



Article

Operationalising FinTech-Related Systemic Risks: An Evidence-Mapped Macroprudential Integration Framework (FMIF)

János Kálmán *  and András Lapsánszky

Deák Ferenc Faculty of Law and Political Sciences, István Széchenyi University, 9026 Győr, Hungary

* Correspondence: kalman.janos@sze.hu

Abstract

Digital finance is reshaping financial intermediation through platform-based credit, stablecoin-based payment and settlement arrangements, and a rapidly deepening reliance on critical third-party technology providers. Existing international frameworks identify many of these vulnerabilities, but macroprudential authorities still lack a traceable operational bridge from FinTech activities to systemic-risk channels, measurable indicators, stress-test assumptions and staged policy escalation. This article proposes the FinTech Macroprudential Integration Framework (FMIF) as an evidence-mapped operationalisation layer for existing macroprudential regimes. The FMIF does not claim to replace the frameworks issued by the FSB, BIS, IMF, BCBS, the EU or cyber-resilience authorities; instead, it translates their risk taxonomies and policy insights into a structured workflow linking activity perimeter, dependency registry, indicator formulas, modular stress tests and governance interfaces. The framework is developed for three activity clusters: platform credit and bank–FinTech partnerships; stablecoin-based payment and settlement; and critical third-party technology dependencies. These clusters are mapped to three channels: liquidity/run dynamics, interconnectedness and market spillovers, and operational concentration/correlated disruption. The article contributes by clarifying the research gap, disclosing the evidence-mapping procedure and source-level coding, classifying evidence quality, specifying indicator formulas and calibration principles, adding a stablecoin-run illustrative application, and discussing legal and institutional feasibility. The FMIF should be understood as a decision-support and decision-preparedness framework rather than as a fully validated decision-ready model. Empirical validation, jurisdiction-specific thresholds and legal triggers remain necessary next steps.

Keywords: FinTech; macroprudential policy; systemic risk; stablecoins; platform credit; cloud outsourcing; operational resilience; stress testing; activity-based regulation



Academic Editor: Xiang Gao

Received: 18 May 2026

Revised: 30 June 2026

Accepted: 17 July 2026

Published: 20 July 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

FinTech has moved from a peripheral innovation story to a core question for financial stability (Arner et al., 2016; Cevik, 2023; Financial Stability Board, 2017; World Bank, 2022). Platform credit and bank–FinTech partnerships can accelerate credit origination and expand access (Bazarbash & Beaton, 2020; Philippon, 2016). They can also create rapid credit cycling, concentrated exposures to partner bank and funding structures that resemble non-bank liquidity transformation. Stablecoin-based payment and settlement arrangements can improve transaction efficiency, but at scale they raise redemption, reserve-liquidity

and operational-convertibility risks. At the same time, the digital stack of finance—cloud computing, application programming interfaces, data vendors, cyber-security providers and machine-learning models—creates common technology dependencies that may be resilient at firm level but systemically fragile when many institutions rely on the same provider, region or model architecture (Basel Committee on Banking Supervision, 2024a; Financial Stability Board, 2019, 2023a; International Monetary Fund, 2022).

The macroprudential problem is not simply that FinTech creates new risks. International organisations and regulators have already developed detailed -risk taxonomies and policy recommendations. The more specific problem is operational integration. Macroprudential authorities require an evidence-based workflow that identifies a relevant activity perimeter, maps activities to systemic-risk channels, specifies measurable indicators and minimum data fields, parameterises stress tests, and connects stress outputs to policy escalation. Without such a workflow, authorities face two opposite failure modes: flying blind when fast-growing activities remain outside monitoring systems, and tool overreach when poorly measured risks trigger blunt measures that may suppress innovation without materially improving resilience (Borio et al., 2022; Restoy, 2021).

This article addresses that operational gap by proposing the FinTech Macroprudential Integration Framework (FMIF). The FMIF is not a new taxonomy of FinTech risks. Its novelty lies in making the translation from recognised risks to macroprudential decision inputs explicit, traceable and reproducible. The framework links FinTech activity clusters to systemic-risk channels, then to indicators, stress-testing modules, instrument families and governance interfaces. The objective is not to create a separate FinTech regime, but to show how existing macroprudential, prudential, payment, security and operational-resilience regimes can be connected through a common workflow linking activities, risks and tools..

The analytical scope is deliberately limited to three activity clusters that recur across the evidence base and satisfy a transparent selection rule: at least four of five criteria must be met—macroprudential materiality, scale potential, perimeter mismatch, evidence density and policy urgency. The clusters are: (A1) platform credit and bank-FinTech partnerships; (A2) stablecoin-based payment and settlement; and (A3) critical third-party technology dependencies. The article does not cover decentralised trading protocols, robo-advice, InsurTech, central bank digital currencies, general open banking or crypto-asset speculation except where these are directly connected to the three scoped clusters. This delimitation is designed to preserve analytical depth while retaining the minimum breadth needed for an integration framework.

The paper is organised around three research questions. RQ1 asks how selected FinTech activities can be mapped to macroprudentially relevant systemic-risk channels. RQ2 asks which indicators and minimum reporting fields can operationalize these channels. RQ3 asks how indicators and stress-test outputs can be linked to staged policy instruments and cross-authority governance. The central proposition is that FinTech becomes macroprudentially material when scale, maturity transformation, interconnectedness, operational concentration and behavioural/model correlation interact.

The contribution is fourfold. First, the article offers a gap-oriented synthesis of academic, policy and legal sources on FinTech-related systemic risk. Second, it provides an auditable traceability contribution: each FMIF output is linked to an activity cluster, risk channel, evidence role and policy layer. Third, it provides an operational contribution through indicator formulas, minimum reporting fields, stress-test calibration principles and a stablecoin-run illustrative application. Fourth, it contributes to macroprudential theory by extending systemic materiality beyond balance-sheet leverage and liquidity transformation to include operational concentration and model monoculture generated by shared technology providers, data sources and algorithmic practices.

The remainder of the paper is organized as follows. Section 2 reviews the conceptual background and develops the research gap through a benchmarking exercise. Section 3 details the evidence-mapping methodology, cluster-selection rule and evidence-to-FMIF transformation rules. Section 4 presents the framework architecture, monitoring dashboard, stress-testing modules, and policy instrument mapping. Section 5 benchmarks the FMIF against established macroprudential models and discusses limitations and future validation. Section 6 concludes.

2. Conceptual Background and Gap-Oriented Literature Review

2.1. Macroprudential Policy, Functional Regulation and the Perimeter Problem

Macroprudential policy emerged to mitigate systemic risks that arise from leverage, liquidity transformation, interconnectedness and procyclicality rather than from the failure of individual firms alone (Borio, 2014; Galati & Moessner, 2013). Empirical evaluations show that macroprudential tools can dampen credit growth and risk-taking, but their design remains closely tied to regulated balance sheets and bank-centred reporting systems (Cerutti et al., 2017). FinTech challenges this institutional architecture because economically similar activities may be distributed across banks, non-bank platforms, payment firms, token issuers, technology providers and data vendors. BigTech business models intensify this perimeter problem because data, network effects and multiple financial services are combined within integrated platforms (Bains et al., 2022; Bank for International Settlements, 2019; Boissay et al., 2021; Doerr et al., 2023; Frost et al., 2019).

The functional and activity-based regulation literature therefore becomes central. The principle is not that every activity requires identical rules, but that similar systemic externalities should be detected and managed even when they arise outside traditional legal forms (Borio et al., 2022; Restoy, 2021). The FMIF builds on this idea by asking what a macroprudential authority would need to observe and stress-test if systemic relevance is activity-based and dependency-based rather than being institution-only. This has prompted proposals for regulatory architectures that address cross-sector interdependencies by combining entity-based and activity-based oversight (Crisanto et al., 2022; Ehrentraud et al., 2022).

