



إدارة المخاطر المالية في الاقتصاد الرقمي: إطار حوكمة تكاملي لدعم الابتكار المالي الآمن والاستقرار والتنمية المستدامة في ليبيا

عبدالحكم العربي الدردير

قسم التمويل والمصارف / كلية الاقتصاد والمحاسبة مرزق / جامعة فزان

Financial Risk Management in the Digital Economy: An Integrated Governance Framework for Safe Financial Innovation, Stability, and Sustainable Development in Libya
Abdulahkam Alderdeer

Department of Finance and Banking / Faculty of Economics and Accounting, Murzuq / University of Fezzan

Abd.alderdeer@fezzanu.edu.ly

<https://orcid.org/0009-0006-1983-9836>

تاريخ الاستلام: 2026/06/30 تاريخ المراجعة: 2026/07/20 تاريخ القبول: 2026/7/28- تاريخ النشر: 2026/08/22

المخلص

هذه الدراسة تبحث كيفية إدارة المخاطر المالية في ليبيا التي تعد بيئة تتسارع فيها رقمنة المدفوعات والخدمات المصرفية والتكنولوجيا المالية. وتنطلق الدراسة من ملاحظة أن الرقمنة لا تحدث فئة منفصلة من المخاطر بقدر ما تعيد تشكيل المخاطر الائتمانية ومخاطر السيولة المخاطر التشغيلية ومدى الامتثال داخل شبكة أكثر ترابطاً واعتماداً على البيانات وعلى مقدمي الخدمات التقنية. واعتمدت الدراسة مراجعة للأدبيات الحديثة وتحليلاً مقارناً لأطر دولية صادرة عن لجنة بازل، وعن صندوق النقد الدولي، ومجلس الاستقرار المالي، والمعهد الوطني الأمريكي للمعايير والتكنولوجيا، ذلك إلى جانب قراءة لبيانات مصرف ليبيا المركزي والبنك الدولي. وتشير النتائج إلى وجود أثر غير خطي ومشروط للتحويل الرقمي، فعندما تقتصر الرقمنة بحوكمة قوية ومؤسسات رقابية فعالة، قد يحسن التحويل الرقمي الكفاءة والشمول والاستقرار، بيد أنه عندما تتقدم التكنولوجيا على نظم الرقابة قد يزيد من التعرض للمخاطر التشغيلية والسيبرانية ومخاطر الطرف الثالث والمنافسة. وبناءً على ذلك، تقترح الدراسة إطاراً من سبع طبقات يربط الحوكمة وشهية المخاطر، وحوكمة البيانات والنماذج، والمرونة السيبرانية والتشغيلية، والقياس والإنذار المبكر، وإدارة الطرف الثالث، وحماية المستهلك والامتثال، والرقابة والتعلم المؤسسي. كما تقدم مؤشرات تطبيقية وخريطة طريق مرحلية للسبيل الليبي. وتتمثل القيمة المضافة في تحويل المبادئ الدولية إلى تصميم حوكمي قابل للتطبيق في سوق ناشئة سريعة الرقمنة، مع التأكيد أن الإطار المقترح يحتاج إلى معايرة واختبار ميداني قبل استخدامه كأداة قياس رسمية.

الكلمات المفتاحية: الاقتصاد الرقمي؛ إدارة المخاطر المالية؛ التكنولوجيا المالية؛ المخاطر السيبرانية؛ المرونة التشغيلية؛ الحوكمة المصرفية؛ ليبيا.

Abstract

This study examines financial risk management in Libya as payments, banking services, and fintech become increasingly digital. It argues that digitalization does not simply create a separate category of risk; rather, it reshapes credit, liquidity, operational, compliance, and reputational risks within a more interconnected ecosystem that depends heavily on data and technology providers. The study uses a structured narrative review of recent peer-reviewed research, comparative content analysis of major international frameworks, and an applied reading of publicly available indicators from the Central Bank of Libya and the World Bank. The evidence suggests a conditional and often nonlinear

relationship between digitalization and financial stability. Digital finance may strengthen efficiency, inclusion, and resilience when supported by effective governance and supervision, but it can increase operational, cyber, third-party, and competitive risk when technological adoption outpaces risk controls. The paper therefore proposes a seven-layer governance framework integrating risk appetite, data and model governance, cyber and operational resilience, quantitative monitoring, third-party risk, consumer protection and compliance, and risk-based supervision and organizational learning. It also develops an indicative supervisory dashboard and a phased implementation roadmap for Libya. The paper's contribution lies in translating international principles into a practical governance design for a rapidly digitalizing emerging financial system, while explicitly treating the proposed framework as a policy prototype that requires field validation and calibration before formal supervisory use.

Keywords: digital economy; financial risk management; fintech; cyber risk; operational resilience; banking governance; Libya.

1. المقدمة

إن الرقمنة في القطاع المالي لم تعد مسألة إضافية لتقديم الخدمة، بل أصبحت جزءاً من نموذج العمل نفسه. فالتطبيقات المصرفية، والمدفوعات الفورية وواجهات البرمجة، والحوسبة السحابية، وتحليلات البيانات، والذكاء الاصطناعي، تدخل اليوم في التسعير والائتمان والتسوية ومكافحة الاحتيال وخدمة العملاء. ويؤدي هذا التحول إلى مكاسب واضحة في السرعة وخفض التكلفة وتوسيع وتسريع الوصول إلى الخدمات، لكنه يغير في الوقت ذاته الطريقة التي تنشأ بها المخاطر وتنتقل بين المؤسسات. وقد خلصت لجنة بازل إلى أن الرقمنة قد تضخم مخاطر تقليدية كالمخاطر المتعلقة بالسيولة والتشغيل والاستراتيجية، وأن الاعتماد المتزايد على الأطراف التقنية (الطرف الثالث) يخلق نقاط تعرض سيبرانية وتركيزات قد يكون لها بعد نظامياً (Basel Committee on Banking Supervision [BCBS], 2024).

إذن المشكلة الأساسية لا تكمن في كون التكنولوجيا مفيدة أو خطيرة في ذاتها، وإنما في العلاقة بين سرعة تبني الرقمنة ونضج الحوكمة وإدارة المخاطر والرقابة. وتظهر الأدلة التطبيقية صورة غير أحادية، فبعض الدراسات تجد أن الشمول المالي القائم على التكنولوجيا يقلل المخاطرة أو يعزز الاستقرار، خاصة عندما تكون البيئة المؤسسية قوية (Banna et al., 2021; Hakimi et al., 2022; Vuković et al., 2024)، بينما توضح دراسات أخرى أن المنافسة المرتبطة بتبني التكنولوجيا المالية والتحول الرقمي قد ترفع المخاطرة أو تزيد الهشاشة في ظروف معينة (Khattak et al., 2023; Cevik, 2024; Elekdag et al., 2025). وهذه النتائج المتباينة تجعل الحوكمة والرقابة متغيرين حاسمين في تفسير أثر الرقمنة.

