Journal of Financial Supervision and Audit
Volume 4, Number 2, 2025

The Evolution of Risk-Based Supervision under Digital Financial Transformation

Yosina Oktoviani Pitna[1*]

[1] Universitas Sarjanawiyata Tamansiswa, Yogyakarta, Indonesia

Abstract

Article history:
Received: July 24, 2025
Revised: August 7, 2025
Accepted: September 29, 2025
Published: December 30, 2025

Keywords:
Cyber Risk, Digital Banking, Financial Supervision, Risk-Based Supervision, Supervisory Assurance, SupTech.

Identifier:
Zera Open
Page: 74-87
https://zeraopen.com/journal/jfsa

Risk-based supervision is being reshaped by digital financial transformation, raising a central question: how can supervisors preserve credible assurance when controls, decisions, and services are increasingly automated, data-driven, and outsourced? This study synthesizes evidence through a systematic literature review focused on financial supervision and audit implications. The reviewed studies show a reallocation of material risk from mainly balance-sheet vulnerabilities toward operational resilience, cyber governance, data integrity, model risk, and third-party dependencies. Findings also indicate that SupTech can strengthen risk-based supervision by enabling earlier risk sensing and targeted interventions, but only when supervisory analytics are governed with validation, explainability, and auditable decision trails. The article discusses these results through thematic synthesis linking supervisory risk taxonomies, technology-enabled supervisory cycles, and auditability of digital controls, including AI systems. Overall, the review concludes that digitally enabled supervision is constrained less by tool availability than by institutional capacity, data readiness, and assurance arrangements that align supervisors, firms, and auditors.

*Corresponding author:
(Yosina Oktoviani Pitna)

1. Introduction

Risk-based supervision has traditionally aligned supervisory resources with the likelihood and impact of prudential and conduct failures, using institution-level assessments of governance, risk management, capital adequacy, and controls to determine supervisory intensity. Digital financial transformation is reshaping each element of that cycle. Platform-based intermediation, instant payments, API-enabled distribution, cloud outsourcing, and AI-assisted decisioning can compress risk transmission from gradual balance-sheet deterioration into operational and conduct events that materialize quickly and propagate across connected firms. Scholarship on fintech and RegTech shows that innovation can improve efficiency and access while simultaneously shifting risk from credit and liquidity channels toward operational resilience, data governance, model risk, and third-party dependencies that challenge legacy supervisory taxonomies (Anagnostopoulos, 2018; Thakor, 2020).

For supervision and audit, the core issue is assurance: how supervisors can maintain confidence in the reliability of firms' risk reporting and control environments when key processes are digitized, outsourced, and increasingly automated. SupTech-enabled approaches are frequently framed as a way to strengthen risk-based supervision through richer data, automated anomaly detection, and earlier risk signals that can trigger targeted reviews outside traditional onsite cycles (Zeranski & Sancak, 2021). Yet this shift introduces audit-like challenges for supervisors themselves, including governance over supervisory analytics, explainability of risk scoring, data lineage, and the risk of overreliance on vendor

solutions. Regulatory governance research therefore emphasizes that supervisory modernization must be paired with disciplined accountability structures and robust validation of technology-enabled tools, otherwise automation may amplify blind spots rather than reduce them (McCarthy, 2023).

Auditability becomes more complex as evidence migrates from documents and sampling frames to event logs, code-based controls, and model outputs. Research on continuous auditing of AI conceptualizes near real-time assurance as an electronic support system that continuously and automatically evaluates whether AI systems remain consistent with relevant norms and standards, which is directly relevant to supervisory expectations around model governance, monitoring, and control effectiveness in AI-enabled finance (Minkkinen et al., 2022). In practical supervisory terms, this reframes the relationship between internal audit, external audit, and supervisors: supervisors increasingly need to assess whether internal audit can test model risk management, data controls, and third-party dependencies at scale, and whether external audit planning appropriately reflects technology-driven operational and conduct risks.

Cyber risk is also central to the evolution of risk-based supervision under digital transformation, because it is both a firm-level operational risk and a system-wide stability concern in highly interconnected digital infrastructures. Work linking fintech development to risk-based thinking highlights how cyber exposures can become embedded in innovation pathways, implying that supervisory risk assessment must treat cyber governance, incident response readiness, and resilience metrics as core drivers of supervisory intensity rather than peripheral compliance

items (Vučinić & Luburić, 2022). This is especially important where digital ecosystems concentrate critical services in a small number of technology providers, increasing correlated failure risk and complicating audit evidence over outsourced controls.

