International Journal of Management Science and Information Technology
IJMSIT

E-ISSN: 2774-5694 P-ISSN: 2776-7388 OPEN ACCESS

Volume 6 (1), January-June 2026, 595-608
DOI: https://doi.org/10.35870/ijmsit.v6i1.6871

Digital Transformation and Adaptive Risk Management in Industry 4.0: A Conceptual Review of the Expanding Spectrum of Organizational Risk

Selvy Afrioza [1*], Irvan Bernandita Primandanu [2]
[1*,2] Digital Business Study Program, Faculty of Technology and Business, Universitas Yatsi Madani, Tangerang City, Banten Province, Indonesia

Email: selvyafrioza@uym.ac.id [1*], Bernandita09@gmail.com [2]

Article history:
Received March 29, 2026
Revised May 18, 2026
Accepted May 22, 2026

Abstract

The acceleration of digital transformation in the industry 4.0 era has fundamentally changed the way organizations conduct business processes, make decisions, and build competitive advantage. These changes have also broadened the spectrum of organizational risks, making them increasingly complex, interconnected, and difficult to predict. This phenomenon has created an urgent need for risk management strategies that are no longer reactive, but rather adaptive, proactive, and data-driven. The purpose of this study is to analyze the relationship between digital transformation and adaptive risk management strategies, focusing on how digitalization expands organizational risk from the operational level to the strategic, socio-technical, and systemic levels. This research uses a structured conceptual literature review that examines academic books, scientific journal articles, industry reports, and relevant policy documents, particularly those published in the last five years. Source collection was carried out through the stages of identification, selection, relevance evaluation, final document determination, and analysis using an interpretive qualitative approach and thematic analysis techniques. The results of the study indicate that digital transformation reconfigures organizational strategies, business processes, and decision-making patterns, while increasing vulnerability to risks in cybersecurity, data privacy, reputation, governance, and human resource readiness. This study confirms that organizations need adaptive risk management supported by digital leadership, data and security governance, organizational readiness, and continuous learning. The article's primary contribution lies in the formulation of an integrative conceptual framework linking digital transformation, the expansion of the organizational risk spectrum, adaptive risk management, and organizational resilience.

Keywords:
Adaptive Risk Management; Digital Transformation; Industry 4.0; Organizational Resilience; Organizational Risk Spectrum.

1. INTRODUCTION

The development of the Industrial Revolution 4.0 has brought about major changes in the work patterns of organizations worldwide. This change is characterized by the use of intelligent technologies such as the Internet of Things (IoT), artificial intelligence (AI), big data, and cloud-based technologies in various operational activities. These technologies can support productivity, transform management systems, business models, and relationships between stakeholders. Research result emphasizes that the comprehensive implementation of 4.0 technologies has become a national priority to address the challenges of competitiveness and efficiency (Hatmoko, 2021). Digital transformation, as the core of the Industrial Revolution 4.0, has become a choice and a strategic necessity. Organizations that fail to adapt to the digital landscape face the risk of stagnation, being left behind, and even failure. This transformation encompasses

the utilization of technology, the reshaping of business processes, organizational structures, and work culture. Therefore, digital transformation is a multidimensional process that changes organizational characteristics through technology adoption and systemic innovation.

Along with the opportunities it offers, digital transformation also broadens the spectrum of risks faced by organizations. These risks are operational, encompassing data risks, privacy risks, cybersecurity risks, business model disruption, and social and organizational risks. The research results note that in the era of digital transformation, risk management must be a key element of organizational strategy to ensure operational continuity and stability (Damayanti et al., 2023; Afrioza, Rasyiddin, et al., 2025). A major challenge in addressing this new spectrum of risks is the high uncertainty and dynamic nature of risk. The digitalization process accelerates the pace of change, exposing organizations to risks that are neither linear nor easily predictable (Pranata & Ismail, 2022). Therefore, a more adaptive, collaborative, and data-driven risk management approach is needed. This approach enables organizations to anticipate, respond to, and mitigate risks at a pace commensurate with the rate of change.

An increasingly prominent phenomenon in the industry 4.0 era is the shift in organizational risk profiles from a relatively linear pattern to interconnected, fast-moving risks that are difficult to separate between technical, managerial, and strategic dimensions. Recent studies show that digital transformation is pushing organizations into digital ecosystems with increasingly blurred organizational boundaries, changing distribution of authority, and increasing reliance on data, platforms, and collaborative networks (Plekhanov et al., 2023). In this context, the integration of cyber-physical systems (CPS) in supporting industrial digital transformation in the industry 4.0 era. CPS integrates various technologies such as Big Data Analytics and Artificial Intelligence to expand efficiency opportunities, improve real-time monitoring and control of manufacturing processes, and increase the complexity of organizational architecture by bringing together software, hardware, networks, data processing, human interfaces, and relationships between stakeholders in a single interdependent value system (Julian et al., 2024) While the use of AI and data-driven decision-making processes can strengthen cyber defenses, they also introduce new risks such as adversarial attacks, data manipulation, information integrity vulnerabilities, and a high reliance on data quality (Jada & Mayayise, 2024). Other studies emphasize the importance of using a more specific cybersecurity framework for each sector to protect organizations, given the increasing risk of data manipulation in Industry 4.0-based manufacturing (Toussaint et al., 2024). This situation demonstrates that digital transformation not only expands organizational capacity but also broadens the spectrum of risks that must be adaptively anticipated.

Based on these developments, the research gap in this study lies in the continued fragmented discussion of digital transformation, organizational readiness, resilience, digital leadership, and cybersecurity in the previous literature. A number of studies have examined digital transformation from the perspective of changing business models, organizational ecosystems, and building resilience through learning and innovation (Plekhanov et al., 2023; Awad & Martín-Rojas, 2024). Other research highlights digital transformation readiness as a combination of technological resources, business processes, managerial capabilities, human resource capabilities, and organizational culture (Michelotto & Joia, 2024). A study on Industry 4.0 security emphasized that many digital risk mitigation frameworks are still generic and high-level, thus not fully adequate to explain the increasingly complex interrelationships between organizational risks (Toussaint et al., 2024). Consequently, there are still limited conceptual studies that integratively position digital transformation as a driver of expanding the spectrum of organizational risks and then link it to the need for cross-functional, predictive, and capability-based adaptive risk management strategies. Therefore, the novelty of this article lies in the effort to formulate a conceptual framework that integrates the dimensions of digital transformation, the expansion of the risk spectrum, and adaptive risk management strategies into a coherent argumentation, thereby providing a more comprehensive, capability-based theoretical foundation for maintaining sustainability and strengthening organizational resilience in the industry 4.0 era. Based on these gaps, the main issue in this study is the lack of a conceptual framework that integratively explains how digital transformation broadens the spectrum of organizational risks and how adaptive risk management strategies need to be designed to respond to these dynamics proactively, predictively and cross-functionally.

