Applied Information System and Management (AISM)
Volume 8, (2) 2025, p. 231–244
P-ISSN: 2621-2536; E-ISSN: 2621-2544; DOI: 10.15408/aism.v8i2.46123

Risk Management in IT Projects for Digital Banking: A Case Study of an Indonesian State-Owned Bank

Aji Prastio Wibowo[1*], Teguh Raharjo[2], Ni Wayan Trisnawaty[3], Gilang Aulia Muhamad[4], Azka Faridy[5]

***Abstract*—The increasing use of information technology in the banking industry has made it more difficult to manage risks in the digital projects of state-owned banks. This study aims to examine the risk management processes of a state-owned mortgage bank in Indonesia and how it manages the information technology risks in the digital banking project lifecycle. This qualitative research is based on content analysis of forty-three risk assessment documents, with thematic coding using ATLAS.ti. This research was further enriched through expert interviews and a quantitative survey conducted among 38 project stakeholders. Risks are defined in a hierarchical classification and mapped to project phases using the PMBOK. Identifying operational, compliance, and third-party risks is most pertinent in the execution and post-implementation phases. Additionally, there are pressing concerns, such as the potential for cyber threats, non-compliance with applicable laws and regulatory frameworks, integration issues, over-reliance on service vendors, and systemic dependence on external vendors. In this case, the study integrates PMBOK, ISO 31000:2018, and the insights of seasoned practitioners to create a singular holistic mitigation strategy. It comprises a risk prioritization matrix, phased actionable treatment plans for each defined stage, and robust governance and responsiveness enhancement mechanisms for high-risk reactive IT environments. The guidance is triangulated with sector-specific intelligence, thereby underscoring proactive risk governance through communication, vendor due diligence, dynamic control, and real-time accountability across boundaries scaffolding. Further single-initiative case studies, multi-institutional case studies, evolving longitudinal risk studies, and the application of AI and blockchain for predictive and autonomous risk steering in digital finance could enhance and refine this work.**

***Index Terms*—IT project risks, digital banking, risk management, PMBOK, ISO 31000, Indonesia state-owned banks.**

Received: 25 April 2025; Revised: 16 June 2025; Accepted: 10 July 2025.
*Corresponding author

[1]Aji Prastio Wibowo, Universitas Indonesia (e-mail: aji.prastio@ui.ac.id).
[2]Teguh Raharjo, Bina Nusantara University, Indonesia (e-mail: teguh.raharjo12@ui.ac.id).
[3]Ni Wayan Trisnawaty, Universitas Indonesia (e-mail: ni.wayan05@ui.ac.id).
[4]Gilang Aulia Muhamad, King Abdulaziz University, Saudi Arabia (e-mail: gmuhamad@stu.kau.edu.sa).
[5]Azka Faridy, King Abdulaziz University, Saudi Arabia (e-mail: afaridy@stu.kau.edu.sa).

I. Introduction

The rapid advancement of digital technologies has significantly transformed the banking industry, necessitating the adoption of digital platforms to enhance customer experience, streamline operations, and maintain competitiveness [1], [2]. State-owned banks are undergoing extensive digital transformation, integrating artificial intelligence (AI), blockchain, and data analytics into their operations to improve service delivery and operational efficiency [3], [4]. Despite technological advancements, organizations must systematically assess and manage substantial IT risks in digital banking projects to ensure successful implementation [5], [6]. Previous studies highlight that information technology (IT) project risks in digital banking stem from various sources, including cybersecurity threats, third-party dependencies, regulatory compliance challenges, and operational inefficiencies [7], [8]. However, PMBOK frameworks offer structured methodologies for project risk management; understanding how to distribute these risks across different project phases and categorize them effectively to enhance risk mitigation strategies remains limited [9].

This research examines the IT risk management practices in digital banking projects through a case study of an Indonesian state-owned bank specializing in mortgage and housing loans. This study identifies the critical risk factors affecting the bank's digital transformation efforts based on an in-depth interview with an IT Project Manager with nine years of experience. This study uses a qualitative approach to assess risk categorization, severity levels, and emerging themes influencing risk management practices in different project phases.

The research aims to address the following key questions:

1) *What are the primary risks associated with IT projects in digital banking platforms across different project phases?*
2) *How are these risks categorized and prioritized based on severity levels in digital banking projects?*
3) *What key themes and recurring risk patterns emerge from the analysis, and how can they inform better risk management practices?*

This study systematically analyzes IT risks in digital banking projects and contributes to the ongoing discourse on IT governance and risk mitigation in financial institutions. The findings provide insights into risk category gaps and highlight

the necessity of integrated risk management approaches, offering practical recommendations for state-owned banks navigating digital transformation challenges.

II. Literature Review

A. Understanding IT Project Risks

Risks in project management are uncertain events or conditions that can positively or negatively impact project objectives [10]. Risk management in IT projects, particularly in the banking sector—a domain massively dependent on technology—is critical due to unique challenges accruing from both digital transformation and emerging technologies. Banks' IT risks originate from various sources, including system integration problems, software malfunctioning, vulnerabilities in cybersecurity, failure to comply with regulations, and resource constraints [7], [11]. IT system disturbances may immensely impact customers' service and operational effectiveness, even affecting financial and reputation losses [12].

An important feature of IT project risks in digital banking is the emphasis on data security and privacy. As client engagement via digital channels escalates, banks must protect sensitive information from breaches and comply with stringent data protection requirements [13]. The dynamic landscape of digital banking presents several operational risks, which demand constant system upgrades and impose a great deal of pressure on sources, primarily in low-information settings [12], [14]. To effectively manage such risks, financial organizations must have robust risk management frameworks, like the PMBOK framework, to systematically identify, evaluate, and mitigate probable threats to implement projects successfully and securely [15].

B. Digital Transformation in the Banking Industry

The banking industry has been at the forefront of this digital transformation in response to changed customer preferences, increased competition from financial technology companies, and new regulatory requirements [16]. The prevalence of the Internet and digital technologies has forced companies, including banks, to move more quickly in digitization by creating business models like digital banking [2].

Digital transformation in the banking sector has caused many changes, such as creating digital channels, incorporating data analytics, and adopting leading-edge technologies, including artificial intelligence and blockchain. These changes have significantly impacted the way banks operate, with digital channels becoming the primary means of customer engagement and the use of data analytics and emerging technologies enabling banks to enhance their decision-making capabilities and improve their overall performance. Several studies have found that banks improve operational efficiency, decrease costs, and increase customer satisfaction by adopting digital transformation strategies [2], [8], [16], [17].

C. PMBOK Framework for Risk Management

Project management body of knowledge framework underlined in PMI-Process Groups: A Practice Guide [9] and PMBOK® Guide Seventh Edition [18] provides a structured way to deal with project-related risks, which are of utmost importance in complex information technology projects in industries such as banking. This framework strongly emphasizes the availability of structured processes and guiding principles organizations should adopt to identify, assess, and mitigate risks systematically. Eventually, it helps project teams anticipate challenges and develop efficient mitigation strategies accordingly.

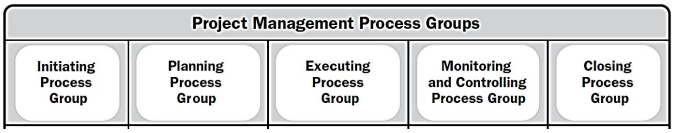

Fig. 1. Project management process groups [9].

The PMBOK framework categorizes project management functions into five process groups: initiating, planning, executing, monitoring and controlling, and closing, as shown in Fig. 1. Each of these categories includes activities on risk management, thereby jeopardizing that risks are dealt with proactively in the whole lifecycle of the project. The PMBOK Seventh Edition also brings important principles for managing project risks by highlighting flexibility, adaptability, and a value-driven methodology. These principles focus on initiative-taking risk management and the ability to adapt to changing project environments—a particularly good thing in IT projects where the environment of digital banking is hazardous and constantly changing. By working with the process groups and principles of the PMBOK, banks can decidedly increase their ability to manage the different risks associated with digital transformation, ensuring effective and secure project delivery. Additionally, the PMBOK framework may help to disseminate knowledge and continuously improve risk management methodologies within the organization so that banks can proactively deal with emerging risks and maintain resilient digital infrastructure.

