Applied Information System and Management (AISM)
Volume 8, (1) 2025, p. 1–10
P-ISSN: 2621-2536; E-ISSN: 2621-2544; DOI: 10.15408/aism.v8i1.41090

Critical Success Factors for IT Risk Management in the Digital Transformation Era: Insights from a Multiple Case Study

Dwi Yuniarto[1*], Aedah Binti Abd. Rahman[2]

***Abstract*—The convergence of Information Technology risk management and digital transformation is a vital consideration for contemporary organizations navigating the rapidly changing digital landscape. This research investigates the intersection of these domains, aiming to identify the critical success factors that enable effective Information Technology risk management within the context of digital transformation. Through a Systematic Literature Review, a comprehensive search on Web of Science and Scopus led to the acceptance of 61 peer-reviewed papers published between 2020 and 2024, providing a solid foundation for understanding current trends and best practices. Employing a qualitative multiple case study approach, this study examines the experiences, strategies, and challenges of organizations that have successfully managed Information Technology risks during their digital transformation journeys. Thematic analysis reveals three key critical success factors: executive leadership and support, cross-functional collaboration, and risk-aware decision-making. These findings offer actionable insights for organizations seeking to align their risk management practices with the complexities of digital transformation. By bridging theoretical frameworks with practical insights, this research provides valuable recommendations for organizations to navigate digital transformation securely. Future research could focus on exploring the implementation nuances of these success factors across various industries, such as healthcare, finance, and manufacturing, to deepen our understanding of the intricate relationship between IT risk management and digital transformation in diverse contexts.**

***Index Terms*—Information technology risk management, digital transformation, critical success factors, multiple case study.**

I. INTRODUCTION

In the contemporary landscape of business operations, the integration of Information Technology (IT) has become an undeniable driving force for organizational growth and innovation [1-3]. As enterprises embark on their digital transformation journeys to capitalize on the opportunities presented by technological advancements, they are equally exposed to a myriad of IT-related risks [4-6]. These risks encompass data breaches, cyberattacks, operational disruptions, and regulatory non-compliance, which can potentially lead to substantial financial losses, reputational damage, and compromised customer trust [7, 8]. As a result, the effective management of IT risks has risen to the forefront of strategic priorities for modern organizations. Extensive research has been conducted in the realm of IT risk management, delving into methodologies, frameworks, and best practices. Scholars have explored various facets, from identifying vulnerabilities in IT infrastructure to assessing the potential impact of security breaches. Existing studies have underscored the dynamic and ever-evolving nature of IT risks, necessitating agile strategies that adapt to emerging threats. Moreover, the literature emphasizes the need to align IT risk management with broader organizational goals, ensuring that risk management becomes an enabler rather than an impediment to digital transformation initiatives.

However, despite the wealth of research available, challenges persist in effectively implementing IT risk management strategies within the context of digital transformation. Organizations often grapple with selecting appropriate risk assessment frameworks, integrating risk management into their agile development processes, and securing executive buy-in for resource allocation [9, 10]. The complexity of modern IT environments, characterized by cloud computing, Internet of Things (IoT) devices, and interconnected ecosystems, further amplifies the intricacies of risk identification and mitigation. Consequently, a gap exists between the theoretical concepts proposed in academic literature and their practical application in real-world scenarios. The primary objective of this study is to bridge the gap between

Received: 27 August 2024; Revised: 04 October 2024; Accepted: 23 October 2024.
*Corresponding author
[1]Dwi Yuniarto, University of Sebelas April Indonesia (e-mail: dwiyuniarto@unsap.ac.id).
[2]Aedah Binti Abd. Rahman, Asia E University Malaysia (e-mail: aedah.abdrahman@aeu.edu.my).

theory and practice in IT risk management during the digital transformation era. This research aims to offer a comprehensive understanding of the critical success factors that lead to effective IT risk management in the context of rapid technological changes. By conducting an in-depth analysis of multiple case studies, we intend to extract valuable insights into the strategies, challenges, and best practices adopted by organizations in managing IT risks during digital transformation. Based on these insights, we will develop a set of practical guidelines and recommendations that organizations can utilize to enhance their IT risk management capabilities and align them with their digital transformation objectives.

The motivation behind this study arises from the pressing need to tackle the practical challenges organizations face as they navigate the complexities of digital transformation and IT risk management. The convergence of these two areas is essential, as it ensures that organizations can advance their digital capabilities while maintaining robust security measures. This research aims to provide a practical framework, informed by real-world case studies, that helps both researchers and practitioners address IT risks in today's rapidly evolving digital landscape. By integrating risk management with digital innovation, organizations can not only strengthen their cybersecurity but also leverage new opportunities with confidence. The insights from this study are intended to empower organizations to innovate safely, enhancing their ability to thrive in an increasingly digital world while minimizing the risks associated with transformation.

This research aims to introduce a novel approach to IT risk management in the digital transformation era by combining the insights from multiple case studies with the rigor of established theoretical frameworks. While existing literature has extensively discussed both IT risk management and digital transformation as separate domains, our study seeks to merge these two critical aspects into a cohesive strategy. The novelty of this research lies in its integration of practical insights derived from real-world case studies with theoretical foundations, offering a holistic perspective that directly addresses the challenges faced by organizations in the rapidly evolving digital landscape.

