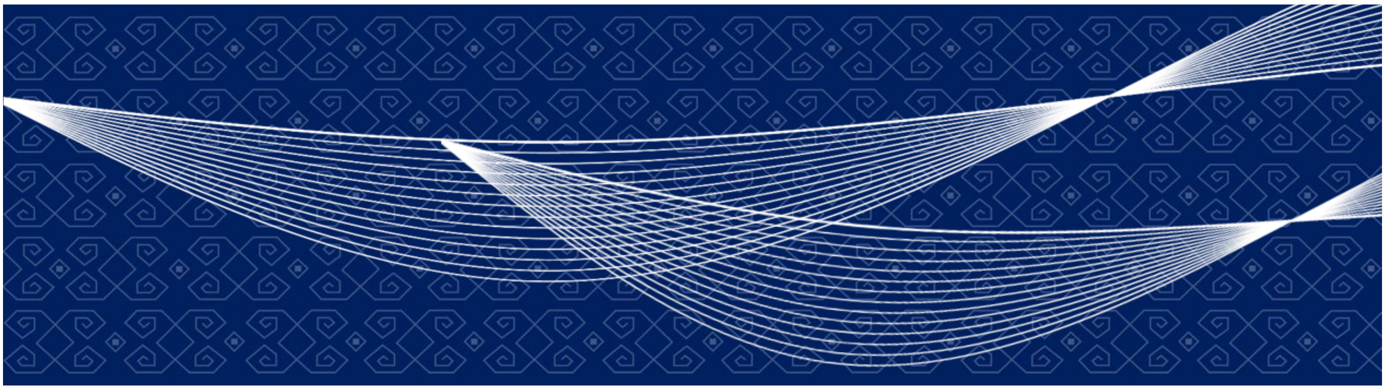
BANK INDONESIA
BANK SENTRAL REPUBLIK INDONESIA



WP/21/2025

WORKING PAPER

RISK MANAGEMENT IN DIGITAL CENTRAL BANK: STRENGTHENING THE TRANSFORMATION OF IDCB

Cicilia Anggadewi Harun, Danny Hermawan, Citra Amanda, Annes Nisrina Khoirunnisa

2025

This is a working paper, and hence it represents research in progress. This paper represents the opinions of the authors and is the product of professional research. It is not meant to represent the position or opinions of the Bank Indonesia. Any errors are the fault of the authors.

RISK MANAGEMENT IN DIGITAL CENTRAL BANK: STRENGTHENING THE TRANSFORMATION OF IDCB

Cicilia Anggadewi Harun, Danny Hermawan, Citra Amanda, Annes Nisrina Khoirunnisa

ABSTRACT

Amid the rapid progression of the digital transformation era, central banks are increasingly expected to not only harness emerging opportunities but also navigate and manage the growing complexity of associated risks in an effective and systematic manner. This study aims to identify and analyze optimal risk mitigation strategies within the context of digital transformation, employing a systems thinking approach and the Bayesian Network (BN) method. The risks analyzed are categorized into five main types: technological, financial, regulatory, cultural, and operational risks. We surveyed the officers in charge in IT risk mitigation to indicate the initial level of optimal risk mitigation for the high classification and medium classification as a starting point and to gain the parameters for the dynamics. Operational risk emerges as the most dominant factor influencing mitigation effectiveness, thereby underscoring the need to prioritize strong internal governance arrangements. This is followed by technological risk, which is an inseparable aspect of the digital transformation process, thus requiring the strengthening of infrastructure and cybersecurity. Scenario analysis using expert judgment can simulate an increase in optimal mitigation by strengthening six key risk nodes. Furthermore, a combination of low technological risk, enhanced system security, low third-party risk, and reduced cybersecurity vulnerabilities is shown to be the most influential set of factors driving effective mitigation. These findings underscore the importance of structured and sustainable mitigation strategies, particularly in strengthening digital security systems and operational risk management, to ensure a secure and sustainable digital transformation within central banks, or public institutions in general.

Keywords: *Risk Mitigation, Central Bank, Digital Transformation, Cybersecurity, Operational Risk*

JEL Classifications: D81, F55, G32

1. Introduction

1.1 Background

Digital transformation, encompassing the implementation of technologies such as Big Data, Artificial Intelligence (AI), Blockchain, and Cloud Computing, has rapidly evolved across various sectors, including the financial industry (Wang et al., 2023) and central banks, where it facilitates the adoption of digital/AI technologies to enhance operational efficiency, data analysis, financial system supervision, and risk management (Bank for International Settlements, 2025). Alongside the acceleration of digitalization, financial institutions, including central banks, are increasingly confronted with complex and multidimensional challenges. The growing global uncertainty, characterized by the digital disruption of the volatile, uncertain, complex, and ambiguous (VUCA) era, demands adaptive and forward-looking strategies to ensure the sustainability and stability of the financial system (Xu et al., 2017). In this context, digital transformation is no longer an option but a necessity for public institutions such as central banks to effectively respond to crises (Fletcher & Griffiths, 2020). Over the past decade, governments in developed countries, particularly in Europe, have accelerated digital transformation through comprehensive digitalization of public services, integrated government service portals, and the development of key components such as digital identity, data sharing, and digital payments (Santiso, 2022). Therefore, enhancing institutional capacity in leveraging digital technologies and innovating services to achieve organizational goals, particularly in the public sector, is aligned with the current challenges and demands faced by government institutions (Agostino et al., 2020; Xie et al., 2020).

In practice, digital transformation in the public sector is not an absolute solution for addressing today's uncertainties; instead, it introduces new challenges that must be confronted. These challenges arise from the very nature of digital transformation itself when implemented within the public sector. Previous research has revealed that the concept of digital transformation in the public sector remains ill-defined and does not adequately reflect the unique characteristics of the public sector, which differ from those of the private sector (Meijer, 2018). Public sector digital transformation is a complex and extensive process that reshapes the operational methods and organizational structures of public institutions and the conditions under which data is accessed and utilized on a large scale (OECD, 2024). Therefore, digital transformation can be viewed as a double-edged sword, presenting positive and negative scenarios. On one hand, the best-case scenario includes accelerated progress in various economic domains and more effective, efficient policymaking. On the other hand, the worst-case scenario stems from the inherent complexity of digital transformation and the potential for unforeseen technological consequences.

In the context of digital transformation, public sector innovation management and risk mitigation are crucial, as government institutions hold the mandate to provide public services and formulate policies, serving as one of the key institutional drivers of a nation's economy (Bason, 2010; Sørensen & Torfing, 2016). Traditionally, public sector institutions often face significant challenges in fostering innovation and tend to have higher failure rates (Eggers & Singh, 2009). A strong aversion to risk frequently hinders the processes of transformation and idea generation within public sector organizations (Roszkowski & Grable, 2009) and bureaucratic constraints (Miller, 1998). Risks arising from digital transformation include operational disruptions, reduced managerial effectiveness, and lower financial performance (Ali & Govindan, 2023). Nevertheless, addressing these emerging risks and challenges requires continuous innovation, effective risk mitigation strategies, and a shift in mindset to achieve digital maturity and to develop solutions aligned with institutional mandates that contribute positively to national policymaking.

Adopting new technologies that fundamentally alter business and operational models introduces risks and challenges that require careful management to ensure institutional operations remain resilient and sustainable. This research takes Bank Indonesia as a case study; however, this research should be able to be replicated for other institutions. It is also important to take into account that Bank Indonesia is also the operator of the Real Time Gross Settlement and BI Fast (instant payment), which makes the information technology system of Bank Indonesia much more important for the sustainable provision of digital payment as a public service. Another example of a digital innovation currently in the pipeline is the digital rupiah, a Central Bank Digital Currency (CBDC). According to data from the Bank for International Settlements (BIS), as of 2022, 93% of central banks had initiated work related to CBDC, with more than half having conducted experiments and proof of concept (PoC) activities. Each institution adopts diverse approaches to realize digital transformation in the implementation process. Applying appropriate and practical risk management is expected to identify potential risks that may arise, thereby enabling the digital transformation process to proceed effectively (European Central Bank, 2023).

Previous research has revealed that digital transformation does not always proceed in alignment with initial planning. A substantial body of scholarly evidence has highlighted the negative consequences associated with using data and technology within public sector institutions. The growing phenomenon of datafication has led to dataveillance and increased control over citizens, resulting in privacy rights violations. Moreover, datafication is often flawed, biased, and exploitative (Crawford, 2022). Criado Perez (2020) and Lyon (2014) shows that algorithm-based decision-making (Artificial Intelligence), which relies on datafication, is also subject to bias, lacks transparency, and frequently exacerbates the impact of misguided policies. In addition, there are risks associated with budgetary constraints and limited human resources that hinder the capacity to foster innovation within digital transformation, particularly in public sector institutions (Mulgary & D, 2003). In line with Jane Fountain (2019) in technological enactment theory, the application of technology requires the active involvement of organizational, political, and cultural actors, built upon the integration of the ICT ecosystem and data-driven decision-making supported by Artificial Intelligence. Accordingly, digital transformation in the public sector is inherently tied to complex institutional dynamics, accompanied by various risks and challenges that necessitate in-depth analysis to ensure the transformation goals are optimally achieved. These dynamics also imply that the efficiency and effectiveness of ongoing business processes and technology implementation must be evaluated periodically and objectively, to formulate necessary adjustments that will enhance the effectiveness and efficiency of digital transformation efforts.

In the pursuit of digital transformation, cost and time savings projected from each digital initiative are often not comprehensively evaluated in terms of the actual benefits and added value generated (European Central Bank, 2023; Xinxian & Jianhui, 2022). This includes the extent to which the success of one initiative contributes added value and supports the achievement of other initiatives. Most projections prepared by finance departments tend to rely on optimistic scenarios, assuming that all targets and milestones will be achieved on time and within the allocated budget (European Central Bank, 2023). The speed of digital transformation implementation must be taken into account in order to assess the efficiency of human resources and the effectiveness of the technologies employed.

Previous research on risk mitigation in digital transformation has yet to provide an in-depth analysis of risks related to timing, technological effectiveness, and human resources. Therefore, this study aims to conduct a more comprehensive analysis of risk mitigation in the implementation of central bank digital transformation by considering the range of potential risks involved. Given the various risk profiles that influence digital transformation, particularly within central banks, this research requires a literature review as well as data enrichment, including the collection of primary data through focus group discussions. These efforts will inform the formulation of a systems thinking and Bayesian network methodology employed in this study. The systems thinking is employed because of its ability to represent complex problem, while Bayesian network is special to represent non-linear causal relationship with limited availability of data. Consequently, a holistic understanding of all aspects of the transformation process toward a digital central bank can be developed, along with strategic measures necessary to strengthen the role of Bank Indonesia as the central bank in contributing to Indonesia's digital financial and economic ecosystem.

The rest of the paper is organized as follows: The next section represents a brief review of related work. Section 3 presents the proposed framework for digital transformation risk management and the research method. Results of applying the proposed method on a test network and discussion are represented in Sect. 4. Finally, in the last section we conclude the paper conclusion and recommendation.

1.2 Research Question

Based on the background previously outlined, this paper addresses three research questions: (1) What are the dimensions of risk faced by central banks in implementing digital transformation processes? (2) How can a risk mitigation process framework be aligned with investment decisions that consider digital risks within the digital transformation process, in order to develop ideal application solutions by taking into account factors such as timing, technological effectiveness, implementation speed, alignment and integration with the RBS (Strategic Business Plan) framework, and the allocation of digital human resources? (3) How to measure the risk dimensions in strengthening the effectiveness of digital transformation from the aspects of technological risk, cultural risk, financial risk, regulatory risk, and operational risk, as well as improving the effectiveness of assessment systems to mitigate these risks?

1.3 Research Objective

The objective of this research can be outlined as the following:

1. A comprehensive understanding of all risk dimensions inherent in the digital transformation process within central banks is essential, particularly through the application of a system thinking approach;
2. Understanding the risk mitigation process framework that aligns with investment decisions considering digital risks within the digital transformation process, to develop ideal application solutions by taking into account factors such as timing, technological effectiveness, implementation speed, alignment and integration with the RBS (Strategic Business Plan) framework, and the allocation of digital human resources; and
3. Understanding the dimensions of digital transformation risk measurement, which encompass technological, operational, financial, regulatory, and

cultural risks, is adapted in accordance with international risk management standards.

1.4 Research Implication

This study aims to analyze effective policies for central bank digitalization by examining potential risks, appropriate mitigation strategies, and relevant regulatory frameworks. The findings of this analysis serve as critical inputs for decision-making related to risk management in digital transformation within central banks. This paper employs a Systems Thinking approach and utilizes the Bayesian Belief Network model to develop a comprehensive and practical risk mitigation framework tailored to the needs of central banks. By constructing a model capable of observing complex structures and real-world phenomena within the system, this research is expected to generate more precise and effective policies to support risk management in strengthening the digital transformation of central banks.

1.5 Research Gap/Novelty

The novelties of this paper are multifold. First, a state-of-the-art methodology will be formulated by utilizing system thinking and Bayesian network methodologies to support an analytical model for risk mitigation in the digital institution. Second, this research can fill the literature gap regarding risk mitigation in government institutions, such as central banks, that play a central role in national economic implementation. Third, analyzing measurable risk mitigation strategies to address emerging risks associated with strengthening digital transformation in central banks. Although previous study Ali & Govindan (2023) have examined operational risks in digital transformation, and others (Vial, 2019) has discussed cultural risks, there remains a significant gap in quantitative modeling that integrates the interdependencies among these various risk categories (technological, operational, cultural, etc.) within the unique context of a central bank. Our study addresses this gap by applying a Bayesian Network model, which can capture probabilistic causal relationships among risks a methodological approach that thus far, has not been comprehensively applied within this domain.

2. Literature Review

2.1 Risk Management in Digital Transformation

Digital transformation necessitates a fundamental shift in mindset and a comprehensive restructuring of established processes. Despite its considerable potential, the benefits of digital transformation remain underutilized in many instances. This is particularly evident in the public sector, where the urgency to accelerate transformation to harness its advantages often conflicts with the need to proceed cautiously due to concerns over potential adverse effects. Consequently, digital transformation initiatives cannot be effectively implemented using a standardized or “one size fits all” approach. Instead, these initiatives must be carefully tailored to align with the organization’s strategic objectives and integrated seamlessly with its operational activities (Strome, 2023). The digital transformation of public service then becomes more urgent when the changes impact areas of the public sector, including the development and provision of digital services, the design of processes, and the development of policy (Edelman et al., 2023). Recall that BI is also the operator of the national payment system that has transformed into a digital service. Edelman et al. (2023) also demonstrates the need for a holistic approach to tackle the digital transformation of the public sector and leadership plays the most important role. This is also in accordance with the result of the past research conducted in Bank Indonesia on digital transformation of a central bank (Azwar et al., 2024).

Previous research by Sun et al. (2024) explains that the speed of digital transformation is associated with improvements in organizational operational cost efficiency, enhanced manufacturing and production effectiveness, and added value in building competitive advantage. Accelerating digital transformation enables companies to increase the speed at which they develop valuable resources (Nonaka, 1994); however, such resources tend to depreciate over time (García-García et al., 2017). In line with this, the utilization of big data in decision-making, particularly through artificial intelligence and machine learning for managing and leveraging information, can be integrated and realized through the acceleration of digital transformation (Vial, 2019).

Figure 2. 1 *Digital Transformation Speed*

The acceleration of digital transformation may lead to a rapid decline in operational efficiency and result in high marginal costs if not accompanied by supporting prerequisites. Digital transformation carried out without adherence to appropriate principles has the potential to cause diseconomies of time compression, a condition in which organizations experience a significant decline in performance as the transformation process progresses (Sun et al., 2024). This occurs due to the complex nature of digital transformation, which involves multiple domains within the organization and thus requires effective cross-functional coordination. From a financial perspective, diseconomies of time compression may lead to a sharp deterioration in operational performance and, ultimately, an increase in the marginal costs borne by the organization (Hashai et al., 2018).

Risk management, particularly in digital transformation, is essential to ensure prospective business decision-making and the effective execution of business activities by anticipating and evaluating various factors or events that may threaten organizational success. In practice, the risk management standard commonly adopted by organizations refers to ISO 31000, which establishes methods and guidelines for addressing risks. ISO 31000 represents a universal framework, the application of which varies significantly depending on the sector and the specific characteristics of each organization. The risk management consists of several key stages, including risk analysis, evaluation, treatment, and monitoring. In order for the risk management approach to be effectively utilized in analyzing the implementation of various case studies in the context of digitalization, it must be holistic, encompassing all relevant dimensions and stages within the digital transformation process.

2.2 Operational Risk

Operational risk in digital transformation encompasses various vulnerabilities related to human resources, operational fraud, and organizational governance. Such risks may arise from inadequacy or failures in internal processes, human resources, systems, or external events (Moosa, 2007; Pleune, 2017; Xu et al., 2017). Operational risk is a multidimensional concept in risk management and is particularly relevant when associated with ICT-based adoption, especially in the context of implementation and integration within the public sector (Slassi-sennou & Elmouhib, 2025). The level of operational risk in digital transformation increases as the adoption process becomes more complex, accompanied by threats of implementation failure that endanger organizational sustainability, efficiency, and reputation (Pleune, 2017; Xu et al., 2017).

The development of measurement frameworks for operational risk remains a significant challenge, particularly concerning digitalization and its implications for public institutions. In the financial sector, operational risk is typically measured by assessing both direct and indirect losses resulting from inadequate or failed internal processes, human errors, system failures, and external events (Basel Committee on Banking Supervision, 2005). Recent research shows that digital transformation can strain operations and profitability because of managing complex technological and organizational change (Warner,2019). Skeptically, its inquiry revealing how digital strategies affect financial stability is limited (Kai Wu, 2025). Market expectations and managerial fads may enable overinvestment in speculative digital initiatives despite unclear returns (Klockner et al., 2022).

2.3 Cultural Risk

Complex digital transformation brings a range of exponential benefits in supporting institutional mandates, particularly within public institutions. However, it simultaneously introduces new risks that may hinder the achievement of organizational goals. One of the key risks faced by organizations during the digital transformation process is cultural risk (Hivo, 2023). This risk emerges from changes in work systems that require employees to adapt to new technologies. Such conditions influence the success of digital transformation processes within organizations, as organizational culture constitutes a critical and influential factor in the course of digital transformation (Vial, 2019).

Previous research by Kane et al. (2017) suggests that organizations must consider new cultural dimensions more relevant to the digital era and transform their structures, values, and assumptions throughout the digital transformation journey to achieve digital maturity. This is primarily because most digital transformation failures are not attributed to the technological implementation itself, but rather to the misalignment between the adopted technology and the organization's strategic objectives, as well as the failure to align the organization and its stakeholders with the digital culture necessary for a successful transformation. This is also supported by the findings of Calin Alexandru (2023), which indicate that innovation and the adoption of new technologies can enhance organizational efficiency. However, on the other hand, such changes also have the potential to induce stress among organizational members due to the shift from legacy systems to a culture of utilizing more advanced technologies. An organizational culture that is aligned with strategically implemented digital transformation enables the realization of innovation, flexibility, organizational agility, transparency, openness, and superior performance (Kolagar et al., 2022; Vial, 2019; Warner & Wäger, 2019). Therefore, cultural risks must be carefully considered and systematically analyzed to ensure that potential risks can be accurately identified and appropriately mitigated.

