International Journal of
Government Accounting Management
Volume 2, Number 2, 2023

Digital Governance, Risk-Based Regulation, and Cyber Risk Management: A Systematic Literature Review

Sufi Sundari[1]

[1] Universitas Bhayangkara Jakarta Raya Bekasi, Bekasi, Indonesia

Abstract

Article history:
Received: July 20, 2023
Revised: August 29, 2023
Accepted: October 15, 2023
Published: December 30, 2023

Keywords:
Cybersecurity,
Data Analytics,
Digital Governance,
Digital Transformation,
Risk-Based Regulation.

Identifier:
Zera Open
Page: 114-133
https://zeraopen.com/journal/ijgam

Digital transformation has become a strategic element in modern organizational renewal, driving the need for more adaptive information technology governance, data regulation, and risk management. This study presents a Systematic Literature Review of academic publications over the past five years to identify conceptual developments, governance practices, and cybersecurity challenges in an increasingly complex digital environment. The results of the analysis show that the success of digital transformation is not only determined by the adoption of technology, but also by the dynamic capabilities, quality of data governance, and resilience of the system to cyber threats. The risk-based regulatory approach stands out as an important framework for balancing innovation with consumer protection, although its effectiveness is influenced by the harmonization of technical standards and institutional capacity. The study also found significant limitations in the availability of cyber incident data, which hindered evidence-based risk assessments and more precise policy formation. These findings underscore the need for a digital strategy that is integrated with IT governance, enhanced analytics capabilities, and strengthened security culture to ensure the continued value of organizational digitalization.

1. Introduction

The development of digital technology over the last five years has significantly changed the way public and private organizations manage information, organize operational activities, and interact with stakeholders. Digital transformation is now understood not just as the adoption of new technologies, but as a structural change that affects business processes, organizational capabilities, and governance models as a whole (Hanelt et al., 2021). In this context, organizations are required to not only integrate technology but also ensure that those changes create value as well as increase operational resilience. Digital transformation also has strategic implications, including the need to develop dynamic capabilities, adapt quickly, and be ready to manage data-driven risks (Mikalef et al., 2021).

The literature suggests that digitalization is driving the need for stronger information governance, especially as organizations increasingly rely on data as a source of competitive advantage and a basis for decision-making. The use of big data analytics and automation technologies allows for faster and more accurate processing of information at scale, but it also opens up new vulnerabilities to cyber risks and data integrity issues (Mikalef et al., 2019). Therefore, digital transformation must be balanced with the strengthening of internal control mechanisms, comprehensive risk assessments, and the implementation of data protection standards in accordance with international regulations. Risk-based approaches in regulations such as GDPR provide an example of how data protection should not only focus on administrative compliance, but on the evaluation of real risks to data subjects and organizations (Gellert, 2018).

As the frequency and complexity of cyberattacks increase, information security issues are becoming a major concern in the development of IT governance. Recent studies show significant limitations in the availability of cyber risk data, making it difficult to assess threats appropriately and consistently (Cremer et al., 2022). This data gap poses methodological and practical challenges for organizations in formulating evidence-based risk mitigation strategies. Therefore, the literature encourages the strengthening of risk data collection frameworks, inter-agency collaboration, and cybersecurity integration into digital transformation design from the initial stage, rather than as an addition at the end.

In addition to technical challenges, digital transformation also has an impact on the regulatory and governance aspects of the financial services sector. The development of open banking, digital banking, and fintech ecosystems has created a new need for interoperability standards, consumer protection, and secure system integration. Research shows that API standardization in the open banking ecosystem is needed to ensure the security of data exchange and strengthen public trust in digital services (Billiam et al., 2022). On the other hand, digital innovation in banking also encourages organizations to pay attention to risk disclosure practices, as exposure to operational, technological, and cyber risks increases with the complexity of digitalization (Tjondro et al., 2021).