The adaptive risk management approach is rooted in the principles of flexibility and cross-functional integration. In a digital context, risks can no longer be addressed sectorally or in isolation, as technological vulnerabilities, business processes, human competencies, and organizational governance are intertwined and linked within a single transformation ecosystem. Studies on organizational digital transformation readiness indicate that an organization's digital transformation readiness is determined by its technological resources, business processes, managerial capabilities, human capabilities, and organizational culture. Therefore, risk management must be positioned as a shared responsibility that transcends work unit boundaries. Instead, organizations need to build a real-time risk monitoring system that involves various work units and utilizes analytical technology to identify threat signals early and respond in a coordinated manner. According to Damayanti in their book “Manajemen Risiko Era Transformasi Digital”, risk mitigation strategies must utilize data as the primary source of decision-making and involve all levels of the organization in the process (Damayanti et al., 2023). This view aligns with previous research which shows that digital transformation (DT) plays an important role in increasing organizational resilience through organizational learning and

innovation conducted on 259 SMEs in Andalusia, Spain, which found that the use of digital technology increases learning capacity and encourages innovation, thus making SMEs more adaptive, flexible, and able to respond to market changes and take advantage of new opportunities (Awad & Martín-Rojas, 2024). Pleknov's research suggests that companies advancing in digital transformation are increasingly integrated into platform ecosystems, with increasingly blurred business boundaries. Furthermore, tensions arise between centralization and decentralization of power within organizations, which impacts corporate strategy and the organization's internal and external boundaries (Plekhanov et al., 2023). In 29 systematic literature review studies of various sources with a time span of 2019 to 2025 and 8 methodological sources, shows that digital transformation readiness is influenced by several key dimensions: technological resources, business processes, management capabilities, human resource capabilities, and organizational culture. Digital readiness and e-readiness share similar concepts in assessing an organization's maturity level toward digital transformation. Based on these findings, this study proposes an integrative framework to evaluate an organization's readiness to undertake digital transformation more effectively (Michelotto & Joia, 2024). AI has a positive impact on cybersecurity by enhancing automation, threat intelligence, and cyber defense systems, making organizations more effective and resilient to cyberattacks. Although AI implementation also faces challenges such as adversarial attacks and the need for high-quality data, making AI more effective than traditional cybersecurity approaches, while also providing a basis for organizations to make strategic decisions regarding AI implementation (Jada & Mayayise, 2024). This suggests that digital transformation will be more effective in strengthening organizational resilience when supported by organizational learning, innovation, and adaptive internal readiness.

Furthermore, digital transformation also demands changes in leadership and decision-making. Organizations need leaders who can understand technological trends, build a work culture open to innovation, and instill risk awareness at every level. The research results state that the success of digital transformation is greatly influenced by the long-term commitment of leaders in managing change and forming a resilient organizational culture (Teichert, 2019). In line with this, recent research shows that digital leadership acts as a catalyst for transformation because leaders will set strategic direction, empower employees to embrace technological change, strengthen organizational commitment, and maintain effective performance in a rapidly changing environment (Qiao et al., 2024). Other studies also confirm that the use of AI and big data analytics in organizations opens up opportunities for efficiency and more strategic decision-making, but simultaneously presents ethical, data security, and privacy challenges that require increasingly reflective and risk-aware leadership (Saeed et al., 2023; Deliu & Olariu, 2024).

This situation creates an urgent need for organizations, both public and private, to reimagine their risk management frameworks. Reactive strategies need to be replaced with proactive and predictive systems. This urgency is further heightened by the continued lack of prior research. Empirical evidence on how digital transformation shapes organizational resilience through learning and innovation mechanisms is still emerging (Awad & Martín-Rojas, 2024). Studies on Industry 4.0 security indicate that many digital security frameworks remain generic and high-level, thus inadequate to address dynamic threats such as data manipulation, system integration vulnerabilities, and cross-platform cyber risk escalation (Toussaint et al., 2024). Digital transformation requires organizations to have the ability to detect potential risks early and develop targeted strategic responses. This includes leveraging big data, machine learning, and predictive models to assess potential future risk scenarios. A systematic study of machine learning in risk management also shows that predictive approaches can improve the accuracy and time efficiency of risk identification, although their application cannot be standardized as they are highly dependent on data characteristics, organizational context, and the digital maturity level of each institution.

In Indonesia, according to 2025 Ministry of Finance data, digital transformation has become a national agenda, driven by the government through programs such as "Making Indonesia 4.0." Indonesia's digital economy is estimated to reach USD 130 billion by 2025 (Oktaviani et al., 2023). This growth is accompanied by the increasing complexity of digital risks in the industrial, education, healthcare, and public service sectors. In this context, the need for adaptive risk management becomes increasingly urgent, as digital transformation readiness involves not only technology investment but also process readiness, human resources, managerial capabilities, and organizational culture. Thus, the integration of risk management in digital transformation strategies is very relevant to study, especially so that the national digitalization agenda accelerates technology adoption, and is accompanied by strengthening organizational resilience as a whole (Michelotto & Joia, 2024).

Through a deeper understanding of the relationship between digital transformation and adaptive risk management, organizations can formulate more comprehensive and responsive strategies. This includes strengthening governance systems, updating information technology policies, and increasing digital literacy across the organization. These changes aim to reduce risk and create added value through systematic and measurable mitigation processes (Kagerman & Wahlster, 2013). Previous research has shown that AI-based technologies can strengthen organizations' ability to detect and respond to cyber threats, but their effectiveness remains heavily influenced by the quality of data governance, policy integration, and organizational readiness to build a security culture (Jada & Mayayise, 2024). Therefore, adaptive risk

management in the digital era, which relies on technological tools, must also be supported by mature organizational governance, competency, and awareness.

Based on this description, this study is important because it seeks to bridge the gap between previous research that has only partially addressed digital transformation, organizational readiness, digital leadership, and cybersecurity. This study aims to analyze the relationship between digital transformation and adaptive risk management approaches. The focus is on exploring how the dynamics of digitalization are changing the nature of organizational risk, expanding the risk spectrum from the operational level to the strategic and socio-technical levels, and identifying strategies that can be implemented to respond to these changes proactively, predictively, and cross-functionally. Therefore, this study can provide a conceptual contribution to the development of digital-based risk management strategies and can serve as an initial reference for both the public and private sectors in building organizational resilience in the industry 4.0 era. This article consists of several sections. The first section presents an introduction that includes the study context, literature review, research gaps, novelty, and research objectives. The second section explains the research method using a structured conceptual literature review. The third section presents the results of the literature synthesis and a discussion regarding the relationship between digital transformation, the expansion of the organizational risk spectrum, and adaptive risk management strategies. The final section presents conclusions, implications of the study, and directions for further research.