D. Risk Categories Specific to the Banking Industry

Bank Indonesia's Regulation No. 11/25/PBI/2009 outlines eight key risk categories that banks must manage: credit risk, market risk, operational risk, liquidity risk, strategic risk, compliance risk, reputation risk, and legal risk [19]. As shown in Fig. 2, each risk category must take on unique dimensions in the digital banking landscape. Credit risk arises from defaults by debtors, and the faster processes followed for credit approvals in digital lending further amplify this risk. Financial institutions necessitate strong data analytical capabilities and secure infrastructures to evaluate and alleviate this risk efficiently [20]. In like manner, online trading and investment sites magnify exposure to market risk, and consequently, they require the inclusion and monitoring of real-time data to control financial volatility effectively [21]. Therefore, operational risk brings many consequences to digital banking since failure in the system, data breaches, and cyberattacks can paralyze services and shake trust. Constructing adequate cybersecurity

Applied Information System and Management (AISM)
Volume 8, (2) 2025, p. 231–244
P-ISSN: 2621-2536; E-ISSN: 2621-2544; DOI: 10.15408/aism.v8i2.46123

and resilient infrastructure is therefore important [22]. Another aspect is liquidity risk, which is becoming more relevant due to high volumes of transactions or fluctuations in digital assets, and thus, it requires adequate management of cash flow to execute operations smoothly [23].

Fig. 2. Banking risk categories in Indonesia.

Digital transformation also brings strategic, compliance, and reputation risks [24]. Non-aligned strategies, unmet customer expectations, or poor compliance with regulations in Anti-Money Laundering (AML) and Know Your Customer (KYC) may translate into operational inefficiencies, penalties, and a damaged confidence base. Social media amplifies reputation risk, calling for initiative-taking customer communication [25]. Lastly, legal risks call for serious reflection on intellectual property, contracts, and data protection throughout the project to avoid litigation or penalties [26].

The literature review highlights several critical aspects of IT risk management in digital banking. First, IT project risks in financial institutions originate from various sources, including cybersecurity vulnerabilities, regulatory compliance challenges, operational inefficiencies, and third-party dependencies inefficiencies [7], [8]. The complexity of digital transformation exacerbates these risks, requiring banks to adopt structured risk management frameworks such as PMBOK to systematically identify, assess, and mitigate potential threats [9]. Despite the availability of established frameworks, previous studies suggest a lack of comprehensive risk categorization tailored to digital banking projects, particularly in the context of Indonesian state-owned banks. While general banking risk categories exist [19], their application to IT project risks remains underexplored. Furthermore, existing literature primarily focuses on theoretical risk management strategies without adequately addressing how risks manifest across different project phases or how their severity levels influence project success [22], [27].

E. Risk Assessment Framework with ISO 31000:2018

ISO 31000:2018 is a globally accepted standard that offers comprehensive guidelines on the principles, framework, and risk management processes to assist organizations with the systematic and sustainable identification, assessment, and mitigation of risks [28]. This framework describes risk management as a coordinated process of directing and controlling organizational activities dealing with uncertainties.

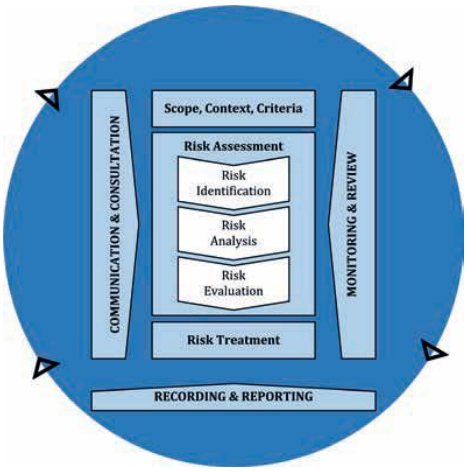

Fig. 3. ISO 31000 risk management process [28].

The standard highlights the importance of embedding risk management in organizational policies and frameworks to facilitate initiative-taking decision-making, governance, and strategic planning while enabling institutions to efficiently manage asset protection, compliance, and stakeholder trust. Regarding digital banking projects, particularly those featuring technological innovations like blockchain or third-party integrations, ISO 31000:2018 provides a foundation for developing agile, multi-faceted, and regulation-compliant risk mitigation strategies. As shown in Fig. 3, The following quoted risk management aspect communicates and consults with stakeholders, scopes the context of an organization's criteria, and determines its value, assesses risks, treats risks, monitors, and reviews separately. These steps form a cohesive whole to monitor record communication, reporting, and review. Strategic evaluation of the legal domain concerning reputational risk determinants segments each examined domain based on risk and impact levels. Many organizations employ five-level risk matrices to represent the edge maps, prioritize from the highest hierarchy downwards, and classify unbearable and critical risks in the pre-defined exclusion zones, as shown in Fig. 4.

Following this, in the risk treatment stage, appropriate methods are selected, bearing in mind the type and extent of the risks. These strategies may comprise avoiding risks, reducing risks, sharing risks, or retaining risks, bearing in mind the organization's risk appetite and operational priorities. Pertaining effectiveness requires ongoing assessment and

review of mitigation strategies for their effectiveness considering market changes, new regulations, or technological advances. The final stages pertain to filing and disclosing documents relevant to risk activities, which, within the context, portray the level of organizational and managerial responsibility within the entity concerned. ISO 31000:2018 provides a flexible, comprehensive model for managing tactical and operational risks in digital banking, particularly concerning vendors and their interconnections with blockchain technology and other complex systems.

Likelihood / Impact	Least Severe	Slightly Severe	Moderate	Severe	Very Severe
Almost Certain	LTM	M	MTH	H	H
Likely	LTM	M	MTH	MTH	H
Moderate	L	LTM	M	M	MTH
Unlikely	L	LTM	LTM	M	M
Least Likely	L	L	L	LTM	LTM

Legend: **L:** Low; **LTM:** Low to Moderate; **M:** Moderate; **MTH:** Moderate to High; **H:** High

Fig. 4. Risk assessment matrix 5 level.

F. Previous Research

The topic of risk management in Information Technology (IT) projects, particularly in the context of electronic banking, has garnered considerable attention in academic circles. A research project focusing on a specific aspect of risk management reveals that success is dependent on a minimum of two conditions: risk detection and the formulation of a response strategy. However, evaluation methods that are too thorough may diminish product performance [27]. This is corroborated by a case study from Vietnam on core banking projects, which identified software implementation function gaps, evolving requirement fulfillment, and real-time execution constraints as major risk factors—all indicative of a significant gap between a system's developmental competencies and the dynamic operational workflows [29].

Risk Management 4.0 emphasizes the importance of data governance in mitigating risk in today's world. An example of such a framework is Big Data Analytics (BDA), which enables real-time monitoring and predictive simulations, as well as integrated risk reporting dashboards that dynamically transform static, compliance-driven processes into automated, compliance-driven processes [30]. Nevertheless, the implementation of such tools in developing nations, such as Indonesia, remains extremely limited. Nicoletti further develops the discussion by noting that risk exposure should be managed through key performance indicators, such as SLA adherence, time-to-market for services, and fraud detection, within risk-aligned business metrics and digital transformation maturity [31]. Evidence continues to show that, in Indonesia, mostly public financial institutions still regard risk and performance as two self-contained domains, lacking the necessary feedback integration that characterizes digital maturity. The increasing use of artificial intelligence and blockchain technology further modifies the risk landscape. AI is effectively utilized in fraud detection, credit risk assessment, and anomaly-based threat mitigation using ensemble learning and behavior-based analytics [32]. At the same time, Blockchain offers secure and unchangeable records of transactions, which promotes transparency while mitigating the exposure to risks of third parties [33]. However, as this research indicates, the adoption of these technologies in the Indonesian banking industry is highly fragmented due to regulatory gray areas and the presence of legacy systems.

The rapid expansion of FinTech introduces ecosystems and strategic risks. Failure by traditional banks to update their governance frameworks puts them at risk of exposure to new vulnerabilities from ecosystem integration, technology aging, and misaligned regulations [34]. In addition, human-centric risks such as social engineering present a relentless threat to systems' integrity, especially where awareness training and behavioral controls are lacking [35]. This is particularly concerning, as many banks are digitizing their services at the front lines while continuing to neglect investments in shifting their internal culture. As demonstrated in the case of Santander Bank, which integrated operational risk management (ORM) with long-term diversification strategies while maintaining operational risks at under 1% of total capital, ORM can be successfully implemented in conjunction with capital allocation strategies to bolster long-term organizational resilience [29], [36] . In contrast, the Indonesian example demonstrates that advocating a digitized ORM framework without infrastructure-led risk diversification reveals a reactive, short-term approach that lacks alignment with long-term strategic growth objectives.

