Eduvest – Journal of Universal Studies
Volume 6 Number 4, April, 2026
p- ISSN 2775-3735- e-ISSN 2775-3727

Analysis of Enterprise Risk Management Maturity Level at PT. XYZ

Muhamad Rifnaldy Pratama[1]*, Dominicus Savio Priyarsono[2], Siti Jahroh[3]
Institut Pertanian Bogor, Indonesia
Email: muhamadrifnaldypratama@apps.ipb.ac.id*, priyarsono@-apps.ipb.ac.id, sitijahro@apps.ip

Keywords:
Enterprise Risk Management, Risk Maturity Index, Maturity Assessment, Risk Management, SOEs, PT. XYZ, SWOT, PESTEL

ABSTRACT

This research aims to evaluate the maturity level of the implementation of Enterprise Risk Management (ERM) at PT. XYZ through a maturity assessment process based on the Technical Guidelines for the Assessment of the Risk Maturity Index (RMI) issued by the Ministry of SOEs, namely Number SK-8/DKU.MBU/12/2023 and PER-2/MBU/03/2023. The research background is based on the increasing complexity of global risks and regulatory demands, which require companies to implement risk management effectively. This study uses a combination of primary and secondary data collected through questionnaires, in-depth interviews, and analysis of company documents. Data analysis was carried out descriptively using a scoring system, as well as SWOT and PESTEL analyses to formulate improvement strategies. The results of the study are expected to illustrate the actual conditions of ERM implementation at PT. XYZ, measure its maturity level based on the five dimensions of the RMI, and develop the necessary follow-up strategies to strengthen the effectiveness of risk management in a sustainable manner. These findings provide practical contributions for companies in improving risk governance, as well as academic contributions by enriching the literature on the application of maturity assessments in corporate risk management.

INTRODUCTION

Rapid technological advances have led to increasingly complex risks. Based on the report (WEF 2025), there are four main global threats: economic, political, environmental, and cyber risks. Referring to the same report (WEF 2025), these rapidly developing technological advances also contribute to increasingly complex risks, with five main threats identified for Indonesia.

According to the survey report from (EY and IIF 2024), under current conditions, companies need to align risk management with volatile market environments and evolving risks. Risk management is a process used to assess and control risks that may result in potential losses or gains for an organization (Ghani et al., 2019; Hopkin, 2018). In the context of business performance, risk management functions to maintain business continuity in achieving strategic objectives. Implementing effective risk management can help reduce the impact of potentially adverse uncertainties while also providing opportunities to enhance company performance. Currently, risk management is widely referred to as Enterprise Risk Management (ERM). ERM is a process of identifying and assessing risks that integrates all types of risks and embeds risk management activities into all business processes within the organization (Iswajuni et al. 2018). By implementing ERM, companies are expected to develop more informed strategies, thereby becoming more resilient and better prepared to achieve their objectives (David et al. 2019). As explained by (Suhaimi, 2020), the implementation of ERM provides value to companies as a

basis for decision-making to reduce potential losses (Leng et al., 2022; Sasmita & Suhaimi, 2020). In practice, companies need to enhance ERM implementation continuously, meaning they must consistently improve their processes. In accordance with the document published by (BSN 2018), one of the principles of ISO 31000 is continual improvement, which requires companies to continuously enhance their capabilities in applying risk management so that ERM implementation improves over time. One form of continual improvement that companies can undertake is conducting a maturity assessment.

A maturity assessment, according to (Sprcic et al. 2017), is a quantitative evaluation conducted to assess the quality of ERM implementation, enabling companies to understand their level of maturity constructively. Risk management maturity is an important indicator for measuring the extent to which a company can effectively identify, analyze, respond to, and monitor risks. ERM maturity serves as a roadmap that illustrates the extent of risk management implementation within an organization; through this roadmap, organizations can identify gaps and develop improvement plans (Brandt 2021). According to (Deloitte 2023), risk management maturity assessments can be categorized into four types: capability-based, activity-based, hybrid, and activity- and outcome-based approaches. The selection of the type depends on the objectives of the assessment. A survey by (CRMS 2019) shows that 76% of companies in Indonesia have implemented integrated risk management, but at a low maturity level. Similarly, research conducted by (Tjahjono 2017) indicates that the maturity of enterprise risk management among companies listed on the Indonesia Stock Exchange remains low, generally at the initial to repeatable level. This suggests that ERM has not yet become an integral process within organizations. Referring to previous studies, the Risk Maturity Index (RMI) level in Indonesian companies remains at an initial or low stage, highlighting the importance of conducting maturity assessments to support the principle of continual improvement in risk management.

