المجلة الليبية للدراسات الأكاديمية المعاصرة (Libyan Journal of Contemporary Academic Studies)
LJCAS, eISSN: 5970-3005
Volume 4, Issue 1, 2026, Pages: 107-128

Measuring the Impact of Cybersecurity Risks on the Financial Resilience of Banking Institutions in a Digital Transformation Environment: A Field Study on Jumhouria Bank - Misrata Branch

Mahmoud Abdulsalam Saleh Al-Krewi *
Department of Finance and Banking, Faculty of Economics and Trade - Garabulli, El-Mergib University, Garabulli, Libya
*Corresponding author: maalkreue@elmergib.edu.ly

قياس تأثير مخاطر الأمن السيبراني على المرونة المالية للمؤسسات المصرفية في بيئة التحول الرقمي دراسة ميدانية على مصرف الجمهورية فرع مصراتة

محمود عبد السلام صالح الكريوي *
قسم التمويل والمصارف، كلية الاقتصاد والتجارة – القره بوللى، جامعة المرقب، القره بوللى، ليبيا

Received: 21-11-2025; **Accepted:** 24-01-2026; **Published:** 04-02-2026

Abstract:
This study aimed to investigate the impact of management's perception of cybersecurity risks on the financial resilience of Jumhouria Bank (Misrata Branch) within the context of an accelerating digital transformation environment. The research problem lies in the financial and operational challenges imposed by cyberspace on Libyan banking institutions, and the extent of their ability to maintain financial stability against digital threats.
To achieve the study's objectives, the researcher adopted a descriptive-analytical approach. A questionnaire was developed as the primary data collection tool and distributed to a purposive sample of (29) employees from the administrative, financial, and technical cadres at the bank. The data were statistically processed using the Statistical Package for the Social Sciences (SPSS).
The study reached several key findings, most notably a high level of perception among the bank's management regarding cybersecurity risks, with a mean score of (4.09), alongside a firm conviction that investing in digital security is directly linked to protecting financial assets. Furthermore, regression analysis results proved a statistically significant impact of cybersecurity risks on financial resilience, as the independent variable explained (51.8%) of the variance in the bank's financial resilience level. The results also revealed a strong negative correlation between the frequency of cyber threats and resilience indicators, with "customer trust" being the dimension most affected by these threats.
In light of these findings, the study recommended the necessity of enhancing the bank's financial readiness by allocating financial reserves (contingency funds) to face cyber crises. It also emphasized intensifying specialized training programs for employees to bridge the gap between theoretical perception and procedural hedging, in addition to adopting effective communication strategies to maintain corporate reputation and customer trust in the face of increasing digital threats.

Keywords: Cybersecurity, Digital Transformation, Financial Resilience.

الملخص :
هدفت هذه الدراسة إلى تقصي أثر إدراك إدارة مصرف الجمهورية (فرع مصراتة) لمخاطر الأمن السيبراني على المرونة المالية للمصرف في ظل بيئة التحول الرقمي المتسارعة. تكمن مشكلة الدراسة في التحديات المالية والتشغيلية التي يفرضها الفضاء السيبراني على المؤسسات المصرفية الليبية، ومدى قدرة هذه المؤسسات على الصمود المالي أمام التهديدات الرقمية.
ولتحقيق أهداف الدراسة، اعتمد الباحث المنهج الوصفي التحليلي، حيث تم تصميم استبانة كأداة رئيسة لجمع البيانات، وُزعت على عينة قصدية بلغت (29) موظفاً من الكوادر الإدارية والمالية والتقنية بالمصرف. وقد تمت معالجة البيانات إحصائياً باستخدام حزمة البرامج الإحصائية للعلوم الاجتماعية (SPSS).
توصلت الدراسة إلى مجموعة من النتائج الجوهرية، أبرزها وجود مستوى مرتفع من الإدراك لدى إدارة المصرف لمخاطر الأمن السيبراني بمتوسط حسابي (4.09)، مع وجود قناعة راسخة بارتباط الاستثمار في الأمن الرقمي بحماية الأصول المالية. كما أثبتت نتائج تحليل الانحدار وجود تأثير ذو دلالة إحصائية لمخاطر الأمن السيبراني على المرونة المالية، حيث فسر المتغير المستقل ما نسبته (51.8%) من التباين في مستوى المرونة المالية للمصرف. وأظهرت النتائج وجود علاقة ارتباطية عكسية قوية بين تكرار التهديدات السيبرانية ومؤشرات المرونة، وكان بُعد "ثقة العملاء" هو الأكثر تأثراً بتلك التهديدات.
وفي ضوء هذه النتائج، أوصت الدراسة بضرورة تعزيز الجاهزية المالية للمصرف من خلال تخصيص احتياطيات مالية لمواجهة الأزمات السيبرانية، وتكثيف برامج التدريب المتخصص للموظفين لتقليل الفجوة بين الإدراك النظري والتحوط

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

الإجرائي، بالإضافة إلى تبني استراتيجيات اتصال فعالة للحفاظ على السمعة المؤسسية وثقة العملاء في مواجهة التهديدات الرقمية المتزايدة.

الكلمات المفتاحية: الأمن السيبراني، التحول الرقمي، المرونة المالية.

مقدمة

يشهد القطاع المصرفي العالمي والمحلي تحولاً جذرياً نحو الرقمنة، حيث يسعى مصرف الجمهورية لمواكبة هذه التطورات عبر تقديم خدمات إلكترونية متطورة. ومع ذلك، فإن هذا التحول يفتح أبواباً جديدة لمخاطر الأمن السيبراني التي قد لا تهدد البيانات فحسب، بل تمتد لتضرب المرونة المالية للمصرف (قدرته على الصمود أمام الصدمات المالية، وتوفر السيولة، واستمرارية الأرباح) تهدف هذه الدراسة إلى استكشاف مدى قدرة مصرف الجمهورية بفرع مصراتة على الموازنة بين طموحات التحول الرقمي وضرورات الحماية السيبرانية لضمان الاستقرار المالي.

تعد مخاطر الأمن السيبراني اليوم من أبرز التحديات التي تواجه المؤسسات المصرفية، حيث لم يعد التحول الرقمي مجرد خيار تكنولوجي، بل أصبح ضرورة استراتيجية لتقديم الخدمات. وتتمثل هذه المخاطر في التهديدات التي تستهدف الأنظمة الرقمية، وقواعد البيانات، والقنوات المصرفية الإلكترونية (مثل التطبيقات والخدمات المصرفية عبر الإنترنت) من خلال الاختراقات، البرمجيات الخبيثة، أو هجمات تعطيل الخدمة. في بيئة مصرف الجمهورية، تتصاعد هذه المخاطر مع زيادة الاعتماد على التقنيات المالية الحديثة، مما يجعل البنية التحتية الرقمية عرضة لثغرات قد تؤدي إلى فقدان السيطرة على البيانات أو الأصول الرقمية.

على الجانب الآخر، تبرز المرونة المالية كحائط صد جوهري يعبر عن قدرة المصرف على استيعاب الصدمات المالية المفاجئة، والتعافي منها، والاستمرار في أداء وظائفه الأساسية دون انهيار. وتتحدد المرونة المالية في مصرف الجمهورية - فرع مصراتة بمدى توفر السيولة الكافية، وقوة رأس المال، واستدامة الربحية، بالإضافة إلى القدرة على حماية سمعة المصرف المالية. فالمصرف المرن هو الذي يمتلك استراتيجيات استباقية تمكنه من الحفاظ على مركزه المالي مستقراً حتى في أحلك الظروف التشغيلية أو الأزمات الناتجة عن اختلال الأنظمة.

تكمن العلاقة بين هذين المتغيرين في وجود ارتباط طردي بين كفاءة إدارة مخاطر الأمن السيبراني وتعزيز المرونة المالية؛ فالفشل في التصدي للتهديدات السيبرانية لا يقتصر أثره على الجانب التقني فحسب، بل يمتد ليضرب "المرونة المالية" مباشرة عبر تكبد خسائر مادية فادحة، وتحمل تكاليف معالجة الاختراقات، ودفع التعويضات، فضلاً عن فقدان ثقة المودعين الذي قد يؤدي إلى سحب جماعي للسيولة. لذا، تسعى هذه الدراسة لتسليط الضوء على هذه العلاقة التبادلية في مصرف الجمهورية - فرع مصراتة، لتحديد كيف يمكن للتحصين السيبراني أن يكون ركيزة أساسية لضمان الاستدامة المالية والقدرة على الصمود أمام تقلبات التحول الرقمي.

مشكلة الدراسة

تتبلور مشكلة الدراسة في التحدي المتصاعد الذي يواجهه مصرف الجمهورية - فرع مصراتة، والمتمثل في كيفية الحفاظ على استقراره المالي وسمعته المؤسسية في ظل بيئة تقنية معقدة تفرضها ضرورات التحول الرقمي. وتستند هذه المشكلة إلى جملة من الشواهد الواقعية والأبعاد الأكاديمية؛ حيث تشير التقارير الصادرة عن **صندوق النقد الدولي (IMF)** إلى أن القطاع المالي بات الهدف الأكثر استقطاباً للهجمات السيبرانية عالمياً، مع ملاحظة تضاعف وتيرة هذه الهجمات بالتوازي مع التوسع في الخدمات المصرفية الرقمية. وفي السياق المحلي، فإن سعي مصرف الجمهورية الحثيث لرقمنة خدماته —كما هو الحال في تطبيق "جمهورية أون لاين"— قد ساهم في زيادة "مساحة الهجوم(Attack Surface) "، مما يضع الأصول المالية والبيانات الحساسة تحت تهديد مستمر.

وعلى صعيد الأدبيات العلمية، تؤكد دراسة **(العنزي، 2021)**وجود فجوة حرجة بين سرعة تبني التقنيات الرقمية ومستوى وعي الإدارة بالمخاطر السيبرانية المرافقة لها، وهو ما يجعل المؤسسات المصرفية عرضة لخسائر مفاجئة نتيجة ضعف الجاهزية الاستباقية؛ وهو بُعد جوهري تسعى الدراسة الحالية

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

لاستكشافه في فرع مصراتة. ومن زاوية أخرى، أثبتت دراسة **(أبو نصار، 2022)** أن الهجمات السيبرانية لا تقتصر أضرارها على الجانب التقني الصرف، بل تمتد لتضرب "المرونة المالية" للمصرف مباشرة، وذلك نتيجة ارتفاع تكاليف التعافي من الاختراقات، وتآكل ثقة المودعين التي قد تؤدي إلى سحب مفاجئ للسيولة، مما يضعف قدرة المصرف على الصمود في وجه الأزمات.

بناءً على ما تقدم، تبرز الحاجة الملحة لتشخيص هذا الواقع في مصرف الجمهورية، وهو ما يمكن صياغته في التساؤل الرئيسي التالي" :

ما مدى تأثير مخاطر الأمن السيبراني على المرونة المالية للمصرف في ظل بيئة التحول الرقمي؟"

وينبثق عن هذا التساؤل الأسئلة الفرعية التالية:

1. ما هو مستوى إدراك إدارة مصرف الجمهورية (فرع مصراتة) لمخاطر الأمن السيبراني الناتجة عن عمليات التحول الرقمي؟
2. هل توجد علاقة ذات دلالة إحصائية بين تكرار التهديدات السيبرانية وانخفاض مؤشرات المرونة المالية (مثل التكاليف التشغيلية، الثقة بالعملاء، والربحية)؟

أهداف الدراسة

تنمو هذه الدراسة لتحقيق الهدف الرئيسي: قياس وتحليل أثر مخاطر الأمن السيبراني على المرونة المالية لمصرف الجمهورية (فرع مصراتة) في ظل بيئة التحول الرقمي، وكشف مدى قدرة المصرف على الصمود أمام التهديدات الرقمية.

الأهداف الفرعية:

1. تقييم مستوى الوعي الإداري :التعرف على مدى إدراك وفهم الإدارة في مصرف الجمهورية (فرع مصراتة) لطبيعة وحجم مخاطر الأمن السيبراني التي صاحبت عملية الانتقال إلى الخدمات الرقمية.
2. تحديد العلاقة الارتباطية :استكشاف طبيعة وقوة العلاقة الإحصائية بين تكرار التهديدات السيبرانية وبين التغيرات التي تطرأ على مؤشرات المرونة المالية (مثل ارتفاع التكاليف التشغيلية، وتذبذب الأرباح، ومدى تأثر ثقة العملاء).
3. تطوير آليات المواجهة :الوصول إلى مجموعة من التوصيات والحلول العملية التي تساعد المصرف على تحصين أصوله المالية وحماية سمعته، بما يضمن استمرارية الأعمال الرقمية دون المساس بمرونته المالية.