تكتسب هذه الإشكالية أهمية خاصة في ليبيا. فالتوسع السريع في نقاط البيع والبطاقات والتطبيقات المصرفية والدفع الفوري يوسع نطاق الخدمة ويقلل الاعتماد على النقد، لكنه في الوقت ذاته يزيد حجم البيانات المتداولة وعدد نقاط الاتصال، والاعتماد على البنية التحتية للاتصالات ومن عدد الموردين الخارجيين. ومن ثم، فإن نجاح التحول الرقمي لا يقاس بعدد الخدمات المقدمة أو حجم المعاملات المنجزة فحسب، بل بقدرة النظام المالي على الاستمرار وقت حدوث الأعطال، وقدرته على اكتشاف الاحتيال، واحتواء الحوادث، وحماية العملاء، سرعة والتعافي.

تهدف هذه الدراسة إلى سد فجوة تطبيقية تتمثل في غياب إطار مكتمل يجمع بين المخاطر المالية التقليدية والمخاطر الناشئة عن الرقمنة، وتوظف المعايير الدولية الحديثة في صورة ترتيبات حوكمة ورقابة قابلة للتكيف في البيئة الليبية. لا تكنف الدراسة بمعالجات تعدد المخاطر، بل تربط بين مصادر الخطر وقنوات انتقاله وضوابطه المؤسسية والمؤشرات القابلة للمتابعة، مع التمييز بوضوح بين ما تدعمه الأدلة المنشورة وما يظل مقترحاً يحتاج إلى اختبار ميداني.

2. مشكلة الدراسة وأسئلتها ومساهمتها

تتمثل مشكلة الدراسة في وجود فجوة زمنية ومؤسسية محتملة بين التوسع في الخدمات المالية الرقمية وبين تطور أنظمة الحوكمة والمرونة التشغيلية وإدارة الطرف الثالث والإبلاغ عن الحوادث. فكلما اتسعت هذه الفجوة، ارتفع احتمال تحول حدوث مشكلة تقنية محدودة إلى خسارة مالية أو إلى أزمة في الثقة أو تعطل في خدمة حرجية. ومن هذه المشكلة ينبثق السؤال الرئيس التالي: كيف يمكن تصميم إطار متكامل لإدارة المخاطر المالية الرقمية في ليبيا يوازن بين الابتكار والكفاءة من جهة، والاستقرار والمرونة وحماية المستهلك من جهة أخرى؟

وينفرد عنه أربعة أسئلة:

1. ما القنوات التي تعيد الرقمنة من خلالها تشكيل مخاطر كل من الائتمان والسيولة والتشغيل والامتثال والسمعة؟
2. ماذا الذي تقوله الأدلة الحديثة عن العلاقة بين التكنولوجيا المالية والاستقرار المصرفي؟
3. ما هي المبادئ التنظيمية والرقابية الأكثر قابلية للتكيف مع البيئة الليبية؟
4. كيف يمكن تحويل المبادئ التنظيمية والرقابية الأكثر قابلية للتكيف مع البيئة الليبية، إلى مؤشرات تنفيذية ومراحل تطبيق قابلة للمتابعة؟

أما مساهمة الدراسة فتتمثل في ثلاثة مستويات:

- أولاً: تجمع بين أدبيات الاستقرار المصرفي وأدبيات المخاطر التشغيلية والسيبرانية، وهما مساران غالباً ما يدرسان بصورة منفصلة.
- ثانياً: تدمج داخل إطار واحد أحدث التطورات التنظيمية، وبخاصة تقرير لجنة بازل حول رقمنة التمويل (2024) ومبادئ إدارة مخاطر الطرف الثالث (2025).
- ثالثاً: تنتقل إلى تصميم تطبيقي للسياق الليبي يربط الخدمات الرقمية الحرجة بمؤشرات الإنذار المبكر ومتطلبات التعافي والرقابة القائمة على المخاطر بدلا من الاعتماد على النقاش المفاهيمي فقط.

3. المنهجية وحدود الدراسة

تعتمد الدراسة المنهج الوصفي التحليلي مدعوماً بمراجعة سردية منظمة (Structured Narrative Review) وتحليل محتوى مقارنة. ولا تُقدّم المراجعة بوصفها مراجعة منهجية شاملة؛ بل بوصفها عملية انتقائية وشفافة لاستخلاص الأدلة الأكثر صلة بسؤال الدراسة والأسئلة الفرعية، وركز الاختيار على الدراسات المحكمة المنشورة أساساً بين عامي 2020 و2026، مع إعطاء الأولوية للأبحاث التي تناولت التحول الرقمي، والتكنولوجيا المالية، والمخاطر المصرفية، والاستقرار المالي، والشمول الرقمي، والمخاطر التشغيلية والسيبرانية، ولا سيما في الاقتصادات الناشئة ودول منظمة التعاون الإسلامي ومنطقة الشرق الأوسط وشمال أفريقيا.

إلى جانب الأدبيات الأكاديمية، شمل التحليل الأطر والسياسات الصادرة عن لجنة بازل، وصندوق النقد الدولي، ومجلس الاستقرار المالي، والمعهد الوطني الأمريكي للمعايير والتكنولوجيا، والوكالة الأوروبية للأمن السيبراني، والبنك الدولي، ومصرف ليبيا المركزي. وتمت قراءة هذه المصادر عبر خمس فئات تحليلية: نوع الخطر، وقناة انتقاله إلى الخسارة المالية أو عدم الاستقرار، ومستوى الحوكمة المسؤول، وأداة القياس أو الاستجابة، ومدى القابلية للتطبيق في ليبيا.

إدارة المخاطر المالية في الاقتصاد الرقمي: إطار حوكمة تكاملي لدعم الابتكار المالي الآمن والاستقرار والتنمية المستدامة في ليبيا

تستند الدراسة إلى بيانات منشورة وليس إلى بيانات مصرفية سرية أو سجلات حوادث؛ لذلك لا تختبر علاقة سببية ولا تقدر نموذجاً قياسيًّا. كما أن الأرقام المستخدمة من الواقع في ليبيا تعكس مؤشرات عرضية لفترة محددة من عام 2026 ولا بالتالي تكفي وحدها لتقييم مستوى الخطر. وبناءً على ذلك، فإن الإطار ولوحة المؤشرات الواردة لاحقاً هما نموذجان للاسترشاد ويحتاجان إلى تحقق ميداني ومعايرة من خلال بيانات المصارف وشركات الدفع، أو باستخدام أساليب خبراء مثل Delphi وAHP قبل تحويلهما إلى أداة رقابية رسمية.

4. الأدبيات الحديثة: من أثر الرقمنة إلى شروط الاستقرار

تقدم الأدبيات الحديثة نتيجة أكثر تعقيداً من مجرد الافتراض بأن الرقمنة تخفض المخاطر أو تزيدها بصورة مطلقة فدراسة (Uddin et al، 2023)، المبنية على 264 بنكاً في 43 دولة، خلصت إلى أن العمليات المصرفية الرقمية ترتبط بارتفاع التعرض للمخاطر التشغيلية عبر زيادة حجم الأعمال والاعتماد على التكنولوجيا. وذلك يتسق مع تحليل الذي أظهره (Aldasoro et al، 2023) القاضي بأن المخاطر السيبرانية أصبحت مكوناً متزايداً من الخسائر التشغيلية وأن قوة الإشراف ترتبط بانخفاض الخسائر التشغيلية.