The Ministry of State-Owned Enterprises, through Regulation Number PER-2/MBU/03/2023 concerning governance guidelines and significant corporate activities, has established standards for corporate governance implementation. This regulation emphasizes the obligation for SOEs to implement risk management in a comprehensive and integrated manner. It also highlights the importance of maturity assessments as a tool for evaluating risk management implementation. The regulation outlines several governance principles, including transparency, accountability, responsibility, independence, and fairness. Maturity assessment measurement not only functions as an evaluation tool but also serves as a basis for developing roadmaps and strategies to strengthen internal controls and improve corporate governance. Furthermore, risk management implementation is part of Good Corporate Governance (GCG), where a high level of risk management maturity reflects strong management awareness and supports accountability, transparency, and corporate sustainability. Standardizing governance practices also aims to enhance the competitiveness of SOEs at both national and international levels.

PT. XYZ is a company engaged in shared services and IT solutions, acting as a provider for various SOE entities. As a subsidiary of a strategic SOE, PT. XYZ is responsible for supporting digital transformation and operational efficiency for its parent company and other entities. The company employs more than 500 personnel, with business activities covering application development, infrastructure management, and shared services, exposing it to a wide

range of complex and dynamic risks. Over the past five years, the company's revenue has shown consistent growth, driven by an expanded service portfolio and market diversification beyond SOEs. The company contributes significantly to the digitalization of SOE business processes, playing a key role in supporting the digital transformation agenda of the Ministry of SOEs.

Over the same period, the number of projects handled by PT. XYZ has steadily increased, reflecting growing client trust in the company's capabilities in delivering IT solutions. However, alongside increasing business complexity, the risks faced by PT. XYZ have also become more complex, spanning financial, operational, and compliance aspects. To address these risks, the company is required to implement comprehensive and sustainable risk management practices. This condition further emphasizes the need for improved risk management to maintain performance and regulatory compliance. As part of its efforts, PT. XYZ has implemented Enterprise Risk Management (ERM) since 2019 by adopting ISO 31000. The company has established a dedicated risk management team responsible for identifying, analyzing, and mitigating risks across all business lines. Despite these efforts, several limitations remain, including limited human resources, reliance on key individuals, weak integration between risk management and corporate strategy, and suboptimal effectiveness measurement.

One key aspect of Regulation Number PER-2/MBU/03/2023 is the obligation for companies to conduct maturity level measurements in risk management implementation (maturity assessment). As a subsidiary of an SOE, PT. XYZ is required to perform such assessments in compliance with this regulation. Measuring the Risk Maturity Index is essential for PT. XYZ to achieve its objectives and to evaluate the extent of ERM implementation. These assessments can support the development of improved ERM roadmaps and strategies. According to (Leng et al., 2023), comprehensive ERM implementation provides benefits in decision-making by guiding companies in considering both short-term and long-term impacts.

Based on the literature review conducted by the author, previous research indicates that ERM maturity levels, particularly in Indonesia, remain relatively low. This presents an opportunity for further research on maturity assessments to enhance ERM implementation capacity and capability through RMI measurement. This research is particularly important for organizations such as PT. XYZ to evaluate their risk management practices. Furthermore, understanding ERM implementation and maturity assessment can help companies identify areas for improvement, enabling them to maximize opportunities and minimize risks that may hinder organizational objectives.

In an increasingly uncertain and complex digital business environment, PT. XYZ has implemented Enterprise Risk Management (ERM) since 2019 as a response to global threats such as economic, political, environmental, and cyber risks, as reported by (WEF 2025), in line with (Suhaimi, 2020), who emphasizes the value of ERM in decision-making to reduce potential losses. As an SOE subsidiary, PT. XYZ is required to implement effective risk management in accordance with Regulation PER-2/MBU/03/2023 and SK-8/DKU.MBU/12/2023 concerning Risk Maturity Index (RMI) assessment. One method to evaluate the effectiveness of risk management is through maturity assessment, which, according to (Sprcic et al. 2017), is a quantitative evaluation of ERM implementation quality. The RMI assessment based on SK-8/DKU.MBU/12/2023 covers five dimensions: Risk Culture