III. Research Method

In this study, the specific mixed method research design helps analyze the risk management practices in IT projects for digital banking, explicitly utilizing the PMBOK® Guide as its basis. The methodology focuses on document analysis to provide a comprehensive understanding of risk patterns, priorities, and mitigation strategies of risks across digital banking projects. The methodology adopts a structured, step-by-step approach, as shown in Fig. 5, which presents the framework and methods employed to conduct mixed method study, with qualitative thematic analysis as the main approach, also quantitative and expert validation as embedded supporting components.

This research initiated the data collection process by selecting and reviewing documentary sources from forty-three risk assessment documents on digital banking projects conducted by one of the state-owned banks in Indonesia. The research selects these documents according to established parameters, ensuring they are for projects started in 2023 and conform to the risk group requirements per Bank Indonesia's PBI No.11/25/PBI/2009. Each document includes comprehensive details on risk management plans that explain the various risks expected during the projects. These documents are instrumental in assessing the risks involved in the separate phases of the project lifecycle, which are the PMBOK process groups: Initiating, planning, executing, monitoring, controlling, and closing.

Applied Information System and Management (AISM)
Volume 8, (2) 2025, p. 231–244
P-ISSN: 2621-2536; E-ISSN: 2621-2544; DOI: 10.15408/aism.v8i2.46123

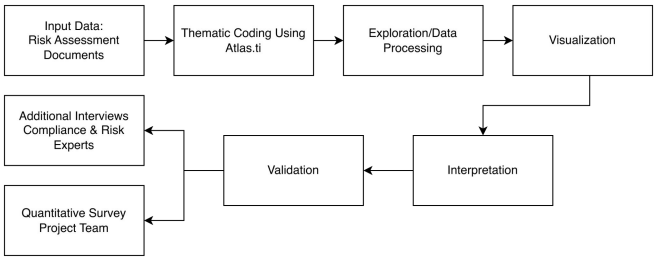

Fig. 5. Mixed method approach methodology.

This research performs the thematic coding of the data within ATLAS.ti software, following the risk management principles recommended by the PMBOK® Guide. The research is concerned with three aspects besides other risks:

- Phases and PMBOK Process Groups encompass pre-project (risks identified during initiation and planning phases), on-project (risks encountered during execution and monitoring phases), and post-project risks (risks arising after implementation, primarily related to maintenance, compliance, and user acceptance).
- The study scope looks at risks that occur frequently from the perspective of the Identify and Monitor Risks processes PMBOK.
- This research ranks risks by severity using the approach detailed in the Perform Qualitative Risk Analysis Process.

This research utilized ATLAS.ti software for thematic analysis of narratives and applied PMBOK tools to categorize and prioritize risks. This research also infused some PMBOK principles—facilitating value delivery, engaging stakeholders, and ensuring adaptability—into the risk management observations. Some ethical issues accompany this research. In all circumstances where risk assessments are needed, the organization's identity will remain hidden. For those participating in the validation interviews, all participants have given consent, and we will ensure their confidentiality throughout the research. Such measures ensure that we conduct the research activities responsibly and ethically.

To bolster the methodological rigor of this study and reduce the likelihood of subjective interpretation, triangulation was employed using two different but complementary methods. These included preliminary semi-structured interviews with two professionals around focus: one serving as an IT compliance specialist and another as a digital operational risk development specialist. Their interviews helped validate the themes and risk categories constructed from the document analysis.

As a second step, an online survey was administered electronically to project team members who participated in the digital banking projects. Risk perception, risk impact, and effectiveness of risk mitigation responses were measured with Likert-scale questions. The results provided quantitative validation for the qualitative analysis, corroborating that the risks needed to be prioritized. These mixed methods not only enhance the rigor of the findings and broaden their relevance but also ensure that the internal artifacts and participants who represent the organization's operations are considered, thereby influencing the findings.

IV. Result and Discussion

A. Document Analysis

The first approach to analyzing the forty-three risk assessment documents compiled from the banks' digital projects enables one to evaluate the distribution of the said documents in terms of two important criteria: the year of the projects and the platform categories. The data in Fig. 6 indicates that of the 43 documents analyzed, 26, or 60.5%, are from 2023-initiated projects, while 17, or 39.5%, are from 2024-initiated projects. The growing demand for digital transformations after the Pandemic influenced the development of various digital banking projects during 2023. This development can explain the rational decrease in the count of projects by the year 2024, as the organizations will have to evaluate their growth and consolidate the already functioning projects.

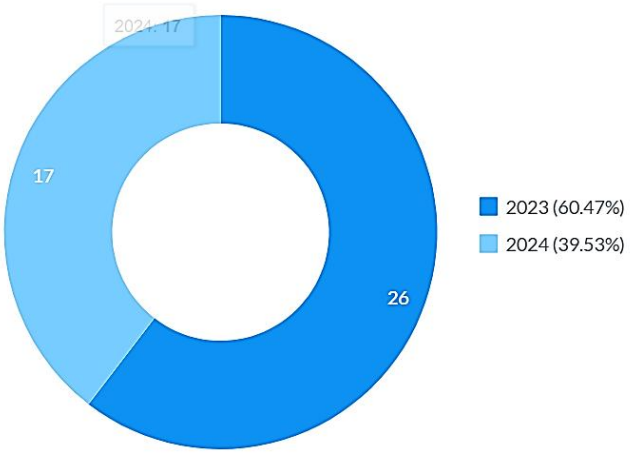

Fig. 6. Document distribution by year.

This research more closely classified the documents according to the precise range of digital platform projects involved, as illustrated in Fig. 7. Mobile banking is the most important, with a significant percentage of 11 documents (25.6%), the primary mode of contact between the bank and its customers. Loan and mortgage digitalization comes second with ten documents (23.3%), cutting across the digitization focus of the bank on facilitating credit and mortgage services. Payment channels & API integration forms nine documents (20.9%) and is part of the strategy of building an electronic payment system that is integrated and interoperable. Six documents (14.0%) represent QRIS (Quick Response Code Indonesian Standard) and show increased use of cashless

payment solutions. EDC Channels (Electronic Data Capture) constitute five documents (11.6%) indicating continued spending on developing these point-of-sale technologies. There is less emphasis on internet banking as a digital platform with only two documents (4.7%), which means there is a greater degree of stability or less concentration on Internet banking projects.

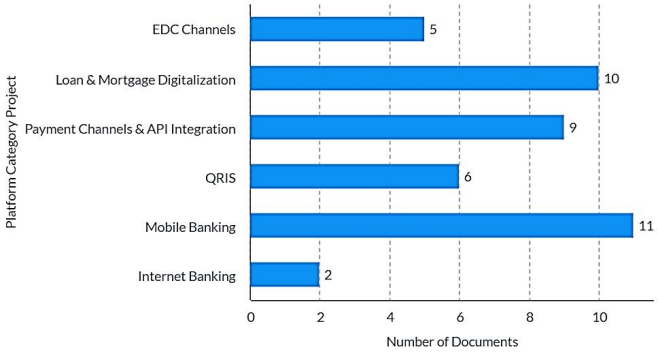

Fig. 7. Document distribution by platform category project.

After entering the 4 code categories, 645 markers for each document were generated through these documents utilizing the ATLAS.ti software. Fig. 8 outlines the outcome of the thematic coding performed on the risk assessment papers. This research utilizes three broad types of analysis to explain a project: its context, risk features, and singular events. In this sense, the project as a practice square entails three clusters of dimensions: Banking risk categories, risk project phase, and inherent risk level. The analysis can examine these dimensions individually or in various combinations within the scope of discourse on risk patterns in the technological projects undertaken. Overall, management will highlight the recurring risk themes from these relationships to identify specific interactions critical for risk mitigation and management. Such a structured approach complements the comprehensiveness of the discussion on the findings and what these findings mean for the management of IT risks in the context of digital banking projects.

B. Banking Risk Categories

Figure 9 demonstrates that out of all categories of banking risk, Operational Risk is the most common one, with 477 markers (78.2%) across all examined projects of digitalized banking. It can also be related to the technological factors of some business industries, hence the marker. Further, it underscores the managerial challenges posed by the operational Risk, hence underlining the systemic issues encompassing technology dependencies accompanying all forms of digital transformation.

