ARTOKULO: Journal of Accounting, Economics and Management
E-ISSN : 3032-0461 | P-ISSN : 3032-047X
Volume 3 No 2 May – August (2026)

Financial Risk Management in the Digital Era: A Systematic Review of Risk Transformation, Governance, and Mitigation Strategies

Udayat[1]

Yasa Anggana College of Economics, Garut, Indonesia

ABSTRACT
Digital transformation has reshaped the structure, processes, and business models of the financial sector while simultaneously introducing increasingly complex, rapidly evolving, and interconnected risks. This study aims to identify changes in the characteristics of financial risks resulting from digitalization, analyze the role of technology as both a source of risk and a risk-mitigation instrument, and formulate relevant risk management strategies for organizations. This study employs a qualitative-descriptive approach using a systematic literature review method. The literature analyzed consists of reputable peer-reviewed journal articles published between 2015 and 2025. The identification and selection of the literature followed the PRISMA 2020 guidelines, while the data were examined through descriptive and thematic analyses. The findings indicate that digitalization does not eliminate traditional financial risks; instead, it transforms their sources, speed, scale, and patterns of propagation. Credit, market, liquidity, and operational risks have become increasingly interconnected with model, cyber, data, compliance, reputational, third-party, and systemic risks. These changes occur through four principal mechanisms: acceleration, interconnectedness, datafication, and digital concentration. Technologies such as artificial intelligence, machine learning, cloud computing, blockchain, and regulatory technology can enhance efficiency, predictive accuracy, and early risk-detection capabilities. However, their implementation may also generate algorithmic bias, data breaches, system failures, and dependence on technology providers. This study concludes that financial risk management in the digital era requires an integrated approach involving the strengthening of Enterprise Risk Management, data governance, model validation, cyber resilience, third-party oversight, and risk culture. Aligning digital innovation with effective risk governance is essential for maintaining financial stability, stakeholder trust, and organizational sustainability.

Keywords: Financial Risk Management, Digital Transformation, Fintech, Cyber Risk, Enterprise Risk Management

Corresponding Author:
Udayat
(udayatse@gmail.com)

Received: April 28, 2026
Revised: May 18, 2026
Accepted: June 30, 2026
Published: July 22, 2026

1. INTRODUCTION

Digital transformation has fundamentally changed how economic value is created, transferred, stored, and monitored within the financial system. The emergence of financial technology (FinTech), mobile banking, cloud computing, artificial intelligence, big data analytics, blockchain, and application programming interfaces has fostered an increasingly rapid, open, and interconnected financial ecosystem. These developments represent more than the modernization of transaction channels; they also constitute a restructuring of business processes, patterns of customer interaction, competitive structures, and financial

decision-making mechanisms. Financial digitalization has even generated new products, services, and business models that integrate finance and information technology within a complex ecosystem (Gomber et al., 2017; Gomber et al., 2018).

The use of digital technology offers a range of strategic benefits to financial institutions and businesses more generally. Automation enables transactions to be processed more quickly, operating costs to be reduced, service quality to be improved, and financial decisions to be informed by broader datasets. Digital technology also enables individuals and businesses that were previously underserved by conventional financial services to access payments, financing, investment, and insurance. The entry of FinTech and BigTech firms into the financial industry has intensified competition while encouraging traditional financial institutions to innovate. Digitalization therefore has the potential to improve efficiency and consumer welfare, although its ultimate effects remain strongly influenced by governance, regulation, and the adaptive capacity of individual institutions (Frost et al., 2019; Thakor, 2020; Vives, 2019).

Alongside these opportunities, digitalization introduces risk characteristics that differ from those found in conventional financial environments. Financial risks do not disappear when business processes migrate to digital platforms; instead, they become faster-moving, more complex, more interdependent, and, under certain conditions, more difficult to detect. Credit risk, for example, is no longer determined solely by a debtor's capacity to meet financial obligations but also by the quality of the data and the reliability of the algorithms used to assess creditworthiness. Market and liquidity risks may evolve more rapidly because of real-time transactions, automated trading, and the dissemination of information through digital platforms. Operational risk, meanwhile, is increasingly associated with cyberattacks, system failures, data breaches, algorithmic errors, privacy violations, and dependence on third-party technology providers. These conditions demonstrate that digital innovation can create efficiency while also becoming a new source of vulnerability when it is not supported by adequate risk controls.

Cyber risk is among the most prominent threats in the digital financial ecosystem. Financial information has substantial economic value, making financial institutions strategic targets for cybercriminals. Attacks on payment systems, customer databases, communication networks, or cloud-computing infrastructure can generate financial losses, operational disruption, litigation, and declining public confidence. Aldasoro et al. (2022) show that the cost of cyber incidents tends to be higher for large firms and for incidents that affect multiple organizations simultaneously. Their study also indicates that dependence on cloud-service providers can increase the risk of extreme losses as those providers become more systemically important within the financial system (Aldasoro et al., 2022).