Regulatory sources and applied literature also emphasize the importance of IT governance and risk management in the development of digital services, especially in financial sectors that operate under strict scrutiny. In the banking digital transformation guideline document, it is highlighted that the success of digitalization

is greatly influenced by the readiness of governance structures, IT risk management capacity, and adequate control mechanisms (Abubakar & Handayani, 2022). This shows that digital transformation is a multidimensional process that requires regulatory support, organizational readiness, and the integration of security and risk principles as a whole.

Thus, the development of digitalization presents great opportunities as well as real challenges. On the one hand, technology is able to improve efficiency, accuracy, and quality of decision-making. On the other hand, new risks such as cyberattacks, system dependencies, and regulatory complexity require a holistic approach in governance. This article aims to analyze the latest findings on digital transformation, information technology governance, and risk management, by reviewing the academic literature of the past five years, in order to provide a comprehensive overview of the direction of development and its implications for modern organizations.

2. Literature Review

2.1. Theoretical Foundations of Digital Transformation

The theoretical foundation of digital transformation emphasizes that digitalization is not just the adoption of technology but a strategic change that involves the entire organization overhauling business models, processes, and capabilities. Researchers place dynamic capabilities as a mechanism by which organizations detect opportunities, take advantage of them, and reconfigure resources to achieve a competitive advantage in the digital environment (Hanelt et

al., 2021). A review of the literature shows that digital transformation research integrates technological, organizational, and managerial dimensions so that new leadership patterns and governance arrangements are needed to align IT investments with strategic goals (Vial, 2019). The methodological survey mapped research clusters on strategy, technology adoption, human factors, and value creation, suggesting a multi-level approach to examining transformation (Zhu et al., 2021). This theoretical orientation implies that the success of digital transformation depends on the interaction between technical infrastructure (cloud, analytics, APIs), organizational readiness (culture, skills, structure), and ecosystem relationships (partners, regulators).

Thus, researchers are pushing for an integrative framework that links capability building with risk governance, recognizing that digital initiatives create opportunities as well as vulnerabilities. Practical implications for managers include prioritizing capability development programs, establishing cross-functional governance mechanisms, and designing metrics that measure innovation outcomes as well as operational resilience. For academics, the research agenda invites mixed-method studies that explore causal mechanisms and boundary conditions of transformation between sectors. Overall, the theoretical basis positions digital transformation as an endogenous process shaped by external strategies, capabilities, and constraints, rather than just exogenous technological shocks (Hanelt et al., 2021; Vial, 2019; Zhu et al., 2021). This perspective also encourages policy dialogue on governance and regulation at the international level as well.

2.2. Data Governance, Privacy, and Regulatory Approaches

Data governance, privacy, and regulatory approaches are important elements in the digitization literature. Regulatory frameworks tend to adopt a risk-based approach that links legal obligations to potential losses as well as organizational risk management processes (Gellert, 2018). This approach encourages regulators to request in addition to administrative compliance also proactive risk assessments, documentation, and mitigation by controllers and data processors. Policy reports and studies, including digital economy measurement efforts, emphasize the need for policies that balance innovation with consumer protection and financial stability (IMF, 2018). Measurement challenges arise as data flows across jurisdictions and as digital services create new intermediaries such as platforms and fintech providers that complicate accountability. In practical terms, data governance should handle data lifecycle management (collection, retention, sharing, deletion), transparency for data subjects, and access and correction mechanisms.

Regulatory design can have benefits when integrating technical standards (e.g. APIs, security controls) with legal principles to ensure interoperability and trust. Sector guidelines and roadmaps show how sectoral regulations and supervisory expectations shape organizational practices; In particular, policy guidance and regulatory explanations serve as a template for governance, risk management, and reporting obligations. For the context of digital banking and related regulations, this policy review also refers to reference materials that present IT governance guidelines and operational risk management requirements. When rules are bundled with capacity building and harmonization of standards, the cost of compliance can be

offset by increased consumer confidence and market integration. Therefore, effective regulation in the digital era is adaptive, principled, and supported by technical infrastructure and public-private collaboration (Gellert, 2018; IMF, 2018).