Furthermore, the unique contribution of this study lies in its focus on critical success factors that facilitate effective IT risk management within the context of digital transformation. By identifying and analyzing these key factors across diverse industries and organizational settings, we provide a nuanced understanding of how organizations can navigate the complexities of risk while embracing the opportunities presented by digital transformation. This research moves beyond the traditional boundaries of theoretical discourse and instead presents actionable insights that organizations can implement to optimize their IT risk management strategies.

In addition, the combination of qualitative analysis from multiple case studies and the development of practical guidelines contributes to a comprehensive approach that can be readily applied by organizations seeking to enhance their IT risk management capabilities. By aligning theoretical principles with real-world challenges, this research offers a fresh perspective on how organizations can proactively manage IT risks, protect their digital assets, and ensure a smooth and secure transition throughout the process of digital transformation. In conclusion, the novelty of this research arises from its integration of case-based insights, theoretical frameworks, and practical guidelines into a unified approach for effective IT risk management during the digital transformation era. This unique amalgamation addresses the gap between theory and practice, enabling organizations to overcome challenges, capitalize on opportunities, and navigate the complexities of the digital landscape with confidence.

II. Related Work

The domain of IT risk management encompasses the identification, assessment, and mitigation of risks associated with the use, deployment, and management of information technology within organizations [11-13]. Research has underscored the importance of effective risk management strategies in safeguarding sensitive data, ensuring operational continuity, and maintaining organizational resilience. Various frameworks and methodologies, such as the ISO 27001 standard and the NIST Cybersecurity Framework, have been developed to guide organizations in implementing structured approaches to IT risk management [14-16]. Existing studies have examined the components of risk management, including risk assessment methodologies, risk communication, and the role of governance in aligning risk management with business objectives.

The domain of information technology (IT) risk management is paramount in contemporary organizations, as it encompasses the systematic identification, assessment, and mitigation of risks associated with the use, deployment, and management of information technology systems. IT risks manifest in various forms, including but not limited to cybersecurity threats, data breaches, software vulnerabilities, technology failures, and regulatory non-compliance. As the reliance on digital systems grows, organizations face heightened vulnerabilities that could lead to financial losses, reputational damage, and legal liabilities.

Research within this domain has yielded a rich array of methodologies, frameworks, and best practices to aid organizations in effectively managing IT risks. One prominent framework is the ISO 27001 standard, which provides guidelines for establishing an information security management system (ISMS) to ensure the confidentiality, integrity, and availability of information assets [17]. Additionally, the NIST Cybersecurity Framework offers a comprehensive approach to managing and reducing cybersecurity risks across critical infrastructure sectors.

The literature highlights the multidimensional nature of IT risk management, which encompasses several critical components: risk assessment methodologies, risk identification, risk communication, risk treatment strategies, and continuous risk monitoring. Table 1 presents a detailed overview of these components. Research has explored both quantitative and

Applied Information System and Management (AISM)
Volume 8, (1) 2025, p. 1–10
P-ISSN: 2621-2536; E-ISSN: 2621-2544; DOI: 10.15408/aism.v8i1.41090

qualitative approaches to risk assessment, including the use of risk matrices, probabilistic models, and threat modeling techniques. Additionally, scholars emphasize the significance of cultivating a risk-aware organizational culture, ensuring that risk management is integrated into decision-making processes across all levels of the organization.

Table 1.
Information Technology Risk Management

Components of IT Risk Management	Frameworks and Methodologies	Best Practices
Risk Identification	- ISO 27005: Risk Management Standard [18]	- Regular risk assessments to identify emerging threats
	- NIST SP 800-30: Risk Assessment Guide [14, 19]	- Collaboration between IT and business stakeholders
	- FAIR (Factor Analysis of Information Risk) [20, 21]	- Utilizing threat intelligence to inform risk assessment
Risk Assessment	- COSO ERM Framework [22]	- Quantitative and qualitative risk assessment
	- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [23]	- Identifying critical assets and their vulnerabilities
	- IRAM (Information Risk Assessment Methodology) [24]	- Evaluating potential impacts and likelihood of risks
Risk Communication	- ISO 31000: Risk Management Guidelines [25]	- Clear communication of risks to decision-makers
	- RIMS Risk Maturity Model [26]	- Tailoring risk communication to different stakeholders
	- ISACA's Risk IT Framework [10]	- Addressing risks in business terms
Risk Treatment Strategies	- NIST Cybersecurity Framework [19]	- Implementing technical controls to mitigate risks
	- COBIT (Control Objectives for Information and Related Technologies) [27]	- Developing incident response plans
	- CIS Controls (Center for Internet Security) [21]	- Regularly reviewing and updating risk treatment plans
Ongoing Risk Monitoring	- ISO 27001: Information Security Management System [28]	- Continuous monitoring of IT systems and assets
	- ISF IRAM (Information Risk Analysis Methodology) [24]	- Incorporating feedback and insights from incidents
	- SANS Critical Security Controls [24]	- Periodic reassessment of risk profiles

Moreover, the role of governance in IT risk management has gained attention. Effective risk governance involves clear delineation of roles and responsibilities, establishment of risk appetite, and integration of risk management into strategic planning. Research emphasizes that risk governance should involve collaboration between IT teams, legal departments, compliance officers, and executive leadership to ensure a holistic approach to risk mitigation.

IT risk management serves as a critical safeguard against the rapidly evolving landscape of digital threats. The literature reveals a comprehensive array of tools, frameworks, and strategies that organizations can employ to mitigate vulnerabilities and maintain their operational integrity in the face of ever-changing technological risks.