في المقابل، تشير مجموعة من الدراسات إلى أن الرقمنة قد تكون عاملاً للاستقرار عندما تعمل من خلال الكفاءة والبيانات وتوسيع قاعدة العملاء فقد وجد (Banna et al، 2021) في دراسته القائمة على عينة من 534 بنكاً في 24 دولة من دول منظمة التعاون الإسلامي أن ارتفاع الشمول المالي القائم على التكنولوجيا له ارتباط بانخفاض سلوك المخاطرة، وفي دراسة أقيمت في منطقة الشرق الأوسط وشمال أفريقيا، أظهر (Hakimi et al، 2022) أن الشمول المالي يدعم استقرار البنوك، مع أهمية السيولة والبيئة الكلية كما خلص (Kasri et al، 2022) إلى وجود علاقة طويلة الأجل بين انتشار المدفوعات الرقمية والاستقرار المصرفي في اقتصاد ناشئ ذي نظام مصرفي مزدوج.

لكن تمت أدلة لا تبرر تبني موقفاً متفائلاً غير مشروط، فقد بين (Khattak et al، 2023) أن الاستثمار في التكنولوجيا مع وجود تنويع مرتفع للدخل قد يرتبط بزيادة الهشاشة، في حين وجد (Cevik، 2024) أن الأثر الذي تحدثه التكنولوجيا المالية على الاستقرار يتغير بتغير نوع الأداة ومستوى التطور، وأن بعض أشكال الإقراض الرقمي قد تحمل مخاطر أكبر في الاقتصادات النامية، وتوصل (Elekdag et al، 2025) باستخدامه قاعدة عالمية تحوي أكثر من عشرة آلاف مؤسسة مالية، إلى أن انتشار التكنولوجيا المالية يمكن أن يرتبط بزيادة المخاطرة، لكن قوة المؤسسات المحلية قد تعدل هذا الأثر. وهذه النتيجة بالذات تعزز منطق الدراسة الحالية: أثر الرقمنة مشروط بجودة الحوكمة والإشراف لا بحجم التكنولوجيا وحده.

أما الاستنتاج المشروط فتدعمه دراسات أحدث حيث يؤكد (Saidi، 2026) أن أثر التكنولوجيا المالية يصبح أكثر إيجابية عندما يقترن بالشمول والمؤسسات القوية، وعلى المستوى الأفريقي، خلص (Elnahass et al، 2026) إلى أن الشمول المالي الرقمي يعزز استقرار البنوك عبر جودة الأصول والسيولة واستقرار التمويل، أما (Anton and Afloarei Nucu، 2024) يقدمان دليلاً على وجود علاقة غير خطية بين الشمول المالي الرقمي والاستقرار المصرفي عبر دراسة أجريت لعدد 81 دولة؛ وفي العام ذاته فإن (Vuković et al، 2024) لا يجدون دليلاً على أن التكنولوجيا المالية تهدد الاستقرار في دول BRICS على المدى القصير،.. وتظهر المراجعات المنهجية بدورها أن العلاقة بين التكنولوجيا المالية والشمول والاستقرار تتوسطها جودة الأطر التنظيمية والقدرات المالية والرقابية (Sant'Anna & Figueiredo، 2024; Gallegos et al., 2025).

إدارة المخاطر المالية في الاقتصاد الرقمي: إطار حوكمة تكاملي لدعم الابتكار المالي الآمن والاستقرار والتنمية المستدامة في ليبيا

جدول (1): مصفوفة مختصرة لأبرز الأدلة التي بُني عليها الإطار التحليلي

الدراسة	النطاق/المنهج	النتيجة الرئيسية	الدلالة لهذه الدراسة
Uddin et al. (2023)	264بنكاً / 43 دولة / 10 سنوات	الرقمنة توسع التعرض للمخاطر التشغيلية عبر حجم الأعمال والاعتماد التقني.	يدعم دمج الرقمنة في إطار المخاطر التشغيلية بدل فصلها تقنياً.
Aldasoro et al. (2023)	بيانات خسائر تشغيلية عبر دول ومؤسسات	المكون السيبراني يتزايد، والإشراف الأقوى يرتبط بخسائر تشغيلية أقل.	يدعم الإبلاغ والقياس والإشراف القائم على المخاطر.
Banna et al. (2021)	534بنكاً في 24 دولة OIC	الشمول المالي القائم على التكنولوجيا يرتبط بانخفاض المخاطرة.	مرجع ملائم للسياق الإسلامي والاقتصادات النامية.
Hakimi et al. (2022)	بنوك MENA ، 2004–SGMM، 2017	الشمول المالي يعزز الاستقرار مع دور مهم للسيولة والبيئة الكلية.	يؤكد أن أثر الرقمنة يجب أن يقرأ داخل البيئة المصرفية والكلية.
Khattak et al. (2023)	بنوك آسيوية / تحول رقمي وتنويع	التحول الرقمي مع التنويع المرتفع قد يزيد الهشاشة	ينبه إلى أن الفوائد ليست آلية وأن بنية نموذج العمل مهمة.
Cevik (2024)	198دولة، 2012–2020	أثر <i>fintech</i> يختلف حسب الأداة ومستوى التطور؛ الإقراض الرقمي أكثر حساسية.	يدعم الرقابة المتناسبة مع نوع النشاط لا مع مسمى المؤسسة.
Anton & Afloarei Nucu (2024)	81دولة Quantile / regression	علاقة غير خطية بين الشمول الرقمي والاستقرار.	يدعم منطق العتبات والرقابة المتدرجة.
Elekdag et al. (2025)	أكثر من 10,000 مؤسسة مالية	انتشار <i>fintech</i> قد يرفع المخاطرة؛ المؤسسات القوية تخفف الأثر.	يجعل جودة المؤسسات متغيراً حاكماً في السياسة.
Saidi (2026)	30دولة، 2011–2024	الاستقرار يتحسن حين يقتصر <i>fintech</i> بالشمول والمؤسسات القوية.	يدعم التركيز على البنية المؤسسية لا التوسع الرقمي منفرداً.
Elnahass et al. (2026)	37دولة أفريقية / بنوك	الشمول الرقمي يعزز الاستقرار عبر جودة الأصول والسيولة والتمويل.	يوفر دليلاً حديثاً من سياق أفريقي قريب من تحديات ليبيا.