Digital vulnerabilities can also escalate from institution-specific risks into systemic risks. The extensive interconnectedness among banks, FinTech firms, payment systems, cloud-service providers, and financial market infrastructures allows a disruption at one entity to spread to others. Eisenbach et al. (2022) demonstrate that cyberattacks against important institutions in payment networks can produce spillover effects and disrupt financial-system activity on a broad scale. Dependence on technology-service providers and financial market utilities creates additional channels through which such risks can propagate (Eisenbach et al., 2022). Digital risk should therefore not be regarded merely as a technical issue assigned to the information technology function; it is a strategic risk capable of affecting liquidity, reputation, operational stability, and organizational continuity.

These changing risk characteristics require financial risk management approaches to be renewed. Conventional approaches that rely exclusively on historical data, periodic reports, and reactive controls are increasingly inadequate as the sole basis for decision-making. Digital risks can emerge rapidly, behave nonlinearly, and be shaped by the interconnection of systems that are not fully controlled by the organization. Financial risk management in the digital era must therefore be integrated, adaptive, and forward-looking. The process should

encompass the establishment of governance and risk appetite, the identification of digital assets and dependencies, exposure measurement, real-time monitoring, scenario testing, data protection, third-party oversight, incident response, and the development of recovery and business-continuity plans.

The success of risk management is ultimately determined not only by the sophistication of the technology deployed but also by the quality of organizational governance and risk culture. Analytical technologies and artificial intelligence can strengthen the capacity to detect anomalies, forecast losses, and issue early warnings. Their use nevertheless requires human oversight, algorithmic transparency, model validation, decision-making accountability, and the protection of user rights. The fundamental principle is that the speed of risk management must keep pace with the speed of innovation. Without this alignment, innovations intended to improve efficiency may instead expand financial exposure and weaken stakeholder trust.

Against this background, examining financial risk management in the digital era is important because it brings together two objectives that must be pursued in balance: harnessing technological innovation and safeguarding financial security and stability. The central challenge facing organizations is not to choose between innovation and risk control, but to build a risk management system that enables both to operate in alignment. Accordingly, this article aims to identify the financial risks that arise or change as a result of digitalization, analyze how technology affects the characteristics and propagation of risk, and explain risk management strategies relevant to organizations. The review is expected to provide conceptual understanding and a practical foundation for companies and financial institutions seeking to build resilient, responsive, and sustainable risk governance amid continuing technological change.

2. METHOD

Research Design

This study adopts a qualitative-descriptive approach using a systematic literature review (SLR). This method was selected because the study seeks to identify, evaluate, compare, and synthesize research findings on financial risk management in the digital era. The SLR not only summarizes previous theories and findings but also identifies patterns, divergent results, relationships among concepts, research limitations, and knowledge gaps that warrant further investigation.

A literature review can serve as a research method when the processes of searching, selecting, evaluating, and synthesizing sources are conducted systematically and transparently and can be traced and replicated. Snyder (2019) explains that literature reviews as a research method are particularly relevant in business and management when knowledge on a topic develops rapidly, is dispersed across disciplines, and requires conceptual integration (Snyder, 2019). These characteristics correspond to financial risk management in the digital era, which lies at the intersection of finance, risk management, information systems, artificial intelligence, cybersecurity, and regulation.

The study follows the systematic-review framework developed by Tranfield et al. (2003), which comprises review planning, review execution, and the reporting and dissemination of findings (Tranfield et al., 2003). The article-identification and selection process was reported in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 principles. PRISMA was used to enhance transparency in explaining how articles were identified, screened, evaluated, and ultimately selected as research data sources (Page et al., 2021).

Research Focus and Questions

This study focuses on changes in the characteristics of financial risk resulting from digital transformation and on the strategies organizations can use to manage those risks. Financial risk is understood broadly to include credit, market, liquidity, operational, cyber, model, data,

compliance, reputational, third-party, and systemic risks. The study also considers the use of technologies such as FinTech, BigTech, artificial intelligence, machine learning, cloud computing, blockchain, crypto-assets, digital payment systems, and RegTech.

The unit of analysis consists of scholarly journal articles addressing the relationship between digital technology and financial risk management. The study is directed toward several central questions: which financial risks have emerged or changed in the digital era; how technology affects the characteristics and propagation of risk; how technology functions both as a source of risk and as a mitigation instrument; which organizational capabilities are required to manage digital risk; and which gaps remain in the existing literature. These questions guided the selection of keywords and articles, the construction of coding categories, and the interpretation of review findings.

Data Sources

This study uses secondary data in the form of peer-reviewed scholarly journal articles. Journal articles were selected because they undergo a structured academic assessment process and provide information on research objectives, methods, data, findings, limitations, and implications. Scopus and Web of Science served as the principal article-search databases because both offer broad publication coverage and structured bibliographic information that supports systematic screening.

Full-text retrieval and verification were conducted through ScienceDirect, SpringerLink, Wiley Online Library, Oxford Academic, Taylor & Francis Online, and Emerald Insight. Google Scholar was used as a supplementary source to identify articles that might not appear in the initial search and to trace articles citing influential studies. Nevertheless, every article identified through Google Scholar was verified through the official journal or publisher website. Source authenticity was also confirmed by matching the authors' names, article title, journal name, year of publication, volume, issue, page range, and DOI.

The substantive articles analyzed were limited to the 2015-2025 period. This timeframe was selected to capture a full decade of financial digitalization, including the growth of FinTech, the adoption of artificial intelligence and cloud computing, blockchain-based transactions, digital assets, and increasing concern about cyber risk. Methodological literature published before 2015 was retained where relevant as a foundation for the SLR and thematic analysis.