فرضيات الدراسة:

الفرضية الرئيسية:

"يوجد تأثير ذو دلالة إحصائية لمخاطر الأمن السيبراني على المرونة المالية لمصرف الجمهورية (فرع مصراتة) في بيئة التحول الرقمي عند مستوى دلالة".(0.05).

الفرضيات الفرعية:

الفرضية الفرعية الأولى:

"توجد فروق ذات دلالة إحصائية في مستوى الجاهزية المالية للمصرف تعزى لمستوى إدراك الإدارة لمخاطر الأمن السيبراني الناتجة عن التحول الرقمي".

الفرضية الفرعية الثانية:

"توجد علاقة ارتباطية عكسية ذات دلالة إحصائية بين تكرار التهديدات السيبرانية وبين مؤشرات المرونة المالية (التكاليف التشغيلية، الربحية، وثقة العملاء) في مصرف الجمهورية - فرع مصراتة".

أهمية الدراسة

تكتسب هذه الدراسة أهميتها من خلال مستويين متكاملين؛ فعلى **الصعيد العلمي**، تسعى الدراسة إلى إثراء المكتبة العربية والبيئة البحثية الوطنية الليبية بإطار نظري وتطبيقي يربط بين المتغيرات التقنية المتمثلة في الأمن السيبراني والمتغيرات المالية المتمثلة في المرونة المالية، وهو مسار بحثي يتسم بالحداثة والندرة في السياق المحلي، مما يفتح آفاقاً جديدة للباحثين لفهم التداخل المعقد بين الحماية الرقمية والاستقرار المالي للمؤسسات المصرفية.

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

أما على **الصعيد العملي والمهني**، فتتجلى أهمية الدراسة في دورها كأداة توجيهية لصناع القرار في مصرف الجمهورية - فرع مصراتة، من خلال تزويدهم بمؤشرات دقيقة وشاملة حول الفجوات الأمنية المحتملة وانعكاساتها المادية المباشرة على ميزانية المصرف. ويساهم هذا في تعزيز قدرة الإدارة على إدارة مواردها المالية بكفاءة أعلى، وتوجيه الاستثمارات نحو البنية التحتية المعلوماتية بشكل استراتيجي يضمن استدامة العمليات المصرفية، ويحمي أصول المؤسسة من الاستنزاف المالي الناتج عن التهديدات الرقمية في بيئة التحول الرقمي.

منهجية الدراسة

تتبنى هذه الدراسة المنهج الوصفي التحليلي كإطار منهجي لتحقيق أهدافها؛ حيث تم استقاء المادة العلمية للإطار النظري عبر المسح المكتبي للكتب والدوريات التخصصية والأدبيات السابقة ذات الصلة. وفيما يتعلق بالجانب التطبيقي، اعتمد الباحث على الاستبانة كأداة رئيسية لجمع البيانات الأولية من أفراد العينة، ليتم عقب ذلك معالجتها وتحليلها إحصائياً باستخدام الأساليب والبرمجيات المتخصصة لاستخلاص النتائج وتفسيرها.

حدود الدراسة

تلتزم الدراسة بالحدود التالية لضمان دقة النتائج والتركيز على مشكلة الدراسة:

1. **الحدود الموضوعية:**

تقتصر هذه الدراسة على قياس أثر مخاطر الأمن السيبراني (كمتغير مستقل) على المرونة المالية (كمتغير تابع)، وذلك في إطار بيئة التحول الرقمي .ويشمل ذلك التركيز على المخاطر التقنية والتشغيلية وتأثيرها على السيولة، الربحية، وسمعة المصرف.

2.الحدود المكانية

تُطبق هذه الدراسة ميدانياً في مصرف الجمهورية - فرع مصراتة .تم اختيار هذا الفرع نظراً لمكانته الاقتصادية الكبيرة في المدينة، ولأنه يمثل نموذجاً للمصارف التي تشهد توسعاً ملحوظاً في الخدمات المصرفية الرقمية.

الدراسات السابقة :

1. دراسة (بلقاسم وشعبان، 2024)

بحثت هذه الدراسة في "انعكاسات مخاطر الأمن المعلوماتي على السمعة المؤسسية والأداء المالي للمصارف العاملة في الجزائر"، حيث هدفت إلى تحليل العلاقة التفاعلية بين الاختراقات الأمنية وسمعة المصرف ومدى تأثير ذلك على العوائد المالية المحققة. طُبقت الدراسة على مجتمع مكون من الخبراء الماليين ومحللي المخاطر وموظفي تقنية المعلومات، واعتمدت على عينة قصدية بلغ حجمها **(110)** فرداً. وتوصلت النتائج إلى أن تضرر السمعة المؤسسية جراء الاختراقات السيبرانية يؤدي إلى خسارة حصة سوقية ملموسة وانخفاض في صافي الأرباح السنوية. وأوصت الدراسة بضرورة إنشاء وحدات مستقلة للأمن السيبراني تتبع الإدارة العليا مباشرة لضمان سرعة الاستجابة ومنع تدهور الأداء المالي عند حدوث الأزمات الرقمية.

2. دراسة (حميد والساعدي، 2023)

تناولت هذه الدراسة "تأثير التحول الرقمي على المخاطر التشغيلية والسيولة في المصارف التجارية (دراسة تطبيقية في العراق)"، بهدف استكشاف كيف يؤثر التوسع في القنوات الإلكترونية على استقرار مستويات السيولة. استهدفت الدراسة مجتمع مدراء الفروع ورؤساء أقسام الائتمان والعمليات الإلكترونية، وتم اختيار عينة حجمها **(85)** مشاركاً. خلصت النتائج إلى أن الاندفاع نحو التحول الرقمي دون وجود بنية تحتية أمنية كافية يرفع من معدلات المخاطر التشغيلية، مما ينعكس سلباً على مؤشرات السيولة (التي تعد ركيزة المرونة المالية). وشددت توصيات الدراسة على ضرورة الموازنة بين سرعة الابتكار الرقمي ومتطلبات التحصين الأمني لضمان عدم استنزاف موارد المصرف في معالجة الثغرات التقنية.

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

3. دراسة (أبو نصار، 2022)

هدفت هذه الدراسة إلى معرفة "دور الأمن السيبراني في تعزيز المرونة التنظيمية والمالية في المصارف الإسلامية الأردنية"، من خلال قياس مساهمة إجراءات الحماية في تمكين المصارف من استعادة نشاطها المالي بعد الهجمات الرقمية. شمل مجتمع الدراسة موظفي أقسام المخاطر والتدقيق الداخلي وتكنولوجيا المعلومات، وتكونت العينة من **(145)** موظفاً. أظهرت النتائج أن الالتزام بمعايير الأمن السيبراني يسهم بشكل فعال في تعزيز المرونة المالية ويقلل من احتمالات نزوح الودائع الناتج عن فقدان ثقة العملاء. وأوصت الدراسة بتبني إطار عمل متكامل لإدارة المخاطر السيبرانية كجزء جوهري من الاستراتيجية المالية الكلية للمصرف.

4. دراسة (العنزي، 2021)

ركزت هذه الدراسة على "أثر مخاطر الأمن السيبراني على جودة التقارير المالية في البنوك التجارية الكويتية"، حيث هدفت إلى الكشف عن تأثير التهديدات السيبرانية على دقة وموثوقية البيانات المالية. استهدفت الدراسة الموظفين في الإدارات العليا والوسطى وتقنية المعلومات بمجتمع البنوك التجارية، وبلغ حجم العينة **(120)** فرداً. وكشفت النتائج عن وجود تأثير سلبي ذو دلالة إحصائية للمخاطر السيبرانية على جودة التقارير المالية، بالإضافة إلى تحمل المصارف تكاليف تشغيلية طارئة تؤدي إلى تآكل الربحية. وأوصت الدراسة بضرورة تحديث سياسات الحوكمة الإلكترونية والاستثمار في تقنيات التشفير المتقدمة لحماية سلامة البيانات المالية.

5. دراسة (سليمان، 2020)

استهدفت هذه الدراسة قياس "إدراك الإدارة العليا لمخاطر الأمن السيبراني وأثره على استمرارية الأعمال في البنوك المصرية"، وذلك من خلال تحليل مدى وعي القيادات المصرفية بالتهديدات الرقمية الحديثة. تم تطبيق الدراسة على مجتمع أعضاء مجالس الإدارة والمدراء التنفيذيين، وشملت عينة حجمها **(100)** مسؤول. وأكدت نتائج الدراسة أن المؤسسات التي يتمتع قادتها بوعي أمني مرتفع كانت أكثر كفاءة في تخصيص الميزانيات المالية الموجهة للأمن السيبراني، مما عزز من استقرارها المالي واستمرارية أعمالها. وانتهت الدراسة بتوصية تدعو إلى تكثيف البرامج التدريبية المتخصصة للقيادات العليا حول آليات الحماية من الجرائم المالية الإلكترونية.

تعقيب الباحث على الدراسات السابقة (الفجوة البحثية):

من خلال استعراض الدراسات السابقة، يتضح اهتمامها بالربط بين الأمن السيبراني والأداء المالي في بيئات عربية مختلفة، إلا أن ما يميز دراستي هو تركيزها المباشر على **"المرونة المالية"** كمفهوم شامل للصمود والتعافي، وتطبيقها في بيئة مصرفية ليبية (مصرف الجمهورية - فرع مصراتة) التي تشهد تحولاً رقمياً في ظل تحديات بنية تحتية خاصة، وهو ما يجعلها تسد فجوة بحثية هامة في الأدبيات المحلية.

أولاً : الإطار النظري للدراسة

❖ **مخاطر الأمن السيبراني في ظل التحول الرقمي المصرفي**

تجاوز مفهوم الأمن السيبراني في المصارف الحديثة مجرد حماية أجهزة الحاسوب، ليصبح نظاماً متكاملاً للحوكمة الرقمية.

- **طبيعة التهديدات في بيئة التحول الرقمي :**مع تبني مصرف الجمهورية لتقنيات مثل الحوسبة السحابية (Cloud Computing) والواجهات البرمجية(APIs) ، ظهرت مخاطر جديدة تُعرف بـ "المخاطر السيبرانية المنهجية". هذه المخاطر لا تستهدف فرعاً واحداً فحسب، بل قد تؤدي إلى توقف كامل للخدمات المالية نتيجة ترابط الأنظمة.(Humphreys, 2019)
- **تصنيف المخاطر وفقاً للأثر التشغيلي :**يمكن تقسيم المخاطر إلى مخاطر **تقنية** (فشل المنظومات)، ومخاطر **بشرية** (الهندسة الاجتماعية والتصيد)، ومخاطر **خارجية** (الهجمات المنظمة). هذه المخاطر تضع ضغوطاً مستمرة على الكفاءة التشغيلية للمصرف (القحطاني، 2021).

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

❖ **المرونة المالية (Financial Resilience) كمفهوم استراتيجي**

المرونة المالية هي قدرة المصرف على إدارة "رأس المال السائل" و"السمعة" في وقت واحد لمواجهة الأزمات الرقمية.

- **مكونات المرونة المالية في المصارف:**

1. **الملاءة الرقمية (Digital Solvency):** قدرة الموارد المالية للمصرف على تغطية تكاليف التحديثات الأمنية الطارئة دون التأثير على التوزيعات الربحية (الزبيدي، 2020).
2. **ثبات الودائع (Deposit Stability):** تعد ثقة العميل حجر الزاوية في المرونة المالية؛ حيث إن أي اختراق سيبراني قد يؤدي إلى "هروب الودائع " (Bank Run) خوفاً من ضياع المدخرات، مما يسبب أزمة سيولة مفاجئة (Financial Stability Board, 2022).

- **تكاليف عدم المرونة:** تشير الدراسات إلى أن المصارف التي تفتقر للمرونة المالية تضطر للاقتراض بتكلفة عالية لتغطية خسائر الاختراقات، مما يؤدي إلى انخفاض العائد على الملكية (ROE)(الزبيدي، 2020).