2. RESEARCH METHOD

This study uses a structured conceptual literature review as the primary approach to analyzing the relationship between digital transformation and adaptive risk management strategies. This literature-based approach was chosen because the topic under study is multidimensional, rapidly evolving, and spread across various scientific domains, such as management, information systems, organizational governance, and cybersecurity. Therefore, it requires conceptual synthesis to comprehensively map the development of ideas, argumentation patterns, and research gaps (Snyder, 2019). The concept of a structured literature review requires a clearer process of searching, assessing, synthesizing, and analyzing, thus ensuring stronger transparency and academic traceability in the study results (Snyder, 2019). In this study, the sources reviewed include academic books, scientific journal articles, industry reports, and policy documents relevant to digital transformation and organizational risk management. All sources are analyzed through the stages of identification, selection, relevance evaluation, and thematic synthesis to reveal how digitalization broadens the spectrum of organizational risks and how adaptive risk management strategies are formulated in various institutional contexts (Kitchenham & Charters, 2007). Thus, this approach was used to build a more comprehensive conceptual understanding of risk dynamics in the industry 4.0 era and a proactive, cross-functional, and data-driven organizational response framework (Snyder, 2019).

Data sources were collected from published documents published within the last five years that were relevant to the themes of digital transformation and risk management. The search was conducted in stages through source identification, initial screening, content suitability assessment, and final determination of the documents most relevant to the research focus (Page et al., 2021). Source selection was conducted purposively, considering the depth of discussion, the recency of the publication, the credibility of the source, and its relevance to the study's objectives (Mohamed Shaffril et al., 2020). To strengthen the traceability of the study process, search keywords were arranged thematically, including digital transformation, Industry 4.0, adaptive risk management, organizational resilience, digital governance, and cyber risk. This stage aimed to build a systematic conceptual synthesis of how digital transformation broadens the spectrum of organizational risks and how adaptive risk management strategies are formulated in various contexts. This work pattern aligns with structured literature review guidelines, which emphasize the importance of clear search procedures, transparent selection, and traceable source reporting to ensure a strong academic foundation for the synthesis (Carrera-Rivera et al., 2022).

The literature search was conducted through several online sources and scholarly publication databases, such as Google Scholar, ScienceDirect, SpringerLink, MDPI, as well as relevant policy documents and industry reports. Inclusion criteria included publications published within the last five years, directly related to digital transformation, Industry 4.0, adaptive risk management, organizational resilience, and cybersecurity, and available in full-text format. Documents irrelevant to the study's focus, duplicative, or lacking adequate conceptual description were excluded from the analysis. This step ensured that the source search process not only served as a source collection tool but also served as a basis for ensuring that the literature used fully supported the conceptual argumentation of this study.

The data analysis process was conducted qualitatively using an interpretive approach (Byrne, 2021). Each selected document was read in-depth and repeatedly to identify patterns of ideas related to digital transformation and organizational risk dynamics. The next stage involved initial coding of key concepts, such as business model change, cyber risk, data risk, organizational readiness, the role of digital leadership, and the use of analytical technology in risk management. These codes were then grouped into broader themes to more systematically understand the relationships between concepts. In this stage, the author used thematic

analysis to summarize the contents of the literature, interpret the interrelationships between ideas, and develop a more comprehensive conceptual explanation of risk dynamics in the era of digital transformation. This approach aligns with recent studies that emphasize that thematic analysis needs to be conducted reflectively, iteratively, and open to the development of themes throughout the review process (Naeem et al., 2023).

This research did not involve direct human participants as all data was sourced from secondary documents and publications. Therefore, formal informed consent and ethics approval were not required. Nevertheless, the research maintained academic integrity through the selection of credible sources, the use of appropriate citations, and the responsible presentation of the synthesis. To maintain scientific rigor, this research employed cross-source comparisons, rereading, and a review of the consistency of themes before developing the final conceptual framework. Content validity was established through triangulation between sources, depth of interpretation, consistency of categorization, and clarity of conceptual argumentation derived from various complementary documents. This step is important so that the resulting themes frequently appear in the sources studied, are truly meaningful in explaining the relationship between digital transformation, the expansion of organizational risks, and the need for more adaptive risk management strategies.

Ultimately, the study's findings are presented in a narrative-conceptual synthesis that positions digital transformation as the context for change, the risk spectrum as its consequence, and adaptive risk management strategies as a proactive, integrated, and data-driven organizational response. The limitations of this study lie in its literature-based nature, meaning the findings are a conceptual synthesis of available literature and have not been empirically tested in a specific organizational context. To minimize these limitations, the researcher employed purposive source selection, repeated reading, cross-source comparisons, and systematic thematic synthesis to ensure the study's findings maintain sufficient argumentative strength and academic relevance.

3. RESULTS AND DISCUSSION

This subsection presents the results of a literature synthesis and conceptual discussion regarding the relationship between digital transformation and adaptive risk management strategies in the industry 4.0 era. Based on the mapping of themes summarized in Table 1 and visualized in Figure 1, the study findings indicate that digital transformation not only reconfigures strategies, business processes, and organizational decision-making patterns, but also expands the risk spectrum from the operational level to socio-technical, strategic, and systemic risks. This synthesis also shows that the integration of technologies such as artificial intelligence (AI), the Internet of Things (IoT), big data analytics, cloud computing, and cyber-physical systems (CPS) increases efficiency and innovation, but at the same time increases the organization's dependence on data governance, internal readiness, digital leadership, and organizational learning capacity in building resilience to increasingly complex risks (Awad & Martín-Rojas, 2024 ;Jada & Mayayise, 2024; Michelotto & Joia, 2024 ; Plekhanov et al., 2023 ; Qiao et al., 2024 ; Toussaint et al., 2024).

3.1. Literature Synthesis Results

The main themes obtained from the literature synthesis, the focus of the findings, references, and their conceptual implications on the relationship between digital transformation and adaptive risk management strategies, are summarized in table 1 regarding the Summary of literature synthesis themes.