The concept of digital transformation has emerged as a pivotal force reshaping the landscape of modern business operations. It entails the integration of digital technologies across various facets of an organization, encompassing processes, customer interactions, products, and services. Digital transformation is not merely a technological shift but a holistic organizational endeavor that brings about profound changes in culture, strategy, and business models.

The literature underscores the multifaceted drivers behind the adoption of digital transformation. Customer expectations, driven by digital experiences in everyday life, have led organizations to reimagine how they engage and serve their clientele. Additionally, the dynamic nature of the market, characterized by rapid technological advancements and disruptions, compels organizations to remain agile and adaptive to stay competitive. The evolving competitive landscape demands innovation and the exploration of new revenue streams, prompting organizations to explore digital avenues to create value [29].

Scholars have highlighted numerous benefits that organizations can reap from effective digital transformation. Enhanced customer experiences, enabled by personalized interactions and streamlined processes, lead to increased customer satisfaction and loyalty [30]. Improved operational efficiency and resource optimization are also commonly observed outcomes, driven by the automation of manual processes and data-driven decision-making. Moreover, digital transformation can foster a culture of innovation and collaboration, enabling organizations to respond swiftly to market changes and opportunities.

However, the literature acknowledges that digital transformation introduces its own set of challenges and complexities. As organizations adopt emerging technologies, they are faced with the intricacies of managing cybersecurity and data privacy risks. The increased interconnectedness of digital systems amplifies the potential impact of cyberattacks and data breaches. Furthermore, the proliferation of data-driven insights necessitates ethical and regulatory considerations regarding data collection, storage, and usage. As organizations strive to harness the power of digital technologies, there is also a growing need for workforce upskilling and talent acquisition to bridge the digital skills gap.

Digital transformation signifies a fundamental shift in how organizations operate and engage with stakeholders. The literature stresses the need for organizations to strategically embrace digital transformation, recognizing its impact across cultural, operational, and strategic dimensions. Table 2 outlines these dimensions in detail. While digital transformation offers

significant advantages, it also demands that organizations address challenges related to cybersecurity, data privacy, ethics, and talent management [31].

Table 2.
Digital Transformation and its Implications [32]

Implications of Digital Transformation	Benefits	Challenges
Customer Experience Enhancement	- Personalized interactions - Streamlined processes - Improved service delivery	- Balancing personalization with data privacy - Ensuring consistent customer experiences
Operational Efficiency	- Automation of manual tasks - Data-driven decision-making - Resource optimization	- Integration complexities - Transitioning legacy systems
Innovation and Agility	- Rapid response to market changes - Flexibility in adapting to disruptions - Accelerated product and service development	- Navigating regulatory compliance - Ethical considerations in data usage
Data-Driven Insights	- Informed decision-making - Predictive analytics - Targeted marketing campaigns	- Data privacy concerns - Data security and cyber threats
Workforce Transformation	- Digital skills development - Remote and flexible work arrangements - Collaborative work environments	- Digital skills gap - Talent acquisition for digital roles

As organizations embrace digital transformation, they are exposed to a new spectrum of risks that demand innovative risk management strategies. Scholars have recognized the need for a paradigm shift in IT risk management to address the dynamic nature of digital transformation. Existing research has explored the integration of risk management practices into the early stages of digital initiatives, emphasizing the importance of risk-aware decision-making. Moreover, the literature has discussed the alignment of risk management with broader organizational objectives, underscoring the role of risk management as an enabler rather than a hindrance to digital transformation efforts.

As organizations embrace the multifaceted challenges and opportunities presented by digital transformation, a compelling need emerges to intertwine the domains of information technology (IT) risk management and the journey of digital metamorphosis. The convergence of these domains signifies a paradigm shift in how organizations strategize, innovate, and manage risks in an interconnected and digitized landscape [33].

1) *Integration of Risk Management into Digital Initiatives.*
Research within this domain accentuates the importance of embedding risk management practices into the early stages of digital initiatives. Organizations are encouraged to adopt a proactive approach by conducting risk assessments before launching digital transformation projects. By aligning risk identification with digital objectives, organizations can anticipate potential vulnerabilities, strategize mitigation plans, and ensure that risk considerations are integrated into the design and implementation phases. This integration promotes risk-aware decision-making and minimizes the likelihood of costly retroactive risk management efforts.
2) *Risk Management as an Enabler of Transformation.*
A pivotal shift in perspective emerges as organizations recognize that effective IT risk management can catalyze digital transformation endeavors. Traditionally perceived as a hindrance, risk management now assumes the role of an enabler. By addressing risks early in the transformation process, organizations can confidently innovate, experiment, and adapt to new technologies. This symbiotic relationship between risk management and transformation underscores the strategic significance of aligning risk management practices with broader business objectives.
3) *Alignment of Governance and Risk Management.*
The literature emphasizes the need for alignment between governance, risk management, and digital transformation strategies. Effective risk governance is marked by clear roles, responsibilities, and communication channels that span across IT teams, legal departments, compliance units, and executive leadership. By integrating risk governance mechanisms into digital transformation strategies, organizations can ensure that risk management remains a fundamental consideration in decision-making processes. This alignment fosters a comprehensive understanding of potential risks and paves the way for effective risk response strategies.
4) *Practical Implementation Challenges.*
While the theoretical framework of converging IT risk management and digital transformation is compelling, practical implementation poses challenges. Organizations often grapple with the complexity of risk assessment in dynamic digital environments, where emerging technologies introduce new vulnerabilities. Striking a balance between enabling innovation and ensuring security can be intricate, requiring collaborative efforts from diverse stakeholders. Furthermore, the pace of technological change can outpace traditional risk assessment methodologies, necessitating agile approaches to risk identification and mitigation.