Literature Search Strategy

The literature search used combinations of keywords representing three principal concepts: risk management, finance, and digital transformation. The primary keywords included “financial risk management,” “enterprise risk management,” “financial risk,” “digital transformation,” “digital finance,” “digital era,” “FinTech,” and “BigTech.” These terms were combined using the Boolean operators AND and OR so that the search could capture articles using different terminology to address similar concepts.

Additional searches employed terms representing specific digital risks, including “cyber risk,” “cybersecurity risk,” “model risk,” “algorithmic risk,” “digital credit risk,” “cryptocurrency risk,” “third-party risk,” and “operational resilience.” These terms were combined with “bank,” “financial institution,” “firm,” or “company.” Other keywords, including “artificial intelligence,” “machine learning,” “cloud computing,” “digital payment,” “blockchain,” “financial stability,” “risk governance,” and “RegTech,” were also used to broaden the search.

Searches were conducted within article titles, abstracts, and keywords. Multiple keyword combinations were necessary because research on digital financial risk originates from several disciplines and does not employ fully standardized terminology. The entire search process was documented by recording the database, search date, keywords, filters, and number of

articles retrieved. This documentation created an audit trail that permits the search process to be reviewed and replicated.

Inclusion and Exclusion Criteria

Articles were eligible for inclusion when they were published in peer-reviewed scholarly journals between 2015 and 2025, written in English or Indonesian, and directly addressed the relationship between digital technology and financial risk management. Selected studies had to concern financial institutions, companies, financial markets, or the FinTech ecosystem. Full text had to be available so that objectives, methods, data, findings, and limitations could be evaluated adequately. Articles were also required to have complete bibliographic information and a valid DOI.

Books, book chapters, theses, dissertations, conference papers, editorials, news reports, commercial reports, and promotional materials were excluded. Articles addressing technology without a clear connection to risk or finance were also omitted. Anonymous sources, retracted articles, publications whose identities could not be verified, and articles for which only a title or abstract was available were likewise excluded.

Systematic review articles were used to map theoretical developments, conceptual progress, and research agendas. Conclusions concerning empirical relationships, however, gave priority to original research articles. When multiple versions of the same study were available, the published journal article was treated as the primary source, while working papers and preprints were not counted as separate units of analysis. This rule was intended to prevent duplicate counting of identical findings.

Literature Selection Procedure

The literature-selection process followed the identification, screening, eligibility assessment, and final-inclusion stages recommended by PRISMA 2020. PRISMA served as a transparent reporting guide, with its implementation adapted to the characteristics of management and finance research. The process was also consistent with Xiao and Watson (2019), who emphasize the importance of systematic planning, searching, evaluation, analysis, and reporting in literature reviews (Xiao & Watson, 2019).

During the identification stage, all articles retrieved from each database were collected and their bibliographic information was recorded. Articles appearing in more than one database were then compared by title, author, publication year, and DOI. Records identified as duplicates were removed so that only one version was retained.

The next stage involved screening titles and abstracts. At this stage, the researcher assessed the initial relevance of each article to financial risk management in the digital era. Articles without a direct connection to the research focus were excluded. Articles that passed the initial screening were then read in full to assess their conformity with the inclusion and exclusion criteria.

Articles that passed the full-text assessment were subsequently evaluated for methodological quality. The assessment considered the clarity of research objectives, appropriateness of methods, quality of data sources, transparency of analysis, and evidentiary support for the conclusions. Articles meeting the relevance and quality requirements were designated as the final sources for data extraction and synthesis. The number of articles at each stage and the principal reasons for exclusion were recorded and reported through a PRISMA flow diagram.

Article Quality Assessment

Quality assessment was conducted to ensure that the synthesis considered not only topical relevance but also the academic strength of the evidence. Each article was evaluated according to the clarity of its objectives and research questions, the alignment of its design with those objectives, the clarity of its data sources and collection process, the transparency of

its analytical techniques, the correspondence between its conclusions and evidence, and its contribution to understanding digital financial risk.

Quality-assessment outcomes were classified as meets the criteria, partially meets the criteria, or does not meet the criteria. An article was not automatically excluded because of a single limitation. It could, however, be excluded if it exhibited fundamental methodological weaknesses, such as unverifiable data sources, an unexplained analytical procedure, or conclusions unsupported by the findings.

The limitations of each article were recorded in the extraction matrix even when the article was retained in the synthesis. This step was important to avoid treating all findings as evidence of equal strength. Findings from studies with robust methods and data received greater analytical weight than findings subject to substantial methodological limitations.

Data Collection and Extraction Techniques

Data from the selected articles were collected using a structured extraction matrix. The information recorded included the authors, publication year, article title, journal, country or research context, and DOI. The matrix also captured the study objectives, research questions, theoretical foundations, methodological approach, data sources, sample characteristics, observation period, and analytical techniques.

The substantive information extracted included the type of digital technology, financial risk category, mechanisms through which risk changed, principal findings, mitigation strategies, managerial implications, limitations, and recommendations for future research. Digital technologies were classified into categories such as FinTech, artificial intelligence, machine learning, blockchain, cloud computing, digital payment systems, and crypto-assets. Risks were classified as credit, market, liquidity, operational, cyber, model, data, compliance, reputational, third-party, or systemic risk.