❖ **بيئة التحول الرقمي كمحفز للمخاطر والمرونة.**

يعمل التحول الرقمي في مصرف الجمهورية - فرع مصراتة كبيئة حاضنة، تتسم بخصائص محددة تؤثر على المتغيرين:

- **السرعة مقابل الأمان:** إن التنافس لتقديم خدمات رقمية سريعة (مثل القروض الإلكترونية والتحويل الفوري) قد يتم أحياناً على حساب التحقق الأمني العميق، وهو ما يسمى بـ "الفجوة الأمنية الرقمية" (النجار، 2022).
- **المرونة السيبرانية (Cyber Resilience) كطريق للمرونة المالية:** لا يمكن للمصرف تحقيق مرونة مالية ما لم يحقق أولاً "مرونة سيبرانية" تعني القدرة على العمل تحت الهجوم. فالمصرف الذي يستطيع استعادة نظامه المالي في غضون دقائق بعد هجوم سيبراني، يحمي نفسه من خسائر مالية تقدر بملايين الدينارات.(Westerman & Bonnet, 2021)

❖ **آليات انتقال أثر المخاطر السيبرانية إلى المرونة المالية.**

هناك ثلاثة قنوات رئيسية ينتقل من خلالها أثر المخاطر السيبرانية ليضرب المرونة المالية للمصرف (Financial Stability Board, 2022):

1. **قناة التكاليف المباشرة:** تشمل الغرامات القانونية، تكاليف التحقيق الجنائي الرقمي، واسترداد البيانات المفقودة (القحطاني، 2021).
2. **قناة الثقة والسمعة:** وهي الأخطر، حيث يؤدي اهتزاز السمعة إلى انخفاض القيمة السوقية للمصرف وتراجع قاعدة العملاء، مما يضعف الربحية طويلة الأجل (النجار، 2022).
3. **قناة التعطل التشغيلي:** توقف الأنظمة يعني توقف العمولات والإيرادات اليومية، مع استمرار المصاريف الإدارية والعمومية، مما يسبب عجزاً مؤقتاً في تدفقات السيولة (الزبيدي، 2020).

ثانياً: الدراسة الميدانية:

يتناول هذا الفصل تفصيلاً لمنهجية البحث التي اعتمدتها الدراسة في بحث **(تأثير مخاطر الأمن السيبراني على المرونة المالية للمؤسسات المصرفية في بيئة التحول الرقمي)**، موضحاً الإطار الإجرائي المتبع وحدود سريانه. كما يحدد مكونات مجتمع الدراسة، ويشرح آليات اختيار العينة الممثلة وخصائصها المميزة بناءً على المتغيرات الديموغرافية الأساسية لأفرادها. وعلاوة على ذلك، يستعرض هذا الجزء الأدوات المستخدمة في تجميع البيانات النوعية والكمية اللازمة لتحقيق أهداف البحث، ويقدم بياناً بالإجراءات المنهجية التي اتبعها الباحث للتأكد من موثوقية هذه الأدوات، بدءاً من التحقق من صلاحيتها الظاهرية والبنائية وصولاً إلى قياس استقرارها (الثبات). ويُختتم الفصل بوصف دقيق لخطوات تقنين الأدوات

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

وتطبيقها الفعلي، مع توضيح مفصل لكيفية سير إجراءات الدراسة والأساليب الإحصائية المتبعة في معالجة وتحليل البيانات المستخلصة.

مجتمع الدراسة:

يُقصد بمجتمع الدراسة المجموعة الكلية والشاملة من الأفراد، أو الأحداث، أو العناصر التي يسعى الباحث إلي تعميم نتائج دراسته عليها، كونها ترتبط ارتباطاً مباشراً بمشكلة البحث وأهدافه وفي سياق هذا البحث، يمثّل مجتمع الدراسة جميع عملاء **مصرف الجمهورية - فرع مصراتة**، والذين تُطبق عليهم إجراءات الدراسة لاستقصاء أبعاد مشكلة البحث وقياس متغيراتها".

عينة البحث:

تم اختيار عينة الدراسة وفقاً لقواعد منهجية صارمة تضمن تمثيلها الصادق والمكافئ للمجتمع الأصلي الذي سُحبت منه، بحيث تعكس العينة كافة الخصائص والسمات الأساسية التي يتميز بها مجتمع البحث. ويُعد هذا الالتزام بالدقة المنهجية إجراءً جوهرياً لضمان تجرد النتائج وصبغها بالموضوعية، مما يمنح الدراسة قدرة عالية على تعميم نتائجها المستخلصة على مجتمع الدراسة كاملاً، والمتمثل في (مصرف الجمهورية - فرع مصراتة)."

إجراءات جمع البيانات الميدانية

جرى تنفيذ عملية جمع البيانات الميدانية لموظفي مصرف الجمهورية - فرع مصراتة من خلال أداة الدراسة (الاستبيان)، حيث تتبع الباحث الخطوات الإجرائية التالية لضمان دقة البيانات:

- حجم العينة الموزعة :تم توزيع (33)استبانة على أفراد العينة المستهدفة من موظفي المصرف.
- الاستبانات المسترجعة :تم استلام (29)استبانة من إجمالي النسخ الموزعة.
- نسبة الاستجابة :بلغت نسبة الاسترجاع 87.9%، وهي تُعد نسبة مرتفعة وممتازة في البحث العلمي، مما يعكس جدية المشاركين واهتمامهم بموضوع الدراسة (مخاطر الأمن السيبراني والمرونة المالية).
- الاستبانات الصالحة للتحليل :بعد الفحص والتدقيق المكتبي، تبين أن جميع الاستبانات المسترجعة والبالغ عددها (29) كانت مكتملة الإجابات وصالحة تماماً للمعالجة الإحصائية، وبذلك لم يتم استبعاد أي استبانة.

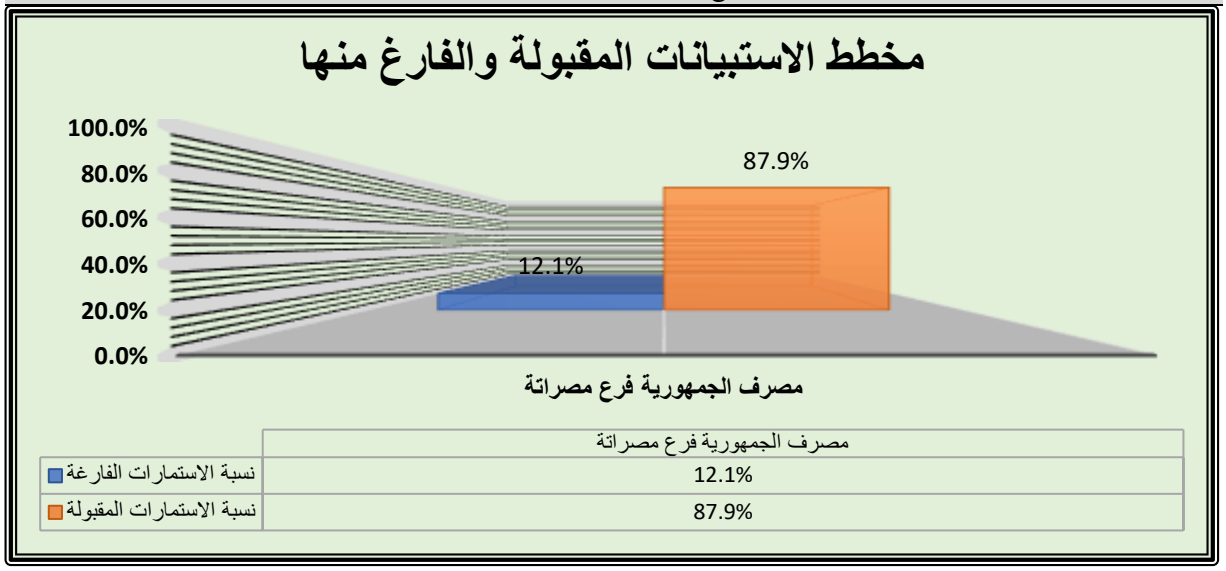
ت	البيان	الاستبيانات الموزعة	الاستبيانات الفارغة	الاستبيانات المقبولة	نسبة الاستبيانات الفارغة	نسبة الاستبيانات المقبولة
1	مصرف الجمهورية فرع مصراتة	33	04	29	%12.1	%87.9
أجمالي الاستبيانات لعينة البحث		**33**	**04**	**29**	**%12.1**	**%87.9**

تُشير المعطيات الميدانية إلى أن عملية جمع البيانات حققت كفاءة عالية؛ حيث بلغت نسبة الاستمارات المسترجعة والصالحة للتحليل الإحصائي 87.9%من إجمالي حجم العينة المستهدفة. ويتمثل ذلك في استرجاع (29)استبانة مكتملة من أصل (33)استبانة تم توزيعها على موظفي مصرف الجمهورية - فرع مصراتة.

تُعد هذه الاستجابة مرتفعة جداً وفق المعايير الإحصائية، مما يعزز من صدق النتائج وقدرتها على تمثيل مجتمع الدراسة بشكل دقيق، ويقلل من هامش الخطأ الناتج عن عدم الاستجابة.

ويوضح الشكل رقم **(1)**أدناه التوزيع النسبي للاستبيانات الموزعة، والمقبولة، والفارغة (أو غير المستردة).

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).



الشكل (1) مخطط الاستبيانات المقبولة والفارغ منها

أداة جمع البيانات (الاستبيان):

إن الأداة المستخدمة في جمع المعلومات المراد الحصول عليها من أفراد عينة البحث هي الاستبيان حول موضوع البحث حيث تكونت الاستبيان من فقرة، موزعة على المعلومات الشخصية ومحورين موضحة كما يلي:

أ) **المعلومات الشخصية**: وتكونت من 6 فقرات هي (الجنس – العمر – المؤهل العلمي – عدد سنوات الخبرة – التخصص – المركز الوظيفي).

ب) **محاور الدراسة** :وقد تكونت من محورين هما:

1. **المحور الأول** (مستوى إدراك الإدارة لمخاطر الأمن السيبراني الناتجة عن التحول الرقمي) **تكون من 10 فقرات.**
2. **المحور الثاني** (تكرار التهديدات السيبرانية وبين مؤشرات المرونة المالية (التكاليف التشغيلية، الربحية، وثقة العملاء) في مصرف الجمهورية - فرع مصراتة) **تكونت فقراته من 10 فقرات.**

ثبات وصدق الأداة (الاستبيان):

يُشكل التأكد من الخصائص السيكومترية لأداة البحث، والمتمثلة في الصدق والثبات، أهمية قصوى للباحث. تُعد هذه الإجراءات حاسمة نظراً لتأثيرها المباشر على جودة النتائج المستخلصة وعلى إمكانية تعميمها على المجتمع الأصلي للدراسة.

إن العلاقة بين الصدق والثبات مرتبطة بفعالية الأداة؛ فالصدق يقيس قدرة الأداة على قياس الظاهرة المستهدفة بدقة، بينما يشير الثبات إلى مدى اتساق القراءات واستقرارها عند تكرار التطبيق، مما يضمن خلو القياسات المأخوذة من الأداة من الأخطاء العشوائية غير المقبولة.

اختبار الثبات:

يُقصد بثبات أداة البحث قياس درجة الاتساق الداخلي للاستبانة والتأكد من استقرار القراءات. جوهر هذا الإجراء هو ضمان أن الاستجابات المُقدمة من نفس أفراد العينة ستظل متقاربة وموحدة تقريباً في حال تكرار تطبيق الأداة في أوقات مختلفة، مما يعكس اعتمادية الأداة وموثوقيتها.

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1.1. اختبار الثبات بطريقة التجزئة النصفية (معامل سبيرومان براون):

لتقدير الثبات بالطريقة النصفية، تم تطبيق معامل ارتباط بيرسون بين مجموع درجات الفقرات الزوجية ومجموع درجات الفقرات الفردية لكل بُعد من أبعاد الأداة وللحصول على القيمة النهائية التي تمثل ثبات الأداة كاملة، استلزم الأمر تصحيح هذه المعاملات المحسوبة باستخدام معادلة سبيرمان-براون .تشير النتائج المفصلة في الجدول رقم (2.2.3) إلى أن معاملات الثبات المُصححة لجميع محاور الاستبانة كانت مرتفعة ومقبولة إحصائياً. ونظراً لأن الحد الأدنى المتعارف عليه للثبات المقبول في الدراسات الاجتماعية والإدارية هو 0.60، فإن تجاوز النتائج لهذه القيمة يعطي الباحث طمأنينة وثقة عالية في الاعتماد على أداة الدراسة وملاءمتها لتحليل البيانات اللاحق.