2.3. IT Governance, Risk Management, and Cybersecurity

IT governance, risk management, and cybersecurity are at the core of operationalizing a secure digital transformation. Cybersecurity research emphasizes that organizational defense requires technological controls as well as governance mechanisms that coordinate third-party responsibility, incident response, and oversight (Cremer et al., 2022). The availability and quality of cyber incident data determine the capacity of researchers and practitioners to model threats and prioritize investments; Lack of data hinders evidence-based decision-making. From an organizational capability perspective, big data analytics capabilities improve detection, prediction, and resilience, but the benefits are mediated by organizational inertia and governance quality (Mikalef et al., 2021). In other words, analytics tools provide value only when embedded in a governance framework that aligns incentives and supports continuous learning.

In the financial services sector, empirical studies show that digital innovation increases the need for risk disclosure and tighter internal controls as exposure to operational and cyber risks increases with the complexity of platforms (Tjondro et al., 2021). Therefore, an effective IT governance framework integrates risk assessment, vendor management, business continuity planning, and regular audit cycles. The framework adopts a standards-based approach (e.g., COBIT, ISO 27001) while tailoring controls to the organization's strategic risk profile. In practice,

governance processes should include cross-functional oversight, clear escalation paths, and stress-based scenario testing for critical systems. Finally, the literature emphasizes that technology investments must be complemented by human capital development, training, digital talent retention, and cultural reform to maintain cybersecurity postures and support adaptive risk management. Board oversight and executive accountability are key elements.

3. Methods

This study uses the Systematic Literature Review (SLR) method to produce a comprehensive understanding of the development of digital transformation, information technology governance, data regulation, and risk management in the context of modern organizations. The SLR method was chosen because it is able to present a structured synthesis of scientific findings in a certain time frame by ensuring that the process of collecting, selecting, and analyzing literature is carried out objectively, transparently, and can be replicated. The SLR procedure in this study follows general stages, which include the formulation of research questions, the determination of inclusion and exclusion criteria, the identification of literature sources, the systematic selection of articles, the extraction of data, and the synthesis of findings to prepare conceptual interpretations and theoretical and practical implications. The publication range set is the last five years with a focus on Google Scholar-indexed articles to ensure academic relevance and accountable scientific quality. The keywords used include digital transformation, IT governance, cybersecurity risk, data governance, risk-based regulation, and financial

digitalization. The identification process begins with searching the Google Scholar database, as well as matching the findings to the reference list in the relevant article through backward and forward citation tracking techniques.

The inclusion criteria include articles that discuss digital transformation at the organizational level, IT governance, cybersecurity, data regulation, big data analytics, and operational risks related to digitalization. Policy articles and industry-specific reports are also considered if they are of academic significance and are widely cited in the scientific literature, including relevant guidance documents on information technology governance and regulatory frameworks listed in discussions of several sources.

Meanwhile, articles that focus on the development of pure technologies with no relation to governance or risk management are excluded from the analysis. Selection is done through a review of the title, abstract, and content of the article to ensure fit with the scope of the research. Each article that passed the selection was then extracted using a worksheet that contained information about the research objectives, methods, key concepts, main findings, and contributions to the SLR theme.

The synthesis stage is carried out narratively by grouping the findings of the article based on the main conceptual themes, namely the foundations of digital transformation, data governance and regulation, as well as IT governance and risk management. This process allows for the identification of patterns, research gaps, and conceptual relationships between themes. This synthesis approach also helps formulate theoretical and practical implications that can support the development of

digital strategies and the strengthening of IT governance in various sectors. Thus, this SLR not only maps the development of the literature, but also provides a direction for future research by highlighting the need for integration between digital innovation, adaptive regulation, and comprehensive risk management.

4. Results

The results of this SLR are presented as a synthesis of empirical and conceptual findings from the literature of the last five years that are identified as relevant to the themes of digital transformation, IT governance, data regulation, and risk management. The analysis organized the findings into six main patterns: (1) the adoption pattern and maturity of digital transformation, (2) the role of dynamic and analytical capabilities, (3) the challenges of data governance and risk-based regulation, (4) the characteristics of cyber risk and the limitations of incident data, (5) the implications on the financial services sector, and (6) the research gap and the prominent research agenda. These six patterns appear consistently in various academic publications, policy reports, and empirical studies, thus providing a strong picture of the direction of development of the digitized literature.