Table 1. Summary of Literature Synthesis Themes

Tema	Fokus temuan	Referensi utama	Implikasi
Digital transformation as a trigger for organizational strategy reconfiguration	Digital transformation replaces analog devices with digital ones, reconfiguring business processes, coordination, decision-making, organizational boundaries, and strategic logic through the integration of AI, big data, cloud computing, and IoT.	(Badghish et al., 2024); (Latupeirissa et al., 2024) (Awad & Martín-Rojas, 2024) (Qiao et al., 2024); (Plekhanov et al., 2023) (Michelotto & Joia, 2024)	Organizations need to view digital transformation as a multidimensional change that demands technological, managerial, human resource, and organizational cultural readiness.
Expanding	Digitalization expands risks from	(Alqudhaibi et	Risk management must move

the spectrum of organizational risk in the industry 4.0	the operational level to socio-technical, strategic, systemic, cyber, data, reputational, governance, and public trust risks.	al., 2025) (Toussaint et al., 2024) (Djatmiko et al., 2025) (Mutlutürk et al., 2024) (IBM, 2025) ; (Cecilia Ka Yuk Chan, 2023). (Julian et al., 2024) (Jada & Mayayise, 2024)	beyond a purely technical approach to encompass the interconnectedness of technology, governance, human resources, and organizational sustainability.
Adaptive risk management as a strategic response	The literature emphasizes a shift from reactive risk management to an adaptive approach that is predictive, data-driven, context-sensitive, and supported by continuous monitoring. Early warning systems, vulnerability assessment, predictive analytics, readiness evaluation, and continuous monitoring become central.	(Badghish et al., 2024); (Stefani et al., 2025) (Tian et al., 2024) (ISO/IEC 27001, 2022); (Alqudhaibi et al., 2025) (Awad & Martín-Rojas, 2024) (Michelotto & Joia, 2024)	Organizations need cross-functional, proactive, and continuously updated risk systems that combine governance, analytics, security standards, and organizational learning.
Digital leadership, governance, and organizational readiness as enabling factors	Digital transformation drives an expansion of the risk spectrum; this expansion demands adaptive risk management capabilities. Adaptive capabilities are operationalized through digital leadership, data governance, governance quality, digital literacy, human resource readiness, real-time monitoring, and organizational learning, all leading to organizational resilience.	(Alqudhaibi et al., 2025) (Awad & Martín-Rojas, 2024) (Michelotto & Joia, 2024) (Deliu & Olariu, 2024) (Qiao et al., 2024)	Organizational resilience in the industry 4.0 era is built through the integration of technology, leadership, learning, and mature risk governance. And should strengthen leadership capacity, technology governance, employee capability

Table 1, a summary of the themes in the literature above, demonstrates the consistent role of digital transformation in driving efficiency and innovation, broadening the spectrum of organizational risks. Therefore, the discussion in the following section is broken down into several key themes that explain how digitalization is transforming organizational strategies, expanding risks, and requiring a more adaptive risk management approach.

3.1.1. Digital Transformation as a Trigger for Organizational Strategy Reconfiguration

The literature synthesis shows that digital transformation cannot be understood simply as the replacement of analog devices with digital ones, but rather as an organizational reconfiguration process that impacts business processes, coordination patterns, decision-making mechanisms, and relationships between work units. Recent literature confirms that digital transformation drives organizations to integrate technologies such as artificial intelligence, big data analytics, cloud computing, and the Internet of Things into core operations, resulting in both technical and strategic changes (Badghish et al., 2024). In this context, digitalization provides a new foundation for efficiency, innovation, and the creation of more agile organizational models, but it also increases the organization's dependence on digital infrastructure and the quality of data governance.

Other literature findings indicate that the success of digital transformation is heavily influenced by an organization's capacity to learn, innovate, and lead purposeful change. (Latupeirissa et al., 2024) emphasize

that digitalization is not only about implementing technology but also requires adjustments in governance and institutional capacity. Similarly, Awad and Martín-Rojas demonstrated that digital transformation strengthens organizational resilience through organizational learning and innovation (Awad & Martín-Rojas, 2024), while Qiao emphasized that digital leadership acts as a catalyst mediating the influence of digital transformation on organizational performance and commitment (Qiao et al., 2024). Therefore, this synthesis positions digital transformation as a process that integrates technology, organizational capabilities, and leadership, resulting in systemic and cross-functional changes. The study also demonstrated that digital transformation changes organizations at the technological level, organizational boundaries, strategic logic, and patterns of relationships with the external ecosystem. Plekhanov emphasized that digital transformation challenges the way organizations formulate strategy and manage operations (Plekhanov et al., 2023), while Michelotto and Joia demonstrated that readiness for digital transformation is determined by technological resources, business processes, managerial capabilities, human capabilities, and organizational culture (Michelotto & Joia, 2024). Therefore, digital transformation needs to be understood as a multidimensional change that requires comprehensive internal readiness, not simply the adoption of digital tools.

3.1.2. Expanding the Spectrum of Organizational Risk in the Industry 4.0 Era

A literature synthesis shows that digital transformation broadens the spectrum of organizational risks, from primarily operational to increasingly socio-technical, strategic, and systemic. In the Industry 4.0 environment, the integration of IoT, automation, cyber-physical systems, and data platforms creates new points of vulnerability, particularly in the manufacturing, supply chain, and critical infrastructure sectors (Alqudhaibi et al., 2025). Industry 4.0 security literature also indicates that many existing cybersecurity frameworks are still generic and high-level, making them inadequate to address the risks of data manipulation, system interdependencies, and fast-moving attacks in a highly connected digital environment (Toussaint et al., 2024). Furthermore, studies on digital transformation and cybersecurity in the business sector confirm that technologies that increase efficiency also increase the likelihood of data breaches, cyberattacks, and operational continuity disruptions.

This risk expansion does not stop at the technical aspects. The literature also shows that digitalization poses reputational, social, and institutional risks, especially when organizations lack the cultural readiness, competencies, and governance to match the pace of technology adoption (Djatmiko et al., 2025). Studies on phishing and human factors confirm that cyber threats depend not only on system strength but also on user behavior, vigilance, and the capacity to recognize threats (Mutlutürk et al., 2024). This is crucial because digital attacks often succeed through human weaknesses, not solely hardware weaknesses. In other words, the spectrum of organizational risk in the digital age must be interpreted as a combination of technology risk, governance risk, human resource risk, and public trust risk. Empirical findings and official reports also reinforce the magnitude of these risk implications. (IBM, 2025) reports that the average global cost of a data breach in 2025 will reach USD 4.4 million, indicating that digital incidents are no longer minor annoyances but real financial and reputational threats. Globally, the World Economic Forum ranks cyber insecurity as one of the most prominent short-term global risks in the contemporary uncertain landscape. Therefore, this synthesis confirms that digitalization broadens an organization's risk spectrum not only in terms of the number of risks, but also in terms of the scale, speed, and interconnectedness of their impacts.

The broadening of the risk spectrum in the industry 4.0 era is increasingly evident as organizations integrate cyber-physical systems, AI, and big data analytics into their core operations (Cecilia Ka Yuk Chan, 2023). (Julian et al., 2024) demonstrate that CPS integrates various technological approaches to improve real-time process monitoring and control, but at the same time increases the complexity of the interconnections between software, hardware, networks, data, and organizational actors. Similarly, (Jada & Mayayise, 2024) assert that AI can enhance automation, threat intelligence, and cyber defense, but also raises challenges in the form of adversarial attacks and the need for high-quality data. These findings strengthen the argument that digital transformation broadens risk from the operational level to the strategic and socio-technical levels.