and Capabilities, Risk Organization and Governance, Risk Framework and Compliance, Risk Processes and Control, and Risk Data and Technology Models, all measured using a Likert scale of 1–5. These regulations require companies not only to focus on operational and administrative aspects but also to ensure effective risk management implementation to achieve business objectives. This raises key questions regarding the extent of ERM implementation at PT. XYZ, its current maturity level, and the strategies required for optimal and sustainable risk management. Accordingly, this study focuses on conducting a maturity assessment to determine the RMI level of ERM implementation at PT. XYZ amid its growth and increasingly complex risk environment. The research aims to describe ERM implementation, measure its maturity level, and formulate follow-up strategies based on the findings to strengthen risk management effectiveness in line with SOE regulations. The expected outcomes include providing companies with insights into their risk maturity levels and a roadmap for improvement, as well as contributing to academic research on maturity assessment and RMI-based risk management frameworks applicable across industries.

METHOD

This research employed a qualitative approach supported by quantitative data using a scoring system method. The focus of the study was to measure the maturity level of Enterprise Risk Management (ERM) at PT XYZ. The analysis was conducted based on the guidelines issued by the Ministry of SOEs (PER-2/MBU/03/2023 and SK-8/DKU.MBU/12/2023). The research was carried out from April to June 2025 at PT XYZ, South Jakarta.

The research population consisted of all officials and employees of PT XYZ who were involved in ERM implementation and were part of the Three Lines Model, namely the Board of Commissioners, the Board of Directors, first-line management (risk owners), and second-line management (risk management function). The questionnaire sample comprised 30 respondents, including Commissioners, Directors, first-line managers, and second-line managers. The in-depth interview sample consisted of seven participants selected through purposive sampling: one Commissioner, two members of the Board of Directors, three first-line managers, and one second-line manager. The selection criteria required participants to have undergone risk management training and to have a direct role in ERM implementation.

Data collection used three main methods, namely:

a) The questionnaire was compiled based on 5 dimensions and 42 Risk Maturity Index (RMI) parameters. The instrument is reviewed by experts to ensure the validity of the content. The questionnaire is sent via email and filled out via Google Form.
b) The collection and review of company documents included 39 documents related to risk culture, governance, risk frameworks, risk processes, and risk data-technology models. Review results are grouped into high, medium, and low priority to determine interview questions.
c) In-depth interviews were conducted with 7 selected respondents. The questions are built on the findings of the questionnaire and document reviews, and cover the five dimensions of ERM.

Data analysis was carried out through three approaches:

a) Descriptive Analysis, to describe the actual conditions of ERM implementation based on secondary data and refer to the risk management component of ISO 31000:2018.

b) Scoring System, used to calculate the level of risk management maturity based on RMI parameters. The scores were given by the respondents (1–5), then averaged and validated with documentary evidence and interview results.
c) SWOT and PESTEL analysis, used to formulate a follow-up strategy after the maturity level was calculated. This analysis connected internal–external factors to generate recommendations for improving ERM.

RESULT AND DISCUSSION

Risk Management Follow-up Strategy Analysis

A comprehensive analysis of internal and external factors needs to be done before making follow-up strategy decisions. One of the methods of situational analysis according to Gürel (2017) analysis involves maximizing the use of strengths and opportunities, while minimizing weaknesses and threats. In this context, the analysis used is a SWOT analysis. The SWOT analysis forms a comprehensive framework to examine the internal elements obtained from the calculation of risk management maturity and external factors obtained from the PESTEL analysis The matrix approach pattern allows a deeper understanding of the interaction between the company's strengths and the company's weaknesses as well as external opportunities and threats.

1. Internal Factors

Internal factors are factors that come from within PT. XYZ is based on the results of the Risk Maturity Index calculation that has been carried out. Given that the average score of the company's maturity in general is still in the range of Initial to Managed, the analysis of this internal factor is carried out with a parameter-based approach, not just looking at the average dimension. This approach aims to identify specific strengths hidden behind low scoring averages, as well as highlight critical points of weakness that require immediate intervention. Strengths are identified from parameters that have an above-average score or have reached a level of development, indicating aspects of compliance, basic infrastructure, or standardized methodologies. The table below is the strength of internal factors in the implementation of risk management at PT. XYZ.