2.4 Technological Risk

Digital Transformation, which is closely linked to technology, inevitably brings about risks that may arise during the process of digital transformation implementation. The implementation of a combination of various complex digital technologies requires substantial investment and careful planning (Menzefricke et al., 2021). Along with the acceleration of digital transformation, issues related to data quality and security become a central focus for institutions such as central banks. In practice, ensuring data security and privacy protection while maximizing the use of data for business innovation and service optimization presents a significant challenge for financial institutions.

The research by Liang & Xu (2025) suggests that cybersecurity is one of the risks that central banks must face during their transformation. This is related to the vulnerability of data encryption, which can pose institutional threats. The computing environment supported by IoT presents significant security risks, including message interception on public channels, data tampering, as well as issues of confidentiality and integrity. This aligns with the research by Oluwatosin Ilori et al. (2024), which indicates that threats to data are also linked to third-party vendor risks, posing significant challenges for organizations across various industries. These risks encompass a range of potential threats, including data breaches, supply chain attacks, and compliance failures, each of which has its own impact on organizational security and operational integrity (Kanojia, 2024). Data breaches are one of the most common risks associated with third-party vendors. These breaches can occur when vendors fail to implement strong security measures, leading to unauthorized access to sensitive information, which in turn can create new risks, such as financial losses, reputational damage, and legal risks. Therefore, during the digital transformation process, organizations must ensure that third parties comply with strict data protection standards and implement adequate security measures to mitigate the risk of breaches.

3. Research Methodology

3.1 Risk Mitigation Framework

The digital transformation process relies on digital infrastructure, which includes digital technologies, products, platforms, and triggers multifaceted changes, including shifts in individual digital skills, organizational management approaches, the role of digital leadership, and business continuity planning (Azwar et al., 2024; Delin et al., 2021). The overall objective of digital transformation is to enhance user experience, improve organizational performance, streamline operational procedures, innovate business models, and create new value within the organization, thereby strengthening the company's value and effectiveness in achieving organizational goals (Vial, 2019). However, these transformations also bring substantial risks at the company level, where the complexity of organizational structure and their dynamic environments introduce uncertainties that need careful management (Criado-Perez et al., 2022). Traditional risk assessment methods generally rely on consistent and comprehensive data (Dou et al., 2024), which is often difficult to gather in rapidly evolving digital environments. Consequently, reliance solely on historical data can lead to incomplete or misleading risk assessments.

3.1.1. Research Design

This paper introduces a state-of-the-art systems thinking and Bayesian network approach for assessing risk management in central banks. This method integrates expert judgment gathered via a survey with objective analysis, enhancing the reliability of risk assessments by reducing subjectivity and aligning weights with the structural characteristics of data. The risk framework proposed in this study still adheres to the existing risk guidelines in current organizational practices, namely the ISO 31000 Risk Management Guidelines (ISO, 2018). According to the ISO 31000 risk management guidelines, risk assessment to evaluate vulnerabilities requires three main steps: identification, analysis, and evaluation. Risk identification focuses on finding, recognizing, and describing risks that may hinder the achievement of set objectives. Risk analysis involves detailed consideration of the likelihood of events and their consequences, the nature and magnitude of those consequences, their complexity and interdependencies, as well as time-related factors and volatility. Risk evaluation is intended to support decision-making by comparing the results of the risk analysis to determine further actions related to the identified risks.

Figure 3. 1 *Methodology Framework*

To analyze risks in digital transformation, particularly in central banks, it is essential to first analyze the potential risks that may occur in central banks. The output from each step will be used as input for the subsequent stage. First, the methodology involves identifying potential risks at the central bank by considering those based on the preferences and priorities of the central bank. The potential risks, based on the total lifecycle, affect the performance of the organization across various aspects, particularly in finance, operations, technology, culture, and regulation. Systems thinking is developed to provide a broader perspective with a "helicopter view," encompassing all the potential risks that have been analysed in collaboration with expert elicitation.

The second step in the risk analysis involves measuring the impact of risks and their interdependencies on performance measures in the risk management assessment of central bank transformation. In this phase, Bayesian Belief Network (BBN) analysis is utilised to accurately analyse and uncover the critical paths of risks present in the digital transformation process. The Bayesian network approach is employed due to its ability to understand causal relationships by using prior knowledge of event occurrences to gain insights into the future likelihood of such events. The capability of BBN to diagnose risk events by investigating the potential root causes that may have led to the occurrence of risks is another possible outcome, facilitated by scenario analysis, which enables decision-makers to make informed choices.

3.2 System Thinking

A fundamental principle of a system is that it constitutes something more than merely the sum of its parts (Meadows, 2008). Based on this reasoning, it becomes evident that systems thinking can be understood as a system in itself. Systems thinking, quite literally, is a system for thinking about systems. As further discussed in this paper, this perspective highlights the limitations found in many existing definitions within the literature. Most of these definitions tend to analyze systems thinking through a reductionist approach, an approach generally regarded as incompatible with the very essence of systems thinking. Reductionist models are unable to fully capture or help us deeply understand new, complex, and dynamic scenarios (Meadows, 2008).

Systems thinking consists of three essential components: elements (in this context, characteristics), interconnections (the ways in which these characteristics relate to and/or influence one another), and a function or purpose (Meadows, 2008). It is important to note that the least visible part of a system, its function or purpose, is often the most critical determinant of the system's behavior (Meadows, 2008). While not all systems have an explicit goal, systems thinking does. Therefore, in order to articulate a clear definition, especially for those unfamiliar with the concept, it is crucial to communicate this underlying purpose. A comprehensive definition of systems thinking must portray it as a goal-oriented system. Therefore, to achieve this, the definition must encompass three key components: elements, interconnections, and function or purpose.

The systems thinking approach is built upon a strong theoretical framework to understand and address system-related challenges and behaviors holistically. This approach emphasizes the interconnections among elements within complex systems, the emergence of systemic properties from component interactions, and the critical role of feedback loops in maintaining or regulating system states. Furthermore, the application of systems thinking focuses on analyzing how systems change, evolve, and respond to both internal and external influences. One advanced method within this approach is system dynamics, which utilizes simulations and computational tools to analyze system behavior and predict potential outcomes (Schlüter et al., 2023) and explore policy interventions for managing complex problems (Laimon et al., 2022; Singh et al., 2023). In this context, policy analysis processes related to risk mitigation can be carried out using the Bayesian Network approach, which enables probabilistic decision-making through the simulation of various complex scenarios.

3.3 Bayesian Network

3.3.1 Bayesian Belief Network (BBN)

A Bayesian Belief Network (BBN) is a directed acyclic graph consisting of nodes representing variables and arcs representing causal relationships. The nodes are assigned probabilistic weights, and the network is modelled using statistical and deterministic functions. In this study, a BBN-based approach is used to predict the likelihood (posterior probabilities) of risks and the corresponding likelihood of optimal risk mitigation measurement. An optimal risk mitigation structure is first developed as System Thinking then transform into Bayesian Network model.

The process of developing an optimal risk mitigation model appropriately follows the risk identification phase, which involves analyzing various categories of risks within the central bank and the variables that trigger them. Once the risks are thoroughly identified, they are connected through a directed acyclic graph (DAG). Each identified risk is represented as a node, with arrows illustrating the dependency relationships between parent and child nodes. To ensure the model is accurately constructed, it is essential to involve domain experts in structured discussions throughout the development of an optimal risk mitigation strategy. As the number of parent nodes linked to a single child node increase, the complexity of the risk model rises dramatically. This escalation significantly complicates the process of gathering data for all related conditional (prior) probabilities. Therefore, it is critical to focus solely on documenting the most relevant risk interdependencies when formulating an effective risk mitigation model within the central banking framework.

A previous study by Enyoghasi & Badurdeen (2023) employed a guideline based on the 80–20 principle, which involves identifying the 20% of risk drivers that contribute to 80% of the potential impact. It is important to note that considerations of risk interdependency should be made after the risk identification process, as outlined in the previous section. This step needs to be conducted progressively, as thorough identification is necessary before determining the nodes with the highest potential impact. Prematurely focusing on interdependencies during the assessment phase may introduce bias into the risk identification process and could result in overlooking critical risks that may have significant consequences.

To acquire the prior probability and conditional probability table (CPT) for the nodes, historical data with domain expert knowledge can be leveraged. Following the acquisition of the prior probability and CPT for all nodes, Bayes theorem is applied to determine the posterior probabilities of the nodes. According to Bayes' theorem (Equation (1)), the relationship between each pair of connected events (X_1/X_2) is expressed in the form of a probability distribution (Uffe B. Kjærulff, 2013).

$$\mathrm{P}(X_2/X_1) = \frac{\mathrm{P}(X_1/X_2)\mathrm{P}(X_2)}{\mathrm{P}(X_1)} \tag{1}$$

Where P(X_1/X_2) is the conditional probability of X_1 given X_2, P(X_2) is the probability of X_2, and P(X1) is the probability of X1. According to Bolstad (2007) and and Fenton and Neil (2012), the joint probability distribution of the Bayesian Network model can be simplified to product of CPTs. Hence the posterior probability of a Bayesian model with events *Xi* (*i* = *1,.....,n*) is generally evaluated using Equation (2).

$$\mathrm{P}\left(X_{1,\ldots\ldots,}X_n\right) = \prod_{i\varepsilon R} \mathrm{P}(X_1 |\ \mathrm{Parents}\ (X_1) \tag{2}$$

Where $\mathrm{P}(X_1 |\ \mathrm{Parents}\ ((X_1))$ represents the CPTs and prior probability of Bayesian Network. Representing the risk and mitigation in the form of Equation (2), the posterior probability of risks and mitigation can be estimated using Equations (3) and (4).

$$\mathrm{P}(R_I) = \prod_{i=1}^{n} \mathrm{P}(R_1 |\ pa\ (R_1) \tag{3}$$

$$\mathrm{P}(PM_k) = \prod_{k=1}^{m} \mathrm{P}(MK_k |\ pa\ (PM_k) \tag{4}$$

Where $\mathrm{P}(R_1 |\ pa\ (R_1)$ and $\mathrm{P}(MK_k |\ pa\ (PM_k)$ represent the CPTs and prior probabilities of optimal risk mitigation as previously defined.

The posterior probability (likelihood) of risks and countermeasure nodes is a function of the Prior Probability and the Conditional Probability Tables (CPTs). Accordingly, the predictive inference process, as previously described, enables the estimation of the likelihood of risk occurrences associated with product design throughout its lifecycle. As discussed earlier, as the complexity of the network increases, the size of the CPTs also expands, and the estimation of posterior probabilities becomes increasingly complex due to the large number of computations involved. Therefore, a predictive inference tool has been developed using the GeNIE software platform to enhance computational accuracy and efficiency. The posterior probabilities calculated through this approach assist in identifying critical risks within the constructed Bayesian Network structure.

3.4 Data Collection

Qualitative analyses in risk mitigation research have frequently integrated both quantitative and qualitative methods, supported by expert opinions in the field (Enyoghasi & Badurdeen, 2023) considering that the nature of risk mitigation is characterized by unique evidence that varies from case to case. Accordingly, this study adopts an expert evaluation method by conducting surveys and collecting expert opinions as the primary data source to analyze risks and the corresponding mitigation strategies related to digital transformation within the central bank.

The criteria for respondent selection were based on their professional field (experts in risk mitigation), academic qualifications, and work experience. These criteria reflect factors such as the level of expertise, cognitive capacity, and decision-making ability—all of which can influence the reliability and accuracy of the findings.

The quantitative data collected consists of 52 completed questionnaires submitted by experts in risk mitigation, specifically within the context of central banking.

The risk analysis conducted in this study covers financial, operational, cultural, technological, and regulatory risks. Therefore, data collection was focused on departments responsible for managing these respective domains. The majority of respondents hold positions as Deputy Directors (34.61%), Assistant Directors (28.84%), Managers (19.23%), and Assistant Managers (17.30%).

Table 3. 1 *Respondent Demographics*

Table 3. 2 *Participants of Focus Group Discussion on ST and BN Model*

Within the internal management cluster, the risks perceived as significant and rated at a high level (>0.50) include non-standardized risk assessment (0.683), third-party risk (0.633), and cybersecurity risk (0.783). This is based on a risk assessment threshold determined by the statistical distribution, by calculating the quartile values from the data provided in the questionnaire. According to this criterion, risk categories with values greater than 0.5 are classified as high-level risks.The internal audit management department demonstrates a higher perception of risk compared to other internal management departments. The legal department perceives resource constraints as a high-level risk (0.567), indicating the need for further attention and mitigation efforts. Furthermore, the risk management department perceives that high-level risks faced by the central bank fall within the technology cluster, particularly third-party risk (0.633) and cybersecurity risk (0.633). Meanwhile, the technology department, which focuses on innovation, data digitalization, digital services, and cybersecurity, also perceives that the major technological risks faced by the central bank at a high level are third-party risk and cybersecurity risk (see Fig. 3.3). After the values of each risk are determined within the Bayesian Network model, the next step involves developing a conditional probability table (CPT), which is completed by experts. This conditional probability table describes the probability of occurrence of a node (variable) while considering the condition or status of its parent nodes, namely the preceding nodes that have a direct influence on the given node within the Bayesian network structure (Enyoghasi & Badurdeen, 2023).

The values assigned to the parent nodes represent the state or category of risks that underlie the probability of the occurrence of other risks, in accordance with the causal relationships mapped in the model. Through this approach, conditional probabilities can be estimated more realistically based on expert judgment, thereby strengthening the model's validity in situations where literature or empirical data are limited. Consequently, the conditional probability table plays a crucial role in ensuring that all inter-risk relationships within the Bayesian Network are quantitatively represented in a consistent manner, and reflect a comprehensive risk assessment.

Figure 3. 2 *Potential Risk Occuring in the Central Bank (Internal Management Departments)*

Figure 3. 3 *Potential Risk Occurring in the Central Bank (Digital Departments)*

4. Result and Discussion

4.1 System Thinking in Risk Management

Figure 4. 1 *Causal Loop Diagram of Risk Management in Digital Central Bank*

This research investigates risk mitigation in digital transformation, with a particular focus on how to achieve optimal risk mitigation. Overall, the various risks present within the Central Bank are comprehensively analyzed using a systems thinking approach to obtain a helicopter view of the optimal risk mitigation process through the following stages: (1) analyzing all existing risks and grouping them based on similar risk potentials, (2) categorizing the risks into clusters such as technological risks, regulatory risks, financial risks, operational risks, and cultural risks, (3) identifying and integrating appropriate risk mitigation measures, and (4) evaluating the optimality of risk mitigation by comparing it to the current risk management practices implemented at Bank Indonesia.

The mitigation efforts for each risk represented in these boxes serve as drivers or causal factors that promote the achievement of optimal risk mitigation. The relationships among these variables are illustrated by positively signed arrows in the causal loop diagram, indicating that enhancing the effectiveness of one type of risk mitigation tends to reinforce mitigation efforts in other areas, ultimately leading to optimal risk mitigation. Thus, this diagram provides a comprehensive overview of the complex interactions among various types of risk mitigation in supporting sustainable digital transformation. Given the complexity of the transformation process and the fact that risk management is one of the crucial factors in the overall process, along with its accompanying mitigation efforts, the systems thinking approach is considered an appropriate method to comprehensively capture the system's complexity (Senge & Sterman, 1992). As a follow-up to the systems thinking approach as a participatory modeling method, this study further analyzes the findings using the Bayesian Belief Network method, which provides a deeper analysis of the impact of interrelationships among variables.

The risk mitigation process implemented by the Central Bank essentially encompasses several risk aspects, following management steps aligned with ISO 31000 standards. Each risk aspect is identified to provide a deeper analysis of the potential risks faced by the Central Bank and to categorize them into five major risk clusters. In the Causal Loop Diagram (Figure 4.1), it is explained that each risk is initiated by a causal variable referred to as a parent node. The flow described here indicates that the potential risks arising from various aspects, such as cybersecurity, flawed innovation, and third-party risk, may increase the potential technological risks generated. Furthermore, the risk mitigation measures that have been implemented are also incorporated into the loop to enhance the value of the optimal risk mitigation achieved. From a financial risk perspective, potential risks involve budget overruns and unexpected costs arising from the occurrence or continuation of risk events, which may lead to substantial financial burdens. Furthermore, risks associated with the Central Bank's regulatory processes in implementing digital transformation include the lack of standardized risk assessment practices, resulting in inconsistent assessment approaches across different risk types. Additionally, the absence of a national regulatory framework concerning digital transformation constitutes a critical risk factor in implementing digital transformation within the organization.

Cultural risk within a central bank encompasses all forms of risk related to organizational culture. This includes the values, norms, behaviors, and mindsets that develop within the institution, which can directly or indirectly influence decision-making processes, operational integrity, and the effectiveness of policy implementation. Cultural risk is critical, as it can impact the institution's governance, regulatory compliance, and public trust. In line with the implementation of digital transformation within the central bank, several cultural risks may emerge, including resistance to change and the persistence of legacy systems, which are defined as dependence on outdated technologies. These issues pose significant challenges to technical and operational aspects and shifting organizational mindsets, which is essential to support the effective and sustainable adoption of new technologies.

Operational risk refers to losses resulting from deficiencies or failures in internal processes, human errors, systems, or external events within the context of digital transformation in the central bank. In this context, the identified operational risks include resource constraints, limited digital capabilities, and governance/compliance misalignment. The analyzed and applicable risk mitigation strategies include strengthening organizational governance, enhancing human resource capabilities, and improving organizational culture to become more adaptive to digital change. In the era of digital shifts within central banks, organizations must carefully evaluate the costs and benefits of digital transformation initiatives, including potential disruptions to existing business models and processes, as well as changes to organizational structures, workflows, and job roles. This evaluation needs to be carried out comprehensively, as the transition process may result in system failures. Digital transformation has the potential to disrupt traditional structures, alter work patterns, and affect data privacy and security. By examining failures, organizations can assess unintended consequences, evaluate ethical implications, and develop frameworks to ensure responsible and sustainable implementation of digital transformation initiatives (Grover et al., 2022; Matzler et al., 2018; Oludapo et al., 2024; Warner & Wäger, 2019).

4.2 Bayesian Network Structure

The Bayesian Network structure was developed based on the causal loop diagram model in system thinking, with several adjustments. The Bayesian Network is considered a quantitative analytical tool capable of representing complex relationships through diagrammatic representation. Applying the Bayesian Network within the system thinking framework was conducted by simplifying the network structure and considering respondent-related aspects. The Bayesian Network (BN), which represents the initial probabilities of mitigation actions within the central bank, is illustrated in Figure 4.3. Based on the current risk mitigation values at Bank Indonesia, analyzed through expert elicitation, the results indicate that the probability of optimal risk mitigation in a high level, namely 42%.Furthermore, each identified risk, as evaluated from the expert perspective, produced the following prior probability values: technology risk at a low level of 32%, financial risk at a low level of 31%, regulatory risk at a low level of 34%, cultural risk at a low level of 29%, and operational risk at a low level of 36%.