3.1.3. Adaptive Risk Management as a Strategic Response

Based on emerging themes, the literature consistently points to the need for adaptive risk management. This approach is characterized by an organization's ability to move from reactive control patterns to predictive, data-driven systems that are responsive to changing contexts. (Badghish et al., 2024) recommend a phased cybersecurity readiness framework for organizations undergoing digital transformation, while (Stefani et al., 2025) offer an information security risk framework that helps organizations more systematically identify and manage cyber risks arising from digital transformation technologies. Together, these studies demonstrate that effective risk response requires continuous monitoring, vulnerability evaluation, readiness assessment, and the integration of security policies into the transformation strategy. The literature also emphasizes the role of analytics technology in strengthening adaptive risk management. (Tian et al., 2024) systematic review shows that machine learning is increasingly being used to detect patterns, predict risk scenarios, and improve response speed in internet-based finance risk management. Although the context is in the financial sector, the underlying logic is relevant more broadly: organizations that leverage big data, predictive analytics, and anomaly detection will have an advantage in building early warning

systems. This means that risk mitigation strategies in the digital era cannot simply be based on past experiences but must be designed as a continuously updated learning and anticipation mechanism.

Beyond technology, the synthesis results show that adaptive risk management requires broader governance. ISO/IEC 27001, 2022, remains relevant because it provides requirements for an information security management system that emphasizes the establishment, implementation, maintenance, and continual improvement (ISO/IEC 27001, 2022). However, recent literature suggests that standards will be insufficient without cross-functional coordination, digital literacy, and investment in employee cyber awareness. In the manufacturing context, (Alqudhaibi et al., 2025) found a cybersecurity knowledge gap among workers, demonstrating that risk awareness needs to be built at the individual level, not just at the organizational policy level. The need for adaptive risk management becomes increasingly apparent as organizations must respond to risks that are fast-moving, interconnected, and inextricably linked to the digital transformation process itself. (Awad & Martín-Rojas, 2024) demonstrate that digital transformation can strengthen organizational resilience through organizational learning and innovation. Therefore, risk responses should not be limited to post-incident controls alone, but should also be built through continuous learning and renewal capacity. Furthermore, (Michelotto & Joia, 2024) emphasize that organizational digital transformation readiness is determined by technological readiness, processes, managerial capabilities, human resource capabilities, and organizational culture. This means that adaptive risk management strategies cannot be built solely through technology investment but must be supported by the organization's overall internal readiness.

3.1.4. Conceptual Framework: The Relationship Digital Transformation and Adaptive Risk Management

Based on the synthesis results, this article proposes the following conceptual relationship: digital transformation drives an expansion of an organization's risk spectrum; this expansion of the risk spectrum demands adaptive risk management capabilities; and adaptive capabilities are then operationalized through digital leadership, data and security governance, human resource readiness, real-time monitoring systems, and organizational learning. All of these mechanisms culminate in organizational resilience (Awad & Martín-Rojas, 2024). Within this framework, digital transformation is positioned not only as a driver of innovation but also as a generator of new vulnerabilities that must be managed in an integrated manner. Thus, the main findings of this study confirm the relationship between digitalization and risk, and the two are linked through cross-level and continuous organizational adaptation mechanisms. Substantively, this conceptual framework demonstrates that organizations must not simply adopt technology but also develop risk sense-making, predictive capacity, response procedures, and post-incident evaluation. This makes adaptive risk management an inherent part of digital transformation itself, rather than a supporting function that only comes into play after a risk emerges. Therefore, the results of this synthesis strengthen the argument that digital resilience arises from a combination of technology, leadership, learning, and sound risk governance. A visual summary of the results of the literature synthesis is presented in Figure 1.

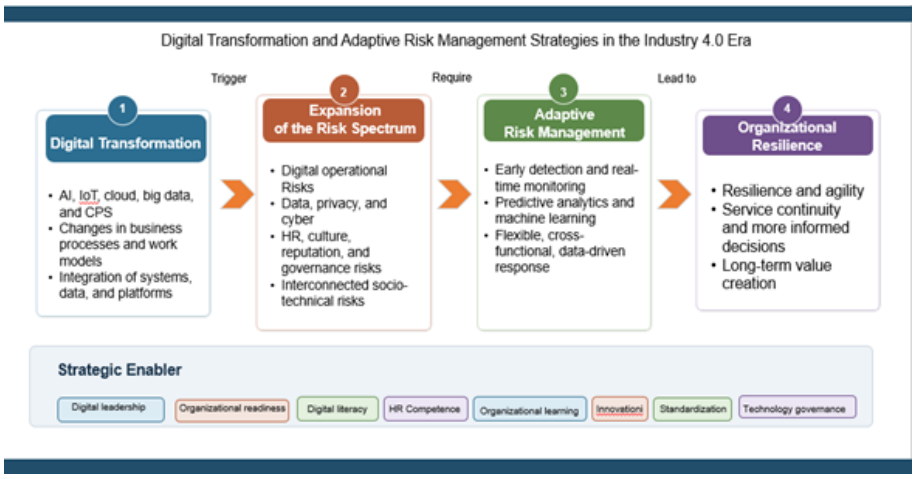

Figure 1. Conceptual Framework of the Research

3.2. Discussion

3.2.1. Theoretical Meaning: From Operational Risk to Socio-Technical and Systemic Risk

Theoretically, the above findings broaden the perspective on organizational risk management in the industry 4.0 era. Risk can no longer be limited to threats to day-to-day operations, but rather must be understood as a consequence of the interconnectedness of digital systems, data governance, human behavior, and environmental pressures that move simultaneously (Awad & Martín-Rojas, 2024). In this sense, digital transformation has shifted the focus of risk management from the protection of physical assets and static procedures to the management of complex, adaptive systems that are vulnerable to cross-functional spillover

effects. This position aligns with recent literature that emphasizes that organizational resilience in the digital era is underpinned by the ability to learn, innovate, and integrate security functions into the transformation strategy itself. The findings of this study also reinforce the view that digital transformation is not simply an efficiency agenda, but a process that shifts the nature of organizational risk. (Plekhanov et al., 2023) demonstrated that digital transformation pushes organizations into a more open and interdependent ecosystem, necessitating a rethinking of organizational strategies, operations, and boundaries. Linked to (Julian et al., 2024) this shift becomes even more crucial as the industry 4.0 environment brings together CPS, AI, and data within a single, complex architecture. This means that organizational risk in the digital era must be understood as increasingly systemic, cross-functional, and interconnected.