2.2. Platform Credit and Bank-FinTech Partnerships

Platform and FinTech credit can reduce search, screening and processing frictions, but it can also migrate activity to less regulated segments and create faster credit cycles. Evidence from mortgage and marketplace lending shows that technology can improve processing speed and borrower convenience while changing origination capacity, selection and cyclicity (Buchak et al., 2018; Fuster et al., 2019; Tang, 2019). Cross-country data show that FinTech and BigTech credit scale unevenly across jurisdictions and are shaped by banking-sector competition, unmet credit demand and regulatory architecture (Claessens et al., 2018; Cornelli et al., 2020).

The macroprudential relevance of platform credit is therefore conditional. It does not arise from digital origination itself, but from rapid growth, run-prone funding, concentrated relationships with partner banks, common underwriting models and links to securitisation or warehouse funding. FMIF operationalises this conditionality through a platform-credit reporting perimeter, funding-fragility measures, bank-partnership concentration metrics and a funding-shock stress module.

2.3. Stablecoin-Based Payment and Settlement

Stablecoins convert technology and reserve management into a macroprudential issue when redemption-at-par promises become embedded in payment chains or liquidity man-

agement. Policy analyses focus on reserve quality, redeemability, operational convertibility, cross-border spillovers, and links to banks, custodians, exchanges and money-market funds (Arner et al., 2020; European Union, 2023; Financial Stability Board, 2020, 2023d; Gorton & Zhang, 2023). Empirical work shows that peg stability depends on redemption mechanisms, arbitrage capacity and market microstructure, while large-scale stablecoin adoption can interact with bank deposits, safe assets and monetary transmission (Ahmed & Aldasoro, 2025; Aldasoro et al., 2026; Altavilla et al., 2026; Lyons & Viswanath-Natraj, 2023). Broader policy analyses also assess stablecoins against the requirements of a tokenised monetary and financial system (Bank for International Settlements, 2025).

The research gap is that stablecoins are often analysed under crypto-asset or payment regulation, while macroprudential stress testing requires a different output format: redemption shock assumptions, reserve haircuts, operational redemption capacity, banking/custody links, market spillovers and escalation triggers. FMIF addresses this gap by translating stablecoin risks into a run module and reserve-liquidity indicators that can be connected to system-wide stress exercises.

2.4. Critical Third-Party Dependencies, Cyber Risk and AI/Model Concentration

Digitalisation also changes the nature of systemic risk by intensifying common operational dependencies. Cloud adoption, third-party service provision, cyber incidents and shared AI/model infrastructures can create system-wide externalities even where each individual firm believes its outsourcing arrangement improves resilience (Amromin et al., 2025; European Securities and Markets Authority, 2021; Financial Stability Board, 2023a, 2023b; International Monetary Fund, 2024; U.S. Department of the Treasury, 2023). The policy response has increasingly moved from firm-level outsourcing controls toward oversight of critical third-party providers and convergence in incident reporting (Basel Committee on Banking Supervision, 2021; European Banking Authority, 2019; European Securities and Markets Authority, 2025; European Union, 2022; Financial Stability Board, 2023c; Koh & Prenio, 2023; Kun, 2024).

This literature motivates an expansion of macroprudential materiality. Cyber incidents can also propagate through common service and network dependencies, turning operational disruptions into liquidity and financial-stability events (Adelmann et al., 2020; European Systemic Risk Board, 2022). Operational concentration is not merely a firm-level operational-risk problem when a provider outage can disrupt payments, settlement, risk engines, liquidity management or critical data flows across institutions. Similarly, shared AI/ML models and common data sources may generate behavioural correlation and procyclicality, especially if model updates or data shifts occur simultaneously (European Systemic Risk Board & Advisory Scientific Committee, 2025).

2.5. Synthesis: The Research Gap

The literature and policy frameworks already identify the main vulnerabilities. The remaining gap is not taxonomic; it is operational and architectural. Existing work does not consistently provide a single auditable chain from activity selection to indicator construction, stress-test calibration, instrument mapping and institutional responsibility. To avoid treating this as a merely descriptive claim, the gap is specified through a benchmarking test: an existing framework would close the FMIF gap only if it simultaneously provided (i) a scoped activity-based perimeter, (ii) source-to-risk-channel traceability, (iii) computable indicators and minimum data fields, (iv) stress-module calibration logic, and (v) staged policy/governance escalation. Table 1 summarises the evidence base and Table 2 benchmarks FMIF against this five-part test.

Table 1. Gap-oriented synthesis of the evidence base and FMIF response.

Literature Stream	What Existing Work Provides	Remaining Gap	FMIF Response
Platform credit and bank–FinTech partnerships	Evidence shows benefits for speed, access and segmentation, but also funding fragility, regulatory-arbitrage channels and concentrated bank partnerships.	No common macroprudential reporting template linking platform origination, funding mix, bank partners and model/vendor dependence.	A1 reporting fields, funding-fragility and bank-partnership indicators, platform-credit funding-shock module.
Stablecoin-based payment and settlement	Policy and empirical work identifies redemption, reserve quality, peg deviations and spillovers to banks, MMFs and safe assets.	Stablecoin risks are often treated as crypto/payment regulation rather than as inputs to macroprudential stress testing.	A2 reserve/redemption dashboard, digital-run module and cross-authority escalation map.
Critical third-party technology dependencies	Operational-resilience regimes recognise cloud, ICT, cyber and third-party concentration risks.	Firm-level outsourcing controls do not by themselves produce a system-wide dependency registry or macroprudential outage scenarios.	A3 critical-function registry, CSP/region concentration metrics and cloud/cyber stress modules.
Macroprudential and functional regulation theory	Existing theory supports activity-based, functional and perimeter-neutral approaches to same-risk/same-outcome regulation.	Systemic materiality tests remain centred on balance-sheet leverage/liquidity and understate operational concentration and model monoculture.	FMIF proposes conditional macroprudential materiality: scale + maturity transformation + interconnectedness + operational concentration + behavioural correlation.

Table 2. Benchmarking FMIF against existing policy and regulatory frameworks.

Benchmark Criterion	What Existing Frameworks Provide	FMIF Addition	Main Contribution
Activity-based perimeter	FSB, BIS, IMF and EU work identify many activities and risks, but usually within separate policy domains.	FMIF uses a transparent cluster-selection rule and excludes non-material activities.	Improves risk identification by defining the monitoring perimeter before tools are calibrated.
Source-to-output traceability	Policy frameworks generally cite vulnerabilities but rarely disclose a source-level activity/risk/policy-layer code.	FMIF discloses a source matrix and transformation rules T1–T6.	Improves reproducibility and reduces narrative discretion.
Computable indicators	Existing reports discuss redemptions, and concentration and outsourcing risks but do not always supply indicator formulas and minimum fields.	FMIF specifies formulas, data owners, frequency and calibration notes.	Improves operational monitoring and early-warning dashboards.
Stress-module calibration	Stablecoin, liquidity, cyber and outsourcing frameworks contain scenario ideas but not a combined macroprudential plug-in design.	FMIF links shocks to inputs, outputs and policy use for run, platform-credit, cloud and cyber modules.	Improves stress-testing integration rather than only risk identification.
Staged escalation and governance	DORA, MiCA, prudential and macroprudential regimes allocate responsibilities separately.	FMIF maps outputs to Stage 0–3 escalation and cross-authority coordination.	Improves regulatory coordination efficiency and policy calibration.

2.6. What the FMIF Adds Relative to Existing Frameworks

The FMIF's novelty does not lie in identifying new FinTech risks. Its incremental contribution is an integrated architecture linking activities, risk channels, indicators, stress tests and policy tools, together with transformation rules that specify how a coded evidence base

produces framework outputs. Existing frameworks often provide risk taxonomies, issuer requirements, outsourcing standards or high-level policy recommendations. FMIF turns these dispersed outputs into a macroprudential workflow. It adds five specific elements: a scoped activity-based perimeter; minimum reporting templates; an evidence-coded indicator dashboard; modular stress-test calibration principles; and staged governance/escalation logic. Table 2 specifies the benchmark used to separate these outputs from existing frameworks.