The convergence of IT risk management and digital transformation marks a paradigm shift in organizational strategies. As outlined in Table 3, by integrating risk management into digital initiatives, viewing it as a key enabler of transformation, and aligning governance with risk management practices, organizations can navigate the digital landscape with greater resilience and confidence. However, challenges remain in implementing this convergence effectively, requiring adaptive methodologies that can keep pace with the rapid evolution of digital change and its associated risks.

While the literature presents valuable insights into IT risk management and digital transformation, there is a noticeable gap in the integration of practical insights from case studies into theoretical frameworks. Many existing studies tend to focus on either theoretical discussions or individual case studies, often

Applied Information System and Management (AISM)
Volume 8, (1) 2025, p. 1–10
P-ISSN: 2621-2536; E-ISSN: 2621-2544; DOI: 10.15408/aism.v8i1.41090

lacking a cohesive synthesis that combines both perspectives. This research seeks to bridge this gap by conducting a multiple case study analysis that integrates practical experiences with theoretical concepts, offering a holistic approach to IT risk management in the digital transformation era.

Table 3.
Convergence of IT Risk Management and Digital Transformation [34]

Aspects of Convergence	Key Points
Integration of Risk Management into Digital Initiatives	- Embedding risk assessments in early stages of digital projects - Addressing risks early allows confident experimentation - Promoting collaboration between risk management and innovation teams
Risk Management as an Enabler of Transformation	- Viewing risk management as a facilitator of innovation - Addressing risks early allows confident experimentation - Promoting collaboration between risk management and innovation teams
Alignment of Governance and Risk Management	- Clear roles and responsibilities across IT, legal, and compliance units - Integration of risk considerations into digital transformation strategies - Ensuring risk governance mechanisms are communicated and adhered to
Practical Implementation Challenges	- Dynamic digital environments introduce complexity to risk assessment - Balancing innovation with security requires collaborative efforts - Rapid technological change may outpace traditional risk assessment methodologies

While the existing body of literature offers valuable insights into the domains of information technology (IT) risk management and digital transformation, several challenges and gaps emerge that warrant attention for a comprehensive understanding of their convergence [35].

1) *Integration of Practical Insights.*
   One notable challenge lies in the integration of practical insights from real-world case studies into theoretical frameworks. Many studies tend to focus on theoretical discussions or individual case studies, often neglecting to bridge the gap between theory and practice. The lack of synthesis between these perspectives hinders the creation of comprehensive strategies that can be directly applied by organizations seeking to manage IT risks during digital transformation.
2) *Dynamic Nature of Digital Risks.*
   The rapidly evolving landscape of digital threats presents a significant challenge. The literature acknowledges that traditional risk assessment methodologies may struggle to keep pace with emerging risks posed by technologies such as artificial intelligence, blockchain, and the Internet of Things. This dynamic nature of digital risks requires adaptive risk assessment approaches that account for the continuously changing threat landscape.
3) *Ethical and Regulatory Considerations.*
   As organizations harness the power of digital technologies, they are confronted with ethical considerations and regulatory complexities related to data privacy, security, and usage. The literature highlights the importance of navigating these considerations, yet there remains a gap in providing actionable guidance on how organizations can strike a balance between innovation and compliance.
4) *Digital Skills Gap.*
   While digital transformation offers the promise of enhanced efficiency and innovation, it also exposes a shortage of skilled professionals capable of managing digital risks. The literature acknowledges the digital skills gap and the need for workforce upskilling, but there is room for further exploration of effective strategies for developing a workforce capable of understanding, mitigating, and managing digital risks.
5) *Evolving Cyber Threat Landscape.*
   The rapid evolution of cyber threats and attack vectors poses an ongoing challenge. The literature often describes historical cyber threats and risk management strategies, but staying ahead of the evolving threat landscape requires continuous updates and adaptation. Organizations need strategies that can swiftly respond to new and sophisticated cyberattacks.

The challenges and gaps in the literature regarding the convergence of IT risk management and digital transformation highlight the need for a holistic approach that integrates theoretical frameworks with practical insights. As shown in Table 4, addressing the dynamic nature of digital risks, ethical considerations, skill shortages, and the ever-evolving cyber threat landscape is crucial for developing effective strategies that enable organizations to navigate the complexities of the digital era successfully.

Table 4.
Challenges and Gaps in the Literature

Challenges and Gaps	Description
Integration of Practical Insights	- Lack of synthesis between theoretical frameworks and practical case studies - Difficulty in translating theoretical concepts into actionable strategies
Dynamic Nature of Digital Risks	- Traditional risk assessment methodologies may struggle to adapt to emerging digital threats - Need for agile risk assessment approaches that account for evolving threat landscape
Ethical and Regulatory Considerations	- Organizations grapple with balancing innovation and compliance with ethical and regulatory requirements - Gap in actionable guidance for navigating ethical and regulatory complexities
Digital Skills Gap	- Shortage of skilled professionals capable of managing digital risks - Need for strategies to bridge the digital skills gap and upskill the workforce
Evolving Cyber Threat Landscape	- Rapid evolution of cyber threats and attack vectors - Existing literature may describe historical threats but requires ongoing updates and adaptation

III. Research Method

This study adopts a qualitative research approach with a multiple case study design. Qualitative research is chosen due to its suitability for capturing rich and contextual insights into complex phenomena [36]. The multiple case study design provides an in-depth exploration of critical success factors by analyzing experiences, strategies, and challenges across diverse organizations undergoing digital transformation. As illustrated in Fig. 1, this research method enables a comprehensive understanding of the key elements that influence successful digital transformation efforts.