First, the literature shows that the adoption of digital transformation is heterogeneous between organizations and relies on strategic maturity and resource allocation. Systematic reviews indicate that digital transformation is not just a technology implementation, but rather a multidimensional process that requires adjustments to organizational structures, business processes, and value models (Hanelt et al., 2021). Organizations that successfully move pilot initiatives to scale

operations tend to have clear leadership, cross-functional governance structures, and metrics that link IT investments to business outcomes. Meanwhile, immature organizations are often stuck on technology initiatives without fundamental process changes (Vial, 2019). The literature also notes that digital transformation works more effectively when organizations develop an explicit strategic vision and make digitalization the core of the strategy, rather than an ancillary project.

Second, the role of dynamic capabilities and analytical capabilities is the main determinant in translating data into strategic value. Some studies emphasize that big data analytics improves an organization's ability to detect patterns, respond to markets, and optimize operations, but these benefits are moderated by organizational inertia and limitations of cross-unit coordination (Mikalef et al., 2021). Organizations with high bureaucratic levels or silo structures tend to be slow to utilize data insights. In addition, strong analytics capabilities tend to result in operational efficiencies and predictive capabilities that are useful in risk management; however, without adequate governance, analytics results do not automatically become responsible or actionable decisions (Mikalef et al., 2019). These findings underscore that analytics technology is not an automated solution, but a tool that must be operationalized through a disciplined decision-making process.

Third, regarding data governance and regulation, the literature consistently recommends a risk-based regulatory approach that requires organizations to identify and mitigate impacts on data subjects, rather than simply meeting administrative compliance checklists (Gellert, 2018). Policy studies and digital economy reports

emphasize that effective regulation must be adaptive and principled so as to encourage innovation while minimizing consumer risk and market stability (IMF, 2018; Asia, 2021). The challenges of implementing this regulation can be seen from the variation in the level of organizational readiness in implementing data governance. Effective data governance practices are generally characterized by a clear data management cycle (collection, retention, sharing, deletion) as well as transparency mechanisms and access rights for data subjects. However, many studies have found inconsistencies in implementation across sectors, particularly in organizations that face commercial pressure to monetize data (Zhu et al., 2021). This shows that there is a "structural tension" between digital innovation and regulatory compliance that has not been fully resolved.

Fourth, the nature and measurement of cyber risk a critical issue in the literature. Research shows an increase in the intensity and complexity of cyber incidents as organizations increase their reliance on digital systems, API integration, and cloud adoption. However, the literature also highlights the limitations of empirical data on cyber incidents that make it difficult to quantitatively estimate risks (Cremer et al., 2022). Lack of comprehensive incident datasets, reporting inconsistencies, and barriers to information sharing between organizations make it difficult to create reliable risk models. This situation causes many organizations to rely on assumption-based risk estimates or external data sources that do not always fit the internal context. Therefore, many studies call for the establishment of more transparent incident reporting mechanisms, standardized data formats, and inter-agency collaborative frameworks to support quantitative research and evidence-

based policymaking. Without adequate cyber data, risk management will continue to be in an unequal state of information (information asymmetry).

Fifth, the findings specifically in the financial services sector confirm that digitalization accelerates changes in business models (e.g. open banking, digital-only services) while increasing exposure to operational and security risks. Empirical studies of the banking sector show an increase in the need for risk disclosure and internal control structuring when institutions expand their digital services either through direct channels or through partnerships with fintech providers (Tjondro et al., 2021; Dubey, 2019). Governance changes are necessary because the relationship between banks, fintechs, and other third parties forms an extended digital ecosystem that adds to potential failure points. In addition, technical standardization initiatives such as API standardization are identified as key to maintaining interoperability and security of data exchange in the digital financial ecosystem (Billiam et al., 2022). However, the implementation still varies, depending on the readiness of the infrastructure and the maturity of sectoral regulations. In some jurisdictions, technical standards and privacy requirements are not yet fully aligned, creating a gray area for industry players.