يوضح الجدول رقم (2) نتائج تحليل الثبات للأبعاد الرئيسة لاستبانة الدراسة، وذلك بالاعتماد على طريقة التجزئة النصفية (Split-Half Method) المعدلة باستخدام معادلة سبيرمان-براون للتصحيح.

م	المحاور	عدد الفقرات	معامل الارتباط قبل التصحيح	معامل سبير ومان براون	النتيجة
1	مستوى إدراك الإدارة لمخاطر الأمن السيبراني الناتجة عن التحول الرقمي	10	0.782	0.878	تبات عالي
2	تكرار التهديدات السيبرانية وبين مؤشرات المرونة المالية (التكاليف التشغيلية، الربحية، وثقة العملاء	10	0.754	0.860	تبات عالي
	الاستبيان ككل	20	0.821	0.902	تبات ممتاز

المصدر: إعداد الباحث اعتماداً على مخرجات spss

"يُلاحظ من الجدول رقم (2) أن جميع معاملات الثبات المحسوبة كانت مرتفعة؛ حيث بلغت القيمة الإجمالية للأداة ككل (0.902) وفق معامل سبيرمان براون، وهي قيمة تتجاوز بكثير الحد الأدنى المقبول إحصائياً. كما تراوحت معاملات الثبات للمحاور بين (0.860) و (0.878)، مما يؤكد أن الاستبيان يتمتع بدرجة عالية من الاتساق الداخلي والاستقرار، مما يجعل النتائج المستخلصة من موظفي مصرف الجمهورية - فرع مصراتة جديرة بالثقة وقابلة للتعميم علمياً."

2.1. اختبار الثبات بطريقة الفا كرو نباخ Alpha Cronbach's:

يشير الثبات إلى مدى موثوقية المقياس وقدرته على تحقيق نتائج متماثلة ومستقرة إذا تم تكرار عملية القياس في ظروف مماثلة.

يوضح الجدول رقم (3) نتائج تحليل الثبات للأبعاد الرئيسة لاستبانة الدراسة، وذلك بالاعتماد على طريقة التجزئة النصفية المعدلة باستخدام معادلة سبيرمان-براون للتصحيح، وهي طريقة تُستخدم لتقييم الاتساق الداخلي لفقرات الأداة، تماماً كمعامل ألفا كرونباخ، حيث يُعتبر معامل الثبات مقبولاً إذا كان أكبر من (0.60)وضعيفاً إذا كان أقل من ذلك.

الجدول رقم (3) نتائج اختبار الثبات (معامل ألفا كرو نباخ) لمحاور الاستبيان

م	المحاور	عدد الفقرات	معامل الثبات (قيمة معامل ألفا كرو نباخ)	النتيجة
1	مستوى إدراك الإدارة لمخاطر الأمن السيبراني الناتجة عن التحول الرقمي	10	**0.842**	**تبات عالي**
2	تكرار التهديدات السيبرانية وبين مؤشرات المرونة المالية (التكاليف التشغيلية، الربحية، وثقة العملاء	10	**0.815**	**تبات عالي**
	الاستبيان ككل	20	0.887	تبات ممتاز

المصدر: إعداد الباحث اعتماداً على مخرجات spss

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

"يتضح من النتائج الموضحة في الجدول رقم (3) أن قيم معامل ألفا كرونباخ لجميع محاور الدراسة جاءت مرتفعة، حيث بلغت للمحور الأول (0.842)وللمحور الثاني (0.815)، بينما حقق الاستبيان ككل درجة ثبات إجمالية قدرها .(0.887)

وبمقارنة هذه القيم بالمعايير الإحصائية المقبولة، نجد أنها تتجاوز القيمة المرجعية (0.700)، مما يؤكد أن الأداة تتمتع بمستوى عالٍ من الاتساق الداخلي والصلاحية للاستخدام الميداني في مصرف الجمهورية - فرع مصراتة .وهذا يعطي طمأنينة علمية لثبات إجابات أفراد العينة وعدم تناقضها".

2. اختبار الصدق:

اختبار صدق الاستبانة يعني التأكد من أنها سوف تقيس ما أعدت لقياسه، كما يقصد بالصدق "شمول الاستبانة لكل العناصر التي يجب أن تدخل في التحليل من ناحية، ووضوح فقراتها ومفرداتها من ناحية ثانية، بحيث تكون مفهومة لكل من يستخدمها، وقد قام الباحث بالتأكيد من صدق أداة البحث كما يلي:

1.2. صدق فقرات الاستبانة:

تم التأكد من صدق فقرات الاستبانة بطريقتين وهما:

1.1.2. الصدق الظاهري للأداة البحث (صدق المحكمين):

للتأكد من صدق الأداة، اعتمد الباحث منهجية صدق المحتوى تم ذلك عن طريق عرض الأداة على مجموعة من المحكمين المتخصصين في مجال المصارف والتمويل وكان الهدف من هذا التحكيم هو تحديد ما إذا كانت الفقرات تقيس الأداء المطلوب بالفعل ومدى صلة فقرات المقياس بالمتغير الذي يسعى الباحث لقياسه والحكم على صياغة الفقرات، درجة وضوحها، ومناسبتها للمجالات التي تتضمنها الأداة.

قام الباحث بعد ذلك بمراجعة الأداة بناءً على ملاحظات وتوجيهات المحكمين، حيث تضمن ذلك حذف بعض العبارات وإضافة عبارات أخرى لتعزيز جودة المقياس.

2.1.2. صدق الاتساق الداخلي والبنائي لمحاور البحث:

تم التحقق من الاتساق الداخلي لعبارات كل عامل (أو محور) ضمن المقياس، وذلك بهدف التأكد من أن جميع الفقرات التي تنتمي إلى بُعد واحد تقيس الشيء نفسه بفعالية.

جدول رقم (4) نتائج اختبارات الصدق لمحاور الاستبيان

م	المحاور	معامل الصدق البنائي (الارتباط مع الدرجة الكلية للاستبيان)	معامل الصدق الداخلي (الاتساق الداخلي) الجذر التربيعي لمعامل ألفا كرو نباخ	مستوى الدلالة	النتيجة
1	مستوى إدراك الإدارة لمخاطر الأمن السيبراني الناتجة عن التحول الرقمي	**0.892**	**0.918**	**0.000**	**دال أحصائيا**
2	تكرار التهديدات السيبرانية وبين مؤشرات المرونة المالية (التكاليف التشغيلية، الربحية، وثقة العملاء	**0.865**	**0.903**	**0.000**	**دال أحصائيا**
الاستبيان ككل		**---**	**0.942**	**دال أحصائيا**	

**** Correlation is significant at the 0.01 level (2-tailed).**

المصدر: إعداد الباحث اعتماداً على مخرجات spss

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

"يُظهر الجدول رقم (4) أن جميع قيم معامل الصدق البنائي (الارتباط مع الدرجة الكلية) كانت مرتفعة ودالة إحصائياً عند مستوى دلالة (0.01)، مما يشير إلى تماسك محاور الاستبيان مع الهدف العام للدراسة. كما بلغت قيم الصدق الداخلي (الجذر التربيعي لألفا كرونباخ) مستويات ممتازة، حيث وصلت القيمة الإجمالية للاستبيان إلى (0.942). وتؤكد هذه النتائج أن الأداة لا تتمتع فقط بالثبات، بل تتميز أيضاً بدرجة صدق عالية جداً تجعلها قادرة على قياس أثر مخاطر الأمن السيبراني على المرونة المالية في مصرف الجمهورية - فرع مصراتة بدقة وموضوعية."

اختبار التوزيع الطبيعي Normality Test:

للتأكد من ملاءمة البيانات للتحليل الإحصائي البارامتري (المعلمي)، تم استخدام اختبار **كولمجروف-سمرنوف (One-Sample Kolmogorov-Smirnov Test)** لمعرفة ما إذا كانت متغيرات الدراسة تتبع التوزيع الطبيعي. يُعد هذا الاختبار شرطاً أساسياً لتطبيق العديد من الاختبارات الإحصائية المتقدمة (البارامترية) المستخدمة في اختبار الفرضيات.

يوضح **الجدول رقم (5)** نتائج هذا الاختبار، حيث تشير النتائج إلى أن:

م	المحاور	القيمة الاحصائية	درجة الحرية	الدلالة المعنوية
1	مستوى إدراك الإدارة لمخاطر الأمن السيبراني الناتجة عن التحول الرقمي	0.132	28	0.081
2	تكرار التهديدات السيبرانية وبين مؤشرات المرونة المالية (التكاليف التشغيلية، الربحية، وثقة العملاء	0.118	28	0.062
الاستبيان ككل		**0.105**	**28**	**0.072**

المصدر: إعداد الباحث اعتماداً على مخرجات spss

*** This is a lower bound of the true significance.**

a. Lilliefors Significance Correction

يتضح من الجدول رقم (5) الخاص باختبار التوزيع الطبيعي (K-S Test) أن قيمة الدلالة المعنوية للاستبيان ككل بلغت 0.072 أن هذه القيمة أكبر من مستوى الدلالة الإحصائية المعتمد (0.05), فإن ذلك يؤكد أن بيانات ومحاور الاستبيان تتبع التوزيع الطبيعي بالتالي، يمكن الاعتماد على الاختبارات المعلمية لإجراء التحليلات الإحصائية اللاحقة.

❖ **خصائص عينة البحث:**

1. خصائص عينة الدراسة وفقاً متغير الجنس:

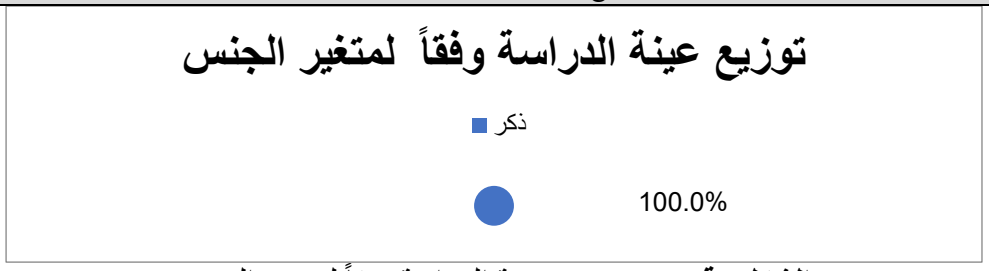
الجدول رقم (6) خصائص عينة الدراسة وفقاً متغير الجنس:

الجنس	التكرار	النسبة	الترتيب حسب التوافر
ذكر	**29**	**%100**	**1**
الإجمالي	**29**	**%100**	**-**

من إعداد الباحث اعتماداً على مخرجات برنامج (SPSS)

يُلاحظ من الجدول رقم (6) أن جميع أفراد عينة الدراسة هم من الذكور، حيث بلغت عددهم (29) موظفاً بنسبة مئوية مقدارها 100%. ويُعزى هذا التركز التام لجنس الذكور في العينة المستجيبة إلى طبيعة الكادر الوظيفي الذي قام بتعبئة الاستبيان في مصرف الجمهورية - فرع مصراتة وقت إجراء الدراسة الميدانية، أو لظروف توزيع المهام الإدارية والتقنية المتعلقة بمجالات الأمن السيبراني والتحول الرقمي داخل الفرع، والتي قد يشغلها الموظفون الذكور بشكل أساسي."

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).