3.2.2. Managerial Implications: Leadership, Governance, and Risk Literacy

From a managerial perspective, this discussion leads to three main implications. First, digital leadership must be understood as the ability to drive innovation while managing risk. Second, organizations need to integrate technology governance, information security, and risk management into a single policy framework, ensuring that digital decision-making is not detached from risk control. Third, digital literacy and cybersecurity awareness must be developed as collective competencies. Findings in the manufacturing sector and phishing studies show that the largest gaps often arise at the human level, making investments in training, risk communication, and a security culture just as important as investments in technology.

From a managerial perspective, the findings of this study confirm that digital leadership cannot be separated from adaptive risk management. Researcher Qiao demonstrates that digital leadership plays a crucial role in driving digital transformation, enhancing performance, and strengthening organizational commitment (Qiao et al., 2024). These findings are relevant to organizations' need to instill risk awareness at all levels, as the success of digitalization is determined not only by technology but also by strategic direction, employee empowerment, and the organizational culture fostered by leaders.

At the same time, the use of AI and big data analytics presents opportunities for efficiency as well as new challenges. Researchers Deliu and Olariu demonstrate that AI and BDA are transforming roles, interactions, and professional competencies, raising new issues regarding the opportunities and challenges of digital technology use (Deliu & Olariu, 2024). Therefore, the managerial implication of this study is the need for a balance between accelerating digital innovation and strengthening risk governance, data ethics, and human resource competency readiness.

To clarify the practical context, an adaptive risk management strategy can be illustrated in organizations that rely on digital platforms for their core services. In digital service organizations, key risks include not only system disruptions but also customer data breaches, access configuration errors, application integration failures, delayed incident response, and a decline in user trust. In such situations, an adaptive strategy can be implemented through real-time risk monitoring dashboards, cross-functional team roles spanning IT, management, legal, HR, and communications, as well as incident response mechanisms that ensure every threat is detected, classified, addressed, and evaluated quickly. This illustration demonstrates that adaptive risk management must function as an integral part of the digital transformation process, rather than merely an administrative procedure executed after a risk has occurred. Operationally, organizations can implement adaptive risk management through several specific steps. First, organizations need to map digital risks, which include cybersecurity risks, data privacy and integrity risks, operational disruptions, reputational risks, governance risks, and risks stemming from human factors. Second, organizations need to compile a digital risk register that is updated periodically based on changes in technology, business processes, and threat patterns. Third, organizations need to form cross-functional teams so that the processes of risk identification, analysis, mitigation, and communication do not operate in silos. Fourth, organizations need to develop data-driven monitoring systems, including the use of predictive analytics and anomaly detection to identify risk signals earlier. Fifth, organizations need to have incident response protocols that include reporting workflows, risk level classification, technical handling, crisis communication, service recovery, and post-incident evaluation. Sixth, organizations need to strengthen risk literacy and a culture of digital security through ongoing training for leadership, employees, and system users.

3.2.3. Implications for the Public Sector and Education

This discussion is also relevant for the public sector and education, two sectors increasingly driven to digitalize but often facing more complex risks because they involve public services, sensitive data, and institutional legitimacy (Latupeirissa et al., 2024), The literature on the digitalization of public services indicates that digital transformation can improve efficiency, accountability, and citizen engagement, but at the same time, it can widen the digital divide if access, literacy, and service design are not inclusive. In the higher education sector, the integration of AI poses challenges related to privacy, data security, academic integrity, ethics, and resource constraints, so institutional leadership requires an implementation framework that balances innovation and risk mitigation. Therefore, adaptive risk management in the public and education sectors must be built across units, involving inclusive policies, infrastructure, human resources, and governance.

In a more concrete context, within the higher education sector, the application of adaptive risk management can be seen in the management of learning management systems, student academic data, digital attendance records, research archives, and the use of AI in the learning process. Educational organizations need to establish data access policies, digital literacy training, system security audits, data breach response protocols, and post-incident evaluation mechanisms. In the Industry 4.0-based manufacturing sector, adaptive strategies can be implemented through real-time monitoring of sensors and machinery, cybersecurity audits of cyber-physical systems, simulations of production disruption risks, training for workers on digital threats, and the development of operational recovery plans. Meanwhile, in digital-based public service organizations, adaptive risk management can be implemented through citizen data protection, integrated complaint channels, service quality monitoring, and crisis communication during system disruptions. These examples underscore that adaptive risk strategies must be tailored to the sector's characteristics, level of digital maturity, and the type of data managed by the organization.

3.2.4. Research Gap and Novelty of the Study

When compared with several relevant Indonesian studies, the novelty of this article becomes clearer. (Zaidan Ramadhan et al., 2025)focused their analysis on physical and operational OHS risks using HIRARC in unloading activities at the Port of Gresik. (Patricia et al., 2025) examined operational, financial, reputational, and legal risks in MSMEs using a business impact analysis approach. (Astuti et al., 2025) analyzed IT risks in the Sevima Edlink LMS application using ISO 31000, while (Afrioza et al., 2025 ; Selvy Afrioza et al., 2025 : Afrioza, Sunandar, et al., 2025) showed that most MSMEs have not implemented a comprehensive risk identification, analysis, evaluation, and management process, and that the digital sector tends to be more responsive to market risks than traditional MSMEs. These studies are important, but each focuses on a relatively specific scope, such as field risks, business unit impacts, market risks, and IT application risks. There has been no clear integration between the dynamics of digital transformation as a change in the organizational landscape and the need for updated risk management strategies that are cross-functional, predictive, participatory, and adaptive. This is where this article takes a different stance, positioning digital transformation as a driver of expanding the organizational risk spectrum and adaptive risk management as a strategic response that must be designed at the organizational level as a whole.

Therefore, the novelty of this study lies in the development of an integrative conceptual framework that connects four elements: digital transformation, expanding the risk spectrum, adaptive capabilities, and organizational resilience (Stefani et al., 2025). While the international literature has addressed cybersecurity, resilience, digital leadership, and data governance, these discussions are often conducted in separate strands (Awad & Martín-Rojas, 2024). This article brings these strands together into a single argument that can serve as a theoretical foundation for further empirical research in both the public and private sectors. This positioning not only fills a conceptual gap but also provides practical guidance for organizations seeking to build risk systems responsive to the acceleration of digitalization.

The novelty of this article can be further emphasized by pointing out that previous research tends to move along separate paths. (Plekhanov et al., 2023)emphasize digital transformation as a strategic organizational change, (Awad & Martín-Rojas, 2024) highlight the influence of digital transformation on resilience through learning and innovation, (Michelotto & Joia, 2024) focus on organizational readiness for transformation; (Qiao et al., 2024) emphasize the role of digital leadership, (Jada & Mayayise, 2024) examine the impact of AI on cybersecurity; and (Toussaint et al., 2024) highlight the limitations of generic cybersecurity frameworks. This article's distinction lies in its attempt to integrate all these paths into a single conceptual framework that positions digital transformation as a driver of expanding the spectrum of organizational risks and adaptive risk management as a cross-functional, predictive, and capability-based strategic response.