Sixth, the literature maps several consistent research gaps from year to year. These gaps include: (a) the need for longitudinal studies on the impact of digital transformation on organizational resilience; (b) quantitative research that uses more reliable cyber incident datasets to model the relationship between governance controls and security outcomes; (c) comparative studies of the effectiveness of risk-based regulatory approaches in various jurisdictions; and (d) studies that causally link

analytics, governance, and business outcomes capabilities (Zhu et al., 2021; Cremer et al., 2022). In addition, the research also shows the need for further exploration of the dimension of human resources, particularly upskilling, organizational cultural characteristics, and digital readiness because technology without cultural change and human capacity tends to result in underperformance of digital initiatives (Winasis et al., 2020). The literature also highlights that organizations often place IT investments as technical projects, rather than transformational policies, thus hindering the diffusion of digital innovation internally.

From a practical perspective, the study emphasizes a gradual strategy: starting from improving data governance and security controls, then strengthening analytics capabilities, and closing with strengthening the process of supervision, reporting, and regulatory harmonization. Organizations that adopt a consistent approach report an increase in customer trust and a decrease in the frequency of operational disruptions due to IT factors (Hanelt et al., 2021; Mikalef et al., 2020). However, the literature also warns of a trade-off between accelerating innovation and tightening controls. Regulators and stakeholders must design policies that balance innovation incentives with consumer protection and systemic stability (IMF, 2018). The overall results of these SLRs show significant progress in the conceptual understanding of digital transformation and IT governance over the past five years, but also affirm the strong need for better empirical data, harmonization of technical and regulatory standards, and research that examines causal mechanisms between digital capabilities, governance, and performance or security outcomes.

5. Discussion

The SLR findings illustrate that digital transformation presents great opportunities for increased efficiency, service innovation, and new value creation, but successful implementation relies heavily on a balance between accelerating technology adoption and strengthening comprehensive governance. In practical terms, the results show that without technical standardization such as APIs and interoperability mechanisms, the benefits of innovation, especially in the financial ecosystem, are at risk of being hampered by system fragmentation and data security issues (Billiam et al., 2022). Therefore, technical drivers (e.g., API standardization) must be combined with clear governance policies so that integration between ecosystem actors does not compromise consumer protection or operational stability.

The discussion also emphasized the role of risk disclosure and transparency as instruments of market control. In the financial services sector, the improvement of digital services requires intensification of risk disclosure practices so that stakeholders can evaluate institutional exposure to operational, technological, and cyber risks (Tjondro et al., 2021). Better disclosure not only benefits regulators in supervision but also encourages market discipline that spurs institutions to improve governance and risk management practices. However, there are trade-offs: exaggerated disclosure without context can lead to confusion or disproportionate market reactions; Therefore, a standard and targeted disclosure format is needed.

The human resource and organizational culture aspects stand out as determinants of implementation. Empirical studies have found that investments in advanced analytics capabilities and detection tools are only effective when followed

by employee upskilling and process reforms, and cross-functional governance mechanisms (Winasis et al., 2020). Digital competency gaps can lead to reliance on external vendors and increase third-party risk, so organizations need to strike a balance between the use of third-party services and the availability of internal capabilities for oversight and auditing.

Further, the literature highlights that principle-based regulatory approaches allow for innovation space while setting minimum protection limits, but their effectiveness depends on the capabilities of regulators and the harmonization of technical standards (Zhu et al., 2021). Overly rigid regulations have the potential to hinder the adoption of new technologies; On the contrary, overly loose regulations can increase systemic risks and harm public trust. Therefore, the hybrid model of a combination of risk-based principles with adaptive technical guidelines emerged as a promising policy direction.

The limitation of cyber incident data is a significant obstacle to quantitative risk assessment and policy evaluation. The absence of reliable datasets reduces the ability of policymakers and researchers to benchmark and develop consistent security performance indicators. Therefore, standardized incident reporting initiatives and secure information sharing mechanisms between industry players need to be prioritized to enhance collective resilience.