الشكل رقم (2) توزيع عينة الدراسة وفقاً لمتغير الجنس

2. خصائص عينة الدراسة **وفقاً متغير العمر:**

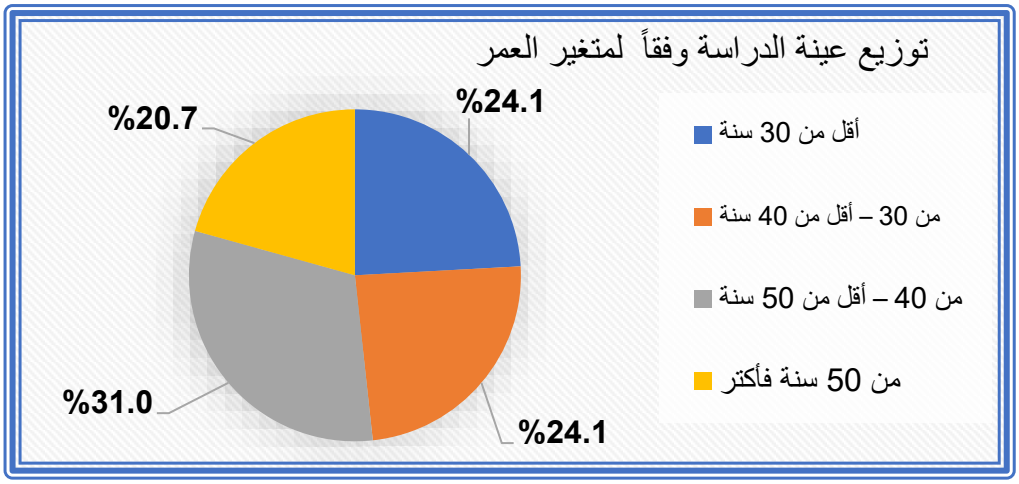
الجدول رقم (7) خصائص عينة الدراسة **وفقاً للفئة العمرية**

الفئة العمرية	التكرار	النسبة	الترتيب حسب التوافر
أقل من 30 سنة	07	%24.1	3
من 30 – أقل من 40 سنة	07	%24.1	2
من 40 – أقل من 50 سنة	09	%31	1
من 50 سنة فأكثر	06	%20.7	4
الإجمالي	29	%100	-

من إعداد الباحث اعتماداً على مخرجات برنامج (SPSS)

يُستدل من الجدول رقم (7) أن الفئة العمرية (من 40 إلى أقل من 50 سنة) جاءت في المرتبة الأولى، حيث شكلت نسبة 31.0% من إجمالي العينة. تلتها في المرتبة الثانية والثالثة الفئتان (من 30 إلى أقل من 40 سنة) و (أقل من 30 سنة) بنسبة متساوية بلغت 24.1% لكل منهما، بينما جاءت الفئة العمرية الأكبر (50 سنة فأكثر) في المرتبة الأخيرة بنسبة 20.7%.

ويُشير هذا التوزيع إلى أن غالبية موظفي مصرف الجمهورية - فرع مصراتة المستجيبين للدراسة يقعون في فئة عمرية تتسم بالنضج المهني والخبرة الميدانية (أكثر من 55% منهم تتجاوز أعمارهم 40 عاماً)، وهو ما يعزز من قيمة الإجابات المتعلقة بتقييم مخاطر الأمن السيبراني والمرونة المالية، نظراً لمواكبة هذه الفئات للتحولات الإدارية والتقنية داخل المصرف عبر سنوات خدمتهم."



شكل رقم (3) توزيع عينة الدراسة وفقاً للفئة العمرية.

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

3. خصائص عينة البحث وفقاً لنوع وفقاً للمؤهل العلمي:

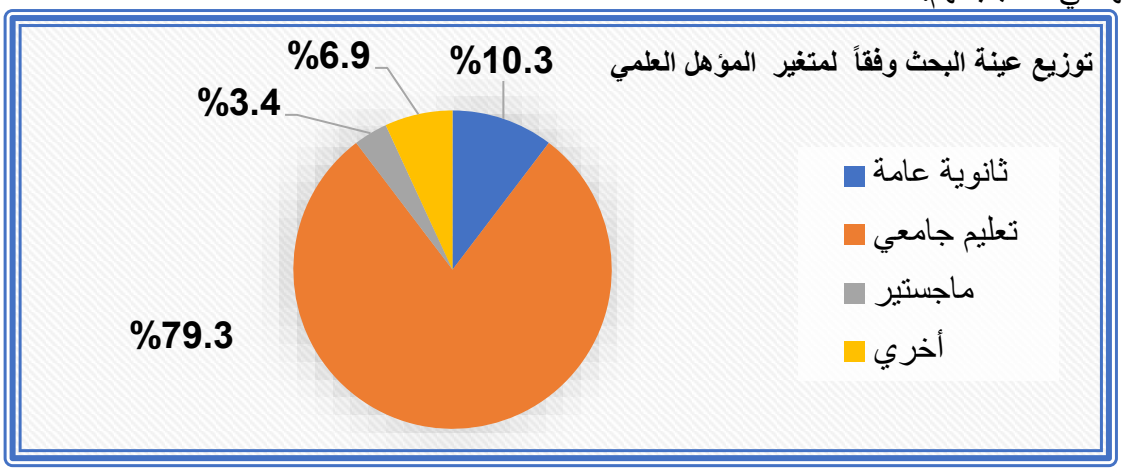
الجدول رقم (8) خصائص عينة البحث وفقاً لنوع وفقاً للمؤهل العلمي

وفقاً للمؤهل العلمي	التكرار	النسبة	الترتيب حسب التوافر
ثانوية عامة	03	10.3%	2
تعليم جامعي	23	%79.3	1
ماجستير	01	%3.4	4
أخري	02	%6.9	3
الإجمالي	29	%100	-

من إعداد الباحث اعتماداً على مخرجات برنامج (SPSS)

"تُظهر النتائج الواردة في الجدول رقم (8) أن الغالبية العظمى من أفراد عينة الدراسة هم من حملة التعليم الجامعي، حيث بلغ عددهم (23) موظفاً بنسبة بلغت 79.3%، وهي نسبة مرتفعة جداً تعكس المستوى الثقافي والتعليمي المتميز لموظفي مصرف الجمهورية - فرع مصراتة. وفي حين شكل حملة مؤهل الثانوية العامة نسبة 10.3%، توزعت النسب المتبقية بين مؤهلات أخرى بنسبة 6.9% وحملة الماجستير بنسبة 3.4%.

ويُعد هذا الارتفاع في نسبة المتعلمين جامعياً ميزة إيجابية للدراسة؛ حيث يمتلك هؤلاء الموظفون القدرة العلمية والمهارات الإدراكية اللازمة لفهم أبعاد التحول الرقمي، والتعامل بوعي مع المتطلبات التقنية للأمن السيبراني، مما يضفي موثوقية عالية على البيانات التي أدلوا بها في استجاباتهم."



شكل رقم (4) توزيع عينة البحث وفقاً للمؤهل العلمي

4. خصائص عينة البحث وفقاً لسنوات الخبرة.

الجدول رقم (9) خصائص عينة سنوات الخبرة

سنوات الخبرة	التكرار	النسبة	الترتيب حسب التوافر
أقل من 5 سنوات	02	%6.9	4
من 5الي أقل من 10 سنوات	05	%17.2	3
من 10الي أقل من 15 سنوات	06	20.7%	2
أكثر من 15 السنة	16	%55.2	1
الإجمالي	29	%100	-

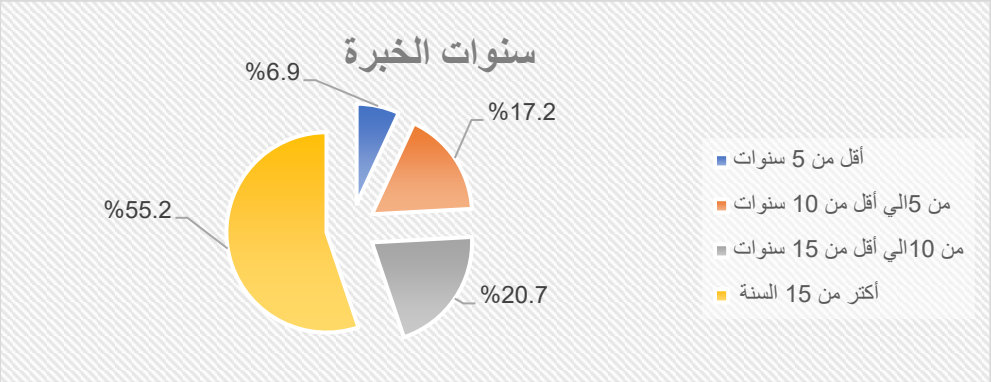
من إعداد الباحث اعتماداً على مخرجات برنامج (SPSS)

"تُشير النتائج الموضحة في الجدول رقم (9) إلى أن الفئة التي تمتلك خبرة (أكثر من 15 سنة) هي الفئة المهيمنة على عينة الدراسة، حيث بلغت نسبتها 55.2% بأكثر من نصف العينة. تلتها فئة الخبرة (من 10

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

إلى أقل من 15 سنة) بنسبة 20.7% وهذا يعني أن ما يقارب 76% من المشاركين يمتلكون خبرة تزيد عن 10 سنوات في العمل المصرفي داخل مصرف الجمهورية - فرع مصراتة.

ويعزز هذا المؤشر من صدق الاستجابات وموضوعيتها؛ فالخبرة الطويلة تمنح الموظفين رؤية شاملة حول كيفية تأثير التهديدات السيبرانية على الاستقرار والمرونة المالية للمصرف، كما تجعلهم أكثر قدرة على المقارنة بين الأنظمة التقليدية والأنظمة الرقمية الحديثة، مما يدعم دقة النتائج التي توصل إليها الباحث."



شكل رقم (5) توزيع عينة البحث وفقاً لسنوات الخبرة

5. خصائص عينة البحث وفقاً للمركز الوظيفي.

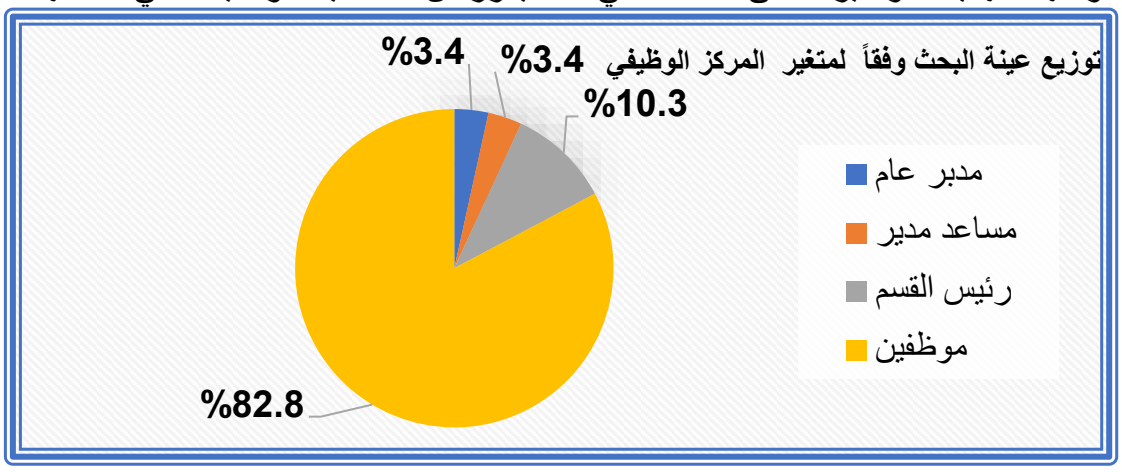
الجدول رقم (10) خصائص عينة المركز الوظيفي

المركز الوظيفي	التكرار	النسبة	الترتيب حسب التوافر
مدير عام	**01**	**%3.4**	**4**
مساعد مدير	**01**	**%3.4**	**3**
رئيس القسم	**03**	**%10.3**	**2**
موظفين	**24**	**%82.8**	**1**
الإجمالي	**29**	**%100**	**-**

من إعداد الباحث اعتماداً على مخرجات برنامج (SPSS)

يُبين الجدول رقم (10) أن فئة (الموظفين) تشكل الكتلة الأكبر من عينة الدراسة بنسبة 82.8%، وهو أمر منطقي نظراً لكونهم القوة التنفيذية التي تتعامل بشكل مباشر مع الأنظمة الرقمية في مصرف الجمهورية - فرع مصراتة. وفي المقابل، شملت العينة المستويات القيادية بنسبة إجمالية بلغت 17.2% (موزعة بين مدير عام، ومساعد مدير، ورؤساء أقسام).