Though only a minor fraction of it is extent-wise, other risk types are also present that have been shaping the risk profile at hand. Legal Risk, which is second in significance to most, tends to comprise 61 markers (10.0%) that stem from issues such as having or lacking the ability to meet legal obligations, entering contracts, and protecting one's inventions. On the other hand, reputation risk comprises nine markers (8.0%) of how the digital aspect can lead to the organization's inability to satisfy the customer, thus reducing their market trust.

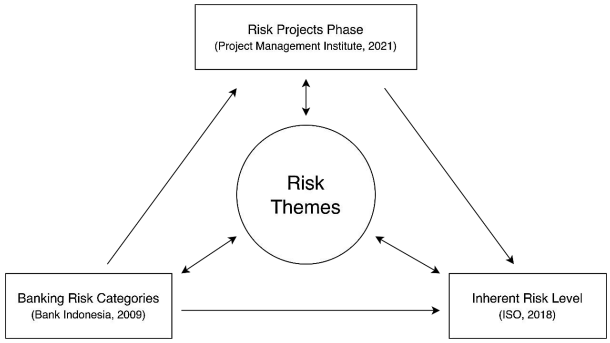

Fig. 8. Risk analysis framework integrating banking risk categories [19], risk project phases [18], inherent risk levels [28], and risk themes.

Compliance risk focuses on the remaining 41 markers (6.7%) challenging areas within the regulatory framework (seen in Fig. 9). Notably, the projects analyzed view strategic risk, with only 17 markers accounting for 2.8% of the total markers, as a comparatively lesser concern. The absence of markers further corroborates the general suggestion that credit risk, liquidity risk, and market risk are irrelevant within the parameters of the analyzed digital banking projects. This result may arise because these projects focus on technological and operational services rather than classical banking services.

C. Risk Project Phase

The phase-wise risk analysis of the project reveals unique risks at each stage of the project's life cycle. As illustrated in Fig. 10, the highest risk in the project is in the on-project phase, with 403 markers (68.6%). This condition is the most challenging part of the project, as executing the digital banking implementations can be very intricate. The areas that incur the most risk during this time include cybersecurity, unreliability of the system, and integration problems. The on-project phase highlights the need for good supervision, adequate testing of the systems, and effective management of vendors, as these can significantly help minimize risks during this phase.

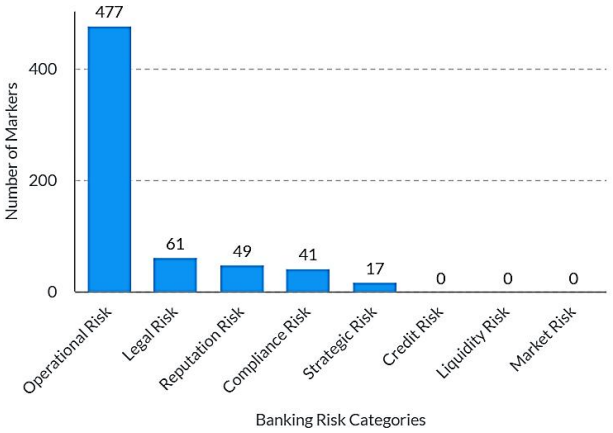

Fig. 9. Analysis of codes for banking risk categories.

Applied Information System and Management (AISM)
Volume 8, (2) 2025, p. 231–244
P-ISSN: 2621-2536; E-ISSN: 2621-2544; DOI: 10.15408/aism.v8i2.46123

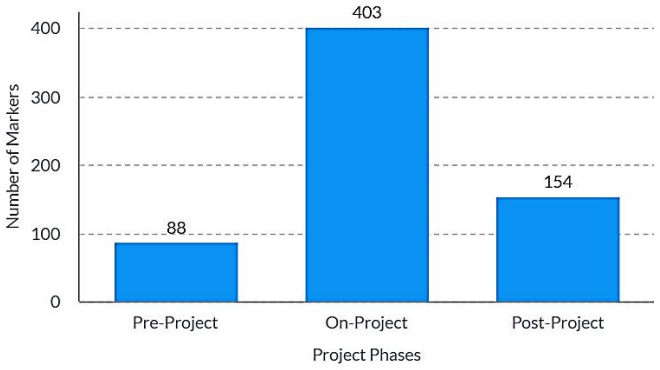

Fig. 10. Analysis of codes for risk project phases.

In the post-project stage, 154 markers (26.2%) revolve around ensuring the sustainability and operational robustness of systems put in place. Significant risks in this phase include legal matters, user satisfaction, and the experience and performance of the operation. Adhering to legal rules and standards and ensuring adequate performance of responsibilities is crucial. Addressing legal and operational issues is essential to ensure project results are durable and comply with legal requirements. The risks remain constant in the pre-project phase, requiring 15% or 88 markers of auxiliary functions. However, everything will be critical for the success of the subsequent phases. The planning and organization of resources become critical due to the business environment's regulatory oversight or standards, such as operational policies and procedures, as well as the competencies in human resources. Chief Threats present are people, policies, and procedures, which all encroach upon the boundaries of legal and regulatory regimes. Conclusion Besides a good business environment analysis, competent pre-planning will ensure robust project execution and closure.

D. Inherent Risk Level

The analysis presented in Fig. 11 shows a risk spectrum within which the more extensive basis of risks lies within the moderate category, which encompasses 468 marks (72.6%), while the remaining equation claims otherwise. The risks within this field are not minimal; instead, most are on the path to achieving long-term stability. The operational and technical risks fall under this category as working in one area can evolve into a more significant risk if managed efficiently while project execution is underway.

A total of 172 marks are to be classified as low to low-moderate, thus falling under the second category, which, as a sum, contributes to 26.7% of the total sum. Compared to the other set of risks, these are trivial as the sensitivity level does not exceed the baselines set for the project's visions. Integration or interdependencies can make these factors detrimental; thus, a cautious approach is necessary. The range of moderate-high risks encompasses a low range of codes 0.8%; this comes alongside the risk of bombs, which, when analyzed, did have codes but an extremely low denominator. Any risk within the analyzed dimensions was improbable in approaching the critical line. The result brings us to the high and low categories; they did not have any presence within this category and fairly balanced the ratios set for the projects.

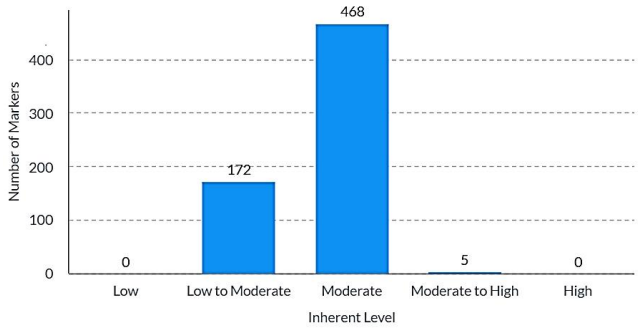

Fig. 11. Inherent Risk Level Code Analysis

E. Banking Risk Categories in the Risk Project Phase

Within the examined parameters, there was a minimal possibility of hitting the red line. There was no presence within this category, and they effectively evened out the project ratio targets. The range of risks spanning from moderated high risks covers a low range of codes of 0.8 percent; this is together with the risk of bombs that were, when looked at, not lacking codes, but the denominator was exceptionally low.

As shown in Fig. 12, legality and various regulatory compliance regulations alongside Contract Compliance still needed to be addressed in the post-project phase, which garnered Legal Risk as the highest. Moreover, trust over reputation risk was paramount, and it overestimated the complexity of the matter while retaining customer trust post-implementation. The operational risk was also present elsewhere; as mentioned, project outcomes must link directly to proper system reliability and maintenance measures. Seeking alignment with the compliance standards of regulators set in place while also ensuring the readiness of the system to undertake operational activities even before a project starts is appreciably fundamental. As for Strategic Risk, the absence of firewalls such as new key goals claims the enhancement in synchronization of individual project targets with the overall strategy of the firm; on the contrary, Reputation Risk occupied a bare minimum space, suggesting that firms must watch their interactions with stakeholders while on the planning phase of a project.

F. Banking Risk Categories with Inherent Risk Levels

The classification of risks from a banking viewpoint distinguishing the inherent risk factors shows the risk severity level within each thematical category. According to Fig. 13, most risks exist in the middle or between moderate to low sectors and none between high or low classifications, indicating the adequate presence of risk.