3. Materials and Methods: Evidence Mapping and Framework Construction

3.1. Review Design and Protocol

The article uses a structured evidence-mapping review for framework construction. Evidence mapping is appropriate because the relevant knowledge base is distributed across peer-reviewed finance articles, central-bank working papers, standard-setter reports, supervisory toolkits and binding legal texts. The purpose is not to estimate pooled effect sizes, but to identify mechanisms, operational indicators, stress-test assumptions and governance requirements relevant to macroprudential integration.

The search window focused on the post-crisis digitalisation period from 2014 to 2026, with earlier foundational macroprudential sources retained where necessary. Sources were collected through targeted searches in Google Scholar, Scopus and Web of Science, and in the repositories of the FSB, BIS, BCBS, CPMI-IOSCO, IMF, ECB, EU institutions, ESRB, EBA, ESMA and selected central banks. Backward and forward citation tracing was used from anchor publications on FinTech credit, stablecoins, cloud outsourcing, cyber risk, BigTech and macroprudential policy. Appendix A provides the search strings and repositories.

3.2. Inclusion and Exclusion Criteria

A source was included if it met two conditions: it addressed at least one scoped activity cluster or cross-cutting macroprudential framework question, and it provided evidence, concepts, legal mandates or policy guidance relevant to at least one of the systemic-risk channels. Purely micro-level adoption studies without stability implications and consumer-interface studies without systemic channels, non-substantive commentary, duplicate versions and sources without a clear link to the activity-risk-tool chain were excluded. Where both a working paper and a peer-reviewed version existed, the peer-reviewed version was preferred, unless the working paper contained more recent policy-relevant data.

3.3. Selection Transparency Statement: Targeted Evidence Map, Not a PRISMA-ScR Review

This article does not claim full PRISMA-ScR compliance and does not present the review as a preregistered systematic scoping review. It is a targeted evidence map for framework construction. To prevent misinterpretation, the manuscript avoids the phrase “PRISMA-ScR-inspired”. Because the original searches were conducted through a combination of academic indices, Google Scholar, institutional repositories and citation tracing, exact initial hit counts are not retrospectively reconstructed: such counts are volatile across dates, locations, repository interfaces and search-engine settings. To avoid false precision, the manuscript discloses the final retained corpus ($n = 54$), the repositories and search strings, inclusion/exclusion logic, source-level coding matrix, evidence-role classification and transformation rules. This transparency supports auditability while preserving the methodological boundary of the study.

3.4. Evidence-Quality and Evidence-Role Classification

The corpus combines academic articles, working papers, policy reports and legal texts. These sources should not be treated as equivalent forms of evidence. Accordingly, each source is classified by its primary evidence role. Peer-reviewed empirical articles are used mainly for mechanism and empirical regularity claims; official reports for supervisory architecture and feasibility; legal texts for mandate and reporting constraints; and conceptual or regulatory architecture papers for theoretical framing. This avoids a mechanical equality of evidentiary weight while preserving the mixed-evidence nature of the field. The five evidence classes and their intended evidentiary roles are summarised in Table 3.

Table 3. Evidence-quality and evidence-role classification used in FMIF.

Class	Source Type	Role in FMIF	Examples
E1	Peer-reviewed empirical or theoretical articles	Mechanism evidence and empirical regularities; highest weight for causal/empirical claims.	Buchak et al.; Fuster et al.; Tang; Lyons & Viswanath-Natraj.
E2	Working papers and central-bank research papers	Emerging evidence and method development; used cautiously and updated when peer-reviewed versions appear.	BIS working papers; IMF working papers; ECB working papers.
E3	Official policy reports and standard-setter guidance	Supervisory architecture, risk taxonomies, feasibility, policy priorities and implementation constraints.	FSB, BIS, BCBS, IMF, ESRB, U.S. Treasury.
E4	Binding legal/regulatory texts	Mandates, reporting powers, institutional feasibility and legal constraints.	DORA; MiCA.
E5	Conceptual/regulatory architecture literature	Theoretical framing for activity-based and functional regulation; used for contribution and limitations.	Borio; Galati & Moessner; Borio et al.; Restoy.

3.5. Coding Procedure and Auditability

Each retained source was coded along four dimensions: activity cluster (A0 cross-cutting macroprudential framework, A1 platform credit, A2 stablecoin-based payment/settlement, A3 critical third-party dependencies), systemic-risk channel (R1 liquidity/run dynamics, R2 interconnectedness and spillovers, R3 operational concentration/correlated disruption), policy layer (L1 monitoring and reporting, L2 stress testing, L3 instruments and governance) and evidence role (E1–E5).

The study deliberately does not report a retrospective Cohen's kappa statistic. The original framework construction was based on author-consensus coding rather than a preregistered double-blind coding exercise. Reporting an ex post reliability coefficient would risk creating a false impression of independent coding. To strengthen credibility without fabricating a statistic, the article provides a fixed codebook, a source-level matrix, an evidence-role classification and explicit transformation rules from evidence to FMIF outputs. Future updates can convert the protocol into a double-coded systematic evidence map and report kappa or Krippendorff's alpha. The corresponding codebook is presented in Table 4.

Table 4. FMIF codebook for activity clusters, risk channels and policy layers.

Code	Category	Definition
A0	Cross-cutting macroprudential/theoretical source	Macroprudential theory, regulatory architecture or broad digital finance framework.
A1	Platform credit and bank-FinTech partnerships	Digital origination, servicing, BaaS, platform funding and partner-bank concentration.
A2	Stablecoin-based payment and settlement	Stablecoin issuance, redemption, reserves, custody, on/off ramps and settlement use.
A3	Critical third-party dependencies	Cloud, ICT providers, APIs, data vendors, cyber dependencies and shared AI/ML models.
R1	Liquidity/run dynamics	Fast redemptions, withdrawals, rollover failure, settlement gridlock or fire-sale pressure.
R2	Interconnectedness and market spillovers	Balance-sheet, market, custody, collateral, links to partner banks, FMI or cross-border links.
R3	Operational concentration/correlated disruption	Common providers, regions, software, models, data sources or incident clusters.
L1	Monitoring/reporting	Indicators, minimum data fields, dashboards, dependency registries and early warning.
L2	Stress testing	Scenario design, calibration assumptions, stress outputs and second-round effects.
L3	Instruments/governance	Escalation, policy tools, legal mandates, MoUs, cross-authority coordination and crisis protocols.

3.6. Transformation Rules from Evidence Map to FMIF Outputs

A central design requirement is that FMIF outputs must not appear as arbitrary author judgement. The framework therefore uses explicit transformation rules. A proposed indicator, stress module or escalation output is included only when the source-level evidence satisfies the relevant rule. These rules do not turn the study into a quantitative meta-analysis; rather, they make the framework-construction logic replicable for a mixed academic-policy-legal corpus. Table 5 sets out the six transformation rules and their minimum evidentiary conditions.

Table 5. Transformation rules from evidence mapping to FMIF indicators, stress modules and policy outputs.

Rule	Operation	Minimum Evidentiary Condition	FMIF Output
T1. Code the source	Assign A/R/L/E codes to each retained source.	Source discusses a scoped activity or cross-cutting architecture and at least one risk channel.	Supplementary source matrix discloses source-level codes.
T2. Identify mechanism	Extract the economic or operational mechanism that can generate a systemic externality.	At least one E1/E2/E3/E5 source supports the mechanism.	Mechanism list: maturity transformation, redemption run, network spillover, operational concentration, model correlation.
T3. Generate indicator	Translate the mechanism into an observable state variable.	Indicator retained only if a formula or operational measure, data owner, and reporting frequency can be specified.	Funding Fragility Index; Redemption Stress Ratio; Top-3 CSP Dependence; Model Similarity Index.