Using a standardized matrix ensured consistency in data collection and facilitated comparisons across articles. The matrix also helped identify similarities, differences, and relationships among digital technologies, risk categories, resulting impacts, and management strategies.

Data Analysis Techniques

Data were examined through descriptive and thematic analyses. Descriptive analysis was used to map the literature by publication year, research country, journal, methodological approach, type of technology, risk category, and organizational or industry context. This mapping provided an overview of research development, dominant topics, methodological distributions, and areas that remained underexamined.

Thematic analysis was used to identify patterns of meaning across findings from previous studies. The process followed the stages developed by Braun and Clarke (2006): familiarization with the data, generation of initial codes, identification of themes, review of themes, definition of themes, and interpretation (Braun & Clarke, 2006).

Initial coding drew on theory-based categories encompassing credit, market, liquidity, operational, cyber, model, data, compliance, reputational, third-party, and systemic risks. The analysis nevertheless remained open to new categories emerging from the articles. It therefore combined a deductive approach derived from theory with an inductive approach grounded in the data.

The findings were then synthesized according to four mechanisms of digital-risk transformation. The first was acceleration, referring to the increasing speed of transactions, decision-making, and risk propagation. The second was interconnectedness, referring to the growing links among financial institutions, payment systems, platforms, and technology providers. The third was datafication, referring to the increasing dependence of decision-making on data and algorithms. The fourth was digital concentration, referring to

organizations' growing dependence on a limited number of technology providers or digital infrastructures.

The synthesis compared findings across articles rather than reporting only convergent results. When findings differed or contradicted one another, the researcher examined the national context, organizational characteristics, observation period, data sources, and analytical methods employed. This approach enabled a more critical understanding of the conditions under which particular risk-management strategies succeed or fail.

Research Validity and Reliability

Research validity was strengthened by using multiple academic databases so that the search results did not depend on a single source. The search strategy, keywords, filters, selection decisions, and reasons for exclusion were documented in an audit trail. The DOI of each article was also verified through the publisher website or DOI registration system to confirm that the sources were authentic and active.

Consistency in data extraction was maintained by applying the same matrix format to every article. Screening and coding decisions were re-examined after a time interval to reduce the likelihood of inconsistent judgments. Articles of uncertain relevance were reassessed against the inclusion and exclusion criteria rather than against their conformity with the researcher's initial expectations.

Both supportive and contradictory findings were retained in the synthesis to reduce confirmation bias. The researcher also distinguished between empirical findings directly reported in the articles and interpretations generated through the synthesis. This distinction was intended to preserve transparency and prevent the researcher's interpretations from being presented as though they were original findings of the reviewed articles.

Research Ethics

This study did not involve respondents, experiments, interventions, or the collection of personal data and therefore posed no direct risk to participants. The research data were derived entirely from published scholarly articles. Nevertheless, principles of academic ethics were applied throughout the research process.

Academic integrity was maintained through accurate attribution, the avoidance of plagiarism, preservation of the original meaning of findings, and avoidance of any manipulation of article conclusions. The study also excluded retracted articles and publications with unclear status. Every idea, concept, and finding drawn from previous research was cited in accordance with the seventh edition of the APA style.

Methodological Limitations

The SLR method has several limitations that should be considered when interpreting the findings. Restricting the articles to English and Indonesian may have excluded relevant studies published in other languages. Reliance on journal articles may also introduce publication bias because studies reporting significant results are generally more likely to be published than studies reporting nonsignificant relationships.

Differences in terminology across disciplines may have prevented some relevant articles from appearing in the initial search. In addition, the rapid pace of technological development may cause certain findings to lose relevance within a relatively short period. The results were also influenced by the availability and quality of articles published during the review period.

These limitations were mitigated by using multiple databases, varying the keywords, examining the reference lists of key articles, tracing studies that cited important sources, and recording the context of each study. The results should therefore be understood as a critical synthesis of literature meeting the stated criteria rather than as absolute conclusions applicable to every organization, industry, and country.

3. RESULTS AND DISCUSSION

Overview of the Research Findings

The findings were derived from a synthesis of journal articles addressing digital transformation, FinTech, financial risk management, cyber risk, model risk, digital-asset risk, risk governance, and financial stability. Based on similarities in focus and findings, the literature was grouped into studies of financial-industry transformation, changes in credit and model risk, developments in market and liquidity risk, the expansion of operational and cyber risk, and the implementation of integrated risk management.

The review indicates that digitalization has transformed products, business processes, customer interactions, and competitive structures in the financial-services industry. These changes have been driven by FinTech, BigTech, artificial intelligence, machine learning, cloud computing, digital payment systems, and crypto-assets. Gomber et al. (2017) find that digital finance encompasses changes in products, technologies, business functions, institutions, and patterns of customer interaction (Gomber et al., 2017). Gomber et al. (2018) further show that FinTech is transforming payments, financing, investment, trading, and asset-management activities (Gomber et al., 2018).