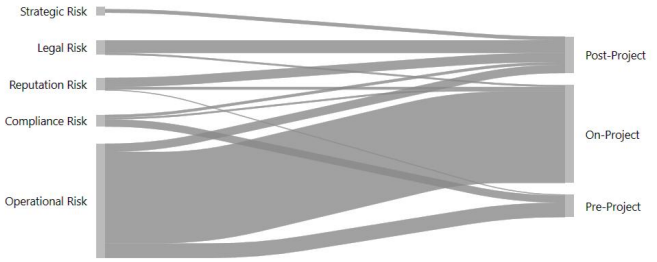

Fig. 12. Banking risk categories in risk projects phase sankey.

Regarding major categories, operational risk blinds the rest because the means are primarily moderate and a smaller percentage low to moderate. Since there are slightly varying instances of risks, specifically moderate to high, it becomes majorly visible that there are severe issues related to innovative technology, system malfunctions, and other forms of high-order disruptions. The analysis concludes that implementing strong operational measures and other contingency strategies is essential to mitigate the negative impacts of escalating risk levels.

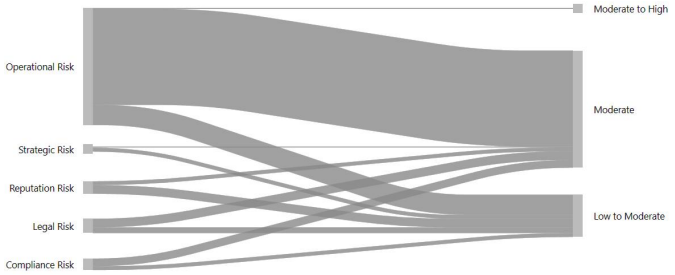

Fig. 13. Banking risk categories with inherent risk level sankey.

Legal risks, on the other hand, are widely in the middle to lower spectrum. These risks include the exposure of failure to adhere to regulation requirements, technology transfer, or breach of contract – all of which are important in the context of e-banking initiatives. The fact that high-severity legal risks are absent shows that there is a formalized strategy for installing and implementing systemic regulation compliance and supervision in the project process and after it. This research labels the risks of non-compliance as average. Knowing compliance with regulatory standards is still challenging; a small category of non-compliance risks emerges, classified as low to average. Compliance risk has never reached a high classification; it has always remained low. Hence, it is relevant when conducting a bank's digital business.

The reputation risks are classified as average and low to average in some cases. Such reputation risks are primarily those relating to satisfaction, the business's image, and the customers' confidence, which are essential in winning the competition in the bank's niche. The low level of these risks suggests that customer management is well-designed and other bank issues are being dealt with comprehensively. Strategic risks primarily fall into the low-to-average category, with only a few classifieds as average. Such risks encompass the issues of coherence of project targets with the goals and objectives set for the organization. They are clearly of an indeterminate low degree, but their content has strategic consequences and needs to be through the planning and implementation phase. The absence of credit, liquidity, and market risks in this analysis implies that such risks are not crucial in evaluating the now-discussed digital banking projects. The analysis is consistent with the objectives of these projects, which are operational and technological rather than the standard financial ones.

G. Risk Projects Phase with Inherent Risk Level

Risk levels can vary from a moderate level to a low or high when evaluating across the three stages of a project, which include pre-project, on-project, and post-project. The interpretation of the data collected from all three stages, as shown in Fig. 14, indicates that the setting has a controllable risk environment due to a lack of high or insignificant risk; most of the risks assessed are moderate during the project.

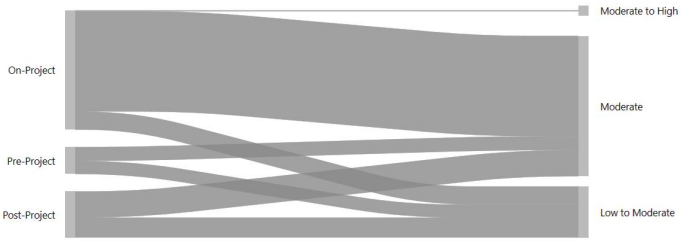

Fig. 14. Risk Project phase with inherent risk level sankey.

The on-project phase is the riskiest, with many risk factors classified as moderate and a smaller number classified as low to moderate. In this regard, this phase caters to moderate to high risks pertaining directly to the difficulties encountered while running the project. Such risks usually relate to system efficiency, protection against breaches, and the amalgamation of several platforms, thereby necessitating active supervision, on-time evaluation, and management of risk factors associated with the quick running of the project. Regarding the risk factors, in the post-project phase, the remaining ones, a sizeable share is estimated to be moderate, with the remaining few being low to moderate. This trend highlights the nature of tasks undertaken after project completion, such as complying with legal conditions, efficiently integrating business processes within the post-implementation phase, and ensuring customer satisfaction with the product or service. While there are no moderate to high risks, managing the system presents some moderate risks. Effective initiative management is necessary to maintain the system and ensure adherence to necessary laws. The risk profile of this phase is evenly split between low to moderate risks associated with resource allocation, regulatory requirements, and strategy during the planning phase of a project and moderate risks, making it a balanced distribution. The absence of moderate to substantial risk during this phase indicates that the commencement stages of any digital banking construction project remain stable when extensive groundwork and

Applied Information System and Management (AISM)
Volume 8, (2) 2025, p. 231–244
P-ISSN: 2621-2536; E-ISSN: 2621-2544; DOI: 10.15408/aism.v8i2.46123

Table 1.
Banking Risk Categories Across Project Phases and Risk Levels

	Pre-Project			On-Project			Post-Project		
	Low to Moderate	Moderate	Moderate to High	Low to Moderate	Moderate	Moderate to High	Low to Moderate	Moderate	Moderate to High
Compliance Risk	√	√	-	√	√	-	√	√	-
Legal Risk	-	-	-	-	√	-	√	√	-
Operational Risk	√	√	-	√	√	√	√	√	-
Reputation Risk	√	-	-	√	-	-	√	√	-
Strategic Risk	-	-	-	-	-	-	√	√	-

evaluations take place.*H. Banking Risk Categories in Projects Phase with Inherent Risk Level*

Figure 15 and Table 1 representation indicate the distribution of categories of banking risks throughout the phases of a project, which are the pre-project phase, the on-project phase, and the post project phase, alongside the levels of inbuilt risks as low to moderate, moderate phases, and moderate to high. This risk distribution analysis not only demonstrates the Risk of each category in multi-directional phases of a project but also gives insight into the areas that are high in attention during the project.

The most common risk observed in all phases was the operational risk, and the height of the graph was most significant in the on-project phase for the moderate level, which suggests the presence of more significant operational woes, for example, issues with system performance, cybersecurity, and other issues during the process of executing the project. Nevertheless, operational risks appeared in the pre-project stage (low to moderate and moderate) and the post-project stage (moderate). Businesses should prioritize planning to ensure longevity and operational stability rather than taking risks.

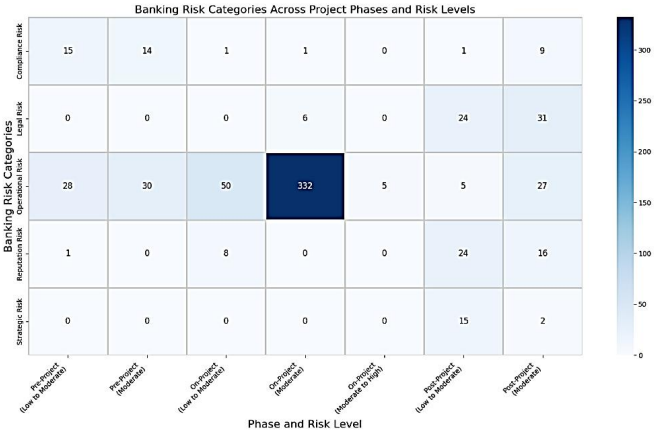

Fig. 15. Heatmap of banking risk categories across project phases and risk levels.

The graph shows compliance risks are more common and concentrated in the pre-project phase. In contrast, project regulations range from low to moderate during the working project phase, indicating the necessity of adhering to rules during project planning. Post-project compliance risks appear lower than excessive compliance requirements, which makes sense since every project requires new regulations. Legal risks occur exclusively in the post-project phase and extend into the moderate category. This condition suggests that it is important to comply with contract commitments, manage intellectual property, and address regulatory issues after project completion. Other legal risks during the on-project phase fall into the moderate category, emphasizing the need for more legal considerations during the project to avoid complications.