Table 1. Internal Factors Strengths & Weaknesses of PT. XYZ

	No	Internal Factors
Strengths	1.	Integrated Risk Reporting Compliance The Company has high discipline in compiling corporate risk profiles on a regular basis to meet its reporting obligations to the *Holding* Company.
	2.	Availability of Basic Framework Documents The company already has guidelines, policies, and risk management procedures in place that formally refer to ISO 31000 standards and SOE regulations.
Weaknesses	1.	Weak Risk Culture & Competence Low employee awareness and lack of participation in risk competency training
	2.	Ineffective Risk Mitigation Execution Action *plans* often stop as administrative documents without real realization and monitoring in the field.
	3.	Governance Infrastructure Is Incomplete There has been no specific supervisory organ (Risk Committee) and no risk limit parameters (*Risk Appetite*).

Source: Primary data processed, 2025

Based on the mapping of internal factors above, it can be concluded that the capabilities of PT. XYZ is currently still dominated by administrative and compliance aspects, but is still very weak in terms of culture and technical execution. The inequality between complete documents (Strength) and minimal implementation (Weakness) confirms that internal encouragement alone is not strong enough to raise the level of maturity. Therefore, it is necessary to identify external factors (Opportunities & Threats) to find more effective momentum for change.

2. External Factors

External factors are factors that come from outside PT. XYZ is based on the results of the Risk Maturity Index calculation that has been carried out. External factors were identified using PESTEL Analysis. External environmental factors are an ever-changing space and can affect the direction and effectiveness of Enterprise Risk Management (ERM) implementation. To understand these dynamics in a more structured way, PESTEL analysis is used as a tool to identify influential macro factors. Through this framework, organizations can assess the extent to which political, economic, social, technological, environmental, and legal changes shape opportunities and threats that are relevant to the development of ERM by sorting out factors that have the potential to become opportunities to accelerate improvement, as well as threats that must be anticipated.

a. Political factor

From the political side, the dynamics of government policies play an important role in shaping the direction and maturity of risk management in companies, especially in the SOE environment which has a stricter level of regulation than the private sector. Regulations such as PER-2/MBU/03/2023 not only affirm administrative obligations, but also set risk governance standards that must be met, starting from the risk organizational structure, policy formulation, to the implementation of periodic maturity assessments. This provision essentially creates positive pressure because it forces companies to adopt a more systematic and documented approach to ERM. This regulatory pressure is also a counterbalance to the variation in management commitments in various SOEs. Not all companies have the same level of risk awareness, so the existence of coercive rules helps ensure that ERM practices run consistently and not rely solely on individual preferences of unit leaders. The Sari study (2022) confirms that policy intervention from regulators can accelerate the process of institutionalization of ERM, as organizations are encouraged to accelerate the development of guidelines, clarify the role of risk managers, and adjust internal processes to higher governance standards.

In addition, the direction of government policies in recent years shows a tendency to strengthen the integrity, accountability, and transparency of SOEs, so that the issue of internal control and risk management is increasingly positioned as key instruments. This political pressure also has an impact on increasing expectations for the board of commissioners and directors in carrying out the oversight function against risks. With clear regulations, top management has a formal foundation to allocate resources for the development of risk capabilities, both in the form of technology investment, competency improvement, and organizational structure arrangement. This ever-evolving political context creates space for companies to strengthen ERM on a sustainable basis. As regulations move toward stricter

maturity assessments, companies are automatically encouraged to improve documentation quality, improve reporting mechanisms, and build a more embedded risk culture. In other words, political factors provide a combination of pressures and opportunities that, if managed appropriately, can significantly accelerate the increase in risk management maturity.

b. Economic Factors

Macroeconomic conditions have a direct impact on the stability of liquidity and the company's cost structure. Based on the World Bank's report (2024) on the global economic slowdown, there is a trend where many corporations and government agencies are tightening their budgets (austerity measures) to maintain cash reserves. For PT. XYZ operates on a project-based business model, this condition significantly increases liquidity risk. Delays in milestone payments by clients lead to cash flow mismatches, where the company has to bear upfront operating expenses while cash flow slows down. On the other hand, global inflationary pressures also affect the structure of the cost of revenue (PPE). Rising software and hardware licensing costs from global technology principals who often make annual price adjustments based on inflation can erode a project's profit margins if contracts with clients are fixed-price in the long run. Without a clear price escalation mechanism in the contract, this cost inflation poses a real threat to the company's profitability.