Figure 4. 2 *Bayesian Network Structure*

The Bayesian Network developed in this study represents a structure that is simpler than the causal loop diagram, yet remains connected to the risk variables used in the system thinking model (See Figure 4.2). Accordingly, the variables constructed within the Bayesian Network are able to represent each process involved in the optimal risk mitigation that has been implemented. This approach was selected by considering time constraints and limitations in data collection. In this context, optimal risk mitigation serves as the end state for each risk faced by the central bank. The risk components represented still refer to the risks illustrated in the system thinking approach, namely technology risk, financial risk, regulatory risk, cultural risk, and operational risk. Subsequently, each of these risks will be analyzed in accordance with the stages of the Bayesian Network, which include strength analysis, scenario analysis, and sensitivity analysis.

Figure 4. 3 *Prior Probabilities Risk Mitigation in Central Bank*

4.3 Strength Analysis in Bayesian Network

After obtaining the prior probability values from experts, based on the input of parent node values and the conditional probability table, the next step is determining the relationships among variables within the network structure. Strength analysis is conducted to identify and understand the potential causal relationships between the analyzed variables using Euclidean distance. Figure 4.4 illustrates the strength of influence within the Bayesian Network structure for risk mitigation in the central bank, indicated by the thickness of the arcs. Strength analysis assists the researcher in understanding the possible cause-and-effect directions, where the width of each arc reflects the strength of the corresponding pathway.

Figure 4. 4 *Strength Analysis in Prior Probabilities*

Table 4.1 presents the results of the static influence analysis using the Euclidean distance function in GeNIe for the established Bayesian Network model. The average values are calculated using the arithmetic mean of the distances, while the maximum values represent the most significant distance observed within the distribution.

Table 4. 1 *Strength analysis of the Bayesian Network model*

Based on the results of the strength analysis presented in Table 4.1, the highest average score is 0.416, and the maximum score is 0.620, indicating that operational risk is the most significant factor influencing optimal risk mitigation in the central bank. As a mitigation measure for technology risk, the security system shows a strong influence on risk mitigation in the central bank, with an average score of 0.262 and a maximum score of 0.393. Additionally, there is a notable influence of good governance on operational risk, with an average score of 0.253 and a maximum score of 0.375 and the influence of environmental and sustainability risk on regulatory risk, with an average score of 0.247 and a maximum score of 0.364.

4.4 Scenario Analysis

One of the strengths of Bayesian Network analysis is its ability to perform scenario analysis or "what-if" analysis. This scenario analysis is conducted to determine how certain variables of focus (end states determined through expert elicitation) would be affected if changes occur in other variables. Changes in variables within the Bayesian Network structure will be reflected in changes in the posterior probabilities of those variables. In the focus group discussion and questionnaire sessions, experts were facilitated to identify the most significant potential risks that may hinder the digital transformation process in the central bank. The sequence of risks selected by the experts is as follows:

Table 4. 2 *Potential Risks in Central Bank*

Scenario analysis was conducted based on the likelihood of risk occurrences in the central bank. Based on the experts' selections, five scenario analyses were carried out to assess the potential occurrence of each identified risk.

1. *First Scenario: Cybersecurity vulnerability is a high-risk possibility.*

If a cybersecurity risk occurs within the central bank, a likely concurrent scenario is the presence of a weak security system. Consequently, the scenario that may unfold is as follows:

Figure 4. 5 *Analysis of the first scenario*

Based on the scenario analysis conducted under the condition where cybersecurity is at a high level, it also indicates that the security system is in a weakened state. In this context, the optimal risk mitigation the central bank can achieve is 37%. This suggests that cybersecurity risks can reduce the potential for optimal mitigation from 42% to 37%. This assumption implies that in the event of a cyberattack targeting the central bank, it is necessary to maximize mitigation efforts, particularly concerning technology-related risks. Concerning the increasing use of Artificial Intelligence (AI) and Big Data, especially in the financial sector and central banking, this trend inevitably leads to an increased potential for risk. The dependency of generative AI systems on data further amplifies existing challenges related to data security and privacy. This is also supported by recent research findings by Aldasoro et al. (2024) the use of AI and Big Data in central banks specifically has the potential to increase risks and introduce new challenges to the system security framework for regulatory and supervisory authorities. Cyber risks in central banks may include social engineering attacks, such as unauthorised access to the central bank's internal network, which could potentially result in system shutdowns and ransom demands, as well as the inadvertent disclosure of sensitive data. These types of attacks can potentially erode public confidence in the central bank and, under severe circumstances, could jeopardise the overall stability of the financial system.

2. *Second Scenario: Third-Party Risk as a high-risk possibility*

The potential occurrence of third-party risk may give rise to additional risks, such as unexpected costs, increased resource constraints, and limited capabilities. Accordingly, the scenario involving third-party risk concerning optimal risk mitigation is as follows:

Figure 4. 6 *Analysis of the second scenario*

Based on the second scenario analysis, if a third-party risk occurs at a high level (100%), it would consequently lead to unexpected costs (high, 100%), resource constraints (high, 100%), and limited digital capabilities (high, 100%), resulting in a optimal risk mitigation level of 37%, which is a 5% decrease from the current prior condition. Third-party risk in the context of a central bank refers to the risk arising from an institution's dependency on one or more services provided by external third-party vendors, whether directly or indirectly, where failures or disruptions in those services can affect the institution’s operations. Therefore, such dependency must be supported by appropriate mitigation strategies and proactive measures to avoid the emergence of cybersecurity threats and reputational risks. This is supported by the Basel Comitee (2010) which states that financial institutions should develop a comprehensive and integrated third-party risk management framework to effectively manage arrangements with external service providers. Consequently, proper assessment of third-party service usage, digital transformation regulations, and digital resource management is essential, particularly given the need for integration across multiple systems.

3. *Third Scenario: Flawed Innovation is a high-risk possibility*

Flawed innovation represents the third potential risk within the central bank. Based on the likelihood of third-party risk, other associated risks that may also emerge include unexpected costs. Accordingly, the scenario of flawed innovation risk concerning optimal risk mitigation is as follows:

Figure 4. 7 *Analysis of the third scenario*

Based on the scenario analysis conducted when flawed innovation occurs during the digital transformation process, several potential risks may arise, such as flawed innovation and unexpected costs. Under the flawed innovation scenario, the resulting level of optimal risk mitigation is 41%. Flawed innovation is viewed as a failure in system design. In the context of digital transformation models in government, it refers to transformation processes that do not align with the intended vision and goals. The absence of appropriate standards in implementing digital transformation is also a contributing factor that institutions must consider to avoid uncertainty. Uncertainty refers to situations where events and outcomes cannot be quantitatively measured through probabilities, whereas risk refers to situations where historical data allows for determining probabilities (Knight et al., 1964). This highlights the need for a clear vision and the presence of transformative digital leadership capable of monitoring and steering the transformation process comprehensively. This finding aligns with studies on innovation in the public sector conducted by Gomes et al. (2025) and Azwar et al. (2024), which emphasises that the sustainability of innovation initiatives depends on the ability of strategic leaders to establish appropriate governance structures to address flawed innovations and uncertainties, as well as to manage risks effectively.

4. *Fourth Scenario: Digital Talent Exodus is a high-risk possibility.*

When a digital talent exodus occurs in the central bank, the potential risks that may arise include:

Figure 4. 8 *Analysis of the fourth scenario*

Based on the potential risks associated with a digital talent exodus, other related risks that may arise include unexpected costs (high, 100%), resource constraints (high, 100%), and limited digital capabilities (high, 100%). As a result, the level of optimal risk mitigation achievable is 37%, reflecting a 5% decrease compared to the current mitigation level in the central bank. This indicates the necessity of a comprehensive "talent retention" strategy alongside the ongoing digital transformation within the central bank. Such a strategy may involve career development and continuous training, fostering a positive and inclusive work environment, and recognizing employee contributions. This aligns with the findings of Montero Guerra et al. (2023) which emphasizes that digital talent management strategies must adapt to the evolving processes of digitalization within organizations. In addition, robust digital transformation initiatives must be supported by a well-defined strategic vision and a well-designed framework for managing and governing digital talent.

5. *Fifth Scenario: National ICT Regulatory Changes*

When national ICT regulatory changes occur during the digital transformation process within an organization, the possible scenario that may unfold is as follows:

Figure 4. 9 *Analysis of the fifth scenario*

The probability of national ICT regulatory changes may lead to the emergence of additional risks, such as non-standardised risk assessment (high, 100%) and compliance with national standards (high, 100%). This indicates that when regulatory risks related to international ICT frameworks arise, the optimal scenario indicator remains at a high level of 41%. This suggests that there is no significant change in the level of optimal risk mitigation. This outcome implies that the standards and regulations already in place within the central bank are more advanced and robust compared to the existing national standards concerning digital transformation.

4.5 Backpropagation Analysis

Figure 4. 10 *Backpropagation Analysis*

Following the backpropagation process using the Bayesian Network model, several risk values, such as operational risk (8%), cultural risk (34%), regulatory risk (30%), financial risk (31%), and technology risk (23%), showed a decrease. By optimizing the overall risk mitigation value to 100%, specific mitigation nodes, such as good governance (62%) and security system (54%), need to be increased by 8% and 3%, respectively. These results indicate that risk mitigation efforts must be enhanced, particularly those related to good governance. In this context, organizational governance, especially in digital transformation, must be strengthened through support for digitally centralized operational processes. Digital transformation can facilitate the automation of governance functions, thereby promoting efficiency. Moreover, a well-structured digital governance framework can enhance certainty and reduce the tolerance for erroneous transactions. In addition, in line with the findings of Hanisch et al. (2023), good governance in the context of digitalization is considered a critical factor in supporting organizations, value creation, and value capture.

The security system plays a crucial role in enhancing optimal risk mitigation. In the central bank's case, an increase of 3% in the security system is required to improve technology risk mitigation. During the digital transformation process within the central bank, the risks encountered include cyber risk, third-party risk, and the risk of flawed innovation. This highlights the need for appropriate measures to address the various technological risks within the central bank to achieve optimal risk mitigation. Furthermore, concerning regulatory risk, a reduction of 1% is needed to reach the desired level of optimal mitigation. A potential strategy involves ensuring compliance with the national regulatory framework and standards governing digital transformation initiatives. These regulations may include provisions for the use of AI and Big Data in central bank use cases, which are intended to support the central bank's functions and mandates as a policy maker.

Cultural risk is one of the key focus areas that must be reduced within the central bank. Based on the backpropagation analysis, cultural risk needs to be decreased by 1% from the current prior level to achieve optimal risk mitigation. Qualitative analysis from the focus group discussion indicates that a paradigm shift is required in addressing cultural risk mitigation. This paradigm shift involves not only the integration of technological advancements but also the redefinition of institutional mindset, work culture, strategic direction, and the utilization of digitalization as a primary driver in fulfilling the institution’s mandate.

In financial risk, a reduction of 3% is required to enhance risk mitigation efforts within the central bank. Digital transformation is closely associated with significant investments in technological resources and human capital, necessitating accurate budget planning in line with the demands of appropriate technological innovation. It is essential to consider a complex set of costs and benefits for various stakeholders, particularly for policymakers, to align technology investments with the objectives of achieving optimal digital transformation (Yunis et al., 2024). Financial risk events in digital transformation are often triggered by other ongoing risks, such as cyber risks, flawed innovation, third-party failures, or other related threats. Therefore, risk mitigation strategies should include budget efficiency measures and financial audits specifically tailored to the domain of digital transformation.

Table 4. 3 *Result of Backpropagation Analysis*

To attain optimal risk mitigation, operational risk emerges as the primary focus that needs to be reduced to a probability level of 8%, achieved through a 21% risk reduction. Subsequently, technological risk becomes the second priority, which should be minimized to 7% to optimize the effectiveness of the risk mitigation policy. In line with this, the probability values of cybersecurity vulnerabilities and third-party risk did not change significantly when the end-state was maximized. Nevertheless, this condition is reflected in the child node of technological risk, as demonstrated by the conditional probability table (CPT), indicating that a 3% increase in the policy action of enhancing the security system is required to achieve optimal risk mitigation. Therefore, although technological risk does not appear prominently in positive inference from a probabilistic perspective, it remains a significant priority for mitigation.

4.6 Scenario Analysis: Combination of Expert Judgement and Strength Analysis

Scenario analysis was also conducted based on a combination of expert judgment and strength analysis, along with appropriate mitigation measures, to achieve a high likelihood of risk mitigation. Consequently, the scenario developed is as follows:

Figure 4. 11 *Combination of Scenario Analysis*

Table 4. 4 *Combination of Scenario Analysis on Optimal Risk Mitigation*

Based on the risk analysis conducted by combining several risks, such as non-standardized regulation (Low), third-party risk (Low), cybersecurity vulnerabilities (Low), and flawed innovation (Low), along with mitigation measures such as a high level of security system and good governance, the optimal risk mitigation that can be achieved is 53%. In line with this, when viewed from the target node, namely high optimal risk mitigation, good governance emerges as a variable with significant influence on achieving optimal risk mitigation at Bank Indonesia. This also indicates that good governance at Bank Indonesia has been appropriately executed, thereby contributing substantially to optimal risk mitigation within the central bank. This finding is consistent with previous research by Yan (2025), which asserts that the ability to innovate must be accompanied by strong and effective organizational governance. Specifically, improvements to the security system are also a significant factor influencing optimal risk mitigation. Therefore, adequate investment and enhancement of robust systems are necessary to support practical mitigation efforts. Cybersecurity risks must be addressed through appropriate mitigation measures and the reduction of potential threats. As highlighted in recent research by Arunthavanathan et al. (2025), institutional digitalization requires strengthening cybersecurity through threat modeling, cyber-attack detection, response mitigation, and resilience. Developing a well-designed and resilient framework to secure the digital environment and strategies for mitigating attacks and enhancing institutional resilience is essential for ensuring a robust and reliable security system.

4.7 Sensitivity Analysis

Figure 4. 12 *Sensitivity Analysis*

Figure 4. 13 *Sensitivity by Tornado Analysis*

One of the capabilities of a Bayesian Network is the ability to carry out sensitivity analysis on target nodes in response to changes in the evidence provided. In this research, a sensitivity analysis is used to determine which nodes or variables are most affected by changes in the mitigation process within the digital central bank. The optimal risk mitigation is considered the target node, while other variables serve as evidence and countermeasure nodes. Figure 4.12 shows the optimal risk mitigation nodes, which are directly influenced by five variables: technological risk, financial risk, cultural risk, organizational risk, and regulatory risk. Furthermore, a sensitivity analysis was conducted using scenarios based on expert judgment, along with a strength analysis under the following assumptions: good governance (high at 100%), security system (high at 100%), non-standardized risk assessment (low at 100%), third-party risk (low at 100%), cyber security (low at 100%), and flawed innovation (low at 100%). Based on this analysis, the sensitivity analysis indicates that the scenario analysis leads to changes in the following nodes: technology risk, resource constraint, and limited digital capabilities.

Figure 4.13 presents a sensitivity analysis using a tornado diagram that visualizes the sensitivity of digital transformation risk mitigation. The horizontal axis in the diagram represents the absolute change in the posterior probability of the risk mitigation process. The length of each bar in the diagram reflects the intensity of impact from specific nodes on the target node, which in this case is optimal risk mitigation. Furthermore, the tornado analysis indicates that the combination of policies that can be implemented and yields a high probability of achieving optimal risk mitigation (target value range 0.276254) includes low technological risk, combined with a high level of security systems, low third-party risk, low cybersecurity vulnerabilities, high sustainable innovation, and low flawed innovation. This suggests that optimal risk mitigation in digital transformation can be enhanced by minimizing technology-related risks through appropriate interventions in technology development. This includes reducing third-party risks, cybersecurity threats, and the likelihood of flawed innovations. Additionally, resource constraint also emerges as a sensitive variable in relation to enhancing optimal risk mitigation in digital transformation (target value range 0.270886). Resource constraints represent one of the key limitations that can hinder the digital transformation process in central banks, both in terms of capabilities and infrastructure. Therefore, capacity-strengthening interventions, such as training programs and governance improvements, effectively address resource constraints in the digital transformation process. Appropriate regulations and financial support must support such efforts throughout the transformation process.

Table 4. 5 *Value of Net Effect on Optimal Risk Mitigation*

Based on the results of the sensitivity analysis using the net effect values (Table 4.5), it can be concluded that the Technology Risk variable has the most significant influence on Optimal Risk Mitigation, with a maximum value reaching 0.09. This indicates that changes in technological risk have the potential to produce the greatest impact on the overall success of risk mitigation efforts. In contrast, other variables such as Financial Risk, Regulatory Risk, and Operational Risk demonstrate much smaller net effect values, with maximums not exceeding 0.019, indicating that their contributions are relatively limited to the outcome of optimal risk mitigation. These findings underscore the need to prioritize the management of technological risks within the context of digital transformation at the central bank, as the high dependency on technology carries considerable consequences for the effectiveness of overall risk mitigation efforts.

4.8 Cluster-Based Analysis

A cluster-based analysis was conducted to further examine the impacts and identify the most appropriate policy scenarios for central banks' risk mitigation processes.

4.8.1 Internal Management Cluster

The internal management cluster in the risk mitigation process encompasses departments responsible for governance and risk management within an institution. Based on the results presented in Figure 4.4, operational risk emerges as a highly influential factor in the risk mitigation process. Therefore, an in-depth analysis is necessary to identify the internal organizational factors that support effective risk mitigation.

Figure 4. 14 *Strength Analysis in Internal Management Cluster*

Figure 4. 15 *Scenario Analysis in Internal Management Cluster*

Figure 4. 16 *Sensitivity Analysis in Internal Management Cluster*

Figure 4. 17 *Sensitivity Analysis (Tornado) in Internal Management Cluster*

The Bayesian Network analysis conducted within the internal management cluster, by integrating data from each expert, indicates that operational risk is the node with the strongest influence on the optimisation of risk mitigation efforts. As shown in Figure 4.14, within the category of operational risk, the most influential node is good governance. This suggests that good governance practices within the central bank have been implemented at a high level, thereby indicating that risk mitigation has been effectively applied in the operational domain. The effective implementation of operational risk management can be supported by well-structured regulations concerning digitalisation processes and the utilisation of technologies powered by data and artificial intelligence, particularly within the central bank environment. AI is also expanding in line with growing awareness and high adoption rates among employees, especially in enhancing productivity. However, on the other hand, the inappropriate use of AI may pose potential risks, such as data poisoning and misguided policies if not applied carefully. Therefore, implementing national technology policies and global cybersecurity regulations plays a crucial role in supporting the success of digital transformation, particularly within government institutions. Supported by the study of Uddin et al. (2023) it is emphasised that the rapid pace of digital transformation within organisations necessitates formulating appropriate operational risk mitigation strategies. These strategies should consider organizational support for technological investment, considering the speed of technological advancement, resource constraints, and the institution's financial capacity. Therefore, effective risk mitigation measures to minimize potential operational risks must be thoroughly analysed. This includes policy alignment of systems with the latest models and use cases within central banks and the need for digitally literate human resources with strong capabilities to support operational functions in the context of digital transformation.