Reputation risk is positioned in the post-project phase, ranging from low to moderate and even moderate, stressing the critical issues of customer trust and public perception of the business after the project is delivered. Reputation risks are less pronounced in the on-project phase, indicating active efforts to reduce these risks with the external context during the project's execution phase. Strategic risk only rarely occurs during the post-project phase. Most instances report it being low to moderate, with a few cases reporting it being mild. The result suggests that such misalignment usually occurs after completing a project. Therefore, there is a need for a regular evaluation of such misalignment to ensure that the organization achieves the project objectives.

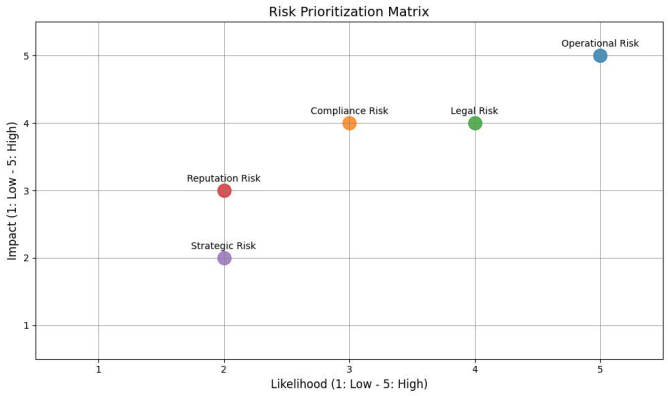

Fig. 16. Risk prioritization matrix.

After completing all evaluations, it is possible to combine

all current and future risks with the aid of the prioritization matrix. The risk prioritization framework also exhibits the probabilities and consequences of various categories of banking risk while aiding in determining relative significance, as displayed in Fig. 16. Operational risk is most critical and sits in the high impact and high likelihood quadrant, meaning that this category is of utmost importance and requires excellent control measures. Both legal risk and compliance risk categories are determined to be in the moderate to high zone in terms of impact and likelihood, and they remain essential throughout the project while executing and in the post-implementation stage. The strategic risk sits in the middle regarding consequences but is low in probability, which shows that it is essential from the perspective of trust management but not something that happens frequently. Market risk is one of those elements that cannot go lower in its impact, and the possibility of it is also low so that it combines as a less critical issue but requires checks from time to time to ensure that actions taken align with the company's objectives. This matrix depicts the risks in such a way as to establish the hierarchy of the risks, the result being that all the stakeholders can direct their resources and strategies on the high-impact areas.

I. Risk Themes Frequency with Word Cloud

The word cloud in Fig. 17 illustrates the importance of key risk themes inherent in digital banking projects. Such a depiction enables one to discern the more commonplace risks easily. Legal issues would maintain the dominant position in the risk map, having the highest number, which underlines the importance of laws and contracts during project implementation. In other words, regulatory compliance, cybersecurity, and third-party compliance are aspects of good security and compliance with outside/inside rules and regulations. On the other hand, User Satisfaction brings in such an essential dimension that customers' views and opinions have significant implications for the effectiveness of different strategies for digital banking.

Fig. 17. Word Cloud of Risk Themes

Moderate and low-frequency themes include system reliability, operational performance, and integration issues. Addressing these areas is necessary to smoothen the system's performance and ensure its stability. Even though it is low frequency, Human Resource Competency and Data Accuracy Issues indicate the essence of operational people and reliable information for executing risk mitigation efforts. This strategy outline helps stakeholders develop mitigation strategies for risks in key risk themes with higher frequency and relevance so that stakeholders do not chase after the vast array of risk themes. The consent makes the risk mitigation strategy more precise in managing digital banking project risks.

J. Risk Mitigation Strategies for Digital Banking Projects

Achieving defined goals within a specific time limit for a digital banking project requires effective risk mitigation due to the need for meticulous diligence [18], [28]. This research adds value by designing a mitigation framework based on commonly occurring and operationally identified risks in the project. Such design requires understanding additional modalities defined through e-governance alongside legal, reputational, and compliance risks while taking a technological-centric problem-solving approach. The approach will aid in addressing multinational legal concerns and ensure the ensuing framework is adaptable.

Table 2.
Risk Categories and Mitigation Strategies in Digital Banking Projects

Risk Category	Common Phase	Mitigation Strategy
Operational Risk	On-Project Phase	- Conduct rigorous system testing and validation - Implement automated performance monitoring tools - Develop contingency and rollback plans for deployment
Legal Risk	Post-Project Phase	- Enforce contract standardization - Conduct legal compliance audits - Engage internal legal counsel for pre-launch review
Compliance Risk	Pre- & On-Project Phase	- Establish an internal regulatory mapping checklist - Integrate Regulation Technology solutions for real-time compliance tracking - Provide periodic training for project teams
Reputation Risk	Post-Project Phase	- Set up initiative-taking customer service and feedback channels - Monitor social media sentiment - Prepare incident response protocols
Strategic Risk	Post-Project Phase	- Align project KPIs with institutional strategy - Conduct post-implementation reviews - Apply scenario planning for major product launches
Third-Party Risk (Additional)	On-Project Phase	- Use vendor risk assessment frameworks - Include SLA clauses with defined risk-sharing terms - Conduct periodic vendor audits

Organizations can customize the ISO 31000:2018 framework by omitting risk transfer through outsourcing or shifting operational control to non-regulated partners, thereby constructing oversight within the framework. Other risks may

Applied Information System and Management (AISM)
Volume 8, (2) 2025, p. 231–244
P-ISSN: 2621-2536; E-ISSN: 2621-2544; DOI: 10.15408/aism.v8i2.46123

remain, including peer-to-peer lending module barriers that stem from the lack of guidance within regulatory frameworks, including lack of support for critical features. In addition, using a multi-approach authentication method, redundancy, and vendor risk scoring can lower peer-to-peer lending modules for critical features. Organizations knowingly accept low-impact risks by not providing critical fallbacks while integrating pedantic UI elements without requiring documentation or periodic review. Executing the defined goals of benchmarking is furthermore accepted with non-regulatory tailored steps.

This framework implements these strategies by converging each risk type with corresponding actions to control it, as presented in Table 2. In this regard, operational risks, which are abundant in the on-project phase, can be alleviated by sophisticated system testing, advanced performance monitoring tools, and detailed fallback plans. Structured contract management alongside legal compliance checklists and internal counsel pre-launch reviews capture legal risks typically post-project. Compliance risks involve not only active tracking of relevant regulations but also active alignment with internal policies. In contrast, reputation risks require customer support automation for initiative-taking engagement and active feedback loops. Also, the proposed framework incorporates aspects of the three lines of defense model, which assigns operational teams the frontline role for all daily risk control functions, whose counterparts in risk management and compliance units comprise the second line overseeing oversight. At the same time, internal audit fulfills the independent assurance role as the "third line." All mitigation responsibilities across the organization are allocated appropriately and enforced through this governance approach. The proposed framework enhances resilience by adapting risk treatment approaches to the severity levels and project phases identified in this study. It reduces the exposure of digital banking institutions to emerging regulatory and technological challenges.

K. Triangulation and Validation of Findings

To reinforce the rigor of the thematic analysis and minimize single-source bias, two expert interviews and a practitioner survey were conducted for triangulation purposes. The subjects of the interviews and surveys were an IT compliance specialist and a digital operational risk development specialist, both experienced professionals in their respective fields. In Indonesia, they worked as digital banking risk managers at a state-owned financial institution. Their contributions aided in confirming the risk types, project phases, and the resulting mitigation strategies following a document analysis and thematic coding which was executed.

Regarding IT compliance, the first expert in the field, who has already gained six years of expertise, noted that the most significant and frequent risks associated with digital banking projects stem from non-alignment with regulations, reliance on third parties, and sudden regulatory changes. These issues generally stem from the planning or pre-implementation phases of a project, particularly when compliance teams are not integrated into the process early on. The specialist pointed out that several post-audit errors were not the result of systems failures, but of not keeping up with changes in POJK or PBI regulations. Highlighted key mitigation strategies include proactive compliance mapping and compliance checklist audits, as well as stricter SLA clauses for vendors regarding audit and data protection compliance. Although there is some merit to the PMBOK and ISO 31000 frameworks, the expert emphasized the importance of practical, interdisciplinary, and collaborative synergy. Other emerging concerns include cloud-related issues, such as data sovereignty, infrastructure transparency, and algorithmic bias resulting from AI decision-making processes.