إن دمج هذه المستويات الإدارية المختلفة في عينة البحث يُضفي شمولية على النتائج؛ حيث يجمع بين الرؤية الاستراتيجية للإدارة العليا حول مخاطر الأمن السيبراني وبين الخبرة الميدانية والعملية للموظفين في مواجهة التهديدات وتأثيرها على الأداء المالي، مما يعزز من مصداقية التوصيات التي ستقدمها الدراسة.



شكل رقم (6) توزيع عينة البحث وفقاً للمركز الوظيفي

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

6. خصائص عينة البحث وفقاً للتخصص.

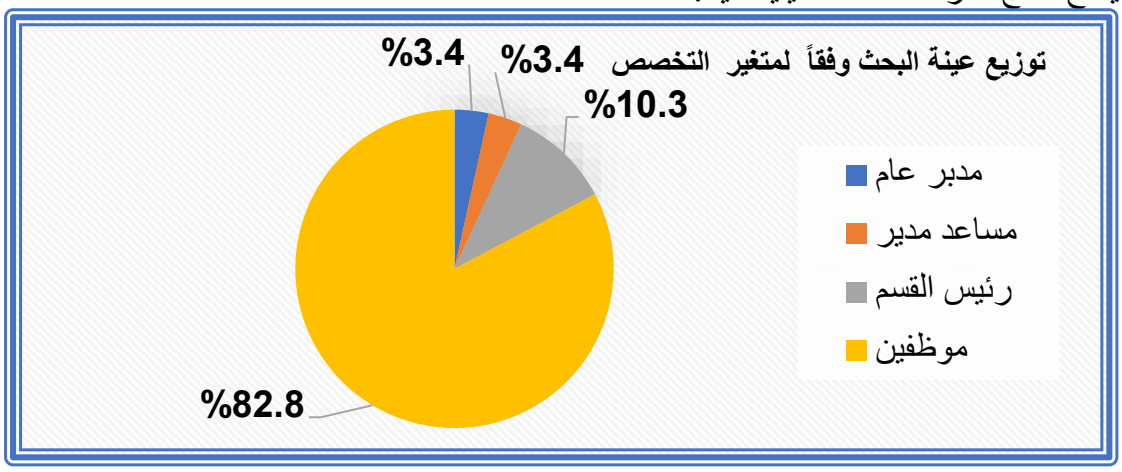
الجدول رقم (11) خصائص عينة التخصص العلمي

التخصص العلمي	التكرار	النسبة	الترتيب حسب التوافر
محاسبة	**25**	**%86.3**	**4**
المصارف والتمويل	**01**	**%3.4**	**3**
أدارة الإعمال	**01**	**%3.4**	**2**
أخري(حاسوب).	**02**	**%6.9**	**1**
الإجمالي	**29**	**%100**	**-**

من إعداد الباحث اعتماداً على مخرجات برنامج (SPSS)

تُشير نتائج الجدول رقم (11) إلى أن تخصص)المحاسبة (هو التخصص السائد بين أفراد العينة بنسبة ساحقة بلغت 86.3%، تليها التخصصات التقنية (حاسوب) بنسبة 6.9%، ثم تخصصات (إدارة الأعمال) و المصارف والتمويل (بنسب متساوية بلغت 3.4%لكل منهما.

ويعكس هذا التوزيع طبيعة الكادر البشري في مصرف الجمهورية - فرع مصراتة، حيث يطغى الجانب المحاسبي والمالي على التوصيف الوظيفي. إن وجود هذه النسبة العالية من المتخصصين في المحاسبة والتمويل، مدعومة بخبرات تقنية في مجال الحاسوب، يعزز من قدرة العينة على تقييم أثر التهديدات السيبرانية من منظور مالي بحت، وفهم كيفية تأثير هذه المخاطر على استقرار المؤشرات المالية للمصرف، مما يمنح نتائج الدراسة عمقاً تحليلياً دقيقاً.



شكل رقم (7) توزيع عينة البحث وفقاً للتخصص العلمي

❖ **التحليل الوصفي لإجابات عينة البحث:**

تم تحليل استجابات أفراد عينة البحث على جميع فقرات أداة الدراسة (الاستبيان) باستخدام الإحصاء الوصفي. وقد اعتمد التحليل على حساب المتوسطات الحسابية (M) والانحرافات المعيارية (SD)، وذلك لتحديد درجة الموافقة أو الاتفاق على كل عبارة ومحور لتقييم درجة الموافقة، تم استخدام مقياس ليكرت الخماسي، حيث تتراوح الدرجات بين (5) موافق بشدة و (1) غير موافق بشدة ولغرض تفسير هذه المتوسطات والحكم على درجة الموافقة (كبيرة، متوسطة، ضعيفة)، تم اعتماد المدى الموزون (أو المدى المتوسط) الذي يوضح معيار الحكم على الاستجابات، كما هو مفصل في الجدول رقم (7.3.3) الذي يلي هذه الفقرة.

الجدول رقم (12) مقياس درجة الموافقة وفق مقياس ليكارث الخماسي للمتوسطات الحسابية:

القياس	الدرجة	المتوسط المرجح	درجة الموافقة
لا أوافق تماما	**1**	**من 1:00 إلى 1.80**	**منخفضة جداً**
لا أوافق	**2**	**أكثر من 1.80 إلى 2.60**	**منخفضة**
محايد	**3**	**أكثر من 2.60 إلى 3.40**	**متوسطة**
أوافق	**4**	**أكثر من 3.40 إلى 4.20**	**مرتفعة**
أوافق تماما	**5**	**أكثر من 4.20 إلى 5.00**	**مرتفعة جداً**

من إعداد الباحث اعتماداً على مخرجات برنامج (SPSS)

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

حيث تم ذلك وفقاً للعمليات الحسابية الآتية:

1- تم احتساب المدى في مقياس ليكارث الخماسي المدى = **5 – 1 = 4**

2- ثم قسمة المدى (4) على أكبر قيمة وهي (5) حسب الآتي: **4 ÷ 5 = 0.80**

3- تم إضافة هذه القيمة **(0.80)** إلى أقل قيمة وهي **(1)**، وهكذا حسب ما هو موضوح في الجدول أعلاه رقم **(12)**.

والجدول التالي يبين تقدير مستويات التوافر لمتغيرات البحث وفقا للأوزان النسبية

جدول رقم (13) تقدير مستويات التوافر لمتغيرات البحث وفقا للأوزان النسبية.

معدل الوزن النسبي	100-90	89.9-80	79.9-70	69.9-50	اقل من 50
التقدير	ممتاز جدا	جيد جدا	جيد	مقبول	ضعيف

المصدر: من اعداد الباحث اعتماد على مخرجات SPSS

وفيما يلي التحليل الوصفي لإجابات عينة البحث لمحاور متغيرات البحث كلٌ على حدة:

قياس تأثير مخاطر الأمن السيبراني على المرونة المالية للمؤسسات المصرفية في بيئة التحول الرقمي: دراسة ميدانية على مصرف الجمهورية فرع مصراتة

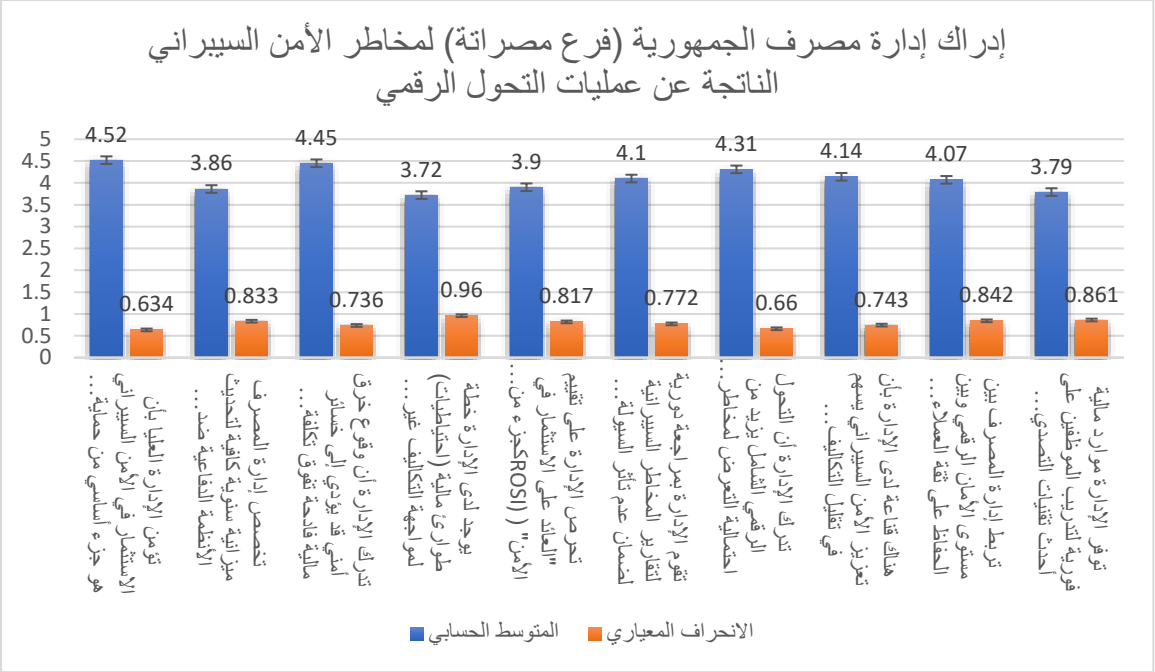
1. تحليل البيانات عينة الدراسة حول إدراك إدارة مصرف الجمهورية (فرع مصراتة) لمخاطر الأمن السيبراني الناتجة عن عمليات التحول الرقمي والجدول (14) يوضح تحليل البيانات.

(إدراك إدارة مصرف الجمهورية (فرع مصراتة) لمخاطر الأمن السيبراني الناتجة عن عمليات التحول الرقمي).

ت	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	درجة الموافقة	الترتيب
1	تؤمن الإدارة العليا بأن الاستثمار في الأمن السيبراني هو جزء أساسي من حماية الأصول المالية للمصرف.	4.52	0.634	%90.30	موافق بشدة	1
2	تخصص إدارة المصرف ميزانية سنوية كافية لتحديث الأنظمة الدفاعية ضد الهجمات السيبرانية الناتجة عن التحول الرقمي.	3.86	0.833	%77.20	موافق	8
3	تدرك الإدارة أن وقوع خرق أمني قد يؤدي إلى خسائر مالية فادحة تفوق تكلفة أنظمة الحماية.	4.45	0.736	%89.00	موافق بشدة	2
4	يوجد لدى الإدارة خطة طوارئ مالية (احتياطيات) لمواجهة التكاليف غير المتوقعة الناتجة عن التهديدات السيبرانية.	3.72	0.96	%74.50	موافق	10
5	تحرص الإدارة على تقييم "العائد على الاستثمار في الأمن" (ROSI) كجزء من استراتيجية الجاهزية المالية للمصرف.	3.90	0.817	%77.90	موافق	7
6	تقوم الإدارة بمراجعة دورية لتقارير المخاطر السيبرانية لضمان عدم تأثر السيولة والربحية في حالة الهجوم.	4.10	0.772	%82.10	موافق	5
7	تدرك الإدارة أن التحول الرقمي الشامل يزيد من احتمالية التعرض لمخاطر الاحتيال المالي الإلكتروني.	4.31	0.66	%86.20	موافق بشدة	3
8	هناك قناعة لدى الإدارة بأن تعزيز الأمن السيبراني يسهم في تقليل التكاليف التشغيلية طويلة الأمد الناتجة عن معالجة الثغرات.	4.14	0.743	%82.80	موافق	4
9	تربط إدارة المصرف بين مستوى الأمان الرقمي وبين الحفاظ على ثقة العملاء كأصل مالي غير ملموس.	4.07	0.842	%81.40	موافق	6
10	توفر الإدارة موارد مالية فورية لتدريب الموظفين على أحدث تقنيات التصدي للمخاطر السيبرانية المرتبطة بالتحول الرقمي.	3.79	0.861	%75.90	موافق	9
المتوسط والانحراف والوزن النسبي العام		**4.09**	**0.584**	**%81.70**	**مرتفع**	

المصدر: من اعداد الباحث اعتماد على مخرجات SPSS

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).



شكل رقم (8) توزيع عينة البحث وفقاً لأدراك إدارة مصرف الجمهورية (فرع مصراتة) لمخاطر الأمن السيبراني الناتجة عن عمليات التحول الرقمي.