4.8.2 Digital Cluster

The Digital Cluster is intended to examine departments that focus on digitalization and technological innovation within the institution. This refers to the policies and decisions made regarding potential risks and the necessary mitigation measures.

Figure 4. 18 *Strength Analysis in Digital Cluster*

Figure 4. 19 *Scenario Analysis in Digital Cluster*

Figure 4. 20 *Sensitivity Analysis in Digital Cluster*

Figure 4. 21 *Sensitivity Analysis (Tornado) in Digital Cluster*

The Bayesian network analysis conducted within the digital cluster reveals that technology risk is the second most significant risk directly influencing optimal risk mitigation in the digital transformation process of central banks. The security system emerges as the node with the most significant impact on achieving optimal mitigation. This indicates a crucial focus on enhancing system security, particularly in relation to cyber defense and data protection. In the financial sector, especially in central banks, these institutions are primary targets of increasingly sophisticated and complex cyberattacks. These threats range from direct financial losses caused by hacking and ransomware to operational disruptions that can paralyze organizational systems, such as those resulting from Distributed Denial of Service (DDoS) attacks. Furthermore, advancements in Artificial Intelligence (AI), while offering positive contributions to technological sophistication, also amplify the potential for harmful attacks. This is closely linked to the vast volume of personal and financial data held by central banks, making data protection a critical and ongoing challenge.

The sensitivity analysis of the risk mitigation scenario involving enhanced security systems and sustainable innovation demonstrates that a high level of optimal risk mitigation can be achieved through good governance, low resource constraints, and low third-party risk. One of the key challenges in the digital transformation process relates to the availability of supporting resources and in-depth industry knowledge. Therefore, governance related to the fulfilment of resource needs, particularly professionals in cybersecurity and digital innovation to support sustainable innovation, is essential.

5. Conclusion and Policy Recommendation

5.1 Conclusion

In the era of digital transformation, institutions, especially central banks, encounter rapid changes that not only offer opportunities but also heighten the complexity of risks that must be carefully managed. Consequently, risk mitigation becomes a vital element in ensuring the success of a sustainable and secure digital transformation. A structured, data-driven approach to identifying, measuring, and controlling risks is essential to guarantee that every policy and digital innovation can be implemented effectively without compromising the institution's operational stability.

The systems thinking approach used in this study provides a comprehensive view of potential risks and their corresponding mitigation policies. During the digital transformation process, various risks may arise, necessitating the implementation of effective risk management strategies. In this study, the risks encountered by the central bank are categorized into several types: technology risk, financial risk, regulatory risk, cultural risk, and operational risk. Subsequently, to further analyse the quantitative data using the Bayesian network method, the results obtained are as follows:

1. Prior probabilities of the BN Construct based on the Expert CPT Survey result show that the initial Optimal Risk Mitigation has reached 42% and 22% of high and medium classification, respectively.
2. The strength analysis of the prior probabilities shows that effective risk mitigation is greatly affected by operational risk, especially where strong governance has been implemented at a high level in the Central Bank, particularly in Bank Indonesia. Additionally, this finding indicates that operational risk should be a focus in the risk management process at Bank Indonesia.

3. Overall Optimal Risk Mitigation Scenario Analysis: Expert judgment approach: Optimal Risk Mitigation increased by 11%, using the six strongest nodes as evidence
4. Sensitivity analysis shows that combining a low level of technology risk, a high level of security system enhancement, low third-party risk, and reduced cybersecurity vulnerability risk represents the most influential set of factors in driving the central bank toward achieving optimal risk mitigation.
5. Internal Management Cluster: Operational risk is the node with the strongest influence on achieving optimal risk mitigation. Scenario analysis indicates that enhancing risk mitigation within internal management could lead to a 5% increase in overall optimal risk mitigation.
6. Digital Cluster: The most influential node in risk mitigation within the digital cluster is system security enhancement. Scenario analysis indicates that optimizing mitigation strategies, particularly through system security enhancement and sustainable innovation, can improve optimal risk mitigation by 5%.

These findings challenge the common view that often places excessive emphasis on technological or cyber risks in digital transformation, while highlighting the importance of strengthening internal governance (good governance), which represents a significant contribution to the development of risk management theory in the public sector. In this study, Bank Indonesia is a central bank that is also operating the national payment system. The most important risk then may be different for central banks that do not run their national payment systems. This study is expected to serve as a theoretical foundation for risk mitigation, particularly within public sector institutions. Future research is expected to expand this model by incorporating external stakeholders into the modeling process, as well as evaluating the dynamic evolution of risk profiles in line with increasing digital maturity in central banks.

5.2 Policy Recommendation

Based on the findings of this study, it is crucial for policymakers and institutional leaders, particularly within central banks, to adopt a proactive and structured approach in addressing the various risks emerging from the digital transformation process. As central banks and other public institutions increasingly rely on digital technologies to enhance operational efficiency and achieve organizational objectives, the need for comprehensive and forward-looking risk mitigation strategies becomes increasingly urgent. Therefore, this study highlights that maintaining risk mitigation measures, as illustrated in scenarios such as strengthening good governance, implementing robust technological mitigation, and improving regulatory frameworks, can enhance the probability of achieving optimal risk mitigation by 11% through the reinforcement of six key mitigation nodes. The following policy recommendations are formulated to support the development of a resilient digital transformation, ensure institutional preparedness in responding to technological advancements, and promote sustainable innovation amid the evolving dynamics of technology and regulation.

1. Establishing standardized frameworks and defined requirements is essential for guiding the digital transformation process at Bank Indonesia, ensuring that each stage is executed clearly and in alignment with governance principles. This necessity is underscored by the critical role of operational risk, identified as the most influential factor in achieving effective risk mitigation throughout the transformation journey. The implementation of the Strategic Risk Assessment should be designed and executed by leveraging the achievements attained

through Operational Risk Management. This integration strengthens institutional capacity to identify, evaluate, and prioritize strategic risks in a more comprehensive manner. Furthermore, the development of a multilayered perspective is essential to anticipate potential risk blindsides, risks that are difficult to predict yet may generate a significant impact if inadequately managed. This approach ensures that the assessment process not only focuses on observable risks (known risks) but also accounts for broader strategic environmental dynamics, including external factors that may be disruptive.

2. Enhancing the security system is essential for strengthening the technological infrastructure and supporting the ongoing digital transformation processes at Bank Indonesia, as this mitigation measure reduces potential risks arising from cyber threats and third-party vulnerabilities. This enhancement can be pursued through a comprehensive cybersecurity gap assessment that encompasses both the central bank's cyber resilience and the preliminary security assurance research and activities required for fintech adoption. In addition, it necessitates the reinforcement of cybersecurity risk management and security assurance practices throughout the evaluation, development, and procurement of both new and existing information technology projects and systems.

3. Financial risk in central banks is considered to have relatively low potential. However, the formulation of financial policies must align with applicable regulations and apply the principles of transparency, accountability, and effectiveness. Effectiveness in this context includes the need for good governance of each investment made by the central bank, to ensure that such investments do not lead to flawed innovation. In addition, an investigative process for each project is also necessary to support accountability and the accuracy of funding allocation.

4. A robust regulatory framework related to technical regulations and governance structures, the integration of personal data protection within institutional management, and regulations governing data and artificial intelligence (AI) technologies need to be developed in an integrated and comprehensive manner. This is essential to strengthen the digital transformation process in central banks.

5. A paradigm shift is required to mitigate cultural risks within the central bank. This must be supported by increased awareness of the digitalization process to enhance task efficiency and avoid the persistence of legacy systems. In addition, organizational support is crucial to foster the development of human resource capabilities in digital that can adapt more rapidly to digital transformation.

References

Agostino, D., Arnaboldi, M., & Lema, M. D. (2020). New development: COVID-19 as an accelerator of digital transformation in public service delivery. *Public Money and Management*. https://doi.org/10.1080/09540962.2020.1764206

Aldasoro, I., Doerr, S., Gambacorta, L., Notra, S., Oliviero, T., & Whyte, D. (2024). Generative Artificial Intelligence and Cyber Security in Central Banking. *Journal of Financial Regulation*, *145*. https://doi.org/10.1093/jfr/fjae008

Ali, I., & Govindan, K. (2023). Extenuating operational risks through digital transformation of agri-food supply chains. *Production Planning and Control*, *34*(12). https://doi.org/10.1080/09537287.2021.1988177

Arunthavanathan, R., Khan, F., Sajid, Z., Amin, M. T., Kota, K. R., & Kumar, S. (2025). Are the processing facilities safe and secured against cyber threats? *Reliability Engineering and System Safety*, *260*(September 2024), 111011. https://doi.org/10.1016/j.ress.2025.111011

Azwar, P., Harun, C. A., & Khoirunnisa, A. N. (2024). Institutional Transformation Effectiveness In Digital Era: The Case Of Bank Indonesia. In *Bank Indonesia Working Papers*.

Bank for International Settlements. (2025). *Consultative Group on Risk Management Governance of AI adoption in central banks* (Issue January).

Basel Comitee. (2010). Basel Committee on Banking Supervision Consultative Document Principles for enhancing corporate governance. *October*, *March*, 34.

Basel Committee on Banking Supervision. (2005). International Convergence of Capital Measurement and Capital Standards for Banks - A Revised Framework (Basel II)-Updated. In *Bank for International Settlement Paper* (Vol. 52, Issue November).

Bason, C. (2010). Leading public sector innovation: Co-creating for a better society. In *Leading Public Sector Innovation: Co-Creating for a Better Society*. https://doi.org/10.1332/policypress/9781847426345.001.0001

Bolstad, W. M. (2007). Introduction to Bayesian Statistics: Second Edition. In *Introduction to Bayesian Statistics: Second Edition*. https://doi.org/10.1002/9780470181188

Calin Alexandru, S. (2023). *Digital Transformation Vulnerabilities: Assessing The Risks And Strengthening Cyber Security*.

Crawford, K. (2022). Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. *Perspectives on Science and Christian Faith*, *74*(1). https://doi.org/10.56315/pscf3-22crawford

Criado Perez, C. (2020). Caroline Criado Perez. Invisible Women: Data Bias in a World Designed for Men. In *Vintage*.

Eggers, W. D., & Singh, S. K. (2009). *The Public Innovator's Playbook. Deloitte Research and the Ash Institute for Democratic Governance at the Harvard Kennedy School Of Government, Canada*.

Enyoghasi, C., & Badurdeen, F. (2023). Bayesian belief network-based risk likelihood assessment for sustainable product design decision making. *Journal of Cleaner Production*, *425*. https://doi.org/10.1016/j.jclepro.2023.138909

European Central Bank. (2023). *Digital transformation requires strong governance and steering*.

Fenton, N., & Neil, M. (2012). Risk assessment and decision analysis with bayesian networks. In *Risk Assessment and Decision Analysis with Bayesian Networks*. https://doi.org/10.1201/b21982

Fletcher, G., & Griffiths, M. (2020). Digital transformation during a lockdown. *International Journal of Information Management*, *55*. https://doi.org/10.1016/j.ijinfomgt.2020.102185

Fountain, J. (2019). The Wicked Nature of Digital Transformation: A policy perspective. *Dubai Policy Review*, *1*(1). https://doi.org/10.46993/dpr/en005

Gomes, L. A. de V., Chaparro, X. A. F., Maniçoba, R. F., Borini, F. M., & Silva, L. E. (2025). Transformation of the governance of failure for radical innovation: The role of strategic leaders. *Research Policy*, *54*(1), 105108. https://doi.org/10.1016/j.respol.2024.105108

Grover, V., Tseng, S. L., & Pu, W. (2022). A theoretical perspective on organizational culture and digitalization. *Information and Management*, *59*(4). https://doi.org/10.1016/j.im.2022.103639

Hanisch, M., Goldsby, C. M., Fabian, N. E., & Oehmichen, J. (2023). Digital governance: A conceptual framework and research agenda. *Journal of Business Research*, *162*. https://doi.org/10.1016/j.jbusres.2023.113777

Hashai, N., Kafouros, M., & Buckley, P. J. (2018). The Performance Implications of Speed, Regularity, and Duration in Alliance Portfolio Expansion. *Journal of Management*, *44*(2). https://doi.org/10.1177/0149206315592030

Hivo. (2023). *How to Conduct a Risk Assessment for Digital Transformation*. https://hivo.co/blog/how-to-conduct-a-risk-assessment-for-digital-transformation#:~:text=Risk assessment is a systematic process that,threats%2C and creating strategies to manage and

Kane, G. C., Palmer, D., Phillips, A. N., Kiron, D., & Buckley, N. (2017). Achieving Digital Maturity. *MIT Sloan Management Review*, *59180*.

Knight, F., Of, R., & Classics, E. (1964). Risk, Uncertainty and Profit. *Climate Change 2013 - The Physical Science Basis*, *XXXI*.

Kolagar, M., Parida, V., & Sjödin, D. (2022). Ecosystem transformation for digital servitization: A systematic review, integrative framework, and future research agenda. *Journal of Business Research*, *146*. https://doi.org/10.1016/j.jbusres.2022.03.067

Laimon, M., Yusaf, T., Mai, T., Goh, S., & Alrefae, W. (2022). A systems thinking approach to address sustainability challenges to the energy sector. *International Journal of Thermofluids*, *15*. https://doi.org/10.1016/j.ijft.2022.100161

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data and Society*, *1*(2). https://doi.org/10.1177/2053951714541861

Matzler, K., Friedrich von den Eichen, S., Anschober, M., & Kohler, T. (2018). The crusade of digital disruption. In *Journal of Business Strategy* (Vol. 39, Issue 6). https://doi.org/10.1108/JBS-12-2017-0187

Meadows, D. H. (2008). Thinking in systems : a primer / Donella H. Meadows ; edited by Diana Wright. In *Thinking in systems : a primer*.

Meijer, A. (2018). Datapolis: A Public Governance Perspective on “smart Cities.” *Perspectives on Public Management and Governance*, *1*(3). https://doi.org/10.1093/ppmgov/gvx017

Miller, C. M. (1998). Banishing Bureaucracy: The Five Strategies for Reinventing Government. *Political Science Quarterly*, *113*(1). https://doi.org/10.2307/2657683

Moosa, I. A. (2007). *The Management of Operational Risk BT - Operational Risk Management* (I. A. Moosa (ed.); pp. 198–225). Palgrave Macmillan UK. https://doi.org/10.1057/9780230591486_8

Mulgary, G., & D, A. (2003). *Innovation in the Public Sector. Strategy Unit, Cabinet Office*.

OECD. (2024). *2023 OECD Digital Government Index: Results and key findings*.

Oludapo, S., Carroll, N., & Helfert, M. (2024). Why do so many digital transformations fail? A bibliometric analysis and future research agenda. *Journal of Business Research*, *174*. https://doi.org/10.1016/j.jbusres.2024.114528

Pleune, T. (2017). *Operational Risk Management BT - Commercial Banking Risk Management: Regulation in the Wake of the Financial Crisis* (W. Tian (ed.); pp. 121–134). Palgrave Macmillan US. https://doi.org/10.1057/978-1-137-59442-6_6

Roszkowski, M. J., & Grable, J. E. (2009). Evidence of lower risk tolerance among public sector employees in their personal financial matters. *Journal of Occupational and Organizational Psychology*, *82*(2). https://doi.org/10.1348/096317908X337725

Santiso, C. (2022). Govtech against corruption: What are the integrity dividends of government digitalization? *Data and Policy*, *4*(3). https://doi.org/10.1017/dap.2022.31

Schlüter, L., Kørnøv, L., Mortensen, L., Løkke, S., Storrs, K., Lyhne, I., & Nors, B. (2023). Sustainable business model innovation: Design guidelines for integrating systems thinking principles in tools for early-stage sustainability assessment. *Journal of Cleaner Production*, *387*. https://doi.org/10.1016/j.jclepro.2022.135776

Senge, P. M., & Sterman, J. D. (1992). Systems thinking and organizational learning: Acting locally and thinking globally in the organization of the future. *European Journal of Operational Research*, *59*(1). https://doi.org/10.1016/0377-2217(92)90011-W

Singh, A. K., Pathak, D. K., & Patra, S. (2023). An integrated systems thinking approach for achieving sustainability in project-based organizations. *Systems Research and Behavioral Science*, *40*(3). https://doi.org/10.1002/sres.2892

Slassi-sennou, S., & Elmouhib, S. (2025). Managing Financial and Operational Risks Through Digital Transformation: The Mediating Influence of Information and Communication Technologies' Adoption and Resistance to Change. *Journal of Risk and Financial Management*, *18*(3), 128.