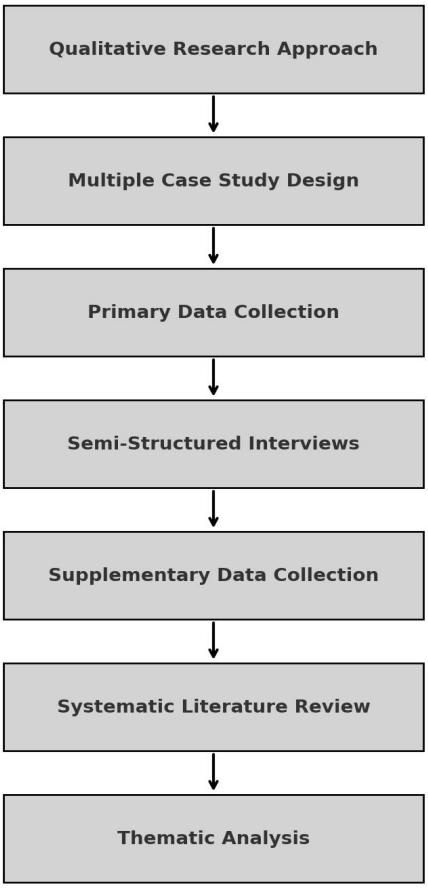

Fig. 1. Research method.

The primary data collection method involves semi-structured interviews with key stakeholders from selected organizations. Participants include IT experts, risk managers, executives, and other relevant personnel. Semi-structured interviews provide flexibility to explore diverse perspectives, while a predetermined set of questions ensures consistency across cases. The interviews delve into the organizations' IT risk management strategies, approaches to digital transformation, and the perceived impact of convergence between the two domains.

Supplementary data is collected through the analysis of relevant organizational documents, such as risk management policies, digital transformation strategies, and incident response plans. Document analysis serves to triangulate findings from interviews and provide a comprehensive view of each organization's risk management practices. Through a Systematic Literature Review (SLR) following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, a comprehensive search on Web of Science (WOS) and Scopus resulted in the acceptance of 61 peer-reviewed papers published between 2020 and 2024. These papers were selected based on their relevance to IT risk management and digital transformation, ensuring the inclusion of high-quality, up-to-date research. The PRISMA framework facilitated a systematic approach to identifying, screening, and selecting studies, enhancing the methodological rigor of the review. In addition to the literature review, the data collected from interviews and documents undergo a thematic analysis, systematically identifying patterns, themes, and insights within the qualitative data. Thematic analysis is conducted in several stages, including data familiarization, coding, theme identification, and interpretation. Each stage builds on the previous one, allowing for a thorough examination of the data. This method facilitates the identification of critical success factors, challenges, and best practices in IT risk management within the context of digital transformation. By combining insights from peer-reviewed literature with thematic analysis of qualitative data, this study ensures a comprehensive and methodologically sound exploration of the subject. A total of 34 participants were involved in the study, all of whom received detailed information regarding the study's purpose, procedures, and potential risks before providing their informed consent to participate in the interviews. Among these participants, 11 expressed reservations about participating and ultimately chose not to engage in the study. Those who did participate were assured of their right to withdraw at any time without facing any consequences, emphasizing the ethical commitment to respecting their autonomy. To maintain confidentiality, the identities and organizational affiliations of all participants are kept anonymous in the reporting of the findings. Additionally, all collected data is securely stored and accessible only to the research team, ensuring the protection of sensitive information throughout the research process.

This study adheres to ethical guidelines, ensuring that research practices are transparent, respectful, and aligned with ethical norms.

IV. Result

Thematic analysis of the collected data yielded several key themes and critical success factors that are pivotal in effectively managing IT risks within the context of digital transformation. These critical success factors are not only essential for navigating the challenges presented by the convergence of IT risk management and digital transformation but also serve as guideposts for organizations seeking to achieve successful outcomes in their digital initiatives. Thematic analysis revealed several key themes and critical success factors that contribute to effective IT risk management during digital transformation. These critical success factors are as follows:

Applied Information System and Management (AISM)
Volume 8, (1) 2025, p. 1–10
P-ISSN: 2621-2536; E-ISSN: 2621-2544; DOI: 10.15408/aism.v8i1.41090

1) *Executive Leadership and Support.*
A common thread across the cases is the significance of executive leadership in championing IT risk management initiatives. Organizations that demonstrated strong commitment from top leadership were better equipped to allocate resources, establish risk-aware cultures, and integrate risk management into digital transformation strategies.
A prominent and recurring theme across all the cases was the critical role of executive leadership and support in driving effective IT risk management during digital transformation. Organizations that demonstrated robust commitment and engagement from top-level executives showcased a more comprehensive and integrated approach to risk management. Strong executive sponsorship was found to have several significant implications:
- Resource Allocation: Organizations with committed executive leadership allocated adequate resources to IT risk management initiatives, ensuring the availability of financial, human, and technological resources to support risk mitigation efforts.
- Risk-Aware Culture: Executive support fostered a culture of risk awareness that permeated throughout the organization. When leaders visibly prioritize risk management, it signals the importance of vigilance against potential risks to the entire workforce.
- Alignment with Strategy: Effective risk management requires alignment with strategic goals. Organizations with engaged executives seamlessly integrated risk management with their digital transformation strategies, leading to more cohesive and effective initiatives.