المصدر: إعداد الباحث استناداً إلى الدراسات الواردة في قائمة المراجع

5. كيف تعيد الرقمنة تشكيل المخاطر المالية؟

الأهم في البيئة الرقمية هو انتقال الخطر بين الفئات، فاختراق بيانات قد ينتج عنه احتيال مباشر وغرامات ونفقات استجابة وتكاليف سمعة في الوقت نفسه، وحادث تقني قد يبدأ كتعطل تطبيق مصرفي، ثم يتحول إلى تعطل في التسوية أو ضغط سيولة أو موجة من الشكاوى وفقدان ثقة. لذلك، لا تكون فائدة التصنيف في وضع كل حادث في معزل عن غيره، بل في فهم قنوات انتقاله ومسؤولية الحوكمة عنه.

هذه النظرة تؤكد الأداة التنظيمية، فقد عدلت لجنة بازل مبادئ الرقابة الأساسية في العام 2024 لتشمل صراحة مخاطر الرقمنة والمخاطر الناشئة ضمن عملية إدارة المخاطر، كما نشرت في 2025 مبادئ لإدارة مخاطر الطرف الثالث نتيجة زيادة اعتماد البنوك على مزودي التقنية والخدمات السحابية (BCBS, 2024, 2025). وذلك يعني أن العقود التقنية لم تعد شأنًا مشتريات، بل جزء من السلامة الاحترافية والمرونة التشغيلية.

إدارة المخاطر المالية في الاقتصاد الرقمي: إطار حوكمة تكاملي لدعم الابتكار المالي الآمن والاستقرار والتنمية المستدامة في ليبيا

جدول (2): خريطة انتقال المخاطر في البيئة المالية الرقمية

فئة الخطر	المصدر الرقمي	الأثر المالي المحتمل	مؤشرات مناسبة للمتابعة
السيولة والتسوية	مدفوعات لحظية، تحويلات رقمية سريعة، انتشار الشائعات عبر القنوات الرقمية	تدفقات خارجة سريعة، ضغط على أرصدة التسوية، تعثر مؤقت في المدفوعات	صافي التدفقات حسب القناة؛ أرصدة التسوية؛ سيناريوهات ضغط لحظية
الائتمان والنماذج	نماذج آلية، بيانات بديلة، توسع سريع في الإقراض الرقمي	تسعير خاطئ، تحيز، تدهور جودة المحفظة	اختبارات صلاحية النموذج؛ معدلات التعثر حسب القناة؛ مراجعة بشرية
التشغيل والسيبرانية	اختراق، توقف منصة، تحديث برمجي، هندسة اجتماعية	خسائر مباشرة، تعطل، تعويضات، غرامات، فقدان ثقة	عدد الحوادث وشدها؛ زمن الاحتواء والتعافي؛ نجاح اختبارات التعافي
الطرف الثالث والتركيز	سحابة، مزود دفع، API، مركز بيانات، برمجيات حرجية	نقطة فشل مشتركة، تسرب بيانات، عجز عن التعافي	تركيز الموردين؛ الالتزام بـ SLA؛ اختبارات خطة الخروج؛ بدائل تشغيل
البيانات والخصوصية	تجميع بيانات واسعة، صلاحيات غير منضبطة، جودة بيانات ضعيفة	احتيا، قرارات نموذجية خاطئة، انتهاك خصوصية	جودة البيانات؛ الحوادث المتعلقة بالوصول؛ مراجعة الصلاحيات
الامتثال والجرائم المالية	KYC رقمي، معاملات عابرة للقنوات، أصول أو خدمات جديدة	غرامات، غسل أموال واحتيا، قيود رقابية	تنبيهات AML؛ فعالية KYC؛ معدل الحالات المغلقة؛ سجلات تدقيق
السمة والثقة	انتشار فوري للحوادث والشكاوى عبر المنصات الاجتماعية	سحب عملاء/ودائع، انخفاض الاستخدام، تكلفة استعادة الثقة	الشكاوى؛ زمن المعالجة؛ مؤشرات رضا/تخلي العملاء

المصدر: إعداد الباحث بالاستناد إلى (BCBS (2021a, 2021b, 2024, 2025)، IMF (2024)، NIST (2024)، Aldasoro et al. (2023).

6. الأطر الدولية وما تضيفه للسياق الليبي

تتقاطع الأطر الدولية الحديثة في فكرة مركزية محورها أن المرونة الرقمية تبدأ من الحوكمة ولا تنتهي عند الأمن السيبراني، فمبادئ بازل للمرونة التشغيلية تطلب تحديد العمليات الحرجة ومستويات تحمل التعطل، بينما يوسع NIST CSF 2.0 وظيفة الحوكمة ويربط الأمن السيبراني بإدارة مخاطر المؤسسة، ويذهب صندوق النقد الدولي إلى أبعد من ذلك حين يعامل الحوادث السيبرانية بوصفها مصدراً محتملاً لعدم الاستقرار الكلي؛ إذ أشار تقرير الاستقرار المالي العالمي لعام 2024 إلى تضاعف الهجمات السيبرانية تقريباً مقارنة بما قبل الجائحة، وأن قرابة 20% من الحوادث المبلغ عنها أصابت مؤسسات مالية (International Monetary Fund [IMF], 2024).

أضافت لجنة بازل بعداً مهماً في العام 2025، وذلك بنشرها مبادئ إدارة مخاطر الطرف الثالث، وهذه المبادئ شديدة الصلة بالأسواق التي تعتمد على عدد محدود من مزودي التقنية، وهذا الاتجاه يتطلب جرداً للعلاقات الحرجة، وفهماً للاعتماد المتسلسل، وحقوقاً تعاقدية للتدقيق والوصول إلى البيانات، وخطط خروج واختبار بدائل التشغيل، وبالنسبة لليبي، فإن أهمية هذا البعد لا تقل عن أهمية الأمن السيبراني نفسه، لأن فشل مورد واحد ربما يؤثر في وقت متزامن على عدة مؤسسات.

جدول (3): أطر دولية مختارة ودلالاتها التطبيقية

الإطار	الفكرة المركزية	الدلالة العملية للمصارف والرقابة في ليبيا
BCBS – Operational Resilience (2021)	استمرار العمليات الحرجة خلال الصدمات	تحديد الخدمات الحرجة ومستوى تحمل التعطل واختبار التعافي.
BCBS – Operational Risk (2021)	حوكمة المخاطر التشغيلية و ICT واستمرارية الأعمال	دمج المخاطر التقنية في إطار المخاطر المؤسسية وخطوط الدفاع.
BCBS – Digitalisation of Finance / Core Principles (2024)	الرقمنة تضخم مخاطر تقليدية وتزيد اعتماد الطرف الثالث	رقابة متناسبة، بيانات أفضل، قدرة إشرافية على الأنشطة الرقمية والموردين.
BCBS – Third-party Risk (2025)	إدارة جميع ترتيبات الطرف الثالث لا «التعميد» فقط	سجل موردين حرجين، تقييم تركيز، حقوق تدقيق، خطط خروج واستمرارية.
NIST CSF 2.0 (2024)	Govern–Identify–Protect–Detect–Respond–Recover	تحويل الأمن السيبراني إلى دورة حوكمة ومساءلة قابلة للقياس.
IMF GFSR (2024)	الخطر السيبراني مصدر محتمل لعدم الاستقرار المالي	إبلاغ إلزامي، اختبارات استجابة وتعاف، مساءلة مجلس الإدارة.
FSB (2023)	النشاط نفسه، الخطر نفسه، التنظيم نفسه في الأنشطة المشفرة	تجنب فجوات الرقابة عندما تتشابه المخاطر بين كيانات مختلفة.
ENISA (2025)	مشهد تهديدات القطاع المالي	استخدام معلومات التهديد القطاعية في تحديث السيناريوهات والاختبارات.