Sørensen, E., & Torfing, J. (2016). Enhancing public innovation through collaboration, leadership and new public governance. In *New Frontiers in Social Innovation Research*. https://doi.org/10.1057/9781137506801_8

Strome, T. (2023). Navigating digital transformation in airports: A disciplined approach to project portfolio selection and execution. *Journal of Airport Management*, *17*(4). https://doi.org/10.69554/gwej7445

Sun, B., Zhang, Y., Zhu, K., Mao, H., & Liang, T. (2024). Is faster really better? The impact of digital transformation speed on firm financial distress: Based on the cost-benefit perspective. *Journal of Business Research*, *179*, 114703. https://doi.org/https://doi.org/10.1016/j.jbusres.2024.114703

Uddin, M. H., Mollah, S., Islam, N., & Ali, M. H. (2023). Does digital transformation matter for operational risk exposure? *Technological Forecasting and Social Change*, *197*. https://doi.org/10.1016/j.techfore.2023.122919

Uffe B. Kjærulff, A. L. M. (2013). Bayesian Networks and Influence Diagrams: A Guide to Construction and Analysis. In *Angewandte Chemie International Edition, 6(11), 951–952.*

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. In *Journal of Strategic Information Systems* (Vol. 28, Issue 2). https://doi.org/10.1016/j.jsis.2019.01.003

Wang, H., Mao, K., Wu, W., & Luo, H. (2023). Fintech inputs, non-performing loans risk reduction and bank performance improvement. *International Review of Financial Analysis*, *90*. https://doi.org/10.1016/j.irfa.2023.102849

Warner, K. S. R., & Wäger, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, *52*(3). https://doi.org/10.1016/j.lrp.2018.12.001

Xie, X., Zang, Z., & Ponzoa, J. M. (2020). The information impact of network media, the psychological reaction to the COVID-19 pandemic, and online knowledge acquisition: Evidence from Chinese college students. *Journal of Innovation and Knowledge*, *5*(4). https://doi.org/10.1016/j.jik.2020.10.005

Xinxian, C., & Jianhui, C. (2022). Digital Transformation and Financial Risk Prediction of Listed Companies. *Computational Intelligence and Neuroscience*, *2022*. https://doi.org/10.1155/2022/7211033

Xu, Y., Pinedo, M., & Xue, M. (2017). Operational Risk in Financial Services: A Review and New Research Opportunities. *Production and Operations Management*, *26*(3). https://doi.org/10.1111/poms.12652

Yan, J. (2025). Assessing the link between digital government development and urban industrial chain resilience : Evidence from public data openness. *Environmental Impact Assessment Review*, *112*(July 2024), 107796. https://doi.org/10.1016/j.eiar.2024.107796

Appendix

Table:

Table 3. 3 Respondent Demographics

Spectrum		Count
Department	Risk Management	6
	Internal Audit	6
	Legal	4
	Internal Finance	10
	Strategic Management and Governance	5
	Digital Service and Cyber Security	7
	Data Digitalization and Innovation	4
	Digital Development and Innovation	5
	Human Resources	5
Job Position	Assistant Manager	9
	Manager	10
	Assistant Director	15
	Deputy Director	18
Education	Bachelor degree	17
	Master's degree	35
	Doctoral degree	0
Employment Duration	1-5 years	8
	6 - 10 years	5
	11 - 15 years	9
	16 - 20 years	16
	> 20 years	12

Table 3. 2 Participants of Focus Group Discussion on ST and BN Model

Participant*	Number of Persons	Role
Internal Audit Department	2	The department responsible for analyzing governance processes and risk mitigation across all departments within the central bank
Internal Finance Department	2	The department is responsible for the central bank's budgeting and financial affairs.
Legal Department	3	The department is responsible for regulatory oversight and the implementation of organizational governance.
Digital Services and Cyber Security Department	1	Cybersecurity and risk mitigation.
Strategic Management and Governance Department	1	The central bank's strategy for implementing an integrated digital central bank.
Risk Management Department	2	Mitigation of risk related to technology and policies in the central bank.

* The explanation of acronyms is provided in the appendix (Table List Acronyms)

Table 4.1 Strength analysis of the Bayesian Network model

Parent Node	Child Node	Average	Maximum	Weighted
Operational Risk	Optimal Risk Mitigation	0.416	0.620	0.416
Security System	Technology Risk	0.262	0.393	0.262
Good Governance	Operational Risk	0.253	0.375	0.253
Environmental & Sustainability Risk	Regulatory Risk	0.247	0.364	0.247
Budget Overruns	Financial Risk	0.246	0.358	0.246
Fixed Mindset	Cultural Risk	0.227	0.327	0.227
Technology Risk	Optimal Risk Mitigation	0.144	0.222	0.144
Third Party Risk	Technology Risk	0.099	0.164	0.099
Resource Constraints	Operational Risk	0.096	0.158	0.096
Non-standardized risk assessment	Regulatory Risk	0.092	0.150	0.092
Unexpected Cost	Financial Risk	0.092	0.148	0.092
Risk Appetite	Cultural Risk	0.086	0.137	0.086
Financial Risk	Optimal Risk Mitigation	0.049	0.074	0.049
Cybersecurity vulnerabilities	Technology Risk	0.034	0.055	0.034
Limited Digital Capabilities	Operational Risk	0.033	0.053	0.033
Regulation on digital transformation	Regulatory Risk	0.032	0.050	0.032
Cost Efficiency	Financial Risk	0.032	0.050	0.032
Legacy System	Cultural Risk	0.030	0.046	0.030
Regulatory Risk	Optimal Risk Mitigation	0.016	0.025	0.016
Sustainable Innovation	Technology Risk	0.012	0.018	0.012
Training	Operational Risk	0.011	0.018	0.011
Compliance to National Standard	Regulatory Risk	0.011	0.017	0.011
Flawed Innovation	Financial Risk	0.011	0.017	0.011
Shifting Paradigm	Cultural Risk	0.010	0.015	0.010
Cultural Risk	Optimal Risk Mitigation	0.005	0.008	0.005
Flawed Innovation	Technology Risk	0.004	0.006	0.004
Governance Misalignment	Operational Risk	0.004	0.006	0.004
Governance Misalignment	Regulatory Risk	0.004	0.006	0.004
Limited Digital Capabilities	Cultural Risk	0.003	0.005	0.003

Table 4. 2 Potential Risks in Central Bank

Potential Risk	Definition	Quantity
Digital Talent Exodus	The phenomenon of the departure of workforce in the digital and ICT sectors from an organization or industry.	6
Flawed Innovation	Inadequate system design, hardware failures, capacity issues related to data dependency, and the characteristics of AI models that are highly reliant on data.	18
Cybersecurity Vulnerabilities	Vulnerabilities in sensitive assets and personal data, misuse of personal data by AI models, exposure of confidential information due to weak cybersecurity controls, and data poisoning.	27
Third Party Risk	Incidents arising from dependency on technology providers developed by external third parties, including privacy breaches, operational disruptions, compliance failures, and cybersecurity threats.	17
Changes in National ICT Regulation	Changes in national ICT regulations (legal uncertainties and policy evolution related to ICT)	4

Table 4. 3 Result of Backpropagation Analysis

Node	Prior	Posterior	Explanation
Measured Risk Dimension			
Technology Risk	30%	23%	Must be reduced by 7%
Financial Risk	31%	31%	No Significant Change
Regulatory Risk	31%	30%	Must be reduced by 1%
Cultural Risk	34%	34%	No Significant Change
Operational Risk	29%	8%	Must be reduced by 21%
Third Party Risk	49%	48%	Must be reduced by 1%
Cyber Security Vulnerabilities	51%	51%	No Significant Change
Flawed Innovation	34%	34%	No Significant Change
Budget Overruns	34%	33%	Must be reduced by 1%
Unexpected Cost	33%	32%	Must be reduced by 1%
Environmental and Sustainability Risk	27%	27%	No Significant Change
Non-standardized risk assessment	29%	29%	No Significant Change
Legacy System	34%	34%	No Significant Change
Risk Appetite	31%	31%	No Significant Change
Fixed Mindset	35%	35%	No Significant Change
Resource Constraint	43%	40%	Must be reduced by 3%
Limited Digital Capabilities	29%	28%	Must be reduced by 1%
Governance and Compliance Misalignment	25%	25%	No Significant Change
Measured Risk Mitigation			
Enhance Security System	51%	54%	Must be increased by 3%
Sustainable Innovation	49%	49%	No Significant Change
Cost Efficiency	43%	43%	No Significant Change
Regulation on digital transformation	47%	47%	No Significant Change
Compliance to National Standard	49%	49%	No Significant Change
Shifting Paradigm	48%	48%	No Significant Change
Good Governance	54%	62%	Must be increased by 8%
Training	47%	47%	No Significant Change

Table 4. 4 Combination of Scenario Analysis on Optimal Risk Mitigation

Variable	**Prior Probability**	**Scenarios Evidence**					
		Security System (High) **a**	**Good Governance (High)** **(a+b)**	**Non-standardised regulation (Low)** **(a+b+c)**	**Third Party Risk (Low)** **(a+b+c+d)**	**Cybersecurity Vulnerabilities (Low)** **(a+b+c+d+e)**	**Flawed Innovation (Low)** **(a+b+c+d+e+f)**
Technological Risk **(Low)**	32%	45%	44%	44%	56%	60%	60%
Regulatory Risk **(Low)**	34%	34%	34%	39%	38%	38%	38%
Operational Risk **(Low)**	36%	36%	48%	36%	36%	36%	36%
Optimal Risk Mitigation **(High)**	42%	44%	51%	51%	53%	53%	**53%**

Note: The scenario analysis was conducted in a stepwise manner, with annotations (a, b, c, ...) used to facilitate understanding when interpreting the results of the scenario analysis. Security system=a, Good governance=b, Non-standardized regulation=c, Third party risk=d, Cybersecurity vulnerabilities=e, Flawed Innovation=f.

Table 4. 5 Value of Net Effect on Optimal Risk Mitigation

Variables	Value of Net Effect
Technology Risk	Max = 0.09
	Min = 0
	Avg = 0
Financial Risk	Max = 0.003
	Min = 0
	Avg = 0
Regulatory Risk	Max = 0.001
	Min = 0
	Avg = 0
Operational Risk	Max = 0.019
	Min = 0
	Avg = 0.001
Optimal Risk Mitigation	Max = 0.015
	Min = 0
	Max = 0.003

List Acronyms

Departments	Acronyms
Internal Audit Department	DAI
Financial Department	DKEU
Law Department	DHK
Digital Services and Cybersecurity Department	DLDS
Strategic Management and Governance Department	DMST
Risk Management Department	DMR
Department of Human Resources	DSDM
Department of Digital Development and Innovation	DPID
Department of Data Innovation and Digitalization	DIDD

Figure:

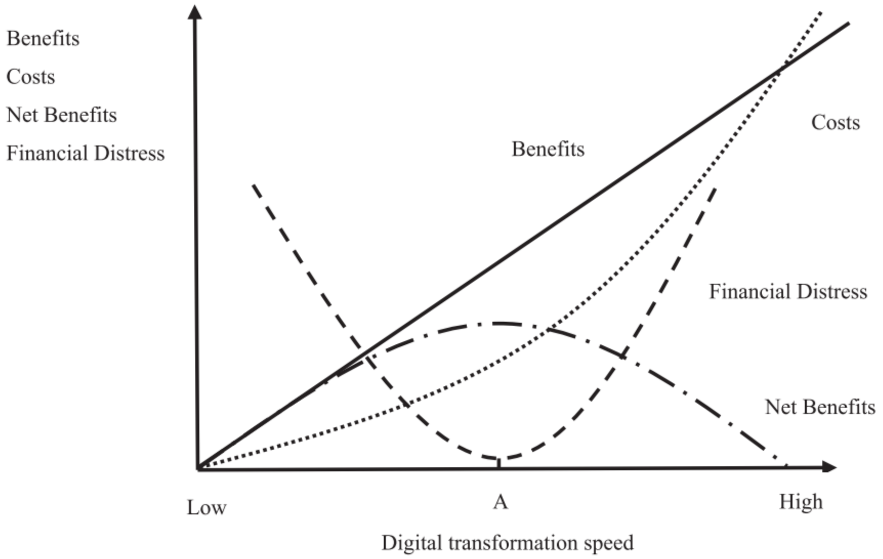


Figure 2. 1 Digital Transformation Speed

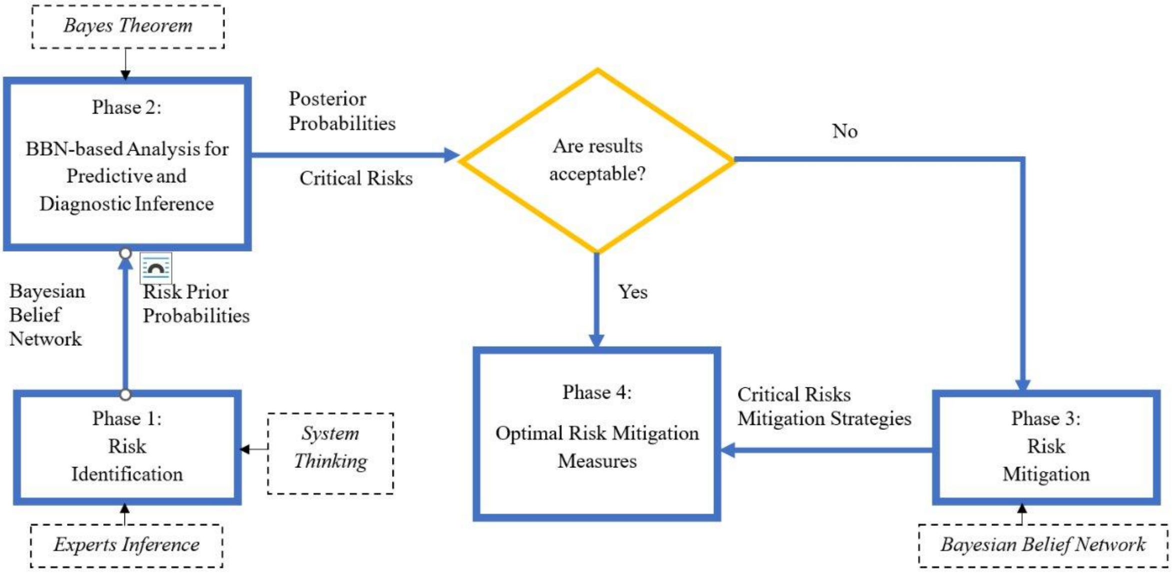


Figure 3. 1 Methodology Framework

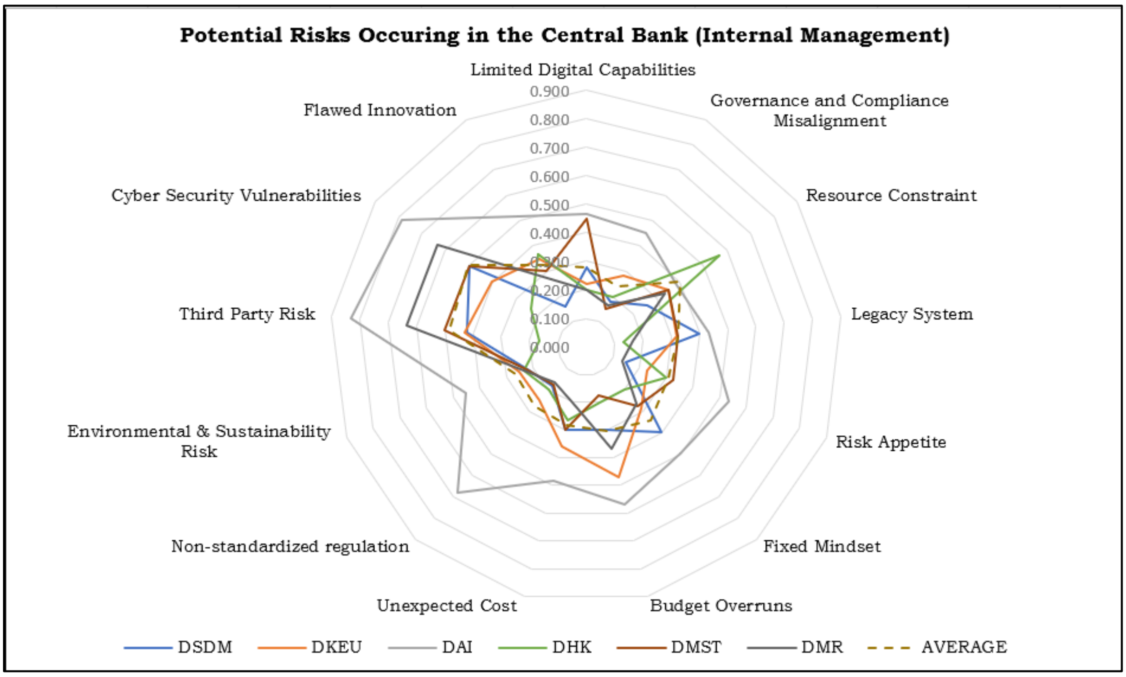


Figure 3. 2 Potential Risk (Internal Management Departments)

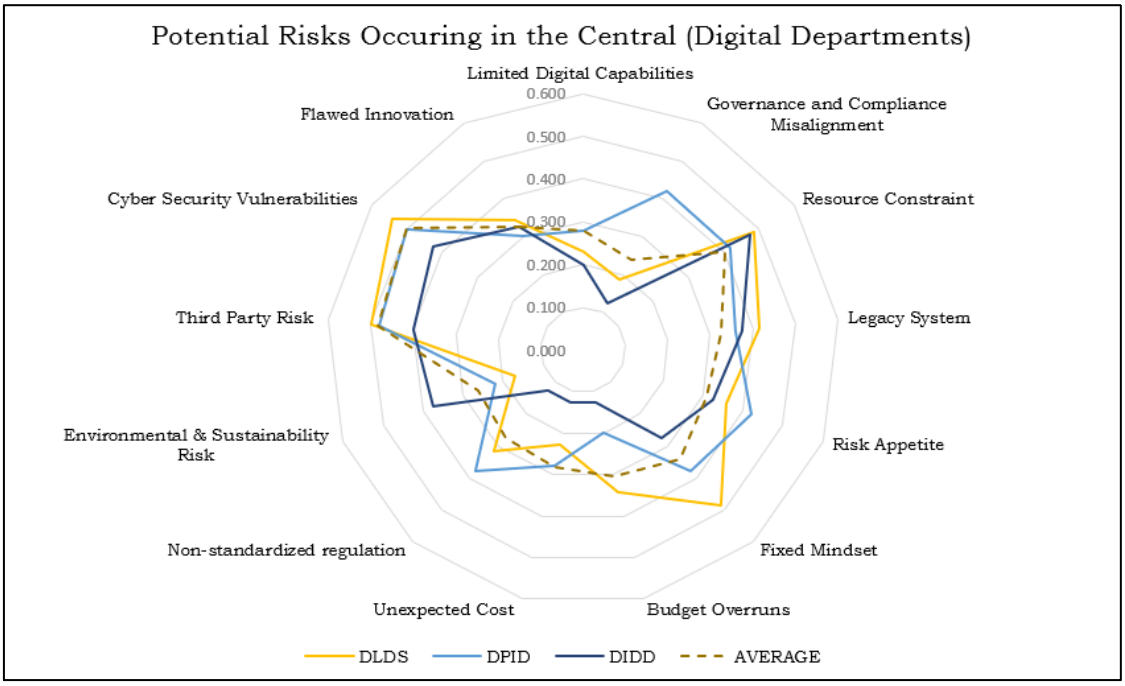


Figure 3. 3 Potential Risk (Digital Departments)