Table 5. *Cont.*

Rule	Operation	Minimum Evidentiary Condition	FMIF Output
T4. Generate stress module	Convert high-priority risk channels into shock templates.	Module retained only if the shock has measurable inputs, outputs and policy use.	Stablecoin run, platform funding shock, cloud outage, correlated cyber incident.
T5. Map policy use	Link indicator or stress output to staged escalation.	At least one E3/E4/E5 source must support supervisory relevance, legal feasibility or governance interface.	Stage 0 measurement; Stage 1 targeted resilience; Stage 2 macroprudential adaptation; Stage 3 crisis protocol.
T6. Exclude output	Exclude candidate outputs that cannot be measured or linked to a systemic channel.	Micro-only adoption, consumer interface, or single-firm compliance topic without systemic propagation channel.	Excluded topics: robo-advice, InsurTech, CBDC, open banking unless directly linked to A1–A3.

The procedure can be summarised as follows: for each retained source, assign activity, channel, policy-layer and evidence-role codes; extract systemic mechanisms; retain only mechanisms that can be linked to observable state variables; construct indicators where formulas, data owners and reporting frequency can be specified; construct stress modules where shocks, inputs, outputs and policy use can be specified; and map outputs to staged governance only where a policy or legal source supports feasibility. The Supplementary File discloses the source-level matrix and a source-to-output audit table.

Supplementary File S1 provides the source-level evidence matrix and the source-to-output audit table, while Supplementary File S2 provides the optional author-verification worksheet for future double-coding and inter-coder reliability assessment.

3.7. Cluster-Selection Rule and Scope Conditions

The retained clusters were not selected because they represent all of FinTech. They were selected because they satisfy a minimum materiality rule. A cluster is retained if it satisfies at least four of five criteria: (1) macroprudential materiality, meaning a plausible system-wide externality beyond firm-level risk; (2) scale potential, meaning capacity to affect credit, money, payments or operational infrastructure at scale; (3) perimeter mismatch, meaning the activity spans more than one supervisory perimeter; (4) evidence density, meaning at least eight retained sources across at least two evidence classes; and (5) policy urgency, meaning explicit treatment in current standard-setter, supervisory or legal frameworks. This rule introduces measurable decision points without implying universal numerical thresholds for systemic importance. Table 6 applies the selection rule to the retained and excluded activity clusters.

Table 6. Scope-selection rule and retained activity clusters.

Candidate Cluster	Selection-Rule Result	Reason for Treatment	Decision
A1 Platform credit and bank-FinTech partnerships	Meets: materiality, scale potential, perimeter mismatch, evidence density, policy urgency.	Credit growth, funding fragility and partner–bank links are observable and stressable.	Retained.
A2 Stablecoin-based payment and settlement	Meets: materiality, scale potential, perimeter mismatch, evidence density, policy urgency.	Redemption runs, reserve-liquidation pressure and payment/custody links are observable and stressable.	Retained.

Table 6. *Cont.*

Candidate Cluster	Selection-Rule Result	Reason for Treatment	Decision
A3 Critical third-party dependencies	Meets: materiality, scale potential, perimeter mismatch, evidence density, policy urgency.	Critical-function dependencies, outage propagation and cloud/provider concentration are observable and stressable.	Retained.
Excluded activities	Do not consistently satisfy the retained-cluster rule within this paper’s macroprudential focus.	Robo-advice, InsurTech, CBDC, general open banking, decentralised trading and crypto speculation require separate frameworks unless directly linked to A1–A3.	Excluded.

4. Results: The FinTech Macroprudential Integration Framework (FMIF)

4.1. Framework Overview

The FMIF is an operational translation layer. It starts with an activity-based perimeter and dependency registry, maps the scoped activities to risk channels, translates the channels into measurable indicators and minimum data templates, parameterises modular stress tests, and links outputs to staged policy escalation. Figure 1 summarises the workflow.

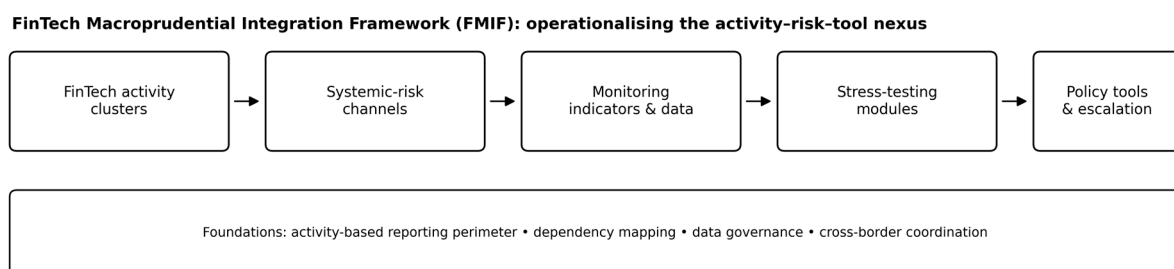


Figure 1. FMIF as an operational translation layer: from activity perimeter and risk channels to monitoring, stress testing and policy escalation.

4.2. Activity Clusters and Systemic-Risk Channels

The three activity clusters are mapped to three channels. Platform credit is most directly linked to funding fragility and interconnectedness with partner banks, but it may also create operational concentration through shared servicing, KYC/AML, scoring, or cloud providers. Stablecoins are linked to run dynamics, reserve-asset spillovers, custody and on/off-ramp concentration. Critical third-party dependencies generate operational concentration, but outages can also trigger liquidity stress and market spillovers if payments, settlement or risk-management functions are disrupted. Table 7 summarises the resulting activity–channel mapping.

4.3. Monitoring Layer: Indicator Formulas and Data Requirements

The monitoring layer follows a core operational requirement: indicators must be measurable, not merely conceptual. Table 8 specifies formulas, data requirements, frequency and interpretation for selected FMIF indicators. Universal thresholds are not proposed because market structure, legal powers and data quality differ across jurisdictions. Instead, the framework recommends risk bands calibrated through peer distributions, historical stress episodes, reverse stress testing and supervisory judgement. The corresponding minimum reporting templates are provided in Appendix B, Table A2.

Table 7. Mapping activity clusters to systemic-risk channels.

Activity Cluster	R1 Liquidity/Run Dynamics	R2 Interconnectedness & Spillovers	R3 Operational Concentration
A1 Platform credit & bank partnerships	Warehouse-line runs, investor redemptions, borrower drawdowns, maturity mismatch.	Partner-bank concentration, securitisation/funding links, shared underwriting models.	Common servicing, KYC/AML, scoring, cloud and API vendors.
A2 Stablecoin-based payment & settlement	Redemption-at-par run, peg deviation, redemption queue and reserve liquidity stress.	Bank/custodian/MMF/exchange links, reserve-asset spillovers, cross-border flows.	Issuer, custodian, settlement-rail and on/off-ramp concentration; operational convertibility.
A3 Critical third-party dependencies	Payment/liquidity gridlock during outages and intraday liquidity stress.	Shared infrastructure causing simultaneous cross-border or cross-sector disruption.	Cloud provider/region concentration, cyber incident clustering, software and model monoculture.

Table 8. Selected FMIF indicators: formulas, data fields, frequency and interpretation.