3.2.5. Limitations of the Analysis and Transition to Conclusions

This study has limitations that require careful consideration. First, the findings are conceptual in nature, as they are developed through a literature synthesis and therefore have not been empirically tested in specific organizational contexts. Second, the study's findings are highly dependent on the breadth, quality, and relevance of the available sources, so it's possible that contextual variations have not been fully addressed. Third, because the discussion integrates various sectors and approaches, the resulting practical implications need to be adapted to suit the characteristics of each organization.

Nevertheless, this synthesis makes an important contribution by clarifying that digital transformation simultaneously creates opportunities and expands the spectrum of organizational risks, thus requiring more proactive, adaptive, cross-functional, and capability-based risk management. Overall, these findings confirm that organizational resilience in the industry 4.0 era cannot be built solely through technology adoption, but also through digital leadership, mature governance, organizational readiness, and continuous learning. These findings form the basis for the conclusion, which summarizes the article's key contributions and highlights its implications for theory and practice.

4. CONCLUSION

This study aims to analyze the relationship between digital transformation and adaptive risk management strategies in the industry 4.0 era, specifically to explain how digitalization broadens the spectrum of organizational risks. Based on a literature review, it can be concluded that digital transformation not only drives organizational efficiency, innovation, and agility but also expands risks from the operational level to the strategic, socio-technical, and systemic levels. These risks include cybersecurity, data privacy and integrity, operational continuity disruptions, reputational risks, governance, as well as risks stemming from human factors and organizational readiness. These findings underscore that conventional, reactive risk management approaches are no longer sufficient, necessitating that organizations adopt adaptive, proactive, predictive, cross-functional, and data-driven risk management strategies.

The main contribution of this study lies in the development of an integrative conceptual framework that links digital transformation, the expansion of the organizational risk spectrum, adaptive risk management, and organizational resilience within a single analytical framework. The practical implication is that both public and private organizations need to embed risk management as an inherent part of their digital transformation strategies by strengthening data governance and security, digital leadership, organizational readiness, risk literacy, and continuous learning. However, since this research is conceptual and based on a literature synthesis, the findings have not yet been empirically tested within specific organizational contexts. Therefore, future research is recommended to test this framework across various sectors to gain a more contextual understanding of the factors influencing the effectiveness of adaptive risk management in the digital era.

Methodologically, the main limitation of this study lies in its conceptual nature, meaning that the resulting framework has not yet been tested using field data. Therefore, future research should empirically test this model in various organizational contexts using quantitative, qualitative, or mixed-methods approaches. Quantitative testing can be directed toward assessing the relationship between digital transformation, the expansion of the risk spectrum, adaptive risk management capabilities, and organizational resilience. Meanwhile, qualitative research can explore organizational experiences in building early-warning systems, data governance, incident response, risk literacy, and post-risk learning. Research in the public sector, higher education, manufacturing, digital SMEs, financial services, and platform-based organizations is essential to ensure this conceptual framework gains stronger validation and can generate more context-specific practical recommendations.

ACKNOWLEDGEMENTS

The author would like to express his gratitude to all parties who have provided support in the preparation of this article, both in the form of academic input, provision of references, and intellectual support during the manuscript development process. Appreciation is also expressed to the institutions and academic environment that have supported the strengthening of scientific discussions on digital transformation, adaptive risk management, and organizational resilience in the industry 4.0 era. Although not directly involved as authors, the contributions of various parties were very helpful in refining the ideas, structure of the analysis, and development of the conceptual framework in this article.

REFERENCES

Afrioza, S., Rasyiddin, A., & Rohmatul Azizah, A. (2025). Penerapan ISO 31000:2018 dalam Manajemen Risiko UMKM: Tinjauan Literatur dan Tantangan pada Sektor Tradisional dan Digital. JEDBUS (Journal of Economic and Digital Business), 2(2), 85–90. https://doi.org/10.37048/jedbus.v2i2.639

Afrioza, S., Sunandar, S., Lestari, W. D., & Permana, M. R. (2025). Strategi Adaptasi Digital Dalam Manajemen Risiko Pemasaran: Studi Kualitatif Pada UMKM Konveksi Pedesaan. Seminar Nasional Ekonomi Manajemen, Bisnis Dan Akuntansi, 231–240. https://proceeding.unived.ac.id/index.php/sn-emba/article/view/354

Alqudhaibi, A., Albarrak, M., Jagtap, S., Williams, N., & Salonitis, K. (2025). Securing industry 4.0: Assessing cybersecurity challenges and proposing strategies for manufacturing management. Cyber Security and Applications, 3, 100067. https://doi.org/10.1016/j.csa.2024.100067

Awad, J. A. R., & Martín-Rojas, R. (2024). Digital transformation influence on organisational resilience through organisational learning and innovation. Journal of Innovation and Entrepreneurship 2024 13:1, 13(1), 69-. https://doi.org/10.1186/s13731-024-00405-4

Badghish, S., Soomro, Y. A., Badghish, S., & Soomro, Y. A. (2024). Artificial Intelligence Adoption by SMEs to Achieve Sustainable Business Performance: Application of Technology–Organization–Environment Framework. Sustainability 2024, Vol. 16, 16(5). https://doi.org/10.3390/SU16051864

Bela Astuti, zidan, & Umar Faruq Vista. (2025). Analisis Manajemen Risiko Teknologi Informasi Pada Aplikasi LMS Sevima Edlink Menggunakan Framework ISO 31000 (Studi Kasus: Prodi Teknologi Informasi). JURNAL MANAJEMEN RISIKO, 6(1), 53–68. https://doi.org/10.33541/mr.v6i1.6926

Byrne, D. (2021). A worked example of Braun and Clarke's approach to reflexive thematic analysis. Quality & Quantity 2021 56:3, 56(3), 1391–1412. https://doi.org/10.1007/s11135-021-01182-y

Carrera-Rivera, A., Ochoa, W., Larrinaga, F., & Lasa, G. (2022). How-to conduct a systematic literature review: A quick guide for computer science research. MethodsX, 9, 101895. https://doi.org/10.1016/j.mex.2022.101895

Cecilia Ka Yuk Chan. (2023). A comprehensive AI policy education framework for university teaching and learning. International Journal of Educational Technology in Higher Education 2023 20:1, 20(1), 38-. https://doi.org/10.1186/s41239-023-00408-3

Damayanti, Martoatmodjo, G. W., Shelby, E., Mukaromah, S., Tubastuvi, N., Solovida, G. T., Sriharyati, S., Mohklas, Luhgiatno, El Zahraa, F., Nugraha, A. E. P., Puryandani, S., Siswanto, E., Santoso, A., & Sari, J. (2023). Manajemen Risiko (Era Transformasi Digital) Penerbit Cv. Eureka Media Aksara (1st ed.). CV. Eureka Media Aksara.

