الذي يتعين معه الاهتمام به وعدم إهماله للحصول على أكبر مستوى من التأثير.

جدول 4 بيانات خريطة الأداء - الأهمية

العامل	مستوى تبني التكنولوجيا الرقمية	كفاءة البنية التحتية	الكوادر البشرية	التشريعات والسياسات الحكومية
الأهمية	0.359	0.0459	0.194-	-0601
الأداء	54.63	54.57	30.62	41.58

10. مناقشة النتائج

أظهرت نتائج الدراسة وجود أثر ذي دلالة إحصائية لكل من جاهزية الكوادر البشرية ومستوى تبني التكنولوجيا الرقمية على قدرة المصارف التجارية الليبية على مواجهة المخاطر السيبرانية، مما يؤكد أن العوامل التشغيلية الديناميكية تمثل المحدد الرئيس

للمصمود السيبراني في بيئة مصرفية تتسم بضعف الاستقرار المؤسسي. ويعكس ذلك الدور المحوري للعنصر البشري المؤهل والقدرة على توظيف التقنيات الرقمية بفعالية، وهو ما يتسق مع ما أكدته دراسات حديثة بأن القصور البشري والتنظيمي يُعد من أبرز مصادر المخاطر السيبرانية في القطاع المصرفي (Oyewole et al., 2024; Von Solms & Van Niekerk, 2013) في المقابل، لم تُظهر النتائج وجود أثر ذي دلالة إحصائية لكفاءة البنية التحتية التكنولوجية، وهو ما يمكن تفسيره بضعف تفعيل هذه البنية وعدم دمجها ضمن إطار متكامل لإدارة المخاطر والحوكمة السيبرانية (Bank for international settlements, 2018). كما لم تكن التشريعات والسياسات الحكومية ذات دلالة إحصائية، الأمر الذي يعكس فجوة بين الإطار القانوني ومستوى التطبيق الفعلي، خاصة في البيئات الانتقالية التي تعاني ضعف التنفيذ المؤسسي (International Monetary Fund, 2021) وتشير هذه النتائج إلى أن تعزيز الصمود السيبراني في المصارف اللبينة يتطلب التركيز على بناء القدرات البشرية وتحسين إدارة التحول الرقمي، بالتوازي مع تفعيل البنية التحتية والتشريعات عمليًا.

11. النتائج

من خلال مناقشة النتائج وتفسيرها توصلت الدراسة إلى النتائج الآتية:

- 1- وجود أثر إيجابي وذو دلالة إحصائية لمستوى تبني التكنولوجيا الرقمية على قدرة المصارف التجارية اللبينة على مواجهة المخاطر السيبرانية.
- 2- وجود أثر إيجابي وذو دلالة إحصائية لجاهزية الكوادر البشرية المتخصصة في الأمن السيبراني على قدرة المصارف التجارية اللبينة في التصدي للتهديدات السيبرانية.
- 3- عدم وجود أثر ذي دلالة إحصائية لكفاءة البنية التحتية التكنولوجية على قدرة المصارف التجارية اللبينة على مواجهة المخاطر السيبرانية.
- 4- وجود أثر ذي دلالة إحصائية للتشريعات والسياسات الحكومية المتعلقة بالأمن السيبراني على قدرة المصارف التجارية اللبينة في مواجهة التهديدات السيبرانية.

12. التوصيات

في ضوء ما خلصت إليه نتائج الدراسة فإن الدراسة توصي بما يلي:

- 1- التركيز على تنمية وتأهيل الكوادر البشرية المتخصصة في الأمن السيبراني داخل المصارف التجارية الليبية، من خلال التدريب المستمر وبناء القدرات الفنية.
- 2- تعزيز التحول الرقمي المصحوب بإجراءات أمن سيبراني فعّالة، بما يضمن الاستخدام الآمن للتقنيات الرقمية في تقديم الخدمات المصرفية.
- 3- تفعيل الاستفادة العملية من البنية التحتية التكنولوجية المتاحة وربطها بسياسات واضحة لإدارة المخاطر السيبرانية داخل المصارف.
- 4- تطوير وتفعيل التشريعات والسياسات الحكومية الخاصة بالأمن السيبراني، مع ضمان تطبيقها ومتابعتها ميدانيًا داخل المصارف.