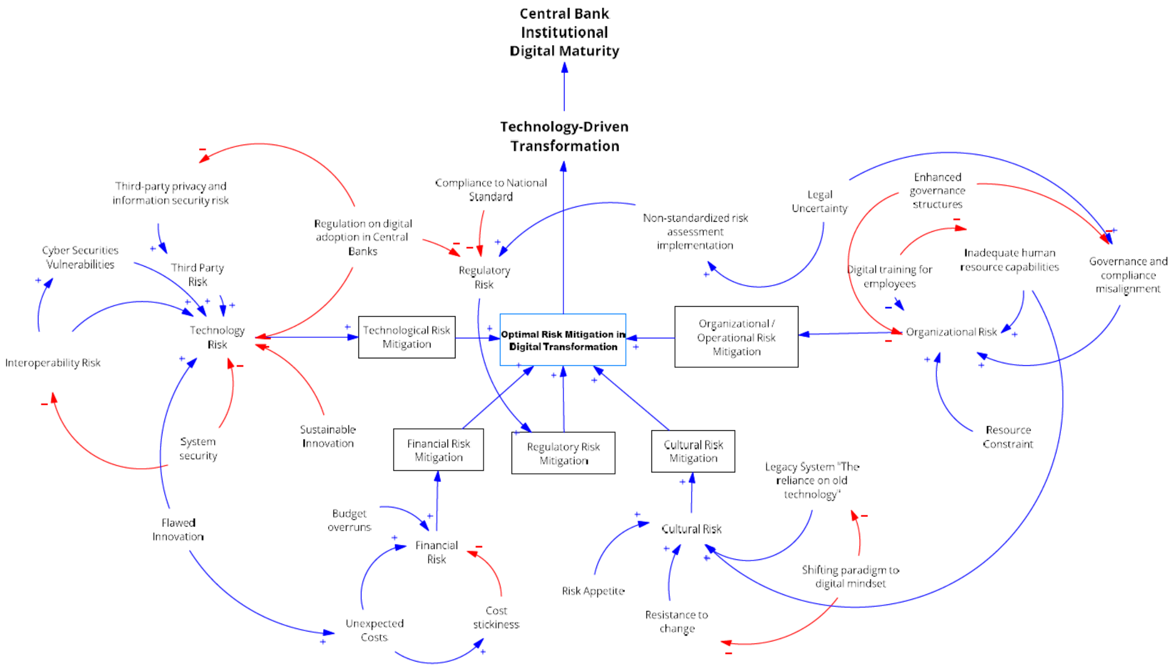

Central Bank Institutional Digital Maturity
Technology-Driven Transformation
Third-party privacy and information security risk
Regulation on digital adoption in Central Banks
Compliance to National Standard
Non-standardized risk assessment implementation
Legal Uncertainty
Enhanced governance structures
Cyber Securities Vulnerabilities
Third Party Risk
Regulatory Risk
Digital training for employees
Inadequate human resource capabilities
Governance and compliance misalignment
Technology Risk
Technological Risk Mitigation
Optimal Risk Mitigation in Digital Transformation
Organizational / Operational Risk Mitigation
Organizational Risk
Interoperability Risk
Sustainable Innovation
System security
Financial Risk Mitigation
Regulatory Risk Mitigation
Cultural Risk Mitigation
Resource Constraint
Legacy System "The reliance on old technology"
Flawed Innovation
Budget overruns
Financial Risk
Cultural Risk
Shifting paradigm to digital mindset
Risk Appetite
Cost stickiness
Unexpected Costs
Resistance to change