Overall, the reviewed articles show that technology offers benefits in the form of faster transactions, lower costs, broader access to financial services, and stronger data-processing capabilities. At the same time, the use of technology creates risks relating to algorithms, cybersecurity, data quality, dependence on technology providers, regulatory compliance, and financial stability.

Findings on the Transformation of the Financial Ecosystem

The findings show that the digital financial ecosystem involves not only banks and conventional financial institutions but also FinTech and BigTech firms, payment-system providers, telecommunications companies, cloud-service providers, and digital platforms. Each participant plays a role in data collection, transaction execution, financing, and infrastructure provision.

Frost et al. (2019) find that BigTech firms have an advantage in using nontraditional data to assess creditworthiness and reach groups underserved by conventional financial institutions (Frost et al., 2019). This advantage stems from their large user bases, data-analytics capabilities, and transaction information obtained through platform ecosystems. The review also indicates that the expanding role of BigTech increases the financial system's dependence on infrastructure and data managed by technology companies.

Vives (2019) finds that digitalization intensifies competition in banking and encourages a shift toward more customer-centered service models. Its ultimate effects on consumer welfare and financial stability, however, are shaped by the structure of competition and regulation (Vives, 2019). This result indicates that digital transformation occurs alongside changes in the relationships among financial institutions, consumers, technology companies, and regulators.

Findings on Credit Risk and Model Risk

The findings indicate that the use of alternative data and machine learning improves financial institutions' capacity to assess credit risk. The data used are no longer limited to income, collateral, and credit history but also include digital footprints, transaction patterns, device characteristics, and customers' behavior on digital platforms.

Berg et al. (2020) find that simple information from digital footprints predicts default about as effectively as credit-bureau information. Digital footprints can complement conventional credit scores and assist in evaluating prospective borrowers with limited credit histories (Berg et al., 2020). Jagtiani and Lemieux (2019) likewise find that alternative data and machine learning can improve risk classification. Some prospective borrowers categorized as high-risk under traditional methods may be placed in better credit categories and obtain lower-priced credit (Jagtiani & Lemieux, 2019).

The reviewed articles also identify model risk and uneven outcomes from algorithmic decision-making. Fuster et al. (2022) show that improved predictive capabilities through machine learning do not necessarily benefit all borrower groups equally. Certain groups may gain less or face wider disparities in credit pricing (Fuster et al., 2022). The findings therefore demonstrate that greater accuracy may coexist with bias risk, limited transparency, and unequal treatment in lending decisions.

Findings on Market Risk and Liquidity Risk

The review indicates that digitalization accelerates the dissemination of information and price formation in financial markets. Digital platforms, social media, and automated trading systems allow information to be translated into transaction decisions more rapidly. These developments increase the speed with which markets respond to sentiment, news, and changing economic conditions.

In the context of digital assets, Liu and Tsyvinski (2021) find that cryptocurrency returns are influenced by market-specific factors such as network adoption, momentum, and investor attention (Liu & Tsyvinski, 2021). This finding indicates that digital assets have risk factors that differ from those of traditional financial assets.

The review also identifies changes in liquidity risk. Digital financial services allow customers to move funds rapidly, which means that inflows and outflows can change within a short period. Negative information disseminated through digital platforms can prompt many users to act simultaneously. These findings indicate that transaction speed and information diffusion are critical elements of liquidity management in the digital era.

Findings on Operational, Cyber, Data, and Reputational Risks

Operational risk emerged as one of the risk categories most extensively reshaped by digitalization. It encompasses software failures, configuration errors, network disruptions, service outages, data loss, and cyberattacks. Dependence on digital systems means that a technological disruption can affect multiple business processes simultaneously.

Aldasoro et al. (2022) find that cyber-incident costs tend to be higher for large firms and for incidents affecting multiple organizations at once. They also find that cloud computing may reduce the cost of smaller incidents, whereas dependence on increasingly important providers can raise the risk of extreme losses (Aldasoro et al., 2022).

The review further shows that the effects of cyberattacks extend beyond the cost of repairing systems. Kamiya et al. (2021) find that successful cyberattacks can generate reputational losses and affect a firm's relationships with customers and other stakeholders (Kamiya et al., 2021). Data breaches and service disruptions can reduce confidence in a firm's ability to protect customer information and funds.

Data risk was found to be closely related to model, cyber, compliance, and reputational risks. Inaccurate data can produce erroneous decisions, while inadequately protected data can result in privacy violations. As data become more extensively embedded in decision-making, organizations become increasingly dependent on their quality, security, and lawful use.

Findings on Third-Party Risk and Systemic Risk

The findings indicate that using third-party technology providers increases organizational dependence on systems beyond direct organizational control. These dependencies include cloud-service providers, data centers, communication networks, digital-identity services, and payment systems. A disruption at a major provider can affect numerous organizations using the same service.

Eisenbach et al. (2022) find that a cyberattack against an important institution in a payment network can propagate and disrupt financial-system activity. Other institutions' responses, including liquidity hoarding, may amplify the initial disruption (Eisenbach et al.,

2022). This result demonstrates how a digital disruption can escalate from an institution-level risk into a systemic risk.

The review also finds that the concentration of services among a small number of providers creates shared points of failure. An organization may maintain adequate internal controls and nevertheless suffer disruption when a technology provider fails. Organizational resilience therefore depends not only on internal controls but also on the resilience of the network and external parties supporting its operations.