The second expert, specializing in digital operational risk who has already gained more than ten years of expertise, emphasized multiple themes of operational risk. As this expert mentioned, the execution phase of a project has the highest risk exposure, especially about system integration, delays, and cross-functional silos. Risk identification is often performed using the Risk and Control Self-Assessment (RCSA), and prioritization follows a qualitative matrix approach based on defined likelihood, impact, and detectability. Common mitigation approaches uncommonly include rollback planning, shadow systems, and SOP revisions on set time intervals. While the ascertained PMBOK and ISO:31000 sound structurally, the expert pointed out the lack of need for swift changes or real-time dashboard monitoring. A concerning trend was observed, namely the increasing dependency on third parties, particularly in open banking frameworks related to API-based fintech integrations. These activities may introduce unanticipated risks unless controlled through explicit Service Level Agreements (SLAs), routine audits, and ongoing due diligence.

To thematically analyze information provided qualitatively, a survey was administered to a digitally oriented banking group comprising 38 members, which included IT, compliance, risk, and digital banking development unit. Respondents assessed the probability and impact of the eight risk categories, as well as the frequency and effectiveness of relevant mitigation measures, using a 5-point Likert scale.

Surveys corroborated the qualitative data that is shown in Fig. 18, identifying cybersecurity, regulatory compliance, and third-party/vendor risks as both probable and impactful throughout the project lifecycle. In addition, integration challenges and implementation delays are paired with the experts' insights into operational bottlenecks. Reputation-related risks were evaluated as high-impact but infrequent, while legal and strategic risks received middling ratings. Notably, algorithmic bias—which was given considerable prominence during the interviews—was not highly rated in the survey, suggesting that practitioners may

have underestimated its significance.

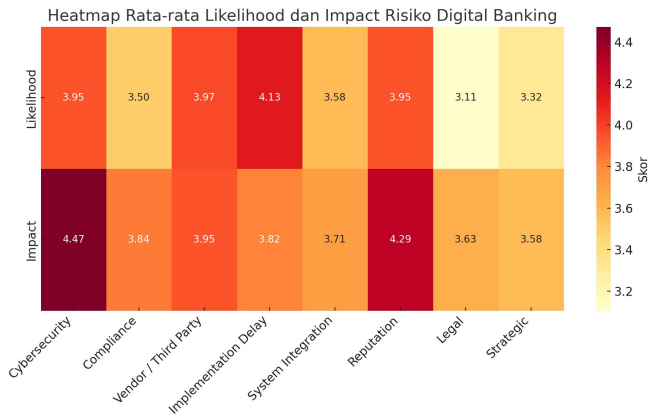

Fig. 18. Heatmap of average risk likelihood and impact based on survey.

The mitigation strategies most cited were system testing paired with rollback strategy formulation, real-time monitoring dashboards for technology supervision, compliance evaluations, regulatory checklists for legal forecasting concerning external entities, in addition to vendor audits featuring strict adherence to service-level agreement enforcement. Concerning efficiency, compliance with the technical aspects of the strategies received the highest scores, thus supporting the mitigation framework in this study (Fig. 19).

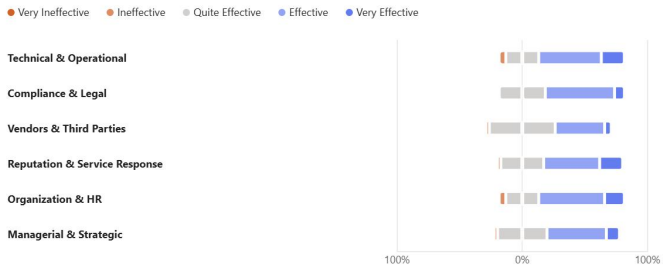

Fig. 19. Perceived effectiveness of risk mitigation strategies in digital banking projects.

V. Limitations and Recommendations for Future Research

Even though this research helps examine IT risk management in digital banking projects, it still has some shortcomings. One example is the lack of available literature because the study's scope was constrained to one case study of a state-owned bank in Indonesia. This condition may have posed a challenge in obtaining diverse results. Another issue is relying on single expert interviews and document analysis, which does not account for many stakeholder perspectives. For example, the study classified risks using thematic coding but did not validate them through simulation-based or statistical modeling, methods widely accepted for quantitative validation. Finally, lacking a longitudinal design restricted the ability to observe dynamic changes in risk exposure after various project phases. All the issues mentioned shed light on the gap for further research in diversifying the result allocation and implementing methodological rigor.

Enhancing the results of this research involves making cross-sectoral comparisons to determine if the patterns of risks in digital banking projects are like those in the banking, insurance, or retail sectors. Studying the interconnected nature of these sectors could provide insight into the sectoral nuances of IT project risk management. Further, analyzing the role that the regulatory regimes for different countries or regions play in shaping compliance requirements could help in understanding contextual risk patterns. In addition, innovative technologies such as artificial intelligence and machine learning have transformed risk management. Predictive modeling utilizes cybernetic or third-party dependencies to highlight specific scenario-driven mitigation strategies. Emerging technologies like blockchain can significantly heighten transparency and accountability in IT project ecosystems. However, the most useful for risk profiling and further developing digital banking initiatives is a profound multidisciplinary focus directed at longitudinal shifts concerning demand dynamics or analytic shifts within the technological paradigm.

VI. Conclusion

This research has offered an in-depth insight into assessing risks in IT projects for digital banking platforms while taking an Indonesian state-owned bank as a case study. This study considers risk categorization and risk level. It establishes essential findings regarding these risks' nature, distribution, and severity. The operational risk was the most notable category, especially during the on-project phase, illustrating the control of internal and technical problems when implementing the system. Compliance risk was more severe in the pre-project phase, highlighting the need for adherence planning to meet regulatory requirements. The legal risk was more severe in the post-project phase, emphasizing the necessity of addressing legal constraints during the contractual phase after implementing the system. The thematic analysis emphasizes various prerequisites for accomplishing the concern, such as cybersecurity, third-party compliance, and user satisfaction.

In the face of risks at certain stages of project completion, visualization techniques are recommended. Those include Sankey diagrams, heatmaps, and matrices aiming at different prioritization of target indicators. With regards to risk management strategy, both the findings and the methodology will help connect the sub-phases such as the Pre-Project and Compliance, which require operational compliance; the On-Project and Integration, which demand operational controls; and finally, the post-project and Legal, which require customer maintenance. These findings also further highlight the significance of the risk management strategy in the post-project, on-project, and pre-project sub-phases and their consequent risks in banking, artificial intelligence, and other emerging technologies. They shed light on crucial themes and risk categories pertinent to the management of risks. Future banking projects should incorporate the proposed tools to identify and mitigate risks, ensuring such frameworks' stability over a more extended period.

Applied Information System and Management (AISM)
Volume 8, (2) 2025, p. 231–244
P-ISSN: 2621-2536; E-ISSN: 2621-2544; DOI: 10.15408/aism.v8i2.46123

ACKNOWLEDGMENT

PT Bank Tabungan Negara Persero Tbk. (BTN) supports funding for this research.

REFERENCES

[1] L. Abubakar and T. Handayani, "Penguatan regulasi: Upaya percepatan transformasi digital perbankan di era ekonomi digital," *Masalah-Masalah Hukum*, vol. 51, no. 3, pp. 259–270, Jul. 2022, doi: 10.14710/mmh.51.3.2022.259-270.

[2] K. Kantika, F. Kurniasari, and M. Mulyono, "The factors affecting digital bank services adoption using trust as mediating variable," *Journal of Business and Management Review*, vol. 3, no. 10, pp. 690–704, Oct. 2022, doi: 10.47153/jbmr310.4882022.