Figure 4. 1 Causal Loop Diagram of Risk Management

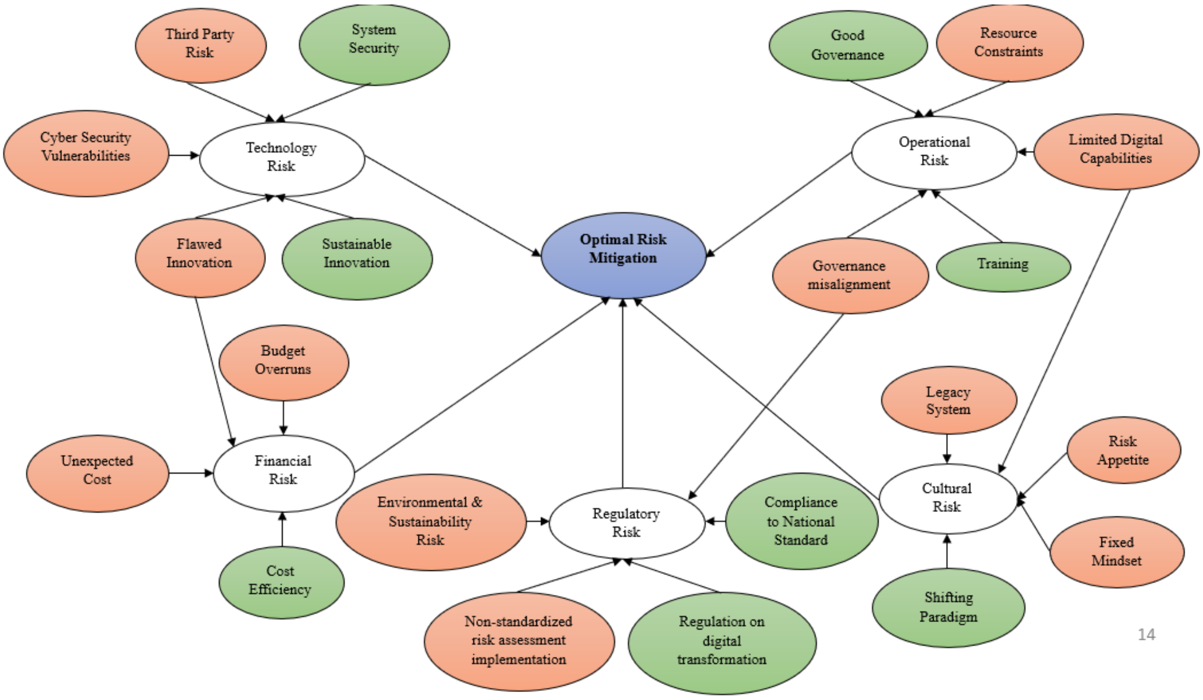


Figure 4. 2 Bayesian Network Structure

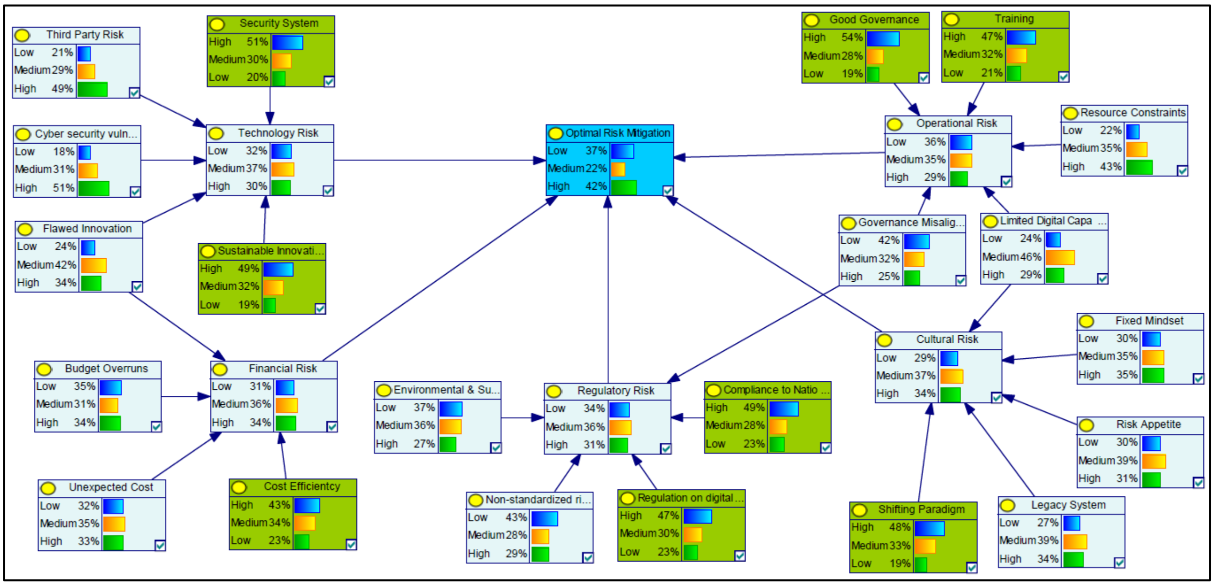


Figure 4. 3 Prior Probabilities Risk Mitigation in Central Bank

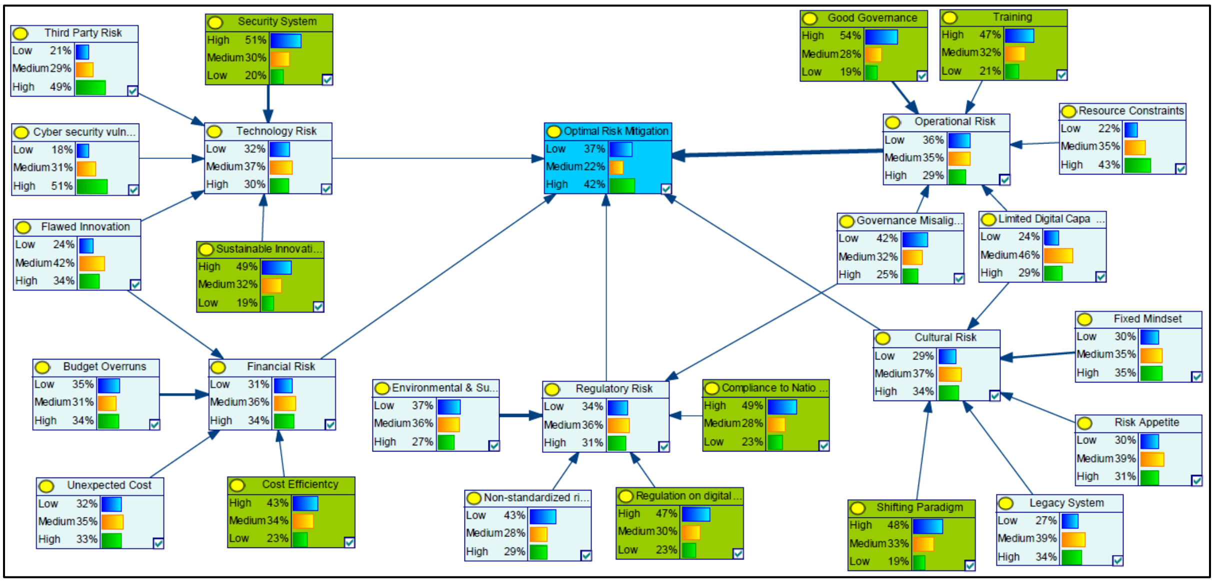


Figure 4. 4 Strength Analysis in Prior Probabilities

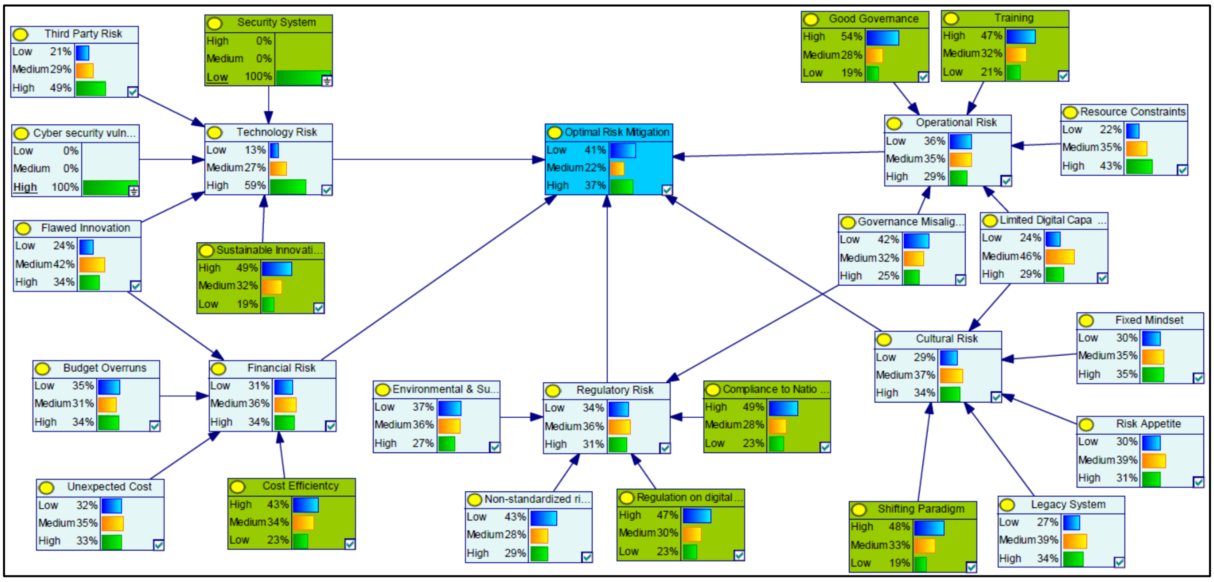


Figure 4. 5 Analysis of the first scenario

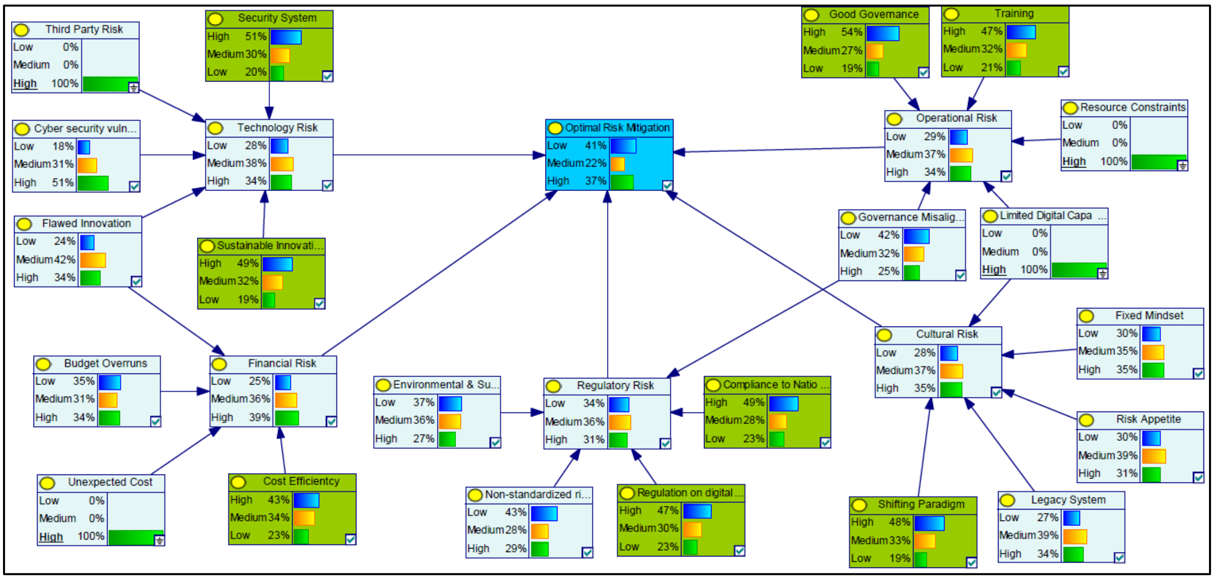


Figure 4. 6 Analysis of the second scenario

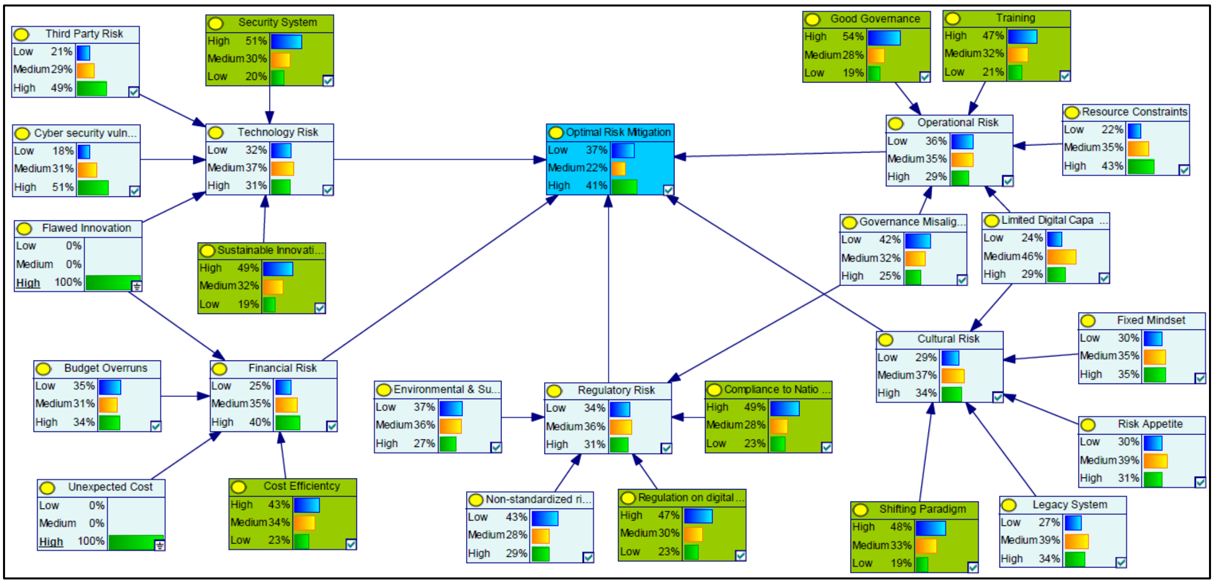


Figure 4. 7 Analysis of the third scenario

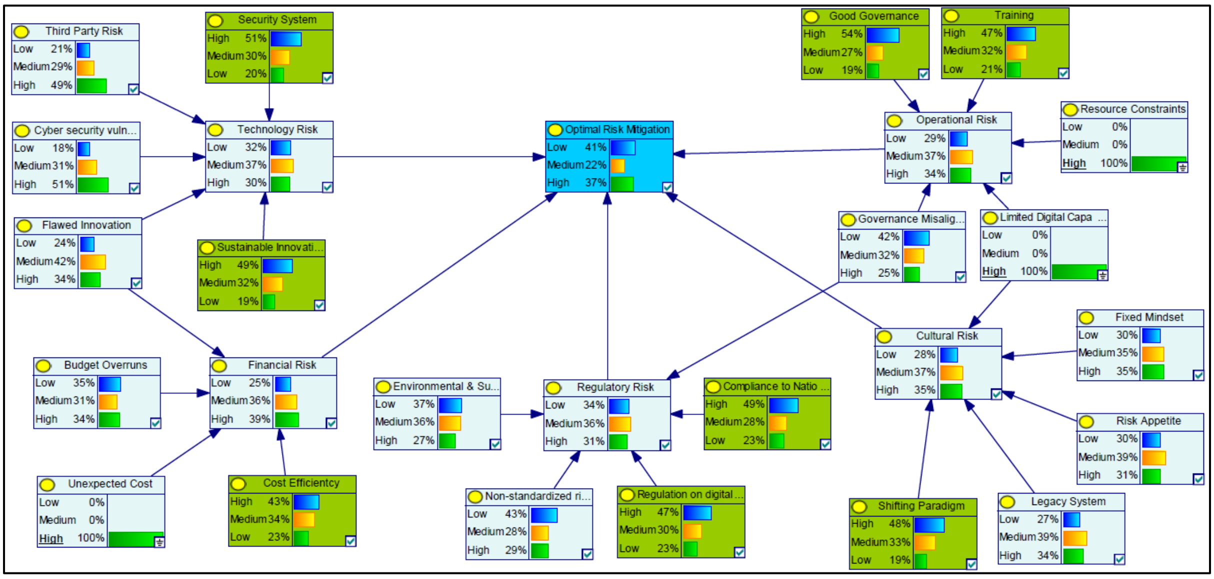


Figure 4. 8 Analysis of the fourth scenario

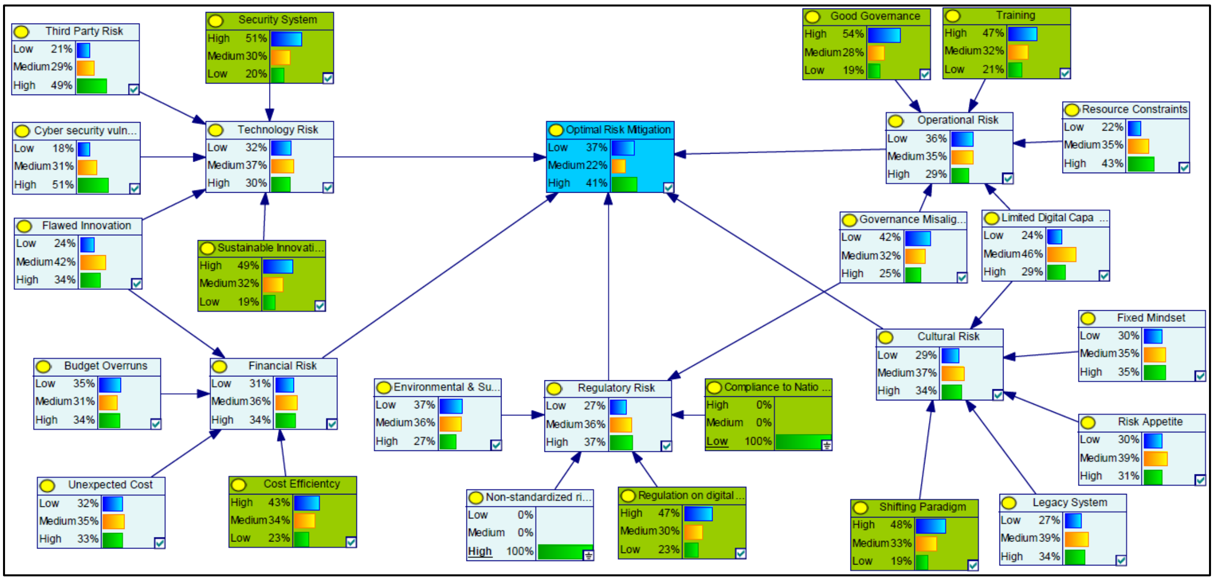


Figure 4. 9 Analysis of the fifth scenario

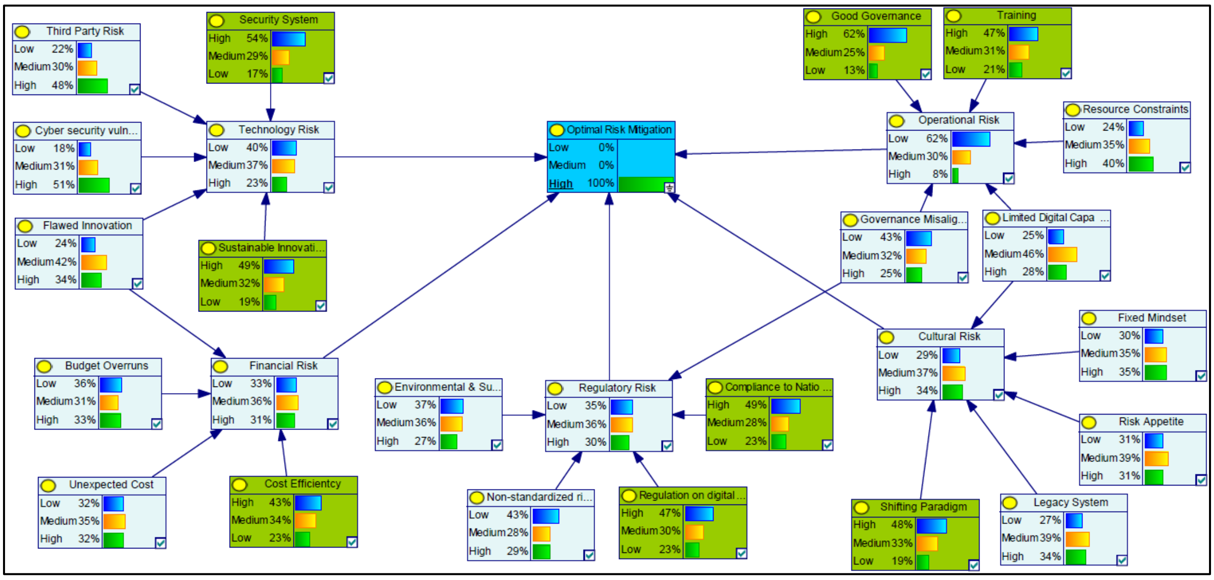


Figure 4. 10 Backpropagation Analysis

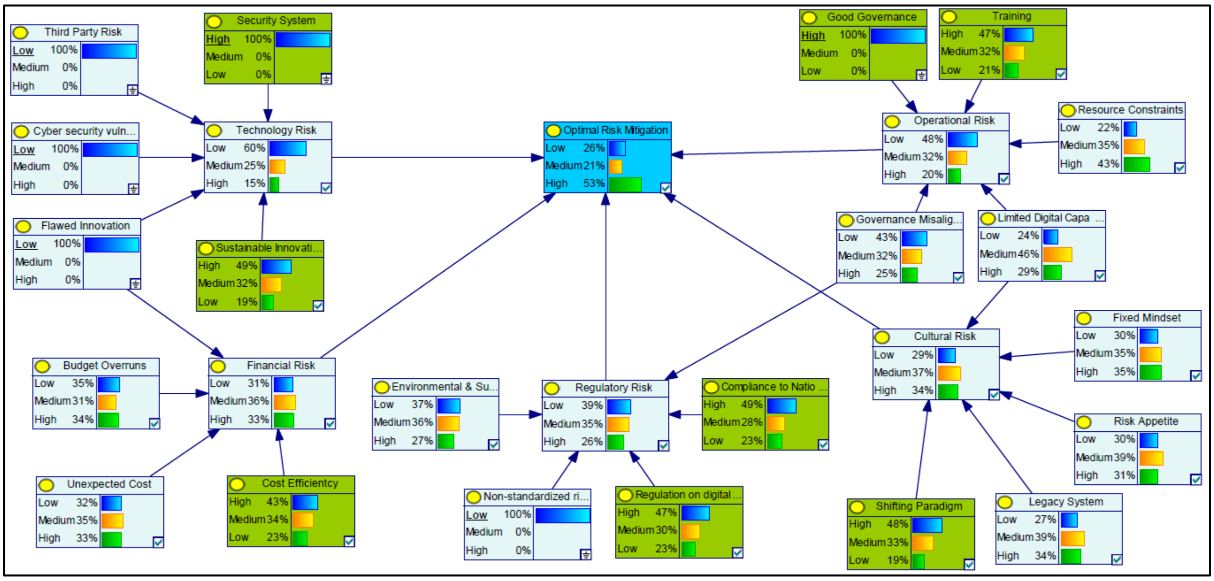


Figure 4. 11 Combination of Scenario Analysis

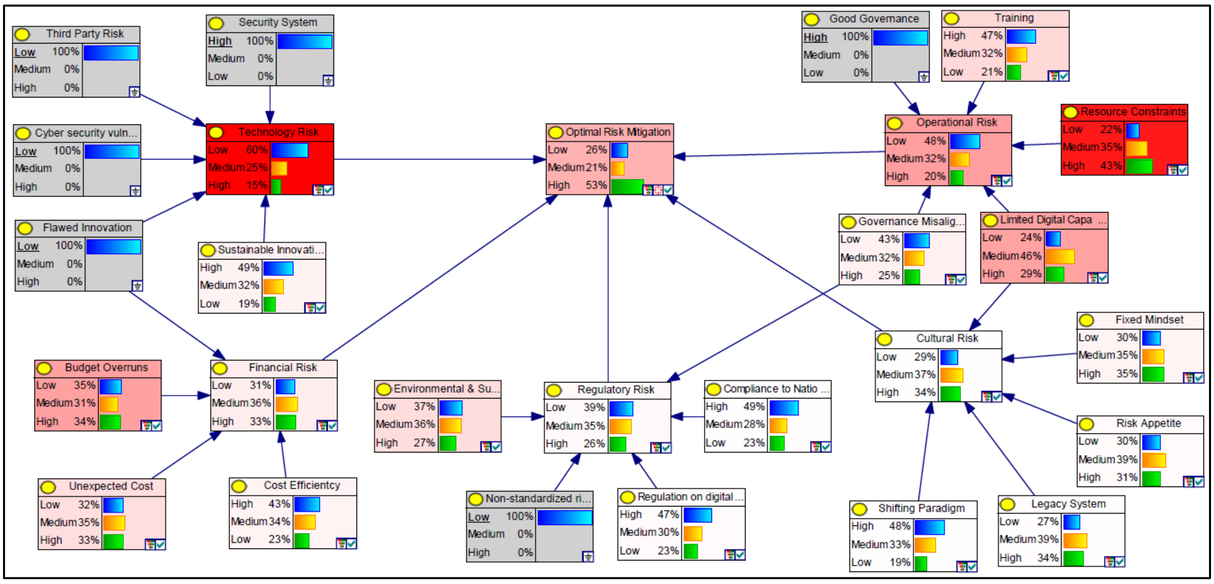


Figure 4. 12 Sensitivity Analysis

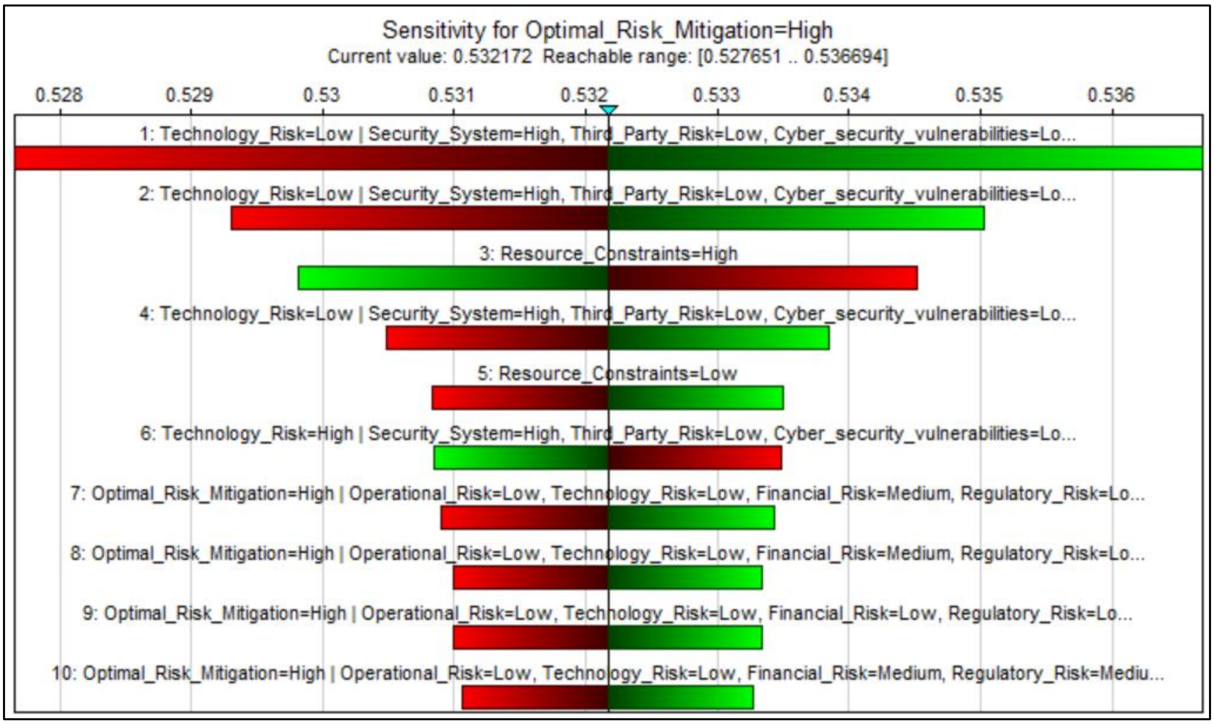


Figure 4. 13 Sensitivity by Tornado Analysis

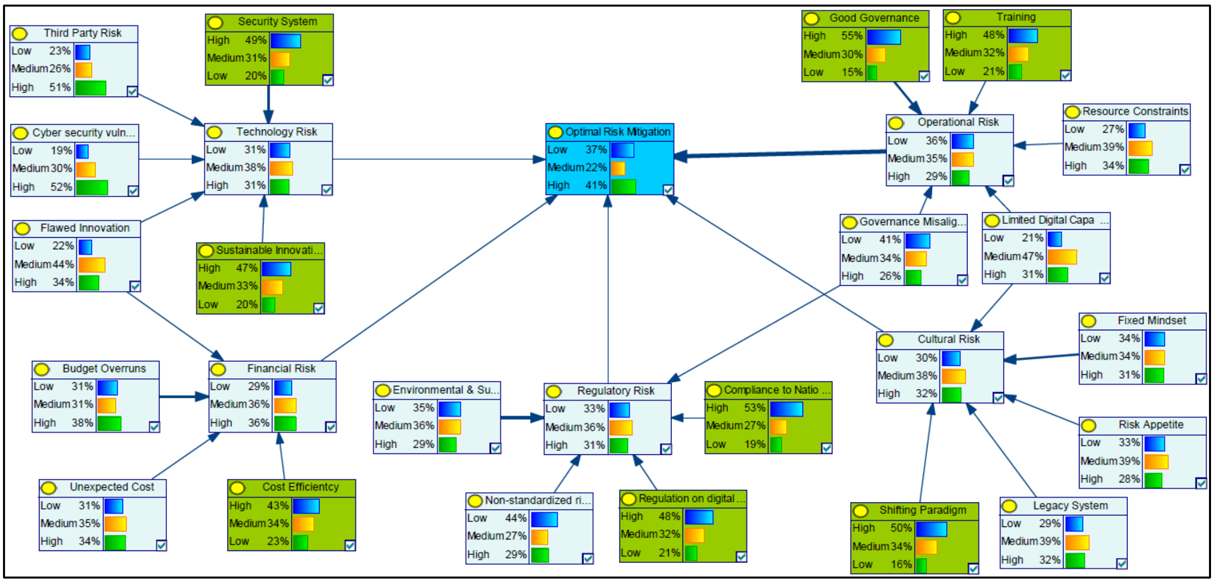


Figure 4. 14 Strength Analysis in Internal Management Cluster

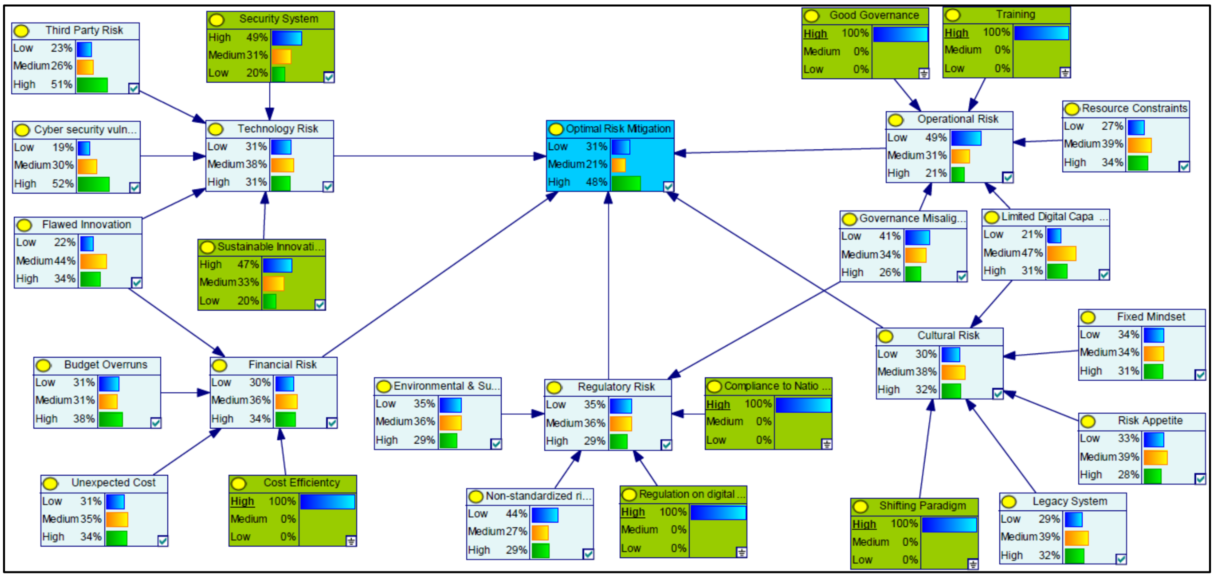

Third Party Risk Low 23% Medium 26% High 51%
Security System High 49% Medium 31% Low 20%
Good Governance High 100% Medium 0% Low 0%
Training High 100% Medium 0% Low 0%
Cyber security vuln... Low 19% Medium 30% High 52%
Technology Risk Low 31% Medium 38% High 31%
Optimal Risk Mitigation Low 31% Medium 21% High 48%
Operational Risk Low 49% Medium 31% High 21%
Resource Constraints Low 27% Medium 39% High 34%
Flawed Innovation Low 22% Medium 44% High 34%
Sustainable Innovati... High 47% Medium 33% Low 20%
Governance Misalig... Low 41% Medium 34% High 26%
Limited Digital Capa ... Low 21% Medium 47% High 31%
Fixed Mindset Low 34% Medium 34% High 31%
Budget Overruns Low 31% Medium 31% High 38%
Financial Risk Low 30% Medium 36% High 34%
Environmental & Su... Low 35% Medium 36% High 29%
Regulatory Risk Low 35% Medium 36% High 29%
Compliance to Natio ... High 100% Medium 0% Low 0%
Cultural Risk Low 30% Medium 38% High 32%
Risk Appetite Low 33% Medium 39% High 28%
Unexpected Cost Low 31% Medium 35% High 34%
Cost Efficiency High 100% Medium 0% Low 0%
Non-standardized ri... Low 44% Medium 27% High 29%
Regulation on digital ... High 100% Medium 0% Low 0%
Shifting Paradigm High 100% Medium 0% Low 0%
Legacy System Low 29% Medium 39% High 32%