Indicator	Formula/Operational Measure	Data Required	Frequency	Interpretation/Calibration
Funding Fragility Index	(short-term wholesale funding + redeemable investor funding + funding maturing ≤ 30 days + undrawn commitments $\times$ drawdown factor)/total funding	Platform funding maturity, warehouse lines, investor redemption terms, undrawn commitments, liquidity buffers.	Quarterly; monthly for fast-growing platforms.	Higher values indicate more run-prone platform funding. Thresholds should be jurisdiction-specific and calibrated to historical stress, supervisory judgement and peer distributions.
Bank Partnership HHI	$HHI = i \sum s_i^2$, where s_i is partner bank i 's share of platform origination, funding or servicing volume.	Partner-bank identifiers, volumes, contract terms, product/geography split.	Quarterly.	Identifies single-point-of-failure partnerships and concentration of bank-FinTech dependency.
Stablecoin Redemption Stress Ratio	$\max(\text{redemptions over } 1/3/7 \text{ days})/\text{circulating supply}$; optionally weighted by redemption queue or failed-redemption rate.	Circulating supply, issuance/redemption flows, queues, settlement delays.	Daily/weekly.	Measures run intensity and supplies calibration inputs for the digital-run module.
Reserve Liquidity Coverage	High-quality liquid reserves after haircuts divided by stressed redemption outflows over the selected horizon.	Reserve composition, maturity, custody location, haircuts, stressed outflow assumptions.	Monthly; higher frequency during stress.	Assesses ability to meet redemptions without fire sales or operational bottlenecks.
Peg Deviation Tail Metric	99th percentile of absolute deviation from peg + persistence measure, e.g., hours/days beyond tolerance band.	Market prices, reference value, trading venue data, liquidity indicators.	Daily/intraday.	Captures market confidence, arbitrage capacity and operational convertibility.
Top-3 CSP Dependence	Critical workloads hosted by the top three cloud or service providers divided by total critical workloads.	Critical-function inventory, provider identifiers, service type, region/zone, fallback capability.	Semi-annual; after major outsourcing changes.	Measures technology-provider concentration and potential systemic single points of failure.
Single-Region Concentration	Critical workloads hosted in the largest cloud region or availability zone divided by total critical workloads.	Hosting region/zone, redundancy and recovery arrangements.	Semi-annual.	Identifies geographic/technical concentration and failure-domain exposure.
Data/Model Concentration Proxy	HHI or top-provider share across scoring vendors, model providers, data providers or common model classes.	Model/vendor registry, feature families, model class, update cycle, outsourcing chain.	Annual; after major model changes.	Detects behavioural correlation and model monoculture risk.
Model Similarity Index	Weighted average of pairwise similarity scores based on vendor identity, model class, feature overlap and update synchronisation.	High-level model documentation, feature families, vendor/model identifiers.	Annual.	Higher values imply greater risk of correlated underwriting, pricing or liquidity-management behaviour.
Dependency Network Centrality	Eigenvector or betweenness centrality of provider nodes in the entity-service-critical-function network.	Entity-provider-function graph, service criticality, cross-border links.	Annual; stress update during incidents.	Identifies providers whose failure could propagate across many institutions or jurisdictions.

4.4. Stress-Testing Layer: Calibration Principles

FMIF stress modules are not universal numerical scenarios. They are parameterised templates that jurisdictions can integrate into existing bank, FMI, cyber and system-wide exercises. Calibration should combine historical stress episodes, scenario design, reverse stress testing, supervisory judgement and dependency-registry data. Historical liquidity episodes, including the 2023 banking turmoil, can also inform severity assumptions and reverse-stress calibration (Basel Committee on Banking Supervision, 2024b). Table 9 summarises the modules and calibration logic.

Table 9. FMIF stress-test modules and calibration principles.

Module	Primary Channel	Calibration Logic	Key Inputs	Outputs	Use in Policy Cycle
Stablecoin run	R1/R2	Historical redemption/depeg episodes; issuer-specific redemption distribution; reserve-market liquidity; reverse stress testing; supervisory severity tiers.	Redemption shock over 1/3/7 days; reserve haircuts; market-maker capacity; on/off-ramp capacity; custodian/bank links.	Liquidity shortfall, reserve fire-sale pressure, failed redemptions, settlement delays and bank/MMF/custodian spillovers.	Reserve-liquidity requirements, disclosure, exposure limits, settlement contingency planning and cross-authority escalation.
Platform credit funding shock	R1/R2	Warehouse-line maturities; securitisation-market freeze; partner-bank withdrawal; borrower drawdown shock; delinquency-vintage deterioration.	Funding mix, rollover share, liquidity buffers, exposures to partner banks, cohort performance and commitments.	Platform liquidity gap, credit-supply contraction, liquidity/capital pressure at partner bank and second-round contraction.	Targeted reporting, concentration limits, supervisory liquidity add-ons and stress-test integration for partner banks.
Cloud outage/service disruption	R3/R1	Outage duration calibrated by plausible severe incidents, resilience-test results, RTO/RPO, substitution capacity and critical-function mapping.	Provider/region dependencies, critical functions, payment volumes, recovery-time objectives and manual fallback capacity.	Payment queue build-up, settlement delay, liquidity hoarding, operational loss and recovery time.	Portability/exit testing, multi-region requirements, critical-provider oversight and joint incident playbooks.
Correlated cyber incident	R3/R2	Common software vulnerability, simultaneous infection rate, data-integrity impairment, confidence shock and recovery capability.	Incident taxonomy, vendor map, backup integrity, recovery capacity and cross-border client share.	Service unavailability, confidence effects, liquidity hoarding, market disruption and cross-border propagation.	Cyber stress testing, incident-reporting convergence, joint exercises and cross-border crisis coordination.

4.5. Policy Instrument Mapping and Staged Escalation

The FMIF uses staged escalation to avoid premature tool use. Stage 0 makes activities and dependencies measurable through reporting and registries. Stage 1 introduces targeted resilience measures, such as liquidity buffers, portability requirements or concentration limits. Stage 2 adapts macroprudential tools where measured systemic materiality is evident. Stage 3 defines crisis protocols, public communication and continuity arrangements. Escalation should be based on a composite materiality assessment combining scale, fragility, interconnectedness and operational concentration rather than on a single mechanical trigger. Table 10 maps the three risk channels to the four escalation stages and associated instrument families.

Table 10. Policy instrument mapping and staged escalation.

Risk Channel	Stage 0: Make Measurable	Stage 1: Targeted Resilience	Stage 2: Macroprudential Adaptation	Stage 3: Crisis Protocols
R1 Liquidity/run dynamics	Redemption/funding templates, intraday liquidity metrics.	Reserve/liquidity buffers, contingency funding, disclosure.	Exposure limits, liquidity add-ons, integration into system-wide stress tests.	Liquidity backstops where legally available, settlement continuity and public communication.
R2 Interconnectedness/spillovers	LEI-based exposure map, bank-platform-stablecoin-FMI links.	Concentration limits, enhanced disclosure, margin/haircut measures where relevant.	Systemic surcharges or macroprudential limits for concentrated exposures.	Cross-border coordination, coordinated market actions and resolution/restructuring links.
R3 Operational concentration	Critical service registry, cloud/provider/region map, incident reporting.	Portability/exit tests, multi-region resilience for critical functions.	Systemic third-party oversight and concentration-related measures.	Joint incident playbooks, substitute/bridge arrangements and crisis exercises.

4.6. Legal and Institutional Feasibility

The FMIF does not assume that one macroprudential authority can impose every relevant measure. For payment and settlement functions, these interfaces should remain consistent with the Principles for Financial Market Infrastructures ([Committee on Payment and Settlement Systems & International Organization of Securities Commissions, 2012](#)). Its governance contribution is to define interfaces among prudential supervisors, payment/FMI overseers, securities or crypto-asset authorities, operational-resilience supervisors, competition/data-protection authorities where relevant, and cross-border colleges. Granular data from platforms, stablecoin issuers, custodians, cloud providers and banks create confidentiality, security and mandate issues. FMIF therefore relies on a tiered disclosure model: granular data to legally empowered supervisors, aggregated concentration indicators to macroprudential committees, and public disclosure only where it strengthens discipline without creating security or competition risks. Table 11 identifies the likely lead authorities, data requirements, legal constraints and proposed coordination solutions.

Table 11. Governance and legal-feasibility map.