Digital transformation is unfolding unevenly across jurisdictions, creating variation in supervisory capacity, legal mandates, and the maturity of audited control environments. Accordingly, the evolution of risk-based supervision must be understood as a general supervisory redesign problem, while also recognizing how emerging markets provide useful stress tests for issues such as data availability, institutional capability, and financial integrity pressures. Evidence from Indonesia is used selectively to illustrate emerging-market supervisory constraints, rather than to define the scope of analysis (Narayan, 2019; Meiryani et al., 2022).

2. Literature Review

Recent supervision and audit scholarship converges on the idea that digital financial transformation changes not only the distribution of risk but also the auditability of the underlying control environment. As financial intermediation becomes platform-mediated and data-intensive, risk-based supervision increasingly extends beyond traditional balance-sheet risks toward operational resilience, data governance, model risk, and third-party dependencies that can transmit disruptions rapidly across interconnected actors (Anagnostopoulos, 2018; Thakor, 2020). This shift implies that supervisory prioritization must rely more heavily on timely signals and observable control performance rather than periodic compliance artifacts.

A central stream in this literature focuses on SupTech and analytics-enabled oversight as mechanisms that can strengthen risk-based supervision through richer data pipelines, anomaly detection, and earlier warning signals. However, supervisory technology introduces its own assurance problem: supervisors must be able to defend the reliability of their models and the integrity of the data feeding supervisory judgments. Work synthesizing machine learning applications in banking supervision highlights both the potential (classification, early-warning, pattern detection) and the governance requirements (data quality, validation, interpretability) that mirror audit expectations around evidence reliability and model governance (Guerra & Castelli, 2021).

A closely related audit-oriented stream emphasizes that digitalization changes what evidence looks like and how assurance is produced. As control activities are embedded in code, logs, and automated decision rules, assurance increasingly depends on continuous monitoring, traceability, and the capacity to evaluate whether technology-enabled controls keep operating as intended. Research on continuous auditing of AI provides a clear conceptual bridge between audit practice and supervisory oversight by framing continuous, automated evaluation of AI systems against norms and standards, which aligns directly with supervisory expectations around model governance and ongoing control effectiveness (Minkkinen et al., 2022). In parallel, audit evidence on digital confirmation mechanisms shows that audit digital transformation can shape audit quality outcomes, reinforcing the need to connect supervisory expectations with how auditors adapt procedures and assurance to digitized processes (Guo et al., 2024). Cyber risk scholarship further

reinforces that supervisory risk scoring must treat cybersecurity and resilience as core drivers of supervisory intensity in digital finance ecosystems (Vučinić & Luburić, 2022).

Emerging-market studies complement the global supervision-and-assurance literature by highlighting implementation constraints and financial integrity pressures that can shape supervisory priorities. Evidence indicates that fintech expansion can be economically consequential, strengthening the rationale for earlier detection of risk build-ups (Narayan, 2019). RegTech evidence from Indonesian banking further suggests measurable AML/CFT monitoring benefits while surfacing supervisory concerns about governance, capability maturity, and assurance over technology-enabled compliance processes (Meiryani et al., 2022). These insights are treated as illustrative for broader emerging-market supervision challenges rather than as the central empirical setting of the review.

3. Methods

This study uses a qualitative systematic literature review approach to examine how risk-based supervision evolves under digital financial transformation, with emphasis on financial supervision and audit implications. The systematic review method was selected to consolidate and critically compare peer-reviewed evidence on supervisory frameworks, SupTech and RegTech-enabled oversight, auditability of digital controls, operational resilience, cyber risk, and technology-driven financial integrity issues. The review adopts a global scope, while drawing selectively on

emerging-market studies, including Indonesia, where it offers concrete illustrations of supervisory capacity and assurance constraints.

The literature was identified through structured searches in Scopus, Web of Science, and Google Scholar using keyword combinations such as "risk-based supervision", "financial supervision", "SupTech", "RegTech", "supervisory analytics", "digital banking supervision", "audit evidence", "continuous auditing", "model risk governance", "operational resilience", "cyber risk", and "AML/CFT technology". Studies were included if they were peer-reviewed, written in English, accessible in full text, and directly connected to financial supervision or audit and assurance questions. The analysis applied thematic synthesis by coding and grouping findings into core themes: (1) supervisory risk taxonomy changes under digital ecosystems, (2) data-driven supervisory cycles and SupTech, (3) auditability of digital controls and AI-enabled decisioning, (4) cyber risk and operational resilience as supervisory drivers, and (5) governance and capability constraints. Robustness was supported through cross-study comparison and critical appraisal of how each study links its evidence to supervisory or audit conclusions.