Findings on Regulatory and Compliance Risks

The findings indicate that technological development creates compliance challenges because products and processes evolve more rapidly than regulation. Uncertainty arises in relation to consumer protection, data ownership, digital-asset security, cross-border transactions, and responsibility for decisions made by algorithms.

Anagnostopoulos (2018) finds that the development of FinTech and RegTech has changed how financial institutions and regulators perform oversight and compliance functions (Anagnostopoulos, 2018). RegTech is used to monitor transactions, identify suspicious activity, automate reporting, and track regulatory changes. The review nevertheless indicates that compliance technology continues to depend on data quality, accurate rules, and human oversight.

Findings on Risk Management and Mitigation

The findings show that organizations use a combination of technological controls, governance arrangements, and management processes to mitigate digital risk. These controls include transaction monitoring, model validation, data protection, security testing, external-provider oversight, scenario testing, and service-recovery planning.

Thakor (2020) shows that FinTech has generated innovations in payments, credit, insurance, cryptocurrencies, and blockchain-based contracts (Thakor, 2020). These technologies can improve decision quality and reduce intermediation costs. Their use, however, requires monitoring and control mechanisms commensurate with their technological complexity.

Studies of Enterprise Risk Management (ERM) demonstrate the importance of managing risk in an integrated manner. Bromiley et al. (2015) explain that ERM connects the management of all risks with organizational strategy and governance (Bromiley et al., 2015). Florio and Leoni (2017) identify a positive relationship between the extent of ERM implementation and firm performance (Florio & Leoni, 2017). These findings indicate that governance quality and risk-management maturity are associated with an organization's capacity to manage uncertainty.

Discussion

Digitalization as an Opportunity and a Source of Risk

The findings demonstrate that the relationship between digitalization and financial risk is not straightforward. Technology does not automatically increase or reduce risk. Its effects depend on how it is designed, implemented, monitored, and integrated into decision-making processes. Digitalization can improve efficiency and service quality, but these benefits are accompanied by changes in risk exposure.

This finding is consistent with Gomber et al. (2018), who frame FinTech as a transformation of operations, business models, and the structure of the financial-services industry rather than merely the application of new technology (Gomber et al., 2018). Risk management therefore cannot be postponed until after technology has been implemented. Risk considerations must form part of technology planning, selection, development, implementation, and evaluation.

Digitalization delivers its greatest benefits when organizations possess the capabilities needed to manage its consequences. Organizations with poor data quality, weak model oversight, and inadequate recovery plans may obtain short-term efficiencies while facing long-term vulnerabilities. Conversely, organizations that integrate innovation with risk governance are more likely to create sustainable value.

Mechanisms of Digital Financial Risk Transformation

The findings indicate that financial risks are transformed through acceleration, interconnectedness, datafication, and digital concentration. Acceleration refers to the increasing speed of transactions, information dissemination, and decision-making. This speed shortens the time available for organizations to identify and respond to problems. Oversight that relies on periodic reporting is therefore increasingly inadequate unless complemented by more dynamic monitoring.

Interconnectedness refers to the increasingly close relationships among financial institutions, digital platforms, payment systems, and technology providers. It expands the reach of services but also creates channels through which risk can spread. The findings of Eisenbach et al. (2022) reinforce this explanation by showing that payment-network disruptions can propagate through interinstitutional connections and liquidity-hoarding behavior (Eisenbach et al., 2022).

Datafication means that financial decisions are increasingly dependent on data and algorithms. Data use can improve predictive capacity, yet errors or biases may also be replicated rapidly and at scale. Digital concentration, meanwhile, arises when many organizations rely on the same provider or infrastructure. Such concentration can create economies of scale while simultaneously establishing points of failure capable of affecting the entire system.

These four mechanisms show that the defining characteristic of digital risk is not merely the emergence of new risk categories. The more fundamental change lies in the speed, interconnectedness, scale, and complexity of risk propagation. Digital-risk measurement must therefore account for temporal dimensions, network relationships, provider concentration, and data dependence.

Model Accuracy and Fairness in Credit Decisions

The findings on credit risk reveal trade-offs among accuracy, access, transparency, and fairness. Alternative data can help organizations assess prospective borrowers who lack formal credit histories. The findings of Berg et al. (2020) and Jagtiani and Lemieux (2019) indicate that digital footprints and machine learning can improve the information available for credit assessment (Berg et al., 2020; Jagtiani & Lemieux, 2019).

Improved predictive performance, however, does not necessarily amount to better decision quality overall. A model may be statistically accurate yet difficult to explain to a prospective borrower. It may also use variables that indirectly proxy for sensitive characteristics. Fuster et al. (2022) show that machine learning can generate different benefits for particular groups of borrowers (Fuster et al., 2022).

The effectiveness of digital credit models should therefore not be measured solely by their ability to predict default. Evaluation must also consider model stability, decision explainability, the potential for discrimination, data quality, and customer-appeal mechanisms. Human oversight remains necessary when assessing decisions with substantial social and economic consequences.

Technological Efficiency and Operational Resilience

The findings on cloud computing and third-party services reveal a trade-off between efficiency and resilience. External providers allow organizations to reduce costs and gain

access to more advanced technologies. However, organizations also relinquish a degree of direct control over data location, service availability, security, and recovery processes.