In practice, executive leadership can apply this by setting clear risk management priorities, supporting ongoing risk assessments, and ensuring that risk considerations are embedded into all strategic initiatives.

2) *Cross-Functional Collaboration.*
Collaboration between IT teams, risk management departments, and other business units emerged as a crucial factor. Successful organizations emphasized the importance of breaking down silos and fostering cross-functional communication to ensure a holistic understanding of risks and alignment with transformation goals.
Another recurring theme centered on the imperative of cross-functional collaboration in the successful convergence of IT risk management and digital transformation. Collaboration emerged as a pivotal factor in bridging gaps between IT teams, risk management departments, and other business units. The benefits of cross-functional collaboration included:
- Comprehensive Understanding of Risks: Collaboration ensured that a diverse range of perspectives was considered when assessing and addressing risks. The involvement of various stakeholders resulted in a more holistic understanding of potential risks.
- Alignment with Transformation Goals: Collaboration facilitated alignment between risk management objectives and digital transformation goals. By involving representatives from different functional areas, risk management strategies were tailored to fit within the broader transformation context.
- Effective Risk Mitigation: Cross-functional collaboration resulted in the identification and implementation of more effective risk mitigation strategies. The combined expertise from various departments led to comprehensive risk assessments and well-informed mitigation plans.

In practice, organizations can foster cross-functional collaboration by encouraging open communication channels, creating cross-departmental teams, and aligning risk management and business transformation goals during planning sessions.

3) *Risk-Aware Decision-Making.*
Embedding risk considerations into decision-making processes was highlighted as a key success factor. Organizations that integrated risk assessments early in digital initiatives were better positioned to anticipate potential pitfalls, prioritize risk mitigation, and make informed decisions that balanced innovation and security.
The theme of risk-aware decision-making underscores the necessity of integrating risk considerations into the decision-making processes of digital initiatives. Organizations that prioritized early risk assessments and proactively managed risks during the planning and execution stages experienced several benefits:
- Anticipating Challenges: Risk-aware decision-making allowed organizations to anticipate potential challenges and vulnerabilities associated with digital transformation initiatives. This proactive approach enabled the development of mitigation strategies before risks escalated.
- Informed Innovation: Integrating risk assessments into decision-making facilitated a balanced approach to innovation. Organizations were better equipped to identify opportunities for innovation while simultaneously addressing potential risks.
- Minimized Retroactive Efforts: By addressing risks at an early stage, organizations minimized the need for retroactive risk mitigation efforts that can be time-consuming, costly, and disruptive to digital transformation projects.

In practice, organizations can implement risk-aware decision-making by embedding risk assessments into the planning stages of projects, training teams to consider risk in their decision-making processes, and continuously monitoring risks throughout project lifecycles.

The findings corroborate existing literature on the pivotal

role of leadership in shaping organizational priorities. The involvement of executives in risk management initiatives underscores the value of a top-down approach, signaling to the entire organization the importance of risk-awareness. Strong executive support facilitates resource allocation, fosters a culture of risk management, and enhances the integration of risk management with digital transformation strategies.

1) *Cross-Functional Collaboration.*
   The focus on cross-functional collaboration supports research showing how risk management connects with different parts of the organization. Successful risk management relies on teamwork among IT experts, legal advisors, compliance officers, and business leaders. This collaborative approach helps everyone understand risks better and aligns risk management with the overall business strategy.
2) *Risk-Aware Decision-Making.*
   Integrating risk assessments into decision-making helps organizations balance innovation and security. By prioritizing risk-awareness from the start of digital initiatives, organizations can better identify potential risks, apply effective controls, and adjust strategies as threats evolve. This proactive approach promotes agility and reduces the need for costly, reactive risk mitigation efforts.

The findings underscore the significance of a holistic approach to IT risk management within the context of digital transformation. Organizations are encouraged to consider the identified critical success factors in their risk management strategies:

1) *Executive Involvement.*
   Organizations should foster strong executive sponsorship for risk management initiatives, integrating risk considerations into the strategic decision-making process.
2) *Collaboration.*
   Encouraging collaboration between IT teams, risk management, and other business units fosters a comprehensive understanding of risks and aligns risk management with transformation objectives.
3) *Early Risk Assessment.*
   Integrating risk assessments at the outset of digital initiatives enables organizations to anticipate challenges, prioritize risk mitigation, and make informed decisions.

V. Conclusion

The primary objective of this research was to investigate the critical success factors that facilitate effective IT risk management during digital transformation. Through a multiple case study approach, the study delved into the experiences, strategies, and challenges faced by organizations that successfully manage IT risks in the context of their digital transformation journeys.