Strategically, organizations are advised to adopt a gradual roadmap: starting from improving data governance and security controls, then building analytics capabilities, and finally strengthening monitoring and reporting mechanisms. This phased implementation helps balance the need for innovation with protection and

compliance obligations. On the research side, there is a strong need for longitudinal and quantitative studies that examine the causal relationship between digital capabilities, governance practices, and security outcomes or institutional performance (Dubey, 2019). This approach will provide a stronger empirical foundation for adaptive and effective policy design.

6. Conclusion

This research confirms that digital transformation is a complex strategic process, involving changes in organizational structures, strengthening IT governance, and integrating data capabilities and cybersecurity. The literature synthesis shows that the success of digitalization is not only determined by technology adoption, but by the organization's ability to build dynamic capabilities, proactively manage risk, and implement consistent data governance. Risk-based regulatory approaches offer an adaptive framework for balancing innovation with consumer protection, but their effectiveness depends heavily on the harmonization of technical standards and institutional competence in implementing them.

On the other hand, the intensification of cyber threats and the limitations of incident data require organizations to strengthen risk management frameworks, improve risk disclosure, and build a sustainable security culture. The financial services sector shows that digitalization expands opportunities for efficiency and innovation, but also increases exposure to operational risks and systemic dependencies, thus requiring stronger internal controls and better interoperability standards.

The SLR identifies a number of important research agendas, including the need for longitudinal studies, better data-driven cyber risk modelling, and comparative studies of regulatory effectiveness across sectors. Overall, the findings underscore the need for a holistic approach that integrates digital strategy, IT governance, risk management, and adaptive policies to ensure that digital transformation delivers sustainable, secure, and accountable value.

References

Abubakar, L., & Handayani, T. (2022). Penguatan regulasi: Upaya percepatan transformasi digital perbankan di era ekonomi digital. *Masalah-Masalah Hukum*, *51*(3), 259-270.

Asia, E. C. S. (2021). Roaring 20s: The SEA Digital Decade. *Google, Temasek, Bain & Company*. Retrieved November 11, 2022 From *https://www. bain. com/globalassets/noindex/2021/e_conomy_sea_2021_report. pdf*.

Billiam, B., Abubakar, L., & Handayani, T. (2022). The urgency of Open Application Programming Interface Standardization in the implementation of open banking to customer data protection for the advancement of Indonesian banking. *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)*, *9*(1), 67-88.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva papers on risk and insurance. Issues and practice*, *47*(3), 698.

Dubey, V. (2019). FinTech innovations in digital banking. *International Journal of Engineering Research & Technology (IJERT)*, *8*(10), 597-601.

Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review*, *34*(2), 279-288.

Hanelt, A., Bohnsack, R., Marz, D., & Antunes Marante, C. (2021). A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change. *Journal of management studies*, *58*(5), 1159-1197.

International Monetary Fund. (2018). *Measuring the digital economy*. IMF Policy Paper. Retrieved November 5, 2022 From https://share.google/ijTSAYIU5NatSJlfZ

Mikalef, P., Boura, M., Lekakos, G., & Krogstie, J. (2019). Big data analytics capabilities and innovation: the mediating role of dynamic capabilities and moderating effect of the environment. *British journal of management*, *30*(2), 272-298.

Mikalef, P., van de Wetering, R., & Krogstie, J. (2021). Building dynamic capabilities by leveraging big data analytics: The role of organizational inertia. *Information & Management*, *58*(6), 103412.

Tjondro, E., Cintya, M. O., Seto, S., & Suherman, Y. G. (2021). Do digital innovation and risk disclosure control performance? Evidence from banking in ASEAN-6. *JIA (Jurnal Ilmiah Akuntansi)*, *6*(2), 200-220.

Vial, G. (2021). Understanding digital transformation: A review and a research agenda. *Managing digital transformation*, 13-66.

Winasis, S., Riyanto, S., & Ariyanto, E. (2020). Digital transformation in the indonesian banking industry: Impact on employee engagement. *International Journal of Innovation, Creativity and Change*, *12*(4), 528-543.

Zhu, X., Ge, S., & Wang, N. (2021). Digital transformation: A systematic literature review. *Computers & Industrial Engineering*, *162*, 107774.