Aldasoro et al. (2022) show that cloud services can reduce the cost of smaller incidents, while dependence on increasingly dominant providers may increase the risk of extreme losses (Aldasoro et al., 2022). This finding demonstrates that operational efficiency does not necessarily correspond to system resilience. Infrastructure that is efficient under normal conditions can become a source of concentrated risk during a major disruption.

Organizations need to treat third-party risk as a strategic risk. Assessment should not be confined to the beginning of a contractual relationship but should continue through monitoring, security testing, performance evaluation, and recovery simulations. Organizations must also understand their principal providers' dependencies on other parties because risk may originate in technology-supply chains that are not directly visible.

Cyber Risk as a Financial and Strategic Risk

The findings show that cyber risk has expanded beyond the boundaries of technology risk. Cyberattacks can halt transactions, reduce revenue, generate recovery costs, and lead to litigation. Disruptions can also weaken customer confidence, allowing their effects to persist after systems have resumed operation.

Kamiya et al.'s (2021) findings on reputational losses indicate that the economic effects of cyberattacks cannot be calculated solely on the basis of technical costs (Kamiya et al., 2021). A firm may lose value when stakeholders question its ability to protect information and maintain service continuity. Cybersecurity is therefore a responsibility of senior management rather than solely a concern of the information technology function.

This discussion underscores the importance of a cyber-resilience approach that extends beyond prevention. No system can be guaranteed to remain entirely free from disruption. Organizations must therefore be able to detect, respond to, recover from, and learn from incidents. The speed of recovery and the quality of stakeholder communication are important components of loss control.

The Relevance of ERM to Digital Risk Management

The findings support the use of ERM as a foundation for managing digital risk. Interconnected risks cannot be managed effectively through fragmented approaches. A technological disruption can simultaneously affect operational, financial, legal, compliance, and reputational risks. ERM provides a framework for viewing these exposures collectively and connecting them to organizational objectives.

Bromiley et al. (2015) emphasize that ERM integrates risk management with organizational strategy and governance (Bromiley et al., 2015). Florio and Leoni's (2017) findings regarding the positive relationship between ERM and performance indicate that mature risk-management practices can contribute to value creation (Florio & Leoni, 2017).

ERM maturity is not demonstrated merely by the existence of a risk committee or policy documents. It is reflected in an organization's ability to use risk information in decision-making, assess cross-functional impacts, establish risk appetite, and prepare responses to extreme scenarios. In the digital era, ERM must also encompass data governance, model validation, cyber resilience, and technology-provider management.

Technology as a Risk-Mitigation Instrument

Technology can strengthen an organization's ability to detect and control risk. Artificial intelligence can be used to identify suspicious transactions, detect anomalies, and estimate changes in credit risk. Real-time data analytics can also provide early warning of changes in liquidity and operational disruption. RegTech can help organizations automate compliance monitoring and reporting.

Nevertheless, risk-mitigation technology cannot function effectively without adequate data and governance. Detection systems using inaccurate data can generate false alerts. Models that are not updated may lose predictive power as conditions change. Errors in automated systems can also spread more rapidly than errors in manual processes.

Risk-mitigation technologies must therefore be supported by independent validation, human oversight, decision documentation, access controls, and periodic evaluation. Technology should improve the quality of human judgment rather than eliminate the accountability of decision-makers.

Theoretical Implications

The findings extend the concept of financial risk management by demonstrating that traditional risks must be examined in conjunction with digital risks. Credit risk must be analyzed alongside model risk, data risk, and algorithmic fairness. Operational risk must be connected to cybersecurity, third-party dependence, and reputation. Liquidity risk must take account of transaction speed and information dissemination, while systemic-risk analysis must incorporate the concentration of technological infrastructure.

These findings support the view that digital risk results from interactions among technology, organizations, people, and the external environment. Technology does not have a uniform effect across organizations. Its impact depends on business characteristics, governance quality, workforce capabilities, market structure, and regulation. Research on digital financial risk therefore requires a multidisciplinary approach.

Managerial and Regulatory Implications

For management, the findings emphasize that digital risk must be incorporated into strategic planning. Technology-investment decisions should consider data security, model risk, third-party dependence, recovery capacity, and effects on customers. Management must also translate digital-risk appetite into clearly defined limits, indicators, and responsibilities.

Collaboration among business, finance, information technology, compliance, audit, and risk-management functions should be strengthened. Excessively rigid functional boundaries can impede information exchange and delay responses to disruptions. Organizations must also develop workforce capabilities so that employees can understand the benefits and limitations of the technologies in use.

For regulators, the findings demonstrate the need for supervisory approaches that keep pace with technological development. Oversight should encompass critical technology providers, data protection, algorithmic transparency, digital assets, and infrastructure concentration. Vives (2019) emphasizes the importance of balancing innovation, competition, consumer protection, and financial stability (Vives, 2019).

4. CONCLUSION

The systematic literature review demonstrates that digital transformation has fundamentally reshaped financial risk management. Digitalization does not eliminate traditional financial risks; rather, it expands their sources, forms, speed, and reach. Credit, market, liquidity, and operational risks are increasingly intertwined with model risk, cybersecurity, data quality, compliance, reputation, third-party risk, and financial-system stability. These interdependencies render fragmented risk-management approaches inadequate for addressing the complexity of the digital financial ecosystem.