Thematic analysis of qualitative data led to the identification of three critical success factors:

1) *Executive Leadership and Support.*
   Strong executive sponsorship of risk management initiatives enhances resource allocation, fosters risk-aware cultures, and aligns risk management with strategic goals.
2) *Cross-Functional Collaboration.*
   Collaboration between IT teams, risk management departments, and other business units ensures a comprehensive understanding of risks and aligns risk management with transformation objectives.
3) *Risk-Aware Decision-Making.*
   Integrating risk assessments early in digital initiatives supports informed decisions that balance innovation and security, preventing costly retroactive risk mitigation efforts.

The research findings offer actionable recommendations for organizations looking to improve their IT risk management during digital transformation. To implement the identified critical success factors, organizations can take the following concrete steps:

1) *Engage executives in risk management initiatives.*
   Organizations should ensure that top-level executives are actively involved in risk management efforts. This can be achieved by establishing a dedicated executive committee focused on IT risk, integrating risk management objectives into executive performance metrics, and holding regular risk reviews. Executive leadership should also champion risk management by visibly supporting risk-related initiatives and communicating their importance across all levels of the organization, fostering a risk-aware culture.
2) *Foster cross-functional collaboration.*
   To enhance collaboration across departments, organizations should create cross-functional risk management teams that include representatives from IT, finance, operations, and other relevant business units. Regular cross-departmental meetings and workshops can be held to facilitate the sharing of perspectives and the development of comprehensive risk assessments. In addition, clear communication channels should be established to ensure that risk information is shared effectively between departments, allowing for quicker identification and resolution of potential issues.
3) *Integrate risk assessments into decision-making.*
   Organizations should embed risk assessments into all key decision-making processes by developing standardized risk evaluation frameworks. This includes conducting risk assessments at the outset of digital initiatives and reviewing risks at major project milestones. Decision-makers should be trained on how to assess risks and incorporate those insights into their planning and execution strategies. By integrating risk management into every phase of digital transformation projects, organizations can proactively address risks before they become significant challenges.

This study bridges the gap between theoretical frameworks and practical insights, providing actionable recommendations for organizations managing the intersection of IT risk management and digital transformation. Future research could focus on exploring the application of these recommendations in specific industries, such as healthcare, finance, and

manufacturing, where the digital transformation process and risk profiles vary significantly. For example, research in the healthcare sector could investigate how IT risk management strategies can address the unique challenges of data privacy and patient safety, while studies in finance could explore how financial institutions manage risks related to fintech innovations. Additionally, further research could examine the evolving nature of digital risks, such as cybersecurity threats or regulatory challenges, and how risk management strategies need to adapt in fast-paced industries like e-commerce or telecommunications. These targeted studies would help deepen the understanding of how IT risk management practices can be optimized within different industrial contexts.

The convergence of IT risk management and digital transformation brings both challenges and opportunities. Key success factors provide a roadmap for organizations to manage risks while navigating digital transformation. By fostering risk-awareness, collaboration, and proactive management, organizations can protect their digital initiatives and ensure a smooth, secure transformation.