المصدر: إعداد الباحث من الوثائق الأصلية للجهات المذكورة.

7. التحول الرقمي المالي في ليبيا: قراءة من منظور المخاطر

من البيانات التي يوفرها مصرف ليبيا المركزي تتوفر صورة واضحة عن سرعة التوسع في الرقمنة، ففي الفترة من 1 يناير إلى 28 فبراير 2026 بلغ عدد نقاط البيع المصدرة 170,149 نقطة، وعدد البطاقات المفعلة 5,531,507 بطاقة، كما سُجلت 4,047,780 عملية عبر أجهزة الصراف الآلي، وبلغ عدد عمليات البطاقات على نقاط البيع 74,169,676 عملية بقيمة تقارب

إدارة المخاطر المالية في الاقتصاد الرقمي: إطار حوكمة تكاملي لدعم الابتكار المالي الآمن والاستقرار والتنمية المستدامة في ليبيا

9.41 مليارات دينار وفق البيان المنشور في 3 مارس 2026 (Central Bank of Libya [CBL], 2026)، هذه الأرقام تؤكد أن القنوات الرقمية أصبحت تشكل جزءاً واسع الاستخدام من البنية المالية وليست مجرد خدمة هامشية. لا يجوز تفسير هذه الأرقام باعتبارها دليلاً بحد ذاتها على أنها ارتفاع في الخطر، فالزيادة في المعاملات قد تكون مؤشراً على كفاءة وشمول أكبر؛ لكنها تزيد حجم التشغيل الذي تتبقي حمايته ومراقبته، فعندما يصبح الملايين من العملاء وعشرات الآلاف من نقاط القبول مرتبطين بأنظمة فورية، ترتفع كلفة التعطل وزمن الاستجابة يصبح أكثر أهمية، ومن ناحية أخرى، يضيف Global Findex 2025 بعداً مهماً للمناقشة؛ حيث صارت السلامة الرقمية والاتصال والقدرة على استخدام الهاتف والإنترنت جزءاً من قياس الشمول المالي، ما يؤكد أن التوسع في الوصول ينبغي أن يقترن بالقدرة على الاستخدام الآمن (Klapper et al., 2025).

توجد كذلك ملاحظة منهجية مهمة، تشير إلى أن الأرقام المنشورة من مصادر رسمية مختلفة خلال الفترة قد تختلف في بعض بنود حجم التعاملات نتيجة التحديثات أو اختلاف تاريخ الاستخراج، لذلك تعتمد الدراسة الأرقام الواردة في البيان الرسمي المحدد بتاريخ 3 مارس 2026، وتتعامل معها كلقطة زمنية لا كسلسلة إحصائية نهائية. ولأغراض الرقابة، ينبغي إنشاء سلسلة موحدة قابلة للمقارنة شهرياً مع تعريف ثابت لكل مؤشر.

جدول (4): مؤشرات مختارة ودلالاتها على إدارة المخاطر

المؤشر	القيمة/الوصف	الدلالة من منظور المخاطر
نقاط البيع POS	170,149 نقطة (يناير-فبراير 2026)	اتساع نقاط الاتصال وزيادة أهمية أمن الطرف النهائي واستمرارية الاتصال.
البطاقات المفعلة	5,531,507 بطاقة	قاعدة مستخدمين كبيرة ترفع أهمية مكافحة الاحتيال والمصادقة وحماية المستهلك.
عمليات ATM	4,047,780 عملية	صلة مباشرة بين القناة الرقمية وإدارة النقد والسيولة والتشغيل.
عمليات نقاط البيع	74,169,676 عملية	ارتفاع الاعتماد على الشبكات والتسوية ومراقبة الشدوذ في الزمن شبه الحقيقي.
قيمة عمليات نقاط البيع	نحو 9.41 مليارات دينار	زيادة الأثر المالي المحتمل لأي انقطاع واسع أو احتيال منظم.
Findex 2025	نحو 148 ألف بالغ في 141 اقتصاداً؛ بيانات جديدة عن السلامة الرقمية	ضرورة دمج السلامة الرقمية والثقة وحماية المستهلك في سياسات الشمول المالي.

المصدر: (Klapper et al. (2025) □ CBL (2026)

8. الإطار المقترح لإدارة المخاطر المالية الرقمية

يقترح هذه الدراسة إطاراً متكون من سبع طبقات مترابطة، الفكرة هنا ليست إنشاء سبع إدارات جديدة، بل ضمان أن تمر المخاطر الرقمية عبر دورة حوكمة واحدة من مجلس الإدارة إلى التشغيل والرقابة والتعلم، ويُفترض تطبيق الإطار بصورة متناسبة مع حجم المؤسسة، وحجم المعاملات الرقمية، وأهمية الخدمات التي تقدمها للنظام المالي.

جدول (5): طبقات الإطار التكاملي المقترح

الطبعة	الغاية	أمثلة للمتطلبات/المخرجات
1. الحوكمة وشبهية المخاطر	اعتماد مجلس الإدارة حدوداً قابلة للقياس لمستوى التعطل والخسائر التشغيلية والاعتماد على الموردين والمخاطر السيبرانية.	سياسة مخاطر رقمية؛ حدود تحمل التعطل؛ مسؤوليات واضحة؛ تقارير دورية للمجلس.
2. حوكمة البيانات والنماذج	تحديد ملكية البيانات وجودتها وتصنيفها وصلاحيات الوصول وحوكمة النماذج والخوارزميات.	سجل بيانات حرجية؛ مؤشرات جودة؛ توثيق النماذج؛ تحقق مستقل؛ آلية اعتراض بشري.
3. المرونة السيبرانية والتشغيلية	الوقاية والكشف والاستجابة والتعافي مع التركيز على الخدمات الحرجة لا على الأنظمة منفردة.	RTO/RPO؛ تمارين محاكاة؛ اختبارات اختراق؛ خطط استمرارية وتعافي.
4. القياس والإنذار المبكر	تحويل المخاطر إلى مؤشرات قابلة للمتابعة في الزمن المناسب.	لوحات مؤشرات للحوادث والاحتيال والسيولة والتوقف والشكاوى.
5. الطرف الثالث والتركيز	إدارة الموردين والسحابة واجهات البرمجة وسلاسل التوريد التقنية.	سجل موردين؛ تقييم تركيز SLA؛ حقوق تدقيق؛ بديل وخطة خروج.
6. المستهلك والامتثال والنزاهة المالية	حماية العميل والخصوصية ومكافحة غسل الأموال والاحتيال الرقمي.	KYC رقمي؛ مصادقة قوية؛ إدارة شكاوى؛ مراقبة معاملات؛ تعويض واضح.
7. الرقابة والتعلم المؤسسي	تجميع الحوادث واختبارات الضغط والتعلم القطاعي وتحديث المتطلبات.	إبلاغ موحد؛ قاعدة حوادث قطاعية؛ تمارين مشتركة؛ رقابة SupTech قائمة على البيانات.