Deliu, D., & Olariu, A. (2024). The Role of Artificial Intelligence and Big Data Analytics in Shaping the Future of Professions in Industry 6.0: Perspectives from an Emerging Market. Electronics 2024, Vol. 13, Page 4983, 13(24), 4983. https://doi.org/10.3390/electronics13244983

Djatmiko, G. H., Sinaga, O., & Pawirosumarto, S. (2025). Digital Transformation and Social Inclusion in Public Services: A Qualitative Analysis of E-Government Adoption for Marginalized Communities in Sustainable Governance. Sustainability 2025, Vol. 17, Page 2908, 17(7), 2908. https://doi.org/10.3390/su17072908

Hatmoko, J. U. D. (2021). Resolusi Industri 4.0 (Perspektif Teknologi, Manajemen, dan Edukasi. CV. Andi Offset.

IBM. (2025). Cost of a data breach 2025 | IBM. https://www.ibm.com/reports/data-breach

ISO/IEC 27001. (2022). ISO/IEC 27001:2022(en),. Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en:ed-2:v1

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Data and Information Management, 8(2), 100063. https://doi.org/10.1016/j.dim.2023.100063

Julian, S., Jalowski, M., Lechner, M., Mirschberger, S., Merklein, M., Vogel-Heuser, B., & Möslein, K. M. (2024). Cyber-Physical Systems in the Context of Industry 4.0: A Review, Categorization and Outlook. Information Systems Frontiers, 26(5), 1731–1772. https://doi.org/10.1007/s10796-022-10252-x

Kagerman, H., & Wahlster, W. (2013). Industry 4.0: Sustainability and design principles (Issue April). Acatech - National Academy of Science and Engineering. https://doi.org/10.1109/REM.2019.8744120

Kitchenham, B., & Charters. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering (2.3). Keele University & University of Durham.

Latupeirissa, J. J. P., Dewi, N. L. Y., Prayana, I. K. R., Srikandi, M. B., Ramadiansyah, S. A., & Pramana, I. B. G. A. Y. (2024). Transforming Public Service Delivery: A Comprehensive Review of Digitization Initiatives. Sustainability (Switzerland) , 16(7), 2818. https://doi.org/10.3390/su16072818

Michell Patricia, Fahsya, F., & Hamijaya, P. D. N. (2025). Analisis Risiko Pada UMKM Hobby Donut & Bakery Menggunakan Metode Business Impact Analysis (BIA). JURNAL MANAJEMEN RISIKO, 6(1), 41–52. https://doi.org/10.33541/mr.v6i1.6966

Michelotto, F., & Joia, L. A. (2024). Organizational Digital Transformation Readiness: An Exploratory Investigation. Journal of Theoretical and Applied Electronic Commerce Research 2024, Vol. 19, Pages 3283-3304, 19(4), 3283–3304. https://doi.org/10.3390/jtaer19040159

Mohamed Shaffril, H. A., Samsuddin, S. F., & Abu Samah, A. (2020). The ABC of systematic literature review: the basic methodological guidance for beginners. Quality & Quantity 2020 55:4, 55(4), 1319–1346. https://doi.org/10.1007/s11135-020-01059-6

Mutlutürk, M., Wynn, M., & Metin, B. (2024). Phishing and the Human Factor: Insights from a Bibliometric Analysis. Information (Switzerland), 15(10), 643. https://doi.org/10.3390/info15100643

Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A Step-by-Step Process of Thematic Analysis to Develop a Conceptual Model in Qualitative Research. International Journal of Qualitative Methods, 22(oktober 2023). https://doi.org/10.1177/16094069231205789

Oktaviani, E., Asrinur, Prakoso, A. W. I., & Madiisriyatno, H. (2023). Transformasi Digital dan Strategi Manajemen. Oikos-Nomos: Jurnal Kajian Ekonomi Dan Bisnis, 16(1), 16–26. https://doi.org/10.37479/jkeb.v16i1.20322

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. https://doi.org/10.1136/bmj.n71

Plekhanov, D., Franke, H., & Netland, T. H. (2023). Digital transformation: A review and research agenda. European Management Journal, 41(6), 821–844. https://doi.org/10.1016/j.emj.2022.09.007

Pranata, & Ismail. (2022). Penerapan manajemen risiko teknologi informasi di era industri 4.0 pada UMKM di Indonesia. Jurnal Informatika Dan Komputer, 7(2), 120–128.

Qiao, G., Li, Y., & Hong, A. (2024). The Strategic Role of Digital Transformation: Leveraging Digital Leadership to Enhance Employee Performance and Organizational Commitment in the Digital Era. Systems 2024, Vol. 12, Page 457, 12(11), 457. https://doi.org/10.3390/SYSTEMS12110457

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors 2023, Vol. 23, Page 6666, 23(15), 6666. https://doi.org/10.3390/s23156666

Selvy Afrioza, Hidayat, R., & Nurlaela, E. (2025). Strategi Pemasaran Digital dan Pengambilan Keputusan Bisnis: Perspektif Gen Z di Paya Jaras Selangor. Komatika: Jurnal Pengabdian Kepada Masyarakat, 5(2), 108–117. https://doi.org/10.34148/KOMATIKA.V5I2.1238

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104(1), 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Stefani, E., Costa, I., Gaspar, M. A., Goes, R. de S., Monteiro, R. C., Petrili, B. R., & Pereira, A. de P. (2025). Information Security Risk Framework for Digital Transformation Technologies. Systems 2025, Vol. 13, Page 37, 13(1), 37. https://doi.org/10.3390/systems13010037

Teichert, R. (2019). Digital Transformation Maturity: A Systematic Review of Literature. Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis, 67(6), 1673–1687. https://doi.org/10.11118/actaun201967061673

Tian, X., Tian, Z. Y., Khatib, S. F. A., & Wang, Y. (2024). Machine learning in internet financial risk management: A systematic literature review. PLOS ONE, 19(4), e0300195. https://doi.org/10.1371/journal.pone.0300195

Toussaint, M., B, S. K., & Herv´e Panetto a. (2024). Industry 4.0 data security: A cybersecurity frameworks review. Journal of Industrial Information Integration, 39(22 Maret), 100604. https://doi.org/10.1016/j.jii.2021.100312

Zaidan Ramadhan, M., Sianturi, I., Ratnaningsih, D., & Rakhman, R. A. (2025). Analisis Pengendalian Risiko Kesehatan dan Keselamatan Kerja (K3) Pada Aktivitas Bongkar di Dermaga Pelabuhan Gresik Menggunakan Metode HIRARC. Innovative: Journal Of Social Science Research, 5(3), 6140–6153. https://doi.org/10.31004/innovative.v5i3.19554