Function	Likely Lead Authority	Data Needed	Legal/Coordination Issue	FMIF Solution
Platform credit monitoring	Macroprudential authority with prudential supervisor and credit registry	Origination, funding mix, partner-bank identifiers, cohort performance and vendor/model metadata.	Non-bank perimeter, BaaS opacity, commercial sensitivity and fragmented credit data.	Activity-based reporting template, LEI-based partner mapping, secure enclave for granular samples and phased reporting.
Stablecoin run monitoring	Payments/FMI overseer, crypto/securities regulator and macroprudential committee	Reserve composition, redemptions, custody/bank accounts, on/off ramps and settlement links.	Cross-border issuers, custody chains, confidentiality and legal divergence between payment and securities regimes.	Confidential supervisory reporting, aggregated dashboards, reserve/redemption stress module and crisis communication protocol.
Critical third-party dependency mapping	Operational-resilience authority with macroprudential coordination	Critical functions, cloud providers/regions, subcontracting, incident data, RTO/RPO and portability tests.	Commercially sensitive data, security risk, subcontractor opacity and cross-border provider location.	Tiered disclosure model, system-wide dependency registry, incident taxonomy and joint operational exercises.
System-wide stress testing	Macroprudential committee plus sectoral authorities	Exposure networks, liquidity assumptions, dependency graphs and incident response capacities.	No single authority holds all powers or data; cross-sector data-sharing constraints.	MoUs, joint stress-test protocol, defined data owners and pre-agreed escalation timelines.

4.7. Illustrative Application: Stablecoin Run Module

To avoid overstating empirical validation while improving practical credibility, this section applies FMIF to a hypothetical stablecoin-run scenario. The application is illustrative and uses stylised inputs. It demonstrates how FMIF translates activity data into indicators, stress assumptions, outputs and escalation decisions; it does not claim to validate the framework empirically.

Activity and channel: The activity is A2 stablecoin-based payment and settlement. The channels are R1 liquidity/run dynamics and R2 interconnectedness/spillovers. The materiality test asks whether the issuer's scale, reserve composition, redemption capacity and links to banks, custodians and on/off ramps could transmit stress to broader markets. The stylised scenario inputs are reported in Table 12.

Table 12. Stylised inputs for the stablecoin-run illustrative application.

Input	Stylised Value	FMIF Use
Circulating supply	100 units	Scale denominator for redemption and reserve metrics.
Reserve composition	25% cash/bank deposits; 55% short-term government bills; 15% repo/MMF; 5% other assets.	Reserve-liquidity coverage and fire-sale mapping.
Operational redemption capacity	15 units/day normally; 8 units/day under cyber/operational stress.	Operational bottleneck in run module.
Severe redemption scenario	30% over 3 days and 45% over 7 days.	Shock calibrated from severe scenario design and reverse stress testing rather than a universal threshold.
Reserve haircuts	0% cash; 2% bills; 5% repo/MMF; 15% other.	Converts accounting reserves to stressed liquid value.
On/off-ramp concentration	Top two intermediaries process 65% of redemptions.	Interconnectedness and operational choke-point indicator.

Step 1 calculates the redemption stress ratio: $30/100 = 30\%$ over three days and $45/100 = 45\%$ over seven days. Step 2 calculates stressed reserve liquidity coverage after haircuts. If immediately available reserves are below expected redemptions or if operational redemption capacity is binding, the module records an operational-liquidity shortfall even when total reserves appear sufficient on a mark-to-market basis. Step 3 maps the shortfall to spillover nodes: reserve asset markets, custodian banks, on/off ramps, payment service providers and any bank with direct exposure. Step 4 assigns an escalation stage. A high redemption ratio combined with peg persistence, operational bottlenecks and concentrated on/off ramps would move the case beyond monitoring into targeted resilience measures and potentially crisis coordination. The resulting indicators, outputs and escalation implications are summarised in Table 13.

The case shows why FMIF is best described as decision-support rather than as a fully decision-ready regime. The formulas and escalation logic are transferable, but the thresholds, legal triggers and available tools depend on the jurisdiction's stablecoin regime, payment law, crisis-management powers and supervisory data access.

Table 13. FMIF outputs in the stablecoin-run application.

Indicator/Output	Illustrative Calculation or Interpretation	Escalation Implication
Redemption stress ratio	30% over 3 days; 45% over 7 days.	Triggers enhanced monitoring and scenario update.
Reserve liquidity coverage	Computed after asset haircuts and time-to-liquidate assumptions.	If coverage < 1 over relevant horizon, targeted reserve/liquidity measures.
Operational redemption bottleneck	Normal capacity 15/day falls to 8/day under operational stress.	Coordinate with payments/operational-resilience authority.
On/off-ramp concentration	Top two intermediaries process 65%.	Assess choke points and contingency routing.
Spillover map	Custodian banks, MMFs/repo, exchanges and settlement rails.	Cross-authority communication and exposure monitoring.

4.8. Implementation Roadmap

FMIF implementation should be sequenced. Months 0–12 focus on perimeter definition, dependency registry and minimum reporting. Months 12–24 add dashboards, calibration exercises and pilot stress modules. Months 24–36 integrate run/outage modules into regular stress-testing programmes and refine governance interfaces. Beyond 36 months, authorities can calibrate tools, crisis playbooks and cross-border colleges using accumulated evidence. The sequencing prioritises measurability before tool recalibration, because unreliable data would produce either inaction or disproportionate intervention.

5. Discussion

5.1. Benchmarking FMIF Against Established Macroprudential Models

The FMIF is complementary to established macroprudential models rather than a replacement for them. The relevant benchmark is not whether FMIF invents an entirely new class of systemic risk, but whether it provides decision inputs that standard models do not generate when digital activities and technology dependencies cross supervisory perimeters. Table 14 compares FMIF with major macroprudential model families.

Table 14. FMIF relative to established macroprudential model families.

Benchmark Model Family	What It Already Does	Digital-Finance Limitation	FMIF Complement
Early-warning indicator systems	Credit growth, leverage, asset prices, liquidity and macro-financial imbalances.	Often bank- or market-centred and weakly connected to FinTech activity perimeters, stablecoin redemption operations or cloud dependencies.	Adds activity-based perimeter, dependency registry and FinTech-specific indicators.
Bank solvency/liquidity stress tests	Capital depletion, funding liquidity, credit losses and bank-balance-sheet channels.	Do not directly model non-bank platform funding, stablecoin redemption capacity or third-party outage propagation.	Adds plug-in run/outage modules that can feed into existing stress tests.

Table 14. Cont.

Benchmark Model Family	What It Already Does	Digital-Finance Limitation	FMIF Complement
Network contagion and SIFI models	Balance-sheet exposures, interbank links and financial network centrality.	Technology providers, cloud regions, data/model vendors and operational service nodes are usually outside exposure networks.	Extends network nodes to technology dependencies and operational concentration.
NBFI liquidity frameworks	Fund redemptions, margining, fire sales and market liquidity.	Stablecoin redemption queues, reserve custody and on/off-ramp choke points are not fully integrated.	Adds stablecoin reserve/redemption stress mapping.
Cyber/operational-resilience frameworks	ICT risk management, incident reporting, resilience testing and third-party oversight.	Often firm-level or operational in orientation; macroprudential escalation and systemic concentration indicators remain underdeveloped.	Connects critical-function registry to macroprudential materiality and staged escalation.
Activity-based regulation theory	Same-risk/same-outcome principle and perimeter-neutral regulatory design.	Does not by itself provide formulas, stress modules or governance playbooks.	Operationalises activity-based theory through measurable indicators and policy interfaces.

The theoretical extension is therefore incremental but substantive. It does not claim that technology risk displaces leverage, liquidity or interconnectedness. It claims that systemic materiality in digital finance also depends on operational concentration and behavioural/model correlation, and that these mechanisms require units of observation—providers, regions, data sources, models and operational conversion capacity—that are not fully captured by traditional balance-sheet reporting.

5.2. Policy Contribution

For regulators, the FMIF implies that the first policy investment should be data architecture: reporting templates, dependency registries, common identifiers, incident taxonomies and data-sharing MoUs. For industry, the implication is that critical third-party dependence and reserve/redemption operations are becoming systemic-risk inputs rather than narrow operational or compliance matters. For stablecoin issuers and platform-credit firms, the framework implies that transparency and resilience expectations increase with scale and interconnectedness.