4. Results and Discussion

The reviewed literature indicates a clear expansion in the supervisory meaning of "material risk" as finance digitalizes. Traditional risk-based supervision has been anchored in balance-sheet vulnerabilities and governance failures that translate into capital, liquidity, or solvency concerns. Under digital financial transformation, however, major risk drivers increasingly arise from technology-mediated operating

models, including outsourced ICT stacks, API-dependent distribution, platform intermediation, and AI-enabled decisioning. Across studies, these changes are associated with a redistribution of risk away from purely financial ratios toward operational resilience, data governance, model risk, and third-party dependencies that can transmit disruptions rapidly across interconnected actors (Anagnostopoulos, 2018; Thakor, 2020). In supervisory terms, this implies that risk-scoring and supervisory planning require updated taxonomies and indicators that give operational and technology risks comparable weight to traditional prudential signals, particularly where business continuity, service availability, and data integrity become binding constraints for stability and consumer protection.

A prominent theme in the reviewed studies is the expanding role of SupTech in reshaping supervisory cycles. Rather than functioning only as a reporting efficiency tool, SupTech is presented as an enabling infrastructure that supports earlier risk sensing, better triage, and more targeted interventions when digital activity evolves faster than conventional onsite routines. Yet the literature also converges on an assurance tension: if supervisors rely more heavily on automated analytics, then the governance of supervisory models and data pipelines becomes part of supervisory legitimacy. Issues such as explainability of risk scoring, validation of analytic tools, data lineage, and dependency on vendor-provided systems are repeatedly framed as constraints that can undermine defensibility and consistency if not addressed through robust oversight arrangements (Zeranski & Sancak, 2021; McCarthy, 2023). From an audit and assurance perspective, this creates a "supervision of supervision" requirement: supervisors need audit-like controls over

their own analytic processes to ensure that technology-enabled judgments remain transparent, repeatable, and contestable.

The audit-focused stream further shows that digital transformation changes what counts as reliable evidence, thereby altering both audit practice and supervisory confidence in control environments. As controls migrate from policy documents and sampled transactions into code, logs, workflow engines, and model outputs, assurance increasingly depends on continuous monitoring, traceability, exception handling, and evidence that automated decision processes remain consistent with governance expectations over time. Conceptual work on continuous auditing of AI emphasizes continuous, automated evaluation of AI systems against relevant norms and standards, which aligns closely with supervisory expectations for model governance, monitoring, and ongoing control effectiveness in AI-enabled finance (Minkkinen et al., 2022). In practical supervisory terms, this reframes what supervisors should look for in internal audit and compliance capability, including the ability to test model risk management, monitor drift and bias, evaluate data controls, and evidence effective oversight of outsourced technology arrangements.

Empirical audit evidence reinforces that audit digital transformation can affect audit outcomes, strengthening the logic for connecting supervisory assurance to the evolving toolkit of auditors. Evidence from digital bank confirmation mechanisms suggests that technology-enabled audit procedures can improve cash-flow related audit quality and that effects may be stronger in higher-risk settings and where auditor capability conditions are favorable (Guo et al., 2024). For risk-based supervision, the implication is not that supervisors should assume technology

automatically improves assurance, but that supervisors may need to evaluate whether institutions and their auditors have the competence, governance, and infrastructure to generate reliable audit evidence in digitized environments. This also supports a more integrated supervisory view of assurance, where supervisory judgments consider both the design of technology-enabled controls and the credibility of assurance processes used to validate them.

Cyber risk and operational resilience emerge as cross-cutting drivers that integrate prudential, operational, and conduct concerns into a single supervisory priority. The literature linking fintech development to risk-based thinking treats cyber exposures as embedded in innovation pathways, implying that cybersecurity governance, incident readiness, and resilience metrics should be core components of supervisory intensity decisions rather than peripheral compliance checks (Vučinić & Luburić, 2022). This becomes especially relevant where digital ecosystems concentrate critical services in a small number of ICT providers, raising correlated failure risk and complicating audit evidence over outsourced controls. Regulatory scholarship on operational resilience regimes further supports this direction by showing how supervisory architectures are being redesigned to address ICT risk, third-party dependency oversight, and resilience testing expectations in a more structured manner (Buttigieg & Zimmermann, 2024). The broader supervisory lesson is that risk-based supervision is increasingly operational-resilience oriented, requiring supervisors to evaluate both firm-level control effectiveness and ecosystem-level interdependencies.

The literature also points to the growing relevance of automation inside audit functions as operational resilience expectations rise. Evidence from financial-sector settings indicates that intelligent process automation can streamline business continuity audit activities and support KPI-based monitoring within audit departments, potentially strengthening timeliness and consistency of assurance work (Brás et al., 2024). For supervisors, this offers a practical indicator: where internal audit can automate evidence collection and continuity-control monitoring, supervisory confidence in the control environment may be stronger, especially for institutions with complex digital operations.