REFERENCES

[1] W. B. Rouse, *Innovation Ecosystems: How Driving Forces and Success Factors Affect Opportunities for Business Innovation*. CRC Press, 2024.
[2] M. Haupt, *The Contemporary CFO: How Finance Leaders Can Drive Business Transformation, Performance and Growth in a Connected World*. Kogan Page Publishers, 2021.
[3] N. Vaz, *Digital Business Transformation: How Established Companies Sustain Competitive Advantage from Now to Next*. John Wiley & Sons, 2021.
[4] B. F. Abrantes and J. L. Madsen, *Essentials on Dynamic Capabilities for a Contemporary World*. Springer, 2023.
[5] M. S. M. Review, *How AI Is Transforming the Organization*. MIT Press, 2020.
[6] M. Ghobakhloo, M. Iranmanesh, B. Foroughi, M.-L. Tseng, D. Nikbin, and A. A. Khanfar, "Industry 4.0 digital transformation and opportunities for supply chain resilience: a comprehensive review and a strategic roadmap," *Production Planning & Control,* pp. 1–31, 2023, doi: 10.1080/09537287.2023.2252376.
[7] S. O. Dawodu, A. Omotosho, O. J. Akindote, A. O. Adegbite, and S. K. Ewuga, "Cybersecurity risk assessment in banking: methodologies and best practices," *Computer Science & IT Research Journal,* vol. 4, no. 3, pp. 220–243, 2023.
[8] R. Rai, A. Rohilla, and A. Rai, "Understanding cybersecurity threats in e-commerce," in *Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning*: IGI Global, 2024, pp. 501–522.
[9] R. Uimonen, "Agile Business Transformations and Strategic Risk Management in Uncertainty," Ph.D. dissertation, Tampere University, Finland, 2023.
[10] S. Jarjoui and R. Murimi, "A Framework for Enterprise Cybersecurity Risk Management," in *Advances in cybersecurity management,* Springer, 2021, pp. 139–161.
[11] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process," *EURASIP Journal on Information Security,* vol. 2020, pp. 1–18, 2020.
[12] O. T. Arogundade, A. Abayomi-Alli, and S. Misra, "An ontology-based security risk management model for information systems," *Arabian Journal for Science and Engineering,* vol. 45, no. 8, pp. 6183–6198, 2020.
[13] H. I. Kure, S. Islam, and H. Mouratidis, "An integrated cyber security risk management framework and risk predication for the critical infrastructure protection," *Neural Computing and Applications,* vol. 34, no. 18, pp. 15241–15271, 2022.
[14] C. Brumfield, *Cybersecurity Risk Management: Mastering the Fundamentals using the NIST Cybersecurity Framework*. John Wiley & Sons, 2021.
[15] O. Giuca, T. M. Popescu, A. M. Popescu, G. Prostean, and D. E. Popescu, "A survey of cybersecurity risk management frameworks," in *Soft Computing Applications: Proceedings of the 8th International Workshop Soft Computing Applications (SOFA 2018), vol. I, no. 8*, 2021, Springer, pp. 240-272.
[16] H. Taherdoost, "Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview," *Electronics,* vol. 11, no. 14, p. 2181, 2022.
[17] O. A. Fonseca-Herrera, A. E. Rojas, and H. Florez, "A model of an information security management system based on NTC-ISO/IEC 27001 Standard," *IAENG Int. J. Comput. Sci,* vol. 48, no. 2, pp. 213–222, 2021.
[18] A. S. C. Junior and C. H. Arima, "Cyber risk management and ISO 27005 applied in organizations: A systematic literature review," *REVISTA FOCO,* vol. 16, no. 02, pp. e1188-e1188, 2023.
[19] D. P. Möller, "NIST cybersecurity framework and mitre cybersecurity criteria," in *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*: Springer, 2023, pp. 231–271.
[20] J. L. Gowen Jr, "An exploratory study of risk quantification loss event frequency (LEF) approaches using the factor analysis of information risk (FAIR) model in non-financial risk areas," Doctoral dissertation, Capitol Technology University, USA, 2023.
[21] I. IGNAT, "Factor analysis of information risk (fair™) when assessing the information security," M.S. Thesis, Dept. of Software Engineering and Automatics, Technical University of Moldova, Moldova, 2022.
[22] K. A. Barreto, A. A. C. Callado, and A. L. C. Callado, "Internal control under the approach of COSO ERM framework components: A study in a higher education institution," *Revista Ambiente Contábil-Universidade Federal do Rio Grande do Norte,* vol. 15, no. 2, pp. 202–223, 2023.
[23] A. I. Awad, M. Shokry, A. A. Khalaf, and M. K. Abd-Ellah, "Assessment of Potential security risks in advanced metering infrastructure using the octave allegro approach," *Computers and Electrical Engineering,* vol. 108, Art. no. 108667, 2023.
[24] N. Alsafwani, Y. Fazea, and F. Alnajjar, "Strategic Approaches in network communication and information security risk assessment," *Information,* vol. 15, no. 6, Art. no. 353, 2024.
[25] T. Widianti, H. Firdaus, and T. Rakhmawati, "Mapping the Landscape: a Bibliometric Analysis of ISO 31000," *International Journal of Quality & Reliability Management,* vol. 41 no. 7, pp. 1783–1810, 2024. doi: 10.1108/IJQRM-09-2023-02872024.
[26] A. Jalilvand and S. Moorthy, "Enterprise risk management maturity: a clinical study of a US multinational nonprofit firm," *Journal of Accounting, Auditing & Finance,* vol. 39, no. 3, pp. 883–902, 2024.
[27] L. Abdurrahman, "Control Self-Assessment on Information Technology Business Processes as COBIT 2019-based Pre-Audit Activities," *International Journal of Knowledge Management in Tourism and Hospitality,* vol. 3, no. 3, pp. 185–200, 2024.
[28] F. Mera-Amores and H. N. Roa, "Enhancing information security management in small and medium enterprises (SMEs) through iso 27001 compliance," in *Future of Information and Communication Conference*, 2024: Springer, pp. 197–207.
[29] K. Antonopoulou and C. Begkos, "Strategizing for digital innovations: value propositions for transcending market boundaries," *Technological forecasting and social change,* vol. 156, Art. no. 120042, 2020.
[30] N. L. Rane, A. Achari, and S. P. Choudhary, "Enhancing customer loyalty through quality of service: Effective Strategies to improve customer satisfaction, experience, relationship, and engagement," *International Research Journal of Modernization in Engineering Technology and Science,* vol. 5, no. 5, pp. 427–452, 2023.
[31] M. Asif, S. Wang, M. F. Shahzad, and M. Ashfaq, "Data privacy and cybersecurity challenges in the digital transformation of the banking sector," *Computers & Security,* vol. 147, Art. no. 104051, 2024.
[32] A. Meena, S. Dhir, and S. Sushil, "Coopetition, strategy, and business performance in the era of digital transformation using a multi-method

approach: some research implications for strategy and operations management," *International Journal of Production Economics,* vol. 270, Apr. 2024, Art. no. 109068.
[33] C. Aksoy, "Digital innovation management: frameworks, strategies, and future perspectives," *Uluslararası İşletme Bilimi ve Uygulamaları Dergisi,* vol. 3, no. 2, pp. 1–19.
[34] C.-H. Lee, D. Wang, S. Lyu, R. D. Evans, and L. Li, "A digital transformation-enabled framework and strategies for public health risk response and governance: China's experience," *Industrial Management & Data Systems,* vol. 123, no. 1, pp. 133–154, 2023.
[35] M. M. Feliciano-Cestero, N. Ameen, M. Kotabe, J. Paul, and M. Signoret, "Is digital transformation threatened? A systematic literature review of the factors influencing firms' digital transformation and internationalization," *Journal of Business Research,* vol. 157, Mar. 2023, Art. no. 113546.
[36] S. J. Tracy, *Qualitative Research Methods: Collecting Evidence, Crafting Analysis, Communicating Impact*. John Wiley & Sons, 2024.