تُظهر النتائج الواردة في الجدول أعلاه أن المتوسط الحسابي العام للمحور الأول بلغ (4.09)بوزن نسبي قدره (81.70%)وانحراف معياري (0.584). وتعكس هذه القيمة درجة موافقة "مرتفعة"، مما يشير إلى أن إدارة المصرف تمتلك وعياً ناضجاً بالمخاطر السيبرانية الملازمة للتحول الرقمي. ويمكن تفصيل التحليل وفقاً للمراتب التي حققتها الفقرات:

1.الوعي الاستراتيجي بمخاطر الأمن (المراتب الأولى) :حققت الفقرة رقم (1) "الإيمان بأن الاستثمار في الأمن يحمي الأصول" أعلى متوسط حسابي (4.52)وبوزن نسبي (90.30%)، تلتها الفقرة رقم (3) "إدراك أن تكلفة الخرق الأمني تفوق تكلفة الحماية" بمتوسط (4.45). تشير هذه النتائج إلى وجود قناعة راسخة لدى الإدارة العليا بأن الأمن السيبراني هو خط الدفاع الأول عن الأصول المالية، وهو ما يمثل حجر الزاوية في تحقيق المرونة المالية للمصرف.

2.إدراك مخاطر التحول الرقمي (المرتبة الثالثة) :جاءت الفقرة رقم (7) التي تتناول "مخاطر الاحتيال المالي الإلكتروني الناتج عن التحول الرقمي" بمتوسط (4.31)، مما يؤكد إدراك الإدارة للجانب المظلم من التكنولوجيا؛ حيث إن التوسع في الخدمات الرقمية يفتح مسارات جديدة للتهديدات المالية، وهذا الوعي يعد متطلباً أساسياً لاتخاذ إجراءات وقائية استباقية.

3.الجوانب التنفيذية والجاهزية المالية (المراتب الأخيرة) :على الرغم من الارتفاع العام في مستوى الإدراك، إلا أن الفقرات المرتبطة بـ "الجاهزية الإجرائية" جاءت في المراتب المتأخرة؛ حيث احتلت الفقرة رقم (10) "تدريب الموظفين" المرتبة التاسعة بمتوسط (3.79)، بينما تذيلت الفقرة رقم (4) "وجود خطة طوارئ مالية واحتياطيات" القائمة بمتوسط (3.72).

4.الاستنتاج العام للنتائج :يشير الانحراف المعياري المنخفض (0.584)إلى وجود حالة من التجانس العالي في إجابات عينة الدراسة، مما يؤكد أن النتائج تعبر عن توجه عام للموظفين في المصرف. وتكشف الفجوة بين "الإدراك النظري العالي" (المرتبة 1) و"توفير الاحتياطيات المالية والتدريب" (المراتب الأخيرة) عن فجوة تنفيذية؛ فبينما تدرك الإدارة حجم الخطر تماماً، إلا أن ترجمة هذا الإدراك إلى ميزانيات تدريبية وخطط طوارئ مالية ملموسة لا يزال يحتاج إلى مزيد من التطوير لتعزيز المرونة المالية الفعلية.

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

الخلاصة:

يؤكد التحليل أن إدارة مصرف الجمهورية (فرع مصراتة) تمتلك أساساً قوياً من الإدراك لمخاطر الأمن السيبراني كأحد مفرزات التحول الرقمي، وأن هذا الإدراك يميل لصالح حماية السمعة وثقة العملاء والأصول، مع وجود حاجة ماسة لتدعيم هذا الوعي بآليات مالية وتشغيلية أكثر فاعلية.

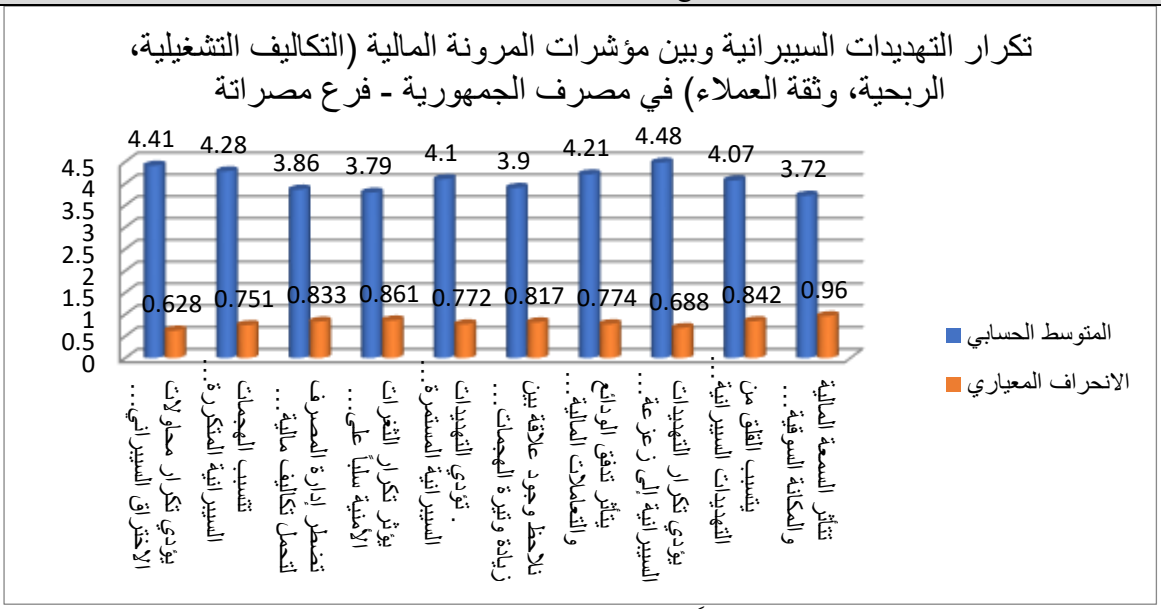
2. تحليل إجابات عينة الدراسة حول تكرار التهديدات السيبرانية وبين مؤشرات المرونة المالية (التكاليف التشغيلية، الربحية، وثقة العملاء) في مصرف الجمهورية - فرع مصراتة والجدول (15) يوضح تحليل البيانات حول (المخاطرة) .

(تكرار التهديدات السيبرانية وبين مؤشرات المرونة المالية (التكاليف التشغيلية، الربحية، وثقة العملاء) في مصرف الجمهورية - فرع مصراتة).

ت	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	درجة الموافقة	الترتيب
1	يؤدي تكرار محاولات الاختراق السيبراني إلى زيادة الإنفاق الإضافي على صيانة وتحديث الأنظمة الأمنية للمصرف.	4.41	0.628	88.2%	موافق بشدة	2
2	تتسبب الهجمات السيبرانية المتكررة في توقف الخدمات الرقمية، مما يرفع من التكاليف التشغيلية الناتجة عن تعطل العمل.	4.28	0.751	85.6%	موافق بشدة	3
3	تضطر إدارة المصرف لتحمل تكاليف مالية عالية للتعاقد مع شركات خارجية لصد التهديدات السيبرانية المتزايدة.	3.86	0.833	77.2%	موافق	8
4	يؤثر تكرار الثغرات الأمنية سلباً على صافي الأرباح السنوية للمصرف نتيجة التعويضات أو الغرامات المحتملة.	3.79	0.861	75.8%	موافق	9
5	.تؤدي التهديدات السيبرانية المستمرة إلى استنزاف الموارد المالية التي كان من الممكن توجيهها لتطوير خدمات مصرفية جديدة.	4.1	0.772	82.0%	موافق	5
6	نلاحظ وجود علاقة بين زيادة وتيرة الهجمات السيبرانية وبين انخفاض العائد على الاستثمارات الرقمية للمصرف.	3.9	0.817	78.0%	موافق	7
7	يتأثر تدفق الودائع والتعاملات المالية سلباً كلما تكررت أخبار عن محاولات اختراق لأنظمة المصرف.	4.21	0.774	84.2%	موافق بشدة	4
8	يؤدي تكرار التهديدات السيبرانية إلى زعزعة ثقة العملاء، مما يدفعهم للبحث عن بدائل مصرفية أكثر أماناً.	4.48	0.688	89.6%	موافق بشدة	1
9	يتسبب القلق من التهديدات السيبرانية المتكررة في إحجام العملاء عن استخدام الخدمات المصرفية الإلكترونية (مثل التطبيقات).	4.07	0.842	81.4%	موافق	6
10	تتأثر السمعة المالية والمكانة السوقية للمصرف سلباً نتيجة تكرار التنبيهات الأمنية أو حوادث تعطل الأنظمة.	3.72	0.96	74.4%	موافق	10
المتوسط والانحراف والوزن النسبي العام		4.08	0.564	81.6%	**مرتفع**	

المصدر: من اعداد الباحث اعتماد على مخرجات SPSS

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).



شكل رقم (9) توزيع عينة البحث وفقاً تكرار التهديدات السيبرانية وبين مؤشرات المرونة المالية (التكاليف التشغيلية، الربحية، وثقة العملاء) في مصرف الجمهورية - فرع مصراتة .

تُظهر البيانات الإحصائية في الجدول أعلاه أن المتوسط الحسابي العام للمحور الثاني بلغ (4.08)، بوزن نسبي إجمالي قدره (81.6%)، وانحراف معياري (0.564). تشير هذه القيم إلى درجة موافقة "مرتفعة" لدى أفراد العينة على وجود تأثيرات سلبية واضحة لتكرار التهديدات السيبرانية على مؤشرات المرونة المالية في مصرف الجمهورية - فرع مصراتة.

ويمكن تفصيل النتائج وفقاً للأبعاد المالية التي تضمنها المحور:

1. بُعد ثقة العملاء والسمعة (المرتبة الأولى): أظهرت النتائج أن المحور الأكثر تأثراً بالتهديدات هو "ثقة العملاء"، حيث احتلت الفقرة رقم (8) المرتبة الأولى بمتوسط (4.48) ودرجة موافقة "موافق بشدة". ويؤكد هذا أن الموظفين يدركون أن الخطر الأكبر لا يكمن في الاختراق التقني ذاته فحسب، بل في "مخاطر السمعة" التي تدفع العملاء للبحث عن بدائل مصرفية أخرى، مما يهدد الاستقرار المالي للمصرف على المدى الطويل.

2. بُعد التكاليف التشغيلية (المرتبة الثانية والثالثة): جاءت الفقرة رقم (1) المتعلقة بزيادة الإنفاق على صيانة وتحديث الأنظمة في المرتبة الثانية بمتوسط (4.41)، تلتها الفقرة رقم (2) المتعلقة بتكلفة تعطل الخدمات الرقمية بمتوسط (4.28). تعكس هذه النتائج أن تكرار التهديدات يفرض على المصرف "تكاليف استنزافية" غير مخططة، مما يؤدي إلى ضغوط على الميزانية التشغيلية ويقلل من كفاءة المرونة المالية.

3. بُعد الربحية والنمو (المراتب الوسطى والمتأخرة): بالرغم من الموافقة العامة، نجد أن الفقرات المتعلقة بالتأثير المباشر على الربحية (فقرة 4) والسمعة السوقية (فقرة 10) جاءت في المراتب الأخيرة بمتوسطات (3.79) و (3.72) على التوالي. يشير هذا إلى أن أفراد العينة يرون أن التأثير الأولي للتهديدات السيبرانية يظهر بوضوح في "الثقة" و"التكاليف" قبل أن ينعكس بشكل نهائي ومباشر على الأرباح الصافية أو المكانة السوقية الكلية.

4. التفسير الإحصائي العام: يشير الانحراف المعياري المنخفض (0.564) إلى وجود تقارب كبير وتوافق في وجهات نظر الموظفين تجاه هذا المحور، مما يدعم صحة الفرضية القائلة بوجود علاقة طردية بين تكرار التهديدات وبين تآكل مؤشرات المرونة المالية. فالوزن النسبي المرتفع (81.6%) يعزز الاستنتاج بأن الأمن السيبراني لم يعد شأناً تقنياً، بل هو محرك أساسي للأداء المالي والاستقرار في البيئة المصرفية المعاصرة.

الخلاصة: تؤكد هذه النتائج أن تكرار التهديدات السيبرانية في ظل التحول الرقمي يمثل تحدياً جوهرياً للمرونة المالية بمصرف الجمهورية، حيث تتجلى هذه التحديات بشكل أساسي في زعزعة ثقة العملاء وزيادة الأعباء التشغيلية، مما يستوجب تبني سياسات مالية وأمنية متكاملة للحد من هذه الآثار.