المصدر: إعداد الباحث بالاستناد إلى: (MF (2024)، NIST (2024)، BCBS (2021a, 2021b, 2024, 2025)

9. من مؤشر مركب إلى لوحة مخاطر قابلة للمعايرة

إن إعطاء أوزان رقمية لمؤشر مركب من دون أساس تجريبي، يعد من نقاط الضعف الشائعة في الأوراق التي تتبع نهجاً مفاهيمياً، لذلك فإن هذه النسخة لا تعتمد أوزاناً ثابتة للمخاطر المالية الرقمية، والبديل الأكثر صلابة الذي اعتمدته هذه الدراسة هو لوحة مؤشرات متعددة الأبعاد تسمح لكل مؤسسة أو جهة رقابية بقياس الاتجاهات والحدود قبل التفكير في بناء درجة مركبة،

إدارة المخاطر المالية في الاقتصاد الرقمي: إطار حوكمة تكاملي لدعم الابتكار المالي الآمن والاستقرار والتنمية المستدامة في ليبيا

وإذا ما رغبت الجهة الرقابية لاحقاً في اعتماد مؤشر واحد، فينبغي اشتقاق الأوزان من بيانات الخسائر والحوادث أو من عملية تحقق منظمة مثل Delphi/AHP، من ثم اختبار حساسية النتيجة للأوزان المختلفة.

تقسم اللوحة المقترحة المؤشرات إلى نتائج خطر (مثل الخسائر والاحتيايل والتوقف) ومؤشرات قدرة (مثل زمن التعافي ونسبة الاختبارات الناجحة) ومؤشرات تعرض (مثل الاعتماد على مورد واحد وحجم المعاملات اللحظية)، وهذه القسمة تمنع الخلط بين (ارتفاع النشاط الرقمي) و(ارتفاع المخاطر)؛ فزيادة المعاملات قد ترافقها مخاطر أقل إذا تحسنت الضوابط والقدرة على التعافي.

جدول (6): لوحة مؤشرات رقابية وتشغيلية مقترحة

المجال	المؤشرات المقترحة	الدورية	مثال لحد الإنذار
استمرارية الخدمة	زمن التوقف للخدمات الحرجة؛ زمن التعافي الفعلي مقابل RTO	لحظي/شهري	تجاوز RTO أو تكرار انقطاع الخدمة
الأمن السيبراني	عدد الحوادث حسب الشدة؛ زمن الاكتشاف والاحتواء؛ نسبة الأنظمة الحرجة المخترقة	فوري/شهري	حدث شديد أو زيادة متكررة في زمن الاحتواء
الاحتيايل الرقمي	خسائر الاحتيايل كنسبة من قيمة المعاملات؛ نسبة العمليات المشتبه بها	يومي/شهري	انحراف عن خط الأساس أو تجاوز حدود الخسارة
السيولة والتسوية	صافي التدفقات حسب القناة؛ رصيد التسوية؛ معاملات غير مسواة	لحظي/يومي	تجاوز حدود السيولة أو تراكم عمليات غير مسواة
الطرف الثالث	نسبة الخدمات الحرجة المعتمدة على أكبر مزود؛ أعطال الموردين؛ نتائج اختبارات الخروج	شهري/ربع سنوي	تركيز مفرط أو فشل متكرر في SLA/اختبار الخروج
البيانات والنماذج	أخطاء جودة البيانات؛ تغير أداء النموذج؛ حالات تجاوز المراجعة البشرية	شهري/ربع سنوي	تدهور جودة أو تحيز/انحراف نموذج
حماية المستهلك	الشكاوى الرقمية؛ متوسط زمن الحل؛ قيمة التعويضات؛ حوادث الاستيلاء على الحساب	شهري	ارتفاع الشكاوى أو تجاوز زمن التسوية المحدد
الامتثال	تنبيهات AML/KYC غير المعالجة؛ الاستثناءات؛ حالات الوصول غير المصرح	يومي/شهري	تراكم الحالات أو حادث امتثال جوهري

المصدر: إعداد الباحث؛ الحدود الرقمية الفعلية يجب أن تُعابَر على بيانات المؤسسة وقطاع

10. مناقشة النتائج

تكشف الأدلة المجمعة عن ثلاث نتائج ذات أهمية مباشرة متمثلة فيما يلي:

1. إن الأثر الذي تحدثه الرقمنة على الاستقرار ليس خطياً ولا ثابتاً بين البلدان والمؤسسات، وهذا يفسر سبب توصل الدراسات إلى نتائج تبدو متعارضة، فالرقمنة قد تحسن الاستقرار عبر الكفاءة والودائع والبيانات، لكنها قد تزيد المخاطرة عبر المنافسة والاعتماد التقني والتركيز والانتمان الرقمي، وهذه تتسجم النتيجة مع الدراسات التي تبرز دور قوة المؤسسات والرقابة في تعديل الأثر (Anton & Afloarei Nucu, 2024; Elekdag et al., 2025; Saidi, 2026).
2. أن الأمن السيبراني لم يعد ملفاً تقنياً منفصلاً، فصندوق النقد الدولي يربطه مباشرة بالثقة والخدمات الحرجة والروابط النظامية، بينما توثق الأدلة المصرفية نمو المكون السيبراني داخل الخسائر التشغيلية (Aldasoro et al., 2023; IMF, 2024). وعليه، فإن لجنة المخاطر ومجلس الإدارة يجب أن ينظرا لمقاييس الأمن والتعافي بالطريقة نفسها التي ينظران بها لمؤشرات السيولة وجودة الأصول، كمخاطر يمكن أن تنتقل إلى الخسارة والاستقرار.
3. إن مخاطر الطرف الثالث تصعد إلى مركز الحوكمة، فالتوسع في السحابة وواجهات البرمجة وشركات الدفع يمنح المؤسسات سرعة وقدرة يصعب بناؤها داخلياً، لكنه يخلق اعتماداً قد يتجاوز حدود المؤسسة الواحدة، لذلك فإن سجل الموردين الحرجين، وتحليل التركيز، وخطط الخروج، وحقوق التدقيق، واختبارات الاستمرارية المشتركة ليست متطلبات تعاقدية ثانوية، بل وسائل لحماية استمرارية النظام المالي (BCBS, 2025).