Changes in the characteristics of digital financial risk occur through four principal mechanisms: acceleration, interconnectedness, datafication, and digital concentration. Acceleration increases the speed of transactions, information dissemination, and loss realization. Interconnectedness allows disruption at one entity to spread to others. Datafication increases the dependence of decisions on data and algorithms, while digital concentration creates reliance on a limited number of platforms or technology providers.

Together, these mechanisms allow digital risk to develop rapidly and produce effects that extend beyond organizational boundaries.

Technology performs a dual role in financial risk management. Artificial intelligence, machine learning, alternative data, cloud computing, blockchain, and RegTech can improve efficiency, enhance predictive capacity, expand financial access, and accelerate risk detection. The same technologies, however, can create algorithmic bias, opaque decisions, data breaches, cyberattacks, system failures, and dependence on external providers. The success of digitalization should therefore be assessed not only by speed, cost reduction, or accuracy but also by security, fairness, transparency, resilience, and recovery capability.

The findings show that Enterprise Risk Management is increasingly relevant to the management of digital risk. It enables organizations to connect technological risks with financial, operational, legal, compliance, and reputational risks. Risk-management maturity is reflected in an organization's ability to establish risk appetite, maintain data quality and security, validate models, oversee third parties, conduct scenario testing, and prepare effective responses and recovery arrangements. Policies and risk committees alone are insufficient without a strong risk culture, capable human resources, and active senior-management involvement.

The essence of financial risk management in the digital era is therefore not to avoid technology, but to ensure that technology is used in a controlled, responsible, and sustainable manner. Organizations that align digital innovation with mature governance and risk-management practices will be better positioned to capture technological opportunities while preserving financial stability, stakeholder confidence, and business continuity. Conversely, digitalization without adequate controls may generate short-term efficiency while increasing long-term vulnerability and loss exposure.

REFERENCES

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability, 60*, Article 100989. https://doi.org/10.1016/j.jfs.2022.100989

Anagnostopoulos, I. (2018). Fintech and RegTech: Impact on regulators and banks. *Journal of Economics and Business, 100*, 7–25. https://doi.org/10.1016/j.jeconbus.2018.07.003

Berg, T., Burg, V., Gombović, A., & Puri, M. (2020). On the rise of FinTechs: Credit scoring using digital footprints. *The Review of Financial Studies, 33*(7), 2845–2897. https://doi.org/10.1093/rfs/hhz099

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long Range Planning, 48*(4), 265–276. https://doi.org/10.1016/j.lrp.2014.07.005

Eisenbach, T. M., Kovner, A., & Lee, M. J. (2022). Cyber risk and the U.S. financial system: A pre-mortem analysis. *Journal of Financial Economics, 145*(3), 802–826. https://doi.org/10.1016/j.jfineco.2021.10.007

Florio, C., & Leoni, G. (2017). Enterprise risk management and firm performance: The Italian case. *The British Accounting Review, 49*(1), 56–74. https://doi.org/10.1016/j.bar.2016.08.003

Frost, J., Gambacorta, L., Huang, Y., Shin, H. S., & Zbinden, P. (2019). BigTech and the changing structure of financial intermediation. *Economic Policy, 34*(100), 761–799. https://doi.org/10.1093/epolic/eiaa003

Fuster, A., Goldsmith-Pinkham, P., Ramadorai, T., & Walther, A. (2022). Predictably unequal? The effects of machine learning on credit markets. *The Journal of Finance, 77*(1), 5–47. https://doi.org/10.1111/jofi.13090

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the FinTech revolution: Interpreting the forces of innovation, disruption, and transformation in financial

services. *Journal of Management Information Systems, 35*(1), 220–265. https://doi.org/10.1080/07421222.2018.1440766

Gomber, P., Koch, J.-A., & Siering, M. (2017). Digital finance and FinTech: Current research and future research directions. *Journal of Business Economics, 87*(5), 537–580. https://doi.org/10.1007/s11573-017-0852-x

Jagtiani, J., & Lemieux, C. (2019). The roles of alternative data and machine learning in FinTech lending: Evidence from the LendingClub consumer platform. *Financial Management, 48*(4), 1009–1029. https://doi.org/10.1111/fima.12295

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics, 139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Liu, Y., & Tsyvinski, A. (2021). Risks and returns of cryptocurrency. *The Review of Financial Studies, 34*(6), 2689–2727. https://doi.org/10.1093/rfs/hhaa113

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, Article n71. https://doi.org/10.1136/bmj.n71

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Thakor, A. V. (2020). Fintech and banking: What do we know? *Journal of Financial Intermediation, 41*, Article 100833. https://doi.org/10.1016/j.jfi.2019.100833

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management, 14*(3), 207–222. https://doi.org/10.1111/1467-8551.00375

Vives, X. (2019). Digital disruption in banking. *Annual Review of Financial Economics, 11*, 243–272. https://doi.org/10.1146/annurev-financial-100719-120854

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research, 39*(1), 93–112. https://doi.org/10.1177/0739456X17723971