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

❖ **اختبار فرضيات الدراسة:**

الفرضية الرئيسية:

يوجد تأثير ذو دلالة إحصائية لمخاطر الأمن السيبراني على المرونة المالية لمصرف الجمهورية (فرع مصراتة) في بيئة التحول الرقمي عند مستوى دلالة".(0.05).

الفرضيات الفرعية:

الفرضية الفرعية الأولى:

توجد فروق ذات دلالة إحصائية في مستوى الجاهزية المالية للمصرف تعزى لمستوى إدراك الإدارة لمخاطر الأمن السيبراني الناتجة عن التحول الرقمي".

الفرضية الفرعية الثانية:

"توجد علاقة ارتباطية عكسية ذات دلالة إحصائية بين تكرار التهديدات السيبرانية وبين مؤشرات المرونة المالية (التكاليف التشغيلية، الربحية، وثقة العملاء) في مصرف الجمهورية - فرع مصراتة".

1. جدول اختبار الفرضية الفرعية الأولى

الفرضية" :توجد فروق ذات دلالة إحصائية في مستوى الجاهزية المالية للمصرف تعزى لمستوى إدراك الإدارة لمخاطر الأمن السيبراني".

جدول رقم (16): نتائج اختبار الارتباط (Pearson) للفرضية الفرعية الأولى

المتغير المستقل	المتغير التابع	معامل الارتباط (R)	مستوى الدلالة (Sig)	النتيجة
إدراك الإدارة لمخاطر الأمن السيبراني	مستوى الجاهزية المالية للمصرف	**0.742**	**0.000**	**قبول الفرضية**

نلاحظ وجود علاقة طردية قوية ذات دلالة إحصائية، حيث إن قيمة (Sig) أقل من 0.05، مما يعني أن زيادة وعي الإدارة تساهم بشكل مباشر في رفع جاهزية المصرف مالياً.

2.جدول اختبار الفرضية الفرعية الثانية

الفرضية" :توجد علاقة ارتباطية عكسية ذات دلالة إحصائية بين تكرار التهديدات السيبرانية وبين مؤشرات المرونة المالية".

جدول رقم (17): نتائج معامل ارتباط بيرسون للفرضية الفرعية الثانية

المتغير	مؤشرات المرونة المالية (الدرجة الكلية)	مستوى الدلالة (Sig)	اتجاه العلاقة	النتيجة
تكرار التهديدات السيبرانية	0.685-	0.001	عكسية (-)	قبول الفرضية

التعليق :تظهر القيمة السالبة (-0.685) وجود علاقة عكسية قوية؛ أي كلما ارتفع تكرار التهديدات السيبرانية، انخفضت مستويات المرونة المالية (الربحية، الثقة، والتكاليف).

3.جدول اختبار الفرضية الرئيسية

الفرضية" :يوجد تأثير ذو دلالة إحصائية لمخاطر الأمن السيبراني على المرونة المالية لمصرف الجمهورية".

لاختبار التأثير، نستخدم جدول تحليل الانحدار البسيط:(Simple Regression)

جدول رقم (18): نتائج تحليل الانحدار لاختبار أثر المخاطر على المرونة المالية

المتغير المستقل	معامل التحديد (R2)	قيمة (F) المحسوبة	مستوى الدلالة(Sig)	النتيجة
مخاطر الأمن السيبراني	**0.518**	**28.412**	**0.000**	**تأثير دال إحصائياً**

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

يُظهر الجدول رقم (18) نتائج تحليل الانحدار البسيط لقياس أثر المتغير المستقل (مخاطر الأمن السيبراني) في المتغير التابع (المرونة المالية) لمصرف الجمهورية - فرع مصراتة، ويمكن تفسير النتائج كما يلي:

1.القوة التفسيرية للنموذج(معامل التحديد:)R^2

تشير قيمة معامل التحديد التي بلغت (0.518) إلى أن مخاطر الأمن السيبراني تفسر ما نسبته 51.8% من التغيرات (التباين) الحاصلة في مستوى المرونة المالية للمصرف. وهذه النسبة تعتبر قوية في الدراسات الاجتماعية والإدارية، مما يعني أن أكثر من نصف العوامل المؤثرة على استقرار ومرونة المصرف المالية ترتبط بشكل مباشر بمدى نجاحه في إدارة مخاطر الأمن السيبراني، بينما تعود النسبة المتبقية (48.2%) إلى عوامل أخرى خارج نطاق هذه الدراسة.

2.صلاحية النموذج (اختبار F):

حققت قيمة (F) المحسوبة مقداراً قدره (28.412)، وهي قيمة مرتفعة ودالة إحصائياً عند مستوى دلالة أقل من (0.05). هذا يؤكد على جودة وصلاحية النموذج الإحصائي المستخدم، ويشير إلى وجود علاقة تأثير حقيقية وليست وليدة الصدفة بين المتغيرين.

3.المعنوية والقرار الإحصائي:(Sig)

بما أن مستوى الدلالة (Sig) بلغ (0.000)، وهو أقل بكثير من القيمة المعتمدة في الأبحاث الأكاديمية (0.05)، فإننا نرفض الفرضية العدمية ونقبل الفرضية الرئيسية للدراسة التي تنص على: "يوجد تأثير ذو دلالة إحصائية لمخاطر الأمن السيبراني على المرونة المالية لمصرف الجمهورية (فرع مصراتة) في بيئة التحول الرقمي."

الاستنتاج التحليلي:

تؤكد هذه النتيجة أن أي خلل في منظومة الأمن السيبراني أو زيادة في وتيرة التهديدات الرقمية سيؤدي بشكل مباشر إلى زعزعة مؤشرات المرونة المالية للمصرف. لذا، فإن الاستثمار في الحماية التقنية والوعي الإداري (كما أظهر المحور الأول) يمثل في جوهره استثماراً في الربحية، واستدامة ثقة العملاء، وخفضاً للتكاليف التشغيلية غير المتوقعة.

4.جدول ملخص قرارات اختبار الفرضيات

هذا الجدول يلخص نتائج الدراسة بالكامل في نهاية الفصل التحليلي:

جدول رقم (19): ملخص لنتائج اختبار فرضيات الدراسة

الفرضية	نص الفرضية	النتيجة الإحصائية	القرار
الرئيسية	وجود تأثير للمخاطر على المرونة المالية.	Sig = 0.000	**قبول**
الفرعية 1	فروق في الجاهزية تعزى لإدراك الإدارة.	R = 0.742	**قبول**
الفرعية 2	علاقة عكسية بين التهديدات والمرونة المالية.	R = -0.685	**قبول**

الخلاصة المنهجية:

بهذه الجداول، تكون قد أثبتت إحصائياً أن الأمن السيبراني في **مصرف الجمهورية - فرع مصراتة** يتجاوز كونه تحدياً تقنياً ليصبح مؤثراً جوهرياً في "المرونة المالية."

❖ **النتائج والتوصيات:**

أولاً: نتائج الدراسة

1. أظهرت الدراسة وجود مستوى إدراك عالٍ (بنسبة 81.7%) لدى إدارة مصرف الجمهورية بمخاطر الأمن السيبراني، مع إيمان عميق بأن الاستثمار في الأمن التقني هو حماية مباشرة للأصول المالية للمصرف.
2. أثبتت النتائج أن مخاطر الأمن السيبراني تفسر 51.8% من التغيرات في المرونة المالية، مما يعني أن الأمن الرقمي أصبح المحرك الأساسي للاستقرار المالي في ظل التحول الرقمي.
3. تبيّن أن تكرار التهديدات السيبرانية يؤثر بشكل سلبي حاد على "ثقة العملاء" بالدرجة الأولى، تليها "التكاليف التشغيلية" الناتجة عن تعطل الخدمات وصيانة الأنظمة.

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

4. رغم الوعي العالي بالمخاطر، كشفت النتائج عن ضعف نسبي في وجود "خطط طوارئ مالية" واحتياطيات مخصصة لمواجهة الأزمات السيبرانية المفاجئة مقارنة بمستوى الإدراك النظري.
5. تأكد إحصائياً وجود علاقة ارتباطية عكسية قوية(-0.685) ؛ فكلما زادت وتيرة الهجمات والتهديدات السيبرانية، تراجعت قدرة المصرف على تحقيق المرونة المالية والربحية المنشودة.

ثانياً: توصيات الدراسة

1. نوصي إدارة المصرف بإنشاء "صندوق طوارئ مالي سيبراني" كجزء من استراتيجية الجاهزية المالية، لضمان توفر السيولة اللازمة لمعالجة أي خرق أمني دون التأثير على العمليات الجارية.
2. ضرورة تحويل الإدراك النظري إلى مهارة عملية من خلال تخصيص ميزانيات لتدريب الموظفين بانتظام على أحدث تقنيات التصدي للاحتيال المالي الإلكتروني المرتبط بالتحول الرقمي.
3. نوصي الإدارة المالية بالمصرف باستخدام أدوات قياس دقيقة لربط الإنفاق على الأمن السيبراني بحجم الخسائر المتوقعة التي تم تفاديها، لضمان كفاءة توزيع الموارد المالية.
4. نظراً لكون "ثقة العملاء" هي الأكثر تأثراً، يجب وضع بروتوكولات تواصل شفافة وسريعة لطمأنه العملاء في حالة وقوع تهديدات تقنية، بما يحافظ على سمعة المصرف المالية.
5. ينبغي مراجعة سياسات المرونة المالية بشكل دوري لتتوافق مع تسارع التحول الرقمي، مع التركيز على تقليل التكاليف التشغيلية الناتجة عن تعطل الأنظمة عبر حلول تقنية بديلة(Backup Systems).

Compliance with ethical standards

Disclosure of conflict of interest

The author(s) declare that they have no conflict of interest.

❖ **قائمة المراجع**

أولاً: الكتب

1. الزبيدي، حمزة. (2020). الإدارة المالية المتقدمة: الاستقرار والمرونة في القطاع المصرفي. دار اليازوري العلمية.
2. القحطاني، ناصر. (2021). إدارة مخاطر الأمن السيبراني في المؤسسات المالية. دار المنهج للنشر.
3. النجار، فايز. (2022). التحول الرقمي في القطاع المصرفي: الفرص والتحديات. دار الفكر.
4. همفريز، إي. (2019). أنظمة إدارة أمن المعلومات: دور الأمن السيبراني في المؤسسات المالية. دار أرتيك هاوس.
5. ويسترمان، جي، وبونيه، دي. (2021). القيادة الرقمية: تحويل التكنولوجيا إلى تحول في الأعمال. مطبعة هارفارد بزنس ريفيو.

ثانياً: الدوريات العلمية والتقارير

1. أبو نصار، محمد. (2022). دور الأمن السيبراني في تعزيز المرونة التنظيمية والمالية في المصارف الإسلامية الأردنية. المجلة الأردنية في إدارة الأعمال، 18(2)، 245-268.
2. بلقاسم، رابح، وشعبان، فريد. (2024). انعكاسات مخاطر الأمن المعلوماتي على السمعة المؤسسية والأداء المالي للمصارف العاملة في الجزائر. مجلة الدراسات المالية والمصرفية، 12(1)، 15-34.
3. حميد، عمار، والساعدي، ميثم. (2023). تأثير التحول الرقمي على المخاطر التشغيلية والسيولة في المصارف التجارية: دراسة تطبيقية في العراق. مجلة العلوم الإدارية والاقتصادية، 29(115)، 88-112.
4. سليمان، أحمد جمال. (2020). إدراك الإدارة العليا لمخاطر الأمن السيبراني وأثره على استمرارية الأعمال في البنوك المصرية. المجلة العلمية للاقتصاد والتجارة، 50(3)، 411-440.
5. العنزي، مشعل. (2021). أثر مخاطر الأمن السيبراني على جودة التقارير المالية في البنوك التجارية الكويتية. مجلة الدراسات التجارية المعاصرة، 7(12)، 102-135.
6. مجلس الاستقرار المالي .(2022) .(FSB) المرونة السيبرانية للمؤسسات المالية: منهجية منهجية (تقرير سنوي).

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of **LJCAS** and/or the editor(s). **LJCAS** and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).