5.3. Avoiding Overstated Policy Readiness and Defining Future Validation

The FMIF improves decision preparedness by specifying formulas, data fields, scenario templates and governance interfaces. It is not a fully validated decision-ready model because thresholds, calibration procedures, legal triggers and institutional responsibilities must be defined by jurisdiction. Practical verification would require confidential supervisory data on platform funding, stablecoin flows and reserves, bank/custodian exposures, operational dependency maps and incident propagation. The revised manuscript therefore does not claim practical verification. Instead, it provides a pilot validation protocol: authorities can compare FMIF indicators with historical stress episodes, run stablecoin and outage modules on confidential supervisory data, back-test warning signals where data exist, and

evaluate whether the framework improves timeliness, proportionality and cross-authority coordination relative to existing dashboards.

5.4. Limitations and Future Research

The study has four main limitations. First, it is a framework-building and evidence-mapping study, not an empirical validation of crisis probabilities. Second, the evidence map is transparent but not a preregistered systematic review with preserved initial hit counts and blinded double coding. Third, the formulas and stress modules require confidential supervisory data for calibration. Fourth, legal feasibility differs across jurisdictions. Future research should empirically test the FMIF proposition using supervisory data on platform funding, stablecoin flows, reserve assets, cloud dependencies, incident propagation and AI/model concentration. A promising direction is to combine dependency graphs with liquidity and operational stress models to quantify second-round effects from technology-provider outages or digital runs.

6. Conclusions

This article proposed the FinTech Macroprudential Integration Framework as an evidence-mapped operationalisation layer for selected FinTech-related systemic risks. The framework responds to a gap in the existing literature and policy architecture: the absence of a traceable workflow from FinTech activity perimeter to systemic-risk channels, indicators, stress modules, policy tools and governance responsibilities. FMIF focuses on platform credit, stablecoin-based payment and settlement, and critical third-party technology dependencies, and maps these activities to liquidity/run dynamics, interconnectedness/spillovers and operational concentration.

The article's main proposition is conditional. FinTech becomes macroprudentially material when scale, maturity transformation, interconnectedness, operational concentration and behavioural/model correlation interact. The recommended policy sequence is to make activities measurable, build a dependency registry, introduce dashboards and stress modules, and only then recalibrate instruments and crisis protocols. FMIF should therefore be read neither as a universal rulebook nor as a separate FinTech regime, but as a structured decision-support architecture for integrating digital finance into existing macroprudential practice.

Supplementary Materials: The following supporting information can be downloaded at: <https://www.mdpi.com/article/10.3390/ijfs14070192/s1>, Supplementary File S1: Source-Level Evidence Matrix and Operational Templates; Supplementary File S2: Author Verification Worksheet for Future Double-Coding and Inter-Coder Reliability Assessment.

Author Contributions: Conceptualization, J.K. and A.L.; methodology, J.K. and A.L.; investigation, J.K.; formal analysis, J.K. and A.L.; writing—original draft, J.K. and A.L.; writing—review and editing, J.K. and A.L.; visualisation, J.K.; supervision, J.K. and A.L.; project administration, J.K. All authors have read and agreed to the published version of the manuscript.

Funding: The APC was funded by István Széchenyi University. Identification number: 166PTP2026.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The study is based on publicly available academic, policy and legal sources cited in the manuscript. The search strategy, repositories, evidence classification and source-level matrix are described in the article and Supplementary Materials. No primary dataset, proprietary dataset, survey data, interview data or confidential supervisory data were generated or analysed.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Search Strategy and Evidence-Selection Transparency

Table A1 reports the core search strings and repositories used to construct the evidence base. The search was intentionally broad to capture an interdisciplinary field spanning banking, payments, crypto-assets, operational resilience, cyber risk and macroprudential regulation. The protocol was targeted and framework-oriented rather than designed for quantitative meta-analysis. Appendix A reports the search strings and repositories, whereas Supplementary File S1 provides the source-level coding matrix and source-to-output audit table.

Table A1. Search strings and repositories.

Domain	Core Search Strings	Repositories/Indices
Platform credit	"fintech credit"; "marketplace lending"; "bank-fintech partnership"; "banking-as-a-service"; "digital lending"; "shadow bank"	Google Scholar; Scopus; Web of Science; BIS; IMF; central-bank working papers
Stablecoins and tokenised payments	"stablecoin" AND run; "redeemability"; "reserve composition"; "tokenised settlement"; "crypto-asset regulation"	FSB; BIS; IMF; ECB; EU legal texts; academic indices
BigTech and platform finance	"BigTech"; "platform finance"; "data-network-activities"; "competition"; "privacy"; "financial intermediation"	BIS AER; BIS working papers; IMF FinTech Notes; academic indices
Cloud and ICT third parties	"cloud outsourcing"; "critical third-party"; "ICT concentration"; "operational resilience"; "outsourcing guidelines"	FSB; BCBS; ESMA; EBA; EU DORA; IMF; U.S. Treasury
Cyber and AI systemic risk	"cyber risk" AND "financial stability"; "incident reporting"; "AI systemic risk"; "model monoculture"	IMF; FSB; ESRB/ASC; academic indices

Appendix B. Minimum Data Templates

Table A2. Minimum data templates for FMIF reporting.

Template	Minimum Reporting Fields	Frequency	Implementation Notes
A1 Platform credit	Origination/outstanding volumes; product/geography; funding source mix; maturity; partner-bank identifiers; underwriting model version/high-level feature families; cohort performance; key vendors.	Quarterly; monthly for high-growth portfolios.	Use LEI where available; start aggregated; move to secure enclave samples where legally feasible.
A2 Stablecoins	Circulating supply; issuance/redemption flows; reserve composition/maturity; custodians/banks; on/off-ramp counterparties; peg deviations; redemption queues; settlement dependencies.	Monthly; daily/weekly for flows during stress.	Align with issuer disclosure regimes; use confidential reporting for bank/custody links.
A3 Critical third parties	Critical functions; provider name/service type; subcontracting chain; hosting region/zone; redundancy; RTO/RPO; severe incident logs; portability/exit-plan tests.	Semi-annual; immediate/quarterly for incidents.	Build on DORA-style templates; aggregate system-level concentration metrics to protect sensitive data.