Figure 4. 15 Scenario Analysis in Internal Management Cluster

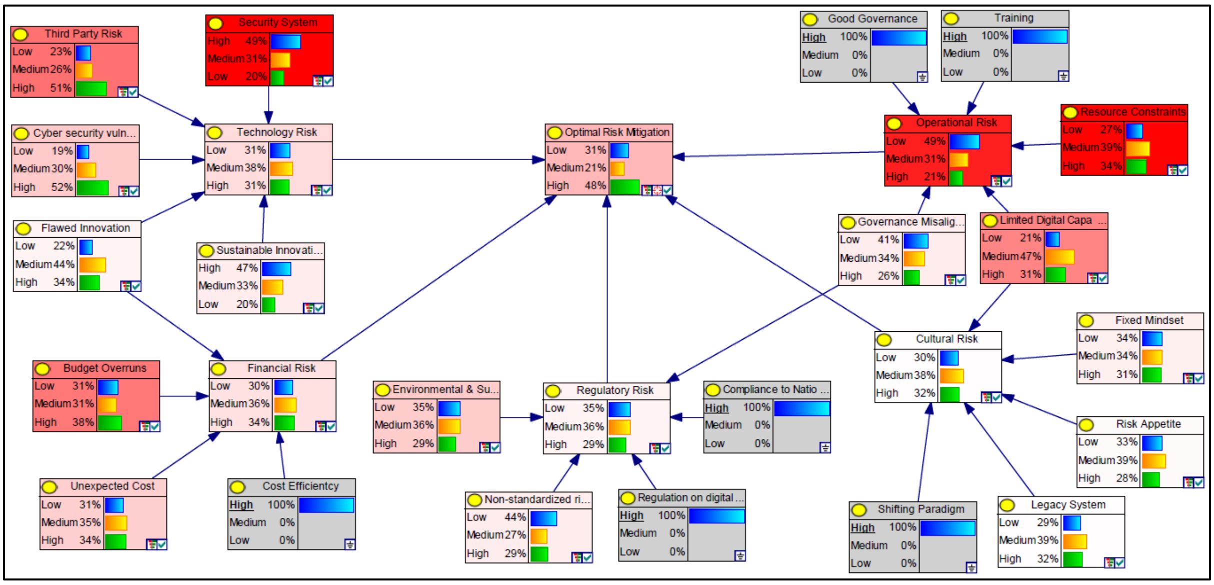

Third Party Risk Low 23% Medium 26% High 51%
Security System High 49% Medium 31% Low 20%
Good Governance High 100% Medium 0% Low 0%
Training High 100% Medium 0% Low 0%
Cyber security vuln... Low 19% Medium 30% High 52%
Technology Risk Low 31% Medium 38% High 31%
Optimal Risk Mitigation Low 31% Medium 21% High 48%
Operational Risk Low 49% Medium 31% High 21%
Resource Constraints Low 27% Medium 39% High 34%
Flawed Innovation Low 22% Medium 44% High 34%
Sustainable Innovati... High 47% Medium 33% Low 20%
Governance Misalig... Low 41% Medium 34% High 26%
Limited Digital Capa ... Low 21% Medium 47% High 31%
Fixed Mindset Low 34% Medium 34% High 31%
Budget Overruns Low 31% Medium 31% High 38%
Financial Risk Low 30% Medium 36% High 34%
Environmental & Su... Low 35% Medium 36% High 29%
Regulatory Risk Low 35% Medium 36% High 29%
Compliance to Natio ... High 100% Medium 0% Low 0%
Cultural Risk Low 30% Medium 38% High 32%
Risk Appetite Low 33% Medium 39% High 28%
Unexpected Cost Low 31% Medium 35% High 34%
Cost Efficiency High 100% Medium 0% Low 0%
Non-standardized ri... Low 44% Medium 27% High 29%
Regulation on digital ... High 100% Medium 0% Low 0%
Shifting Paradigm High 100% Medium 0% Low 0%
Legacy System Low 29% Medium 39% High 32%

Figure 4. 16 Sensitivity Analysis in Internal Management Cluster

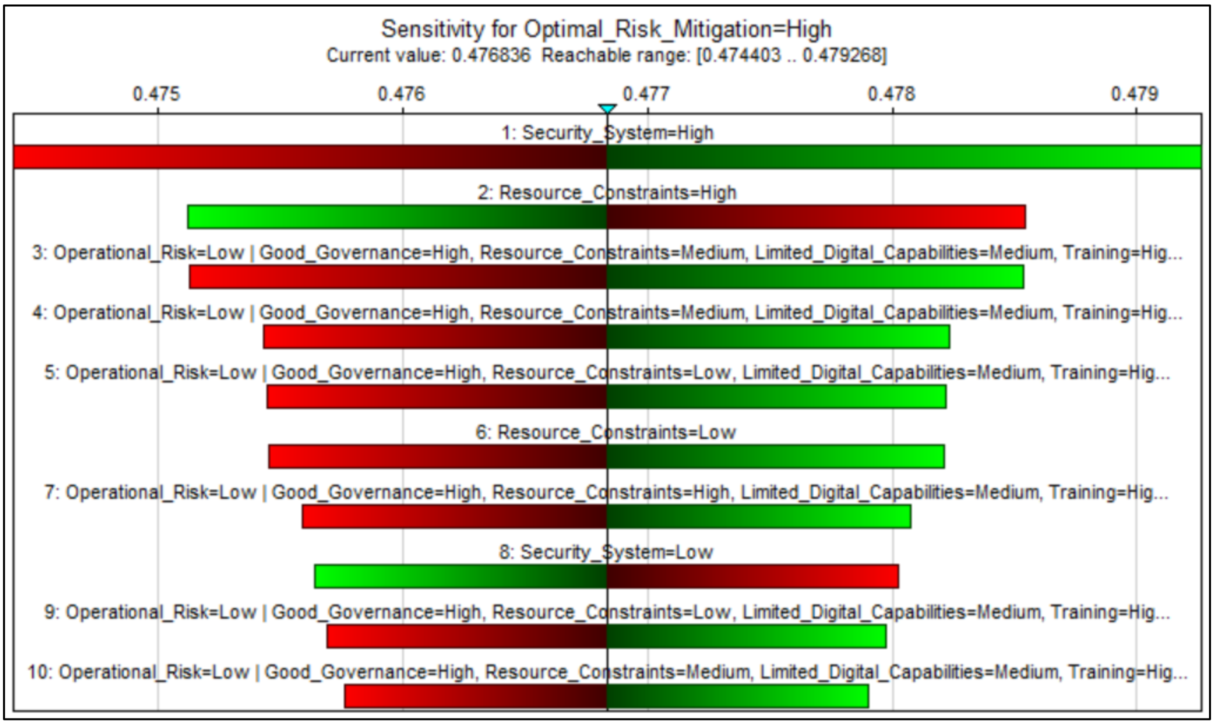


Figure 4. 17 Sensitivity Analysis (Tornado) in Internal Management

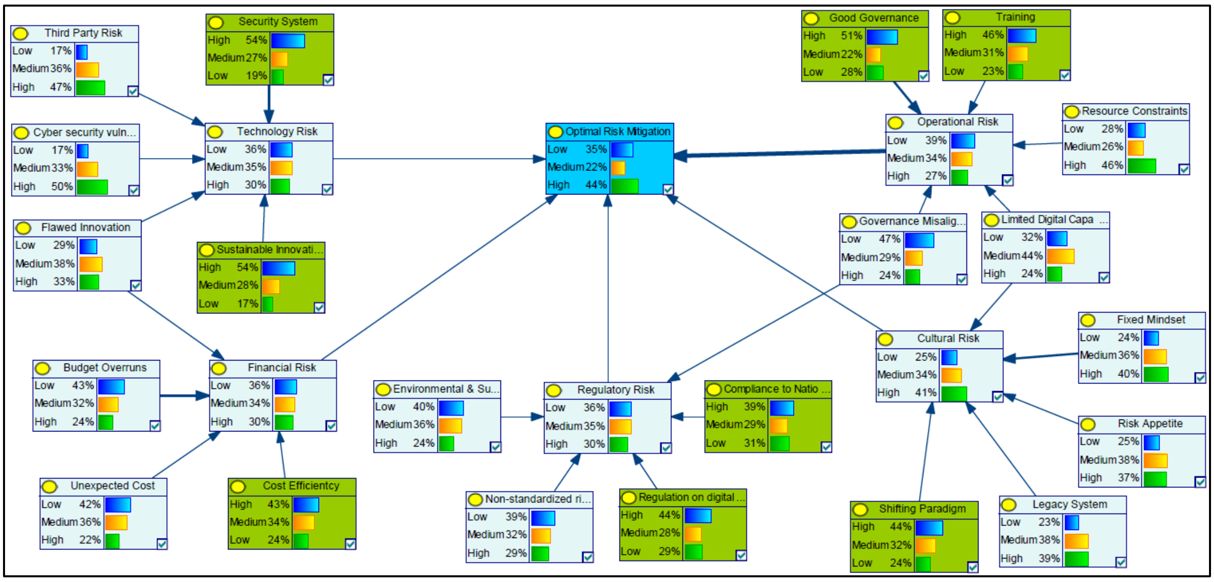


Figure 4. 18 Strength Analysis in Digital Cluster

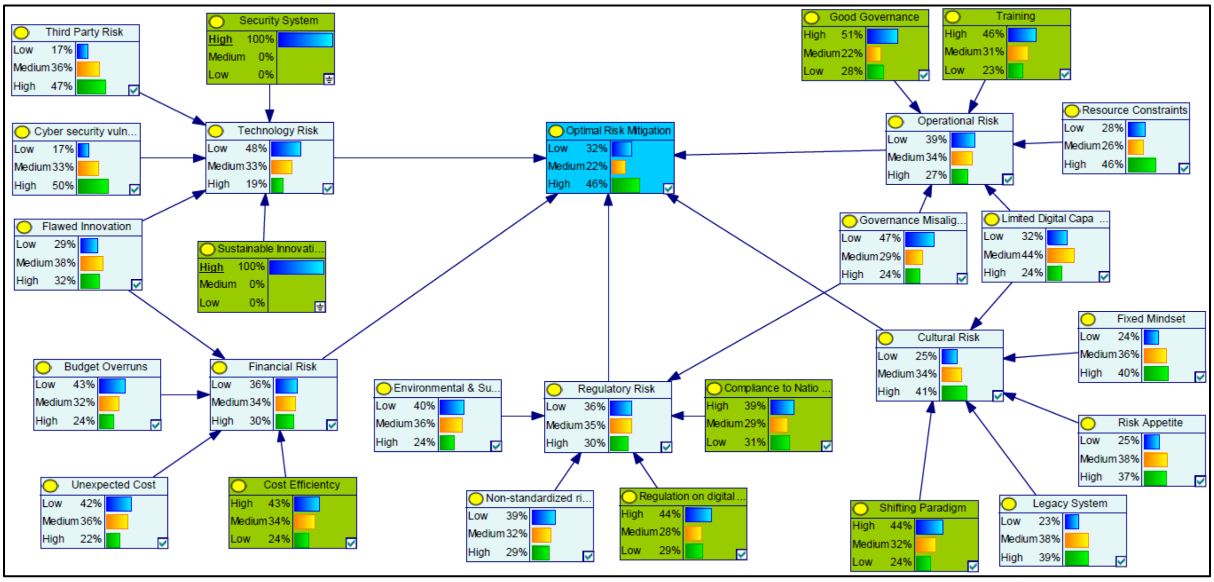

Third Party Risk Low 17% Medium 36% High 47%
Security System High 100% Medium 0% Low 0%
Cyber security vuln... Low 17% Medium 33% High 50%
Technology Risk Low 48% Medium 33% High 19%
Flawed Innovation Low 29% Medium 38% High 32%
Sustainable Innovati... High 100% Medium 0% Low 0%
Optimal Risk Mitigation Low 32% Medium 22% High 46%
Good Governance High 51% Medium 22% Low 28%
Training High 46% Medium 31% Low 23%
Operational Risk Low 39% Medium 34% High 27%
Resource Constraints Low 28% Medium 26% High 46%
Governance Misalig... Low 47% Medium 29% High 24%
Limited Digital Capa ... Low 32% Medium 44% High 24%
Fixed Mindset Low 24% Medium 36% High 40%
Cultural Risk Low 25% Medium 34% High 41%
Risk Appetite Low 25% Medium 38% High 37%
Budget Overruns Low 43% Medium 32% High 24%
Financial Risk Low 36% Medium 34% High 30%
Environmental & Su... Low 40% Medium 36% High 24%
Regulatory Risk Low 36% Medium 35% High 30%
Compliance to Natio ... High 39% Medium 29% Low 31%
Unexpected Cost Low 42% Medium 36% High 22%
Cost Efficientcy High 43% Medium 34% Low 24%
Non-standardized ri... Low 39% Medium 32% High 29%
Regulation on digital ... High 44% Medium 28% Low 29%
Shifting Paradigm High 44% Medium 32% Low 24%
Legacy System Low 23% Medium 38% High 39%

Figure 4. 19 Scenario Analysis in Digital Cluster

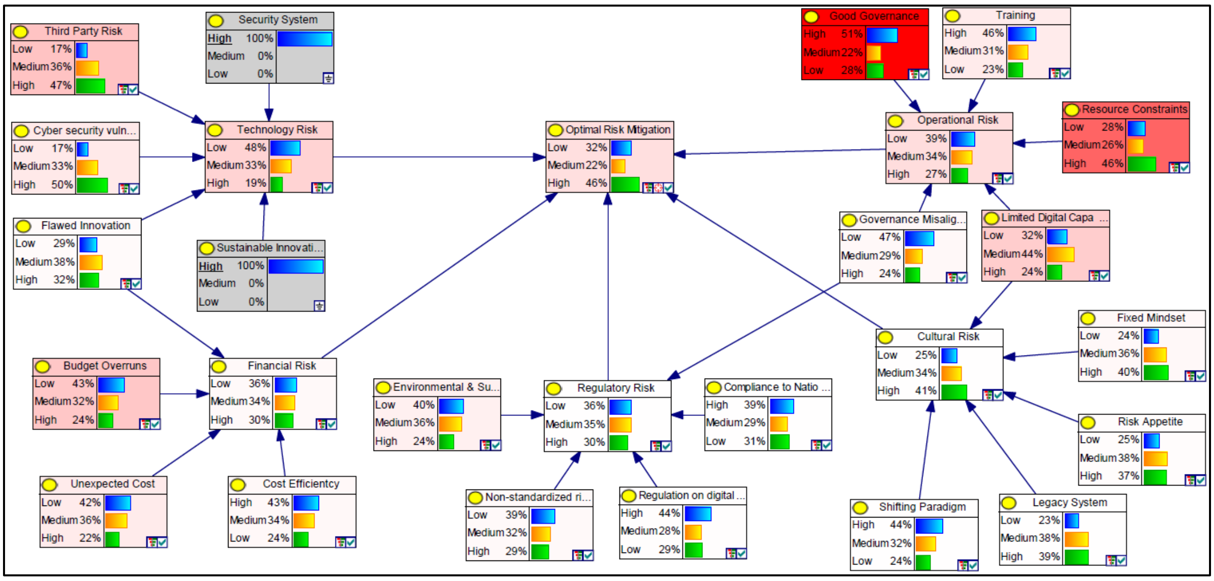

Third Party Risk Low 17% Medium 36% High 47%
Security System High 100% Medium 0% Low 0%
Cyber security vuln... Low 17% Medium 33% High 50%
Technology Risk Low 48% Medium 33% High 19%
Flawed Innovation Low 29% Medium 38% High 32%
Sustainable Innovati... High 100% Medium 0% Low 0%
Optimal Risk Mitigation Low 32% Medium 22% High 46%
Good Governance High 51% Medium 22% Low 28%
Training High 46% Medium 31% Low 23%
Operational Risk Low 39% Medium 34% High 27%
Resource Constraints Low 28% Medium 26% High 46%
Governance Misalig... Low 47% Medium 29% High 24%
Limited Digital Capa ... Low 32% Medium 44% High 24%
Fixed Mindset Low 24% Medium 36% High 40%
Cultural Risk Low 25% Medium 34% High 41%
Risk Appetite Low 25% Medium 38% High 37%
Budget Overruns Low 43% Medium 32% High 24%
Financial Risk Low 36% Medium 34% High 30%
Environmental & Su... Low 40% Medium 36% High 24%
Regulatory Risk Low 36% Medium 35% High 30%
Compliance to Natio ... High 39% Medium 29% Low 31%
Unexpected Cost Low 42% Medium 36% High 22%
Cost Efficientcy High 43% Medium 34% Low 24%
Non-standardized ri... Low 39% Medium 32% High 29%
Regulation on digital ... High 44% Medium 28% Low 29%
Shifting Paradigm High 44% Medium 32% Low 24%
Legacy System Low 23% Medium 38% High 39%

Figure 4. 20 Sensitivity Analysis in Digital Cluster

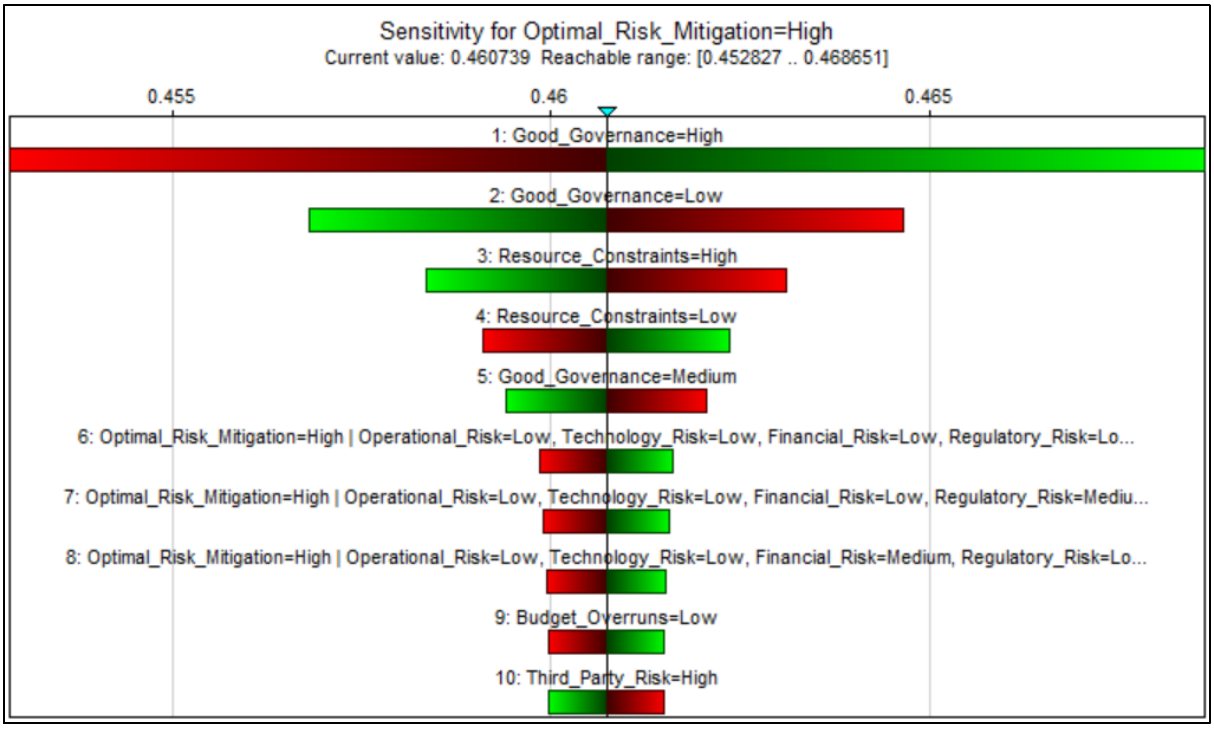


Figure 4. 21 Sensitivity Analysis (Tornado) in Digital Cluster