[3] McKinsey, "McKinsey on Risk, Number 12, April 2022," *McKinsey & Company*, Feb. 18, 2022. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/mckinsey-on-risk/mckinsey-on-risk-number-12

[4] PricewaterhouseCoopers, "From threat to opportunity | PwC's Global Risk Survey 2023," *PwC*. https://www.pwc.com/gx/en/issues/risk-regulation/global-risk-survey.html

[5] H. Adams, and M. Coppola, "Global Risk Study," *Accenture*, Jul. 02, 2025. https://www.accenture.com/us-en/insights/consulting/global-risk-compliance

[6] K. Panetta, "The Top 8 Security and Risk Trends We're Watching," Gartner, Nov. 15, 2021. https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021

[7] S. M. Ali, S. M. N. Hoq, A. B. M. M. Bari, G. Kabir, and S. K. Paul, "Evaluating factors contributing to the failure of information system in the banking industry," *PLoS ONE*, vol. 17, no. 3, Art. no. e0265674, Mar. 2022, doi: 10.1371/journal.pone.0265674.

[8] P. Widharto, A. I. Pandesenda, A. N. Yahya, E. A. Sukma, M. R. Shihab, and B. Ranti, "Digital transformation of indonesia banking institution: case study of PT. BRI syariah," in *2020 International Conference on Information Technology Systems and Innovation (ICITSI)*, 2020, pp. 44–50. doi: 10.1109/ICITSI50517.2020.9264935.

[9] Project Management Institute, *Process Groups: A Practice Guide*. Project Management Institute, 2022.

[10] H. F. Cervone, "Project risk management," *OCLC Systems & Services: International digital library perspectives*, vol. 22, no. 4, pp. 256–262, Jan. 2006, doi: 10.1108/10650750610706970.

[11] O. Bevan, S. Ganguly, P. Kaminski, and C. Rezek, "'The ghost in the machine': Managing technology risk," *McKinsey & Company*, Jul. 21, 2016. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-ghost-in-the-machine-managing-technology-risk

[12] C. C. H. Law, C. C. Chen, and B. J. P. Wu, "Managing the full ERP life-cycle: Considerations of maintenance and support requirements and IT governance practice as integral elements of the formula for successful ERP adoption," *Comput Ind*, vol. 61, no. 3, pp. 297–308, Apr. 2010, doi: 10.1016/j.compind.2009.10.004.

[13] F. Khan, J. H. Kim, L. Mathiassen, and R. Moore, "Data breach management: An integrated risk model," *Information and Management*, vol. 58, no. 1, Art. no. 103392, Jan. 2021, doi: 10.1016/j.im.2020.103392.

[14] R. Ramchand, N. Tatikonda, D. Verma, and R. E. Nance, "Maintenance practices and metrics across defense and commercial systems," *INCOSE International Symposium*, vol. 14, no. 1, pp. 1810–1820, Jun. 2004, doi: 10.1002/j.2334-5837.2004.tb00615.x.

[15] J. T. Yee and S.-C. Oh, "Technology integration project planning and execution," in *Technology Integration to Business: Focusing on RFID, Interoperability, and Sustainability for Manufacturing, Logistics, and Supply Chain Management*, J. T. Yee and S.-C. Oh, Eds., London: Springer London, 2013, pp. 169–236. doi: 10.1007/978-1-4471-4390-1_6.

[16] D. Saxunova and C. L. Le Roux, "Digital transformation of world finance," in *Investment Strategies in Emerging New Trends in Finance*, R. G. Ahangar and A. Salman, Eds., Rijeka: IntechOpen, 2020, doi: 10.5772/intechopen.93987.

[17] A. Kurniawan, A. Rahayu, and L. A. Wibowo, "Pengaruh transformasi digital terhadap kinerja bank pembangunan daerah di indonesia," *Jurnal Ilmu Keuangan Dan Perbankan (JIKA)*, vol. 10, no. 2, pp. 158–181, Aug. 2021, doi: 10.34010/jika.v10i2.4426..

[18] Project Management Institute, *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Seventh Edition and The Standard for Project Management (ENGLISH)*. in PMBOK® Guide. Project Management Institute, 2021.

[19] Bank Indonesia, "PBI No. 11/25/PBI/2009 tentang Perubahan atas Peraturan Bank Indonesia No. 5/8/PBI/2003 tentang Penerapan Manajemen Risiko bagi Bank Umum," 2009. Accessed: Nov. 18, 2024. [Online]. Available: https://ojk.go.id/id/kanal/perbankan/regulasi/peraturan-bank-indonesia/Pages/peraturan-bank-indonesia-nomor-11-25-pbi-2009.aspx

[20] Basel Committee on Banking Supervision, "Principles for the Management of Credit Risk," *BIS*, Sep. 27, 2000. https://www.bis.org/publ/bcbs75.htm

[21] P. Giudici, "Fintech risk management: A research challenge for artificial intelligence in finance," *Frontiers in Artificial Intelligence*, vol. 1, Nov. 2018, doi: 10.3389/frai.2018.00001.

[22] J. Eceiza, I. Kristensen, D. Krivin, H. Samandari, and O. White, "The future of operational-risk management in financial services," *McKinsey & Company*, Apr. 13, 2020. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-future-of-operational-risk-management-in-financial-services

[23] E. Scannella, "Theory and regulation of liquidity risk management in banking," *Int J Risk Assess Manag*, vol. 19, no. 1–2, pp. 4–21, Jan. 2016, doi: 10.1504/IJRAM.2016.074433.

[24] V. A. Dokuchaev, "Digital transformation: New drivers and new risks," in *2020 International Conference on Engineering Management of Communication and Technology (EMCTECH)*, 2020, pp. 1–7. doi: 10.1109/EMCTECH49634.2020.9261544.

[25] M. D. Moberly, "Chapter 6 - Reputation Risks and Their Management," in *Safeguarding Intangible Assets*, M. D. Moberly, Ed., Boston: Butterworth-Heinemann, 2014, pp. 73–90. doi: 10.1016/B978-0-12-800516-3.00006-9.

[26] R. Burnett, "Legal risk management for the IT industry," *Computer Law & Security Review*, vol. 21, no. 1, pp. 61–67, 2005, doi: 10.1016/j.clsr.2004.11.011.

[27] D. Pimchangthong and V. Boonjing, "Effects of risk management practices on IT project success," *Management and Production Engineering Review*, vol. 8, no. 1, pp. 30–37, Mar. 2017, doi: 10.1515/mper-2017-0004.

[28] International Organization for Standardization (ISO), *Risk Management - Guidelines*. BSI, 2018.

[29] C. M. Tae, P. D. Hung, and L. D. Huynh, "Risk management for software projects in banking," in *Proceedings of the 2020 The 6th International Conference on E-Business and Applications.* New York, NY, USA: Association for Computing Machinery, 2020, pp. 65–69. doi: 10.1145/3387263.3387268.

[30] G. Dicuonzo, G. Galeone, E. Zappimbulso, and V. Dell'Atti, "Risk management 4.0: The role of big data analytics in the bank sector," *International Journal of Economics and Financial Issues*, vol. 9, no. 6, pp. 40–47, Oct. 2019, doi: 10.32479/ijefi.8556.

[31] A. Papathomas and G. Konteos, "Financial institutions digital transformation: the stages of the journey and business metrics to follow," *Journal of Financial Services Marketing*, vol. 29, no. 2, pp. 590–606, Jun. 2024, doi: 10.1057/s41264-023-00223-x.

[32] V. Chang, B. Ali, L. Golightly, M. A. Ganatra, and M. Mohamed, "Investigating credit card payment fraud with detection methods using advanced machine learning," *Information (Basel)*, vol. 15, no. 8, Art. no. 478, Aug. 2024, doi: 10.3390/info15080478.

[33] D. Priyadarshana, T. R. Rao, and M. S. Rao, "AI and blockchain technology for secure and transparent financial transactions," *Int. J. Sci. Res. Arch.*, vol. 13, no. 1, pp. 2013–2019, Oct. 2024.

[34] V. Murinde, E. Rizopoulos, and M. Zachariadis, "The impact of the FinTech revolution on the future of banking: Opportunities and risks,"

International Review of Financial Analysis, vol. 81, Art. no.102103, Mar. 2022, doi: 10.1016/j.irfa.2022.102103.

[35] T. R. Peltier, "Social engineering: Concepts and solutions," *EDPACS*, vol. 33, no. 8, pp. 1–13, Feb. 2006.

[36] F. Z. Aguayo and B. Ślusarczyk, "Risks of banking services' digitalization: The practice of diversification and sustainable development goals," *Sustainability (Switzerland)*, vol. 12, no. 10, May 2020, doi: 10.3390/SU12104040.