إدارة المخاطر المالية في الاقتصاد الرقمي: إطار حوكمة تكاملي لدعم الابتكار المالي الآمن والاستقرار والتنمية المستدامة في ليبيا

في ليبيا، تجمع هذه النتائج بين حاجة رقابية عاجلة وفرصة واضحة ينبغي استغلالها، فالنمو السريع في القنوات الرقمية يمكن أن يدعم الشمول ويقلل تكاليف المعاملات والنقد، لكن الفائدة التنموية لن تكون مستدامة ما لم تُبْنِ الثقة في الرقمنة بالتوازي. والثقة هنا مفهوم عملي، وهي بالتالي ناتجة عن أن يعرف العميل حقوقه، وأن تكون المعاملة قابلة للتتبع، وأن يُكتشف الاحتيال بسرعة، وأن توجد بدائل عند التعطل، وأن تكون مسؤوليات البنك وشركة الدفع والمورد التقني واضحة عند وقوع الحادث.

11. التوصيات والسياسات المقترحة لليبيا

1. إصدار إطار وطني للمرونة التشغيلية والمخاطر المالية الرقمية يطبق على المصارف وشركات الدفع بصورة متناسبة مع حجمها وأهميتها النظامية، ويحدد الخدمات الحرجة وحدود تحمل التعطل ومتطلبات الاختبار والتعافي.
2. إنشاء نظام موحد وسري للإبلاغ عن الحوادث التشغيلية والسيبرانية، بتصنيف موحد للشدة والخسارة وزمن الاكتشاف والاحتواء والتعافي، مع آلية للتغذية الراجعة القطاعية دون كشف معلومات حساسة.
3. إلزام المؤسسات بسجل للأطراف الثالثة الحرجة، وتحليل مخاطر التركيز، وبنود تعاقدية لحقوق التدقيق والوصول إلى البيانات والإبلاغ عن الحوادث وخطط الخروج، بما يتوافق مع مبادئ (BCBS (2025
4. تطوير رقابة قائمة على البيانات (SupTech) تعتمد مؤشرات معيارية دورية للحوادث والتوقف والاحتيال والسيولة الرقمية والشكاوى، بدل الاكتفاء بالتفتيش اللاحق.
5. ربط التوسع في الشمول المالي بسياسات سلامة رقمية وحماية مستهلك، تشمل المصادقة القوية، والتوعية بالهندسة الاجتماعية، والإفصاح الواضح عن الرسوم والمسؤولية، وآليات سريعة للشكاوى والتعويض.
6. تنفيذ اختبارات ضغط وتمارين محاكاة قطاعية تشمل سيناريوهات تعطل منصة دفع أو مزود اتصالات/سحابة أو موجة احتيال أو تدفقات نقدية رقمية مفاجئة، مع قياس زمن التعافي الفعلي.
7. بناء قدرات بشرية مشتركة بين الرقابة والمصارف والجامعات في الأمن السيبراني المالي، وتحليل البيانات، وحوكمة النماذج، ومخاطر الطرف الثالث، وتدقيق الأنظمة، مع ربط التدريب بحوادث وسيناريوهات واقعية.

12. خريطة طريق تنفيذية

جدول (7): خريطة طريق مرحلية لتطبيق الإطار المقترح

المرحلة	الإجراء الرئيس	المسؤول	مؤشر المتابعة
0-6 أشهر	جرد الخدمات الرقمية الحرجة؛ اعتماد سياسة مخاطر رقمية؛ تصميم نموذج موحد للحوادث	مجالس الإدارات والإدارة التنفيذية / مصرف ليبيا المركزي	سجل خدمات حرجة؛ حدود تحمل تعطل؛ نموذج إبلاغ معتمد
6-12 شهراً	اختبارات اختراق وتعافي؛ مراجعة عقود الموردين؛ سجل طرف ثالث؛ تدريب أساسي	المخاطر و ICT والامتثال والتدقيق الداخلي	نتائج اختبارات؛ خطط معالجة؛ نسبة تغطية الموردين الحرجين
12-18 شهراً	لوحات مؤشرات؛ ربط بيانات السيولة والاحتيال والحوادث؛ سيناريوهات ضغط	المخاطر والمالية والعمليات والرقابة	مؤشرات شهرية/لحظية؛ حدود إنذار؛ تقارير مقارنة قطاعية
18-24 شهراً	تمرين قطاعي مشترك؛ اختبار فشل مورد حرج أو شبكة دفع؛ تحسين خطط الأزمات	الجهة الرقابية والمؤسسات ومزود الخدمات الرئيسيون	تقرير دروس مستفادة؛ زمن تعافى مقاس؛ إجراءات تصحيحية
مستمر	تحديث الضوابط؛ مراجعة النماذج؛ معايرة مؤشرات الخطر؛ تبادل معلومات تهديدات	لجان المخاطر والتدقيق والجهة الرقابية	انخفاض الخسائر/التوقف؛ تحسن زمن الاستجابة؛ نضج الحوكمة

المصدر: إعداد الباحث.

13. القيود ومسارات البحث المستقبلي

تتمثل أهم قيود الدراسة في طبيعتها المفاهيمية واعتمادها على بيانات منشورة لا تسمح بقياس معدل الحوادث أو الخسائر داخل المؤسسات الليبية. كما أن الأدبيات الدولية تستخدم مؤشرات مختلفة للرقمنة والاستقرار، وهو ما يفسر جزءاً من تباين النتائج

إدارة المخاطر المالية في الاقتصاد الرقمي: إطار حوكمة تكاملي لدعم الابتكار المالي الآمن والاستقرار والتنمية المستدامة في ليبيا

ويحد من إمكان نقل معاملات أو عتبات جاهزة من دولة إلى أخرى. كذلك، لا تتوافر حتى الآن سلسلة عامة موحدة للحوادث السيبرانية والتشغيلية في القطاع المالي الليبي يمكن استخدامها للتحقق من الإطار.

يمكن تطوير الدراسة في ثلاثة اتجاهات. الأول مسح ميداني لقياس نضج إدارة المخاطر الرقمية في المصارف وشركات الدفع الليبية، مع بناء مقياس موثوق واختبار خصائصه الإحصائية. والثاني استخدام Delphi/AHP أو بيانات خسائر فعلية لمعايرة أوزان مؤشر مركب بدل الأوزان الافتراضية. والثالث بناء قاعدة بيانات شهرية أو ربع سنوية تجمع مؤشرات الدفع الرقمي والسيولة والربحية والاستقرار والحوادث، ثم اختبار العلاقات باستخدام نماذج زمنية أو Panel عندما تتوافر المدة والاتساق اللازماني.

14. الخاتمة

تخلص الدراسة إلى أن إدارة المخاطر في الاقتصاد الرقمي ليست عملية كبح للابتكار، بل شرط لجعله قابلاً للاستمرار. فالرقمنة يمكن أن توسع الشمول وتخفف التكلفة وتحسن البيانات، لكنها في الوقت نفسه تجعل المؤسسات أكثر اعتماداً على الأنظمة والموردين والاتصال الفوري. لذلك، فإن الفصل بين «المخاطر المالية» و«المخاطر التقنية» لم يعد مناسباً في الخدمات المصرفية الحديثة.