13. الخاتمة

تُظهر نتائج هذه الدراسة أن المصارف التجارية الليبية تواجه تحديات كبيرة في مواجهة التهديدات السيبرانية، حيث تتفاوت جاهزيتها بحسب كفاءة التنظيم والاستثمار في البنية التحتية التقنية. كما أظهرت الدراسة أن الاستخدام الفعّال للضوابط السيبرانية، والتوعية المستمرة للعملاء، واعتماد استراتيجيات تكاملية بين التكنولوجيا والامتثال، يمكن أن يقلل من فرص الاختراقات بشكل كبير. وتعكس هذه النتائج أهمية تعزيز إطار الحوكمة السيبرانية وتحفيز الاستثمار في أنظمة الأمن الرقمي، لضمان استمرارية الأعمال وحماية البيانات المالية الحساسة.

14. الأبحاث المستقبلية

استنادًا إلى نتائج هذه الدراسة، يقترح للمستقبل عدة مسارات بحثية:

- 1- دراسة مدى تبني منتجات التأمين السيبراني، وكفاءتها في الحد من الخسائر المالية الناجمة عن المخاطر السيبرانية.
- 2- التركيز على التوعية السيبرانية للعملاء وقياس تأثيرها على تقليل المخاطر العملية والمالية.

3-تحليل أثر الأطر التنظيمية الدولية مثل ISO 27001 و NIST Cybersecurity Framework) على تحسين مرونة المصارف السيبرانية.

المراجع

- Anderson, R., Böhme, R., Clayton, R., & Moore, T. (2008). Security economics and the internal market. *Study commissioned by ENISA*.
- Bank for international settlements. (2018). Basel Committee on Banking Supervision Cyber-resilience: Range of practices. *The Bank for International Settlements*. Retrieved from <https://www.bis.org/bcbs/publ/d454.htm>
- Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment*: International Monetary Fund.
- Calder, A. (2018). *NIST Cybersecurity Framework: A pocket guide*: IT Governance Publishing Ltd.
- Hair, J. F. (2014). *A primer on partial least squares structural equation modeling (PLS-SEM)*: sage.
- International Monetary Fund. (2021). Cybersecurity risk supervision: A capacity development tool. . Retrieved from <https://www.imf.org/external/error.htm?URL=https%3A%2F%2Fwww.imf.org%2Fen%2FPublications%2FTNM%2FIssue%2F2021%2F09%2F24%2FCybersecurity-Risk>
- Kolesova, I., & Girzheva, Y. (2018). Impact of financial technologies on the banking sector. *KnE Social Sciences*, 215-220.
- Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews*, 21(3), 625-643.
- Putra, D. S. K., Tistiyani, S., & Sunaringtyas, S. U. (2021). *The Use of ISO/IEC 27001 Family of Standards in Regulatory Requirements in Some Countries*. Paper presented at the 2021 2nd International Conference on ICT for Rural Development (IC-ICTRuDev).
- PwC. (2022). 2022 Global Digital Trust Insights Survey: Simplifying Cyber. PwC. Retrieved from

<https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights-2022.html>

- Shulha, O., Yanenkova, I., Kuzub, M., Muda, I., & Nazarenko, V. (2022). Banking information resource cybersecurity system modeling. *Journal of Open Innovation: Technology, Market, and Complexity*, 8(2), 80 .
- Stallings, W. (2018). *Effective cybersecurity :a guide to using best practices and standards*: Addison-Wesley Professional.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, 38, 97-102 .
- Wilson, C., Gaidosch, T., Adelmann, F., & Morozova, A. (2020). *Cybersecurity risk supervision*: International Monetary Fund.
- عامر العتوم, ن. خ., عدنان ربابعة, عبدالله البدارين. (2019). دور الهيئات الرقابية في ادارة مخاطر الخدمات المصرفية الالكترونية في المصارف الاسلامية. *المجلة الاردنية في الدراسات الاسلامية*.