References

- Adelmann, F., Elliott, J. A., Ergen, I., Gaidosch, T., Jenkinson, N., Khiaonarong, T., Morozova, A., Schwarz, N., & Wilson, C. (2020). *Cyber risk and financial stability: It's a small world after all* (IMF staff discussion note No. SDN/20/07). International Monetary Fund. [\[CrossRef\]](#)
- Ahmed, R., & Aldasoro, I. (2025). *Stablecoins and safe asset prices* (BIS working papers No. 1270). Bank for International Settlements.
- Aldasoro, I., Frost, J., & Ito, H. (2026). *The impact of stablecoins on the international monetary and financial system* (BIS papers No. 170). Bank for International Settlements.
- Altavilla, C., Boucinha, M., Burlon, L., Adalid, R., Fortes, R., & Maruhn, F. (2026). *Stablecoins and monetary policy transmission* (ECB working paper series No. 3199). European Central Bank.
- Amromin, G., Hull, C., Weiss, E., Chmielewski, R., Cowperthwait, P., Solimine, B., Anadu, K., Braeuning, F., Sanders, S., Garza, L., Schulhofer-Wohl, S., Chapel, A., & Cho, M. (2025). *Technology providers and financial stability: Overview of risks and regulatory frameworks* (Working paper No. 2025-08). Federal Reserve Bank of Chicago. [\[CrossRef\]](#)
- Arner, D. W., Auer, R., & Frost, J. (2020). *Stablecoins: Risks, potential and regulation* (BIS working papers No. 905). Bank for International Settlements.
- Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The evolution of FinTech: A new post-crisis paradigm? *Georgetown Journal of International Law*, 47(4), 1271–1319. [\[CrossRef\]](#)
- Bains, P., Sugimoto, N., & Wilson, C. (2022). *BigTech in financial services: Regulatory approaches and architecture* (IMF FinTech notes No. 2022/002). International Monetary Fund.
- Bank for International Settlements. (2019). Big tech in finance: Opportunities and risks. In *Annual economic report 2019*. Chapter III. Bank for International Settlements.
- Bank for International Settlements. (2025). *Annual economic report 2025*. Bank for International Settlements.
- Basel Committee on Banking Supervision. (2021). *Principles for operational resilience*. Bank for International Settlements.
- Basel Committee on Banking Supervision. (2024a). *Digitalisation of finance*. Bank for International Settlements.
- Basel Committee on Banking Supervision. (2024b). *The 2023 banking turmoil and liquidity risk: A progress report*. Bank for International Settlements.
- Bazarbash, M., & Beaton, K. (2020). *Filling the gap: Digital credit and financial inclusion* (IMF working paper No. WP/20/150). International Monetary Fund. [\[CrossRef\]](#)
- Boissay, F., Ehlers, T., Gambacorta, L., & Shin, H. S. (2021). *Big techs in finance: On the new nexus between data privacy and competition* (BIS working papers No. 970). Bank for International Settlements.
- Borio, C. (2014). The financial cycle and macroeconomics: What have we learnt? *Journal of Banking & Finance*, 45, 182–198. [\[CrossRef\]](#)
- Borio, C., Claessens, S., & Tarashev, N. (2022). *Entity-based vs activity-based regulation: A framework and applications to traditional financial firms and big techs* (FSI occasional paper No. 19). Bank for International Settlements.
- Buchak, G., Matvos, G., Piskorski, T., & Seru, A. (2018). Fintech, regulatory arbitrage, and the rise of shadow banks. *Journal of Financial Economics*, 130(3), 453–483. [\[CrossRef\]](#)
- Cerutti, E., Claessens, S., & Laeven, L. (2017). The use and effectiveness of macroprudential policies: New evidence. *Journal of Financial Stability*, 28, 203–224. [\[CrossRef\]](#)
- Cevik, S. (2023). *The dark side of the moon? Fintech and financial stability* (IMF working paper No. 2023/253). International Monetary Fund. [\[CrossRef\]](#)
- Claessens, S., Frost, J., Turner, G., & Zhu, F. (2018). Fintech credit markets around the world: Size, drivers and policy issues. *BIS Quarterly Review*, 29–49.
- Committee on Payment and Settlement Systems & International Organization of Securities Commissions. (2012). *Principles for financial market infrastructures*. Bank for International Settlements.
- Cornelli, G., Frost, J., Gambacorta, L., Rau, R., Wardrop, R., & Ziegler, T. (2020). *Fintech and big tech credit: A new database*. BIS working papers No. 887. Bank for International Settlements.
- Crisanto, J. C., Ehrentraud, J., Fabian, M., & Monteil, A. (2022). *Big tech interdependencies: A key policy blind spot*. FSI insights on policy implementation No. 44. Bank for International Settlements.
- Doerr, S., Frost, J., Gambacorta, L., & Shreeti, V. (2023). *Big techs in finance*. BIS working papers No. 1129. Bank for International Settlements.
- Ehrentraud, J., Evans, J. L., Monteil, A., & Restoy, F. (2022). *Big tech regulation: In search of a new framework*. FSI occasional paper No. 20. Bank for International Settlements.
- European Banking Authority. (2019). *EBA guidelines on outsourcing arrangements*. EBA/GL/2019/02. European Banking Authority.
- European Securities and Markets Authority. (2021). Cloud outsourcing and financial stability risks. In *Trends, risks and vulnerabilities report No. 2*. European Securities and Markets Authority.
- European Securities and Markets Authority. (2025). *Principles on third-party risks supervision*. European Securities and Markets Authority.
- European Systemic Risk Board. (2022). *Mitigating systemic cyber risk*. European Systemic Risk Board.

- European Systemic Risk Board & Advisory Scientific Committee. (2025). *Artificial intelligence and systemic risk*. Report of the advisory scientific committee No. 16. European Systemic Risk Board.
- European Union. (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). *Official Journal of the European Union*, L 333, 1–79.
- European Union. (2023). Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCA). *Official Journal of the European Union*, L 150, 40–205.
- Financial Stability Board. (2017). *Financial stability implications from FinTech: Regulatory and supervisory issues that merit authorities' attention*. Financial Stability Board.
- Financial Stability Board. (2019). *FinTech and market structure in financial services: Market developments and potential financial stability implications*. Financial Stability Board.
- Financial Stability Board. (2020). *Regulation, supervision and oversight of 'global stablecoin' arrangements: Final report and high-level recommendations*. Financial Stability Board.
- Financial Stability Board. (2023a). *Cloud adoption in the financial sector and concentration risk*. Financial Stability Board.
- Financial Stability Board. (2023b). *Enhancing third-party risk management and oversight: A toolkit for financial institutions and financial authorities*. Financial Stability Board.
- Financial Stability Board. (2023c). *Recommendations to achieve greater convergence in cyber incident reporting: Final report*. Financial Stability Board.
- Financial Stability Board. (2023d). *Revised high-level recommendations for the regulation, supervision and oversight of global stablecoin arrangements*. Financial Stability Board.
- Frost, J., Gambacorta, L., Huang, Y., Shin, H. S., & Zbinden, P. (2019). *BigTech and the changing structure of financial intermediation* (BIS working papers No. 779). Bank for International Settlements.
- Fuster, A., Plosser, M., Schnabl, P., & Vickery, J. (2019). The role of technology in mortgage lending. *Review of Financial Studies*, 32(5), 1854–1899. [\[CrossRef\]](#)
- Galati, G., & Moessner, R. (2013). Macroprudential policy: A literature review. *Journal of Economic Surveys*, 27(5), 846–878. [\[CrossRef\]](#)
- Gorton, G. B., & Zhang, J. Y. (2023). Taming wildcat stablecoins. *University of Chicago Law Review*, 90(3), 909–972.
- International Monetary Fund. (2022). *Global financial stability report, April 2022: Chapter 3: The rapid growth of FinTech: Vulnerabilities and challenges for financial stability*. International Monetary Fund.
- International Monetary Fund. (2024). *Global financial stability report, April 2024: Chapter 3: Cyber risk: A growing concern for macrofinancial stability*. International Monetary Fund.
- Koh, T. Y., & Prenio, J. (2023). *Managing cloud risk: Some considerations for the oversight of critical cloud service providers in the financial sector* (FSI insights on policy implementation No. 53). Bank for International Settlements.
- Kun, E. (2024). Challenges in regulating cloud service providers in EU financial regulation: From operational to systemic risks, and examining challenges of the new oversight regime for critical cloud service providers under the Digital Operational Resilience Act. *Computer Law & Security Review*, 52, 105931. [\[CrossRef\]](#)
- Lyons, R. K., & Viswanath-Natraj, G. (2023). What keeps stablecoins stable? *Journal of International Money and Finance*, 131, 102777. [\[CrossRef\]](#)
- Philippon, T. (2016). *The FinTech opportunity*. NBER working paper No. 22476. National Bureau of Economic Research. [\[CrossRef\]](#)
- Restoy, F. (2021). *Fintech regulation: How to achieve a level playing field*. FSI occasional paper No. 17. Bank for International Settlements.
- Tang, H. (2019). Peer-to-peer lenders versus banks: Substitutes or complements? *Review of Financial Studies*, 32(5), 1900–1938. [\[CrossRef\]](#)
- U.S. Department of the Treasury. (2023). *The financial services sector's adoption of cloud services*. U.S. Department of the Treasury.
- World Bank. (2022). *Fintech and the digital transformation of financial services: Implications for market structure and public policy*. World Bank. [\[CrossRef\]](#)

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 MDPI and/or the editor(s). MDPI 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.