في السياق الليبي، تشير سرعة التوسع في المدفوعات والخدمات الرقمية إلى أن الأولوية لم تعد إطلاق مزيد من القنوات فقط، بل بناء الثقة والمرونة حولها. ويقترح البحث إطاراً عملياً من سبع طبقات ولوحة مؤشرات وخريطة طريق، لكنه يتجنب تقديم أوزان أو درجات نهائية غير مختبرة. وتكمن الخطوة التالية في تحويل هذا التصميم إلى أدوات قابلة للقياس عبر بيانات حوادث ومؤشرات مصرفية فعلية، بحيث تصبح الرقابة الرقمية قائمة على الأدلة وقادرة على مرافقة الابتكار بدل اللحاق به بعد وقوع الخسارة.

المراجع

- Abdurrahman, A., Gustomo, A., & Prasetyo, E. A. (2024). Enhancing banking performance through dynamic digital transformation capabilities and governance, risk management, and compliance: Insights from the Indonesian context. *The Electronic Journal of Information Systems in Developing Countries*, 90(2), e12299. <https://doi.org/10.1002/isd2.12299>
- Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2023). Operational and cyber risks in the financial sector. *International Journal of Central Banking*, 19(5), 340–402. <https://www.ijcb.org/journal/v19n5/operational-and-cyber-risks-financial-sector>
- Anton, S., & Afloarei Nucu, A. E. (2024). The impact of digital finance and financial inclusion on banking stability: International evidence. *Oeconomia Copernicana*, 15(2), 563–593. <https://doi.org/10.24136/oc.3046>
- Banna, H., Hassan, M. K., & Rashid, M. (2021). Fintech-based financial inclusion and bank risk-taking: Evidence from OIC countries. *Journal of International Financial Markets, Institutions and Money*, 75, 101447. <https://doi.org/10.1016/j.intfin.2021.101447>
- Basel Committee on Banking Supervision. (2021a). *Principles for operational resilience*. Bank for International Settlements. <https://www.bis.org/bcbs/publ/d516.pdf>
- Basel Committee on Banking Supervision. (2021b). *Revisions to the principles for the sound management of operational risk*. Bank for International Settlements. <https://www.bis.org/bcbs/publ/d515.pdf>
- Basel Committee on Banking Supervision. (2022). *Prudential treatment of cryptoasset exposures*. Bank for International Settlements. <https://www.bis.org/bcbs/publ/d545.htm>
- Basel Committee on Banking Supervision. (2024). *Digitalisation of finance*. Bank for International Settlements. <https://www.bis.org/bcbs/publ/d575.pdf>

- Basel Committee on Banking Supervision. (2025). *Principles for the sound management of third-party risk*. Bank for International Settlements. <https://www.bis.org/publications/202512-guidelines-principles-sound-management-third-party-risk>
- Central Bank of Libya. (2026, March 3). *Governor of the Central Bank of Libya holds an extensive meeting to follow up on digital transformation indicators and electronic payment services*. <https://cbl.gov.ly/en/governor-of-the-central-bank-of-libya-holds-an-extensive-meeting-to-follow-up-on-digital-transformation-indicators-and-electronic-payment-services/>
- Cevik, S. (2024). The dark side of the moon? Fintech and financial stability. *International Review of Economics*, 71(2), 421–433. <https://doi.org/10.1007/s12232-024-00449-8>
- Elekdag, S., Emrullahu, D., & Ben Naceur, S. (2025). Does FinTech increase bank risk-taking? *Journal of Financial Stability*, 76, 101360. <https://doi.org/10.1016/j.jfs.2024.101360>
- Elnahass, M., Iddouch, K., Rezki, S., & Eloueldrhiri, S. (2026). Rewiring finance for inclusion: Digital and traditional mechanisms in African banking. *Emerging Markets Review*, 72, 101448. <https://doi.org/10.1016/j.ememar.2026.101448>
- European Union Agency for Cybersecurity. (2025). *ENISA threat landscape: Finance sector*. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector>
- Financial Stability Board. (2023). *Global regulatory framework for crypto-asset activities*. <https://www.fsb.org/2023/07/fsb-global-regulatory-framework-for-crypto-asset-activities/>
- Gallegos, A., Rodríguez Zavala, L. A., Valencia-Arias, A., & Valencia, J. (2025). Emerging trends in digital banking: Technologies, usability, regulation, and transformation of the financial sector. *F1000Research*, 14, 727. <https://doi.org/10.12688/f1000research.166554.1>
- Hakimi, A., Boussaada, R., & Karmani, M. (2022). Are financial inclusion and bank stability friends or enemies? Evidence from MENA banks. *Applied Economics*, 54(21), 2473–2489. <https://doi.org/10.1080/00036846.2021.1992342>
- International Monetary Fund. (2024). *Global financial stability report, April 2024: The last mile—Financial vulnerabilities and risks* (Chapter 3: Cyber risk: A growing concern for macrofinancial stability). <https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024>
- Kasri, R. A., Indrastomo, B. S., Hendranastiti, N. D., & Prasetyo, M. B. (2022). Digital payment and banking stability in emerging economy with dual banking system. *Heliyon*, 8(11), e11198. <https://doi.org/10.1016/j.heliyon.2022.e11198>
- Khattak, M. A., Ali, M., Azmi, W., & Rizvi, S. A. R. (2023). Digital transformation, diversification and stability: What do we know about banks? *Economic Analysis and Policy*, 78, 122–132. <https://doi.org/10.1016/j.eap.2023.03.004>
- Klapper, L., Singer, D., Starita, L., & Norris, A. (2025). *The Global Findex Database 2025: Connectivity and financial inclusion in the digital economy*. World Bank. <https://doi.org/10.1596/978-1-4648-2204-9>
- Li, G., Elahi, E., & Zhao, L. (2022). Fintech, bank risk-taking, and risk-warning for commercial banks in the era of digital technology. *Frontiers in Psychology*, 13, 934053. <https://doi.org/10.3389/fpsyg.2022.934053>
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.29>
- Saidi, H. (2026). Digital pathways to stability: A cross-country analysis of the fintech–inclusion–stability nexus across selected countries. *Economies*, 14(1), 8. <https://doi.org/10.3390/economies14010008>
- Sant'Anna, D. A. I. M., & Figueiredo, P. N. (2024). Fintech innovation: Is it beneficial or detrimental to financial inclusion and financial stability? A systematic literature review and research directions. *Emerging Markets Review*, 60, 101140. <https://doi.org/10.1016/j.ememar.2024.101140>
- Uddin, M. H., Mollah, S., Islam, N., & Ali, M. H. (2023). Does digital transformation matter for operational risk exposure? *Technological Forecasting and Social Change*, 197, 122919. <https://doi.org/10.1016/j.techfore.2023.122919>
- Vuković, D. B., Hassan, M. K., Kwakye, B., Febtinugraini, A., & Shakib, M. (2024). Does fintech matter for financial inclusion and financial stability in BRICS markets? *Emerging Markets Review*, 61, 101164. <https://doi.org/10.1016/j.ememar.2024.101164>