Finally, emerging-market studies function as an implementation stress test rather than a separate theoretical foundation. Evidence that fintech expansion can be economically consequential strengthens the case for timely detection of risk build-ups as part of risk-based supervisory modernization (Narayan, 2019). Indonesia-focused RegTech evidence suggests that technology can strengthen AML/CFT monitoring effectiveness while also highlighting that governance maturity and capability constraints shape whether technology-enabled compliance is reliable in practice (Meiryani et al., 2022). Treated illustratively, these findings reinforce a broader conclusion from the global literature: the effectiveness of digitally enabled risk-based supervision is often constrained less by the availability of tools and more by assurance capacity, including data readiness, model governance, audit capability, and cross-entity coordination.

5. Conclusion

The reviewed literature indicates that risk-based supervision is being redefined by digital financial transformation in ways that directly affect supervisory assurance and auditability. Digital operating models shift material risk away from exclusively balance-sheet vulnerabilities toward operational resilience, cyber governance, data integrity, model risk, and third-party dependencies, requiring supervisors to recalibrate supervisory taxonomies, indicators, and intervention triggers. As a result, effective risk-based supervision increasingly depends on the ability to observe and evaluate control performance in near real time, rather than relying primarily on periodic compliance artifacts.

A further conclusion is that SupTech can strengthen risk-based supervision by enabling earlier risk sensing and more targeted supervisory responses, but its benefits are conditional on governance and defensibility. The literature repeatedly highlights that supervisors must treat their own analytics, models, and data pipelines as objects of assurance, with clear accountability, validation, explainability, and auditable decision trails. In parallel, the audit-oriented evidence suggests that as controls migrate into code, logs, and AI-enabled processes, supervisory confidence becomes tightly linked to the maturity of internal audit, compliance, and external audit capabilities to generate reliable evidence, monitor control effectiveness continuously, and manage technology-driven risks, including cyber threats and operational disruptions.

This review also suggests that the binding constraint in digitally enabled supervision is often institutional capacity rather than the availability of technology

alone. Differences in legal mandates, data access, supervisory skills, and market infrastructure shape how far supervisory authorities can operationalize continuous, risk-signaled oversight. Future research should therefore examine how supervisory agencies govern SupTech models, how audit standards and practices adapt to AI and outsourced ICT environments, and which supervisory indicators best predict technology-driven failures across different institutional contexts. Comparative evidence that includes emerging-market settings can be particularly valuable for identifying scalable supervisory and audit practices that remain credible under resource and data constraints.

References

Anagnostopoulos, I. (2018). FinTech and RegTech: Impact on regulators and banks. *Journal of Economics and Business, 100*, 7-25.

Brás, J. C., Pereira, R. F., Fonseca, M., Ribeiro, R., & Bianchi, I. S. (2024). Advances in auditing and business continuity: A study in financial companies. *Journal of Open Innovation: Technology, Market, and Complexity, 10*(2), 100304.

Buttigieg, C. P., & Zimmermann, B. B. (2024). The digital operational resilience act: Challenges and some reflections on the adequacy of Europe's architecture for financial supervision. *ERA Forum, 25*, 11-28.

Guerra, P., & Castelli, M. (2021). Machine learning applied to banking supervision: A literature review. *Risks, 9*(7), 136.

Guo, R., Jia, Y., & Shentu, L. (2024). The effect of audit digital transformation on audit quality: evidence from digital bank confirmations. *China Journal of Accounting Studies*, 1-35.

McCarthy, J. (2023). The regulation of RegTech and SupTech in finance: Ensuring consistency in principle and in practice. *Journal of Financial Regulation and Compliance, 31*(2), 186-199.

Meiryani, M., Soepriyanto, G., & Audrelia, J. (2022). Effectiveness of regulatory technology implementation in Indonesian banking sector to prevent money laundering and terrorist financing. *Journal of Money Laundering Control, 26*(4), 892-908.

Minkkinen, M., Laine, J., & Mäntymäki, M. (2022). Continuous auditing of artificial intelligence: a conceptualization and assessment of tools and frameworks. *Digital Society, 1*(3), 21.

Narayan, S. W. (2019). Does FinTech matter for Indonesia's economic growth? *Bulletin of Monetary Economics and Banking, 22*(4), 437-456.

Thakor, A. V. (2020). Fintech and banking: What do we know? *Journal of Financial Intermediation, 41*, 100833.

Vučinić, M., & Luburić, R. (2022). Fintech, risk-based thinking and cyber risk. *Journal of Central Banking Theory and Practice, 11*(2), 27-53.

Zeranski, S., & Sancak, I. E. (2021). Prudential supervisory disclosure (PSD) with supervisory technology (SupTech): Lessons from a FinTech crisis. *International Journal of Disclosure and Governance, 18*(4), 315-335.