c. Social Factors

The biggest challenge from the social aspect is the phenomenon of talent scarcity in the technology sector. Data from the Ministry of Communication and Informatics and the World Bank estimate that Indonesia will experience a deficit of around 600,000 digital talents every year until 2030. This gap between supply and demand triggered the "War for Talent", which had a direct impact on the high turnover rate at PT. XYZ. This high turnover is not just a problem of HR administration, but also a strategic risk for the implementation of risk management. The loss of key personnel is often followed by a loss of institutional knowledge (brain drain), so that efforts to build a culture and risk competence within the company become hampered and unsustainable. In addition, the increasing demands of digital literacy have made clients increasingly critical of data security standards, demanding companies to prove stricter security credibility than ever before.

d. Technology Factor

As a System Integrator company, technology factors present a paradox between existential threats and efficiency opportunities. In terms of threats, the report of the State Cyber and Cryptography Agency (BSSN) recorded a drastic increase in cyber traffic anomalies, with the dominance of Ransomware and Supply Chain Attack types of attacks. For PT. XYZ, cyberattacks are not just technical risks, but fatal reputational risks; A single incident of a leak on a company-managed client's system can permanently destroy market confidence. However, on the other hand, advances in Artificial Intelligence (AI) and Robotic Process Automation (RPA) technology offer significant efficiency opportunities. Industry studies show that the adoption of AI in the Governance, Risk, and Compliance (GRC) process can automate the administrative tasks of risk reporting. This is a strategic opportunity for PT. XYZ to address the weaknesses of manual processes (as found in the internal dimensions) by adopting technologies that can improve the accuracy of early detection of risks.

e. Environmental Factors

The environmental dimension is becoming increasingly relevant in risk management practices as global attention increases on sustainability issues and the environmental impact of business activities. In the technology sector, reliance on digital infrastructure poses new challenges related to energy consumption, carbon footprint, and the need for systems that are resistant to environmental disturbances. Data centers, server networks, and intensive computing systems are vital components but have significant ecological consequences, especially in the context of energy efficiency and the resulting emissions.

The issue of sustainability has now transformed from just a social responsibility to a business compliance requirement. Referring to OJK Regulation No. 51/POJK.03/2017 concerning Sustainable Finance, Holding Companies (Holdings) have begun to integrate Environmental, Social, and Governance (ESG) parameters into their subsidiaries' performance indicators. This demands that PT. XYZ to expand its risk management scope. Operational risk identification must now include environmental impacts, such as energy efficiency in data centers and e-waste management. Although the impact is not currently as heavy as the manufacturing sector, failure to meet the carbon emission reporting standards set by the Parent can have an impact on the company's GCG rating.

f. Legal Factors

On the legal dimension, increasing regulations regarding data protection, security s In the legal dimension, the increasingly stringent regulatory landscape related to personal data protection, cybersecurity, and corporate compliance encourages organizations to strengthen internal control frameworks and ensure that all governance processes run consistently and well-documented. Regulations such as the Personal Data Protection Act (PDP Law), cyber incident reporting obligations, and other audit and compliance rules create new standards that must be met by companies, especially those that manage data at scale and have a high reliance on digital systems.

The legality aspect brings material financial risk consequences. The biggest legal risk comes from the full implementation of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). Article 57 of this Law stipulates administrative fine sanctions that can reach 2% of annual income for the violation variable. For data management companies such as PT. XYZ, this potential fine represents a huge exposure to financial risk. In addition to regulatory risks, companies also face high contractual risks. The complexity of service level agreements (SLAs) in IT project contracts often includes strict late penalty clauses. Without precise legal risk mitigation in the pre-contract phase, companies are vulnerable to losses due to penalty claims that can significantly erode project profits.

3. SWOT Matrix

The determination of ST, SO, WT and WO strategies is carried out based on the results of the evaluation of internal and external factors that encompass strengths, weaknesses, opportunities and threats. This approach uses the SWOT method, where the SO strategy focuses on the use of the company's strengths to be able to exploit opportunities, the ST strategy focuses on the utilization of the company's strengths to be able to face threats that can occur, the WO strategy focuses on overcoming the company's weaknesses by taking advantage of existing opportunities, the WT strategy focuses on reducing weaknesses and threats that may occur. This model emphasizes that an effective strategy must focus on an effective response

that refers to internal and external factors that can affect the organization of Belal Dahiam Saif Ghaleb (2024). In the context of risk management, understanding and applying SWOT strategies assists organizations in designing adaptive actions that are appropriate to changes in the environment and internal resources they have (Phadermrod et al. 2019). Therefore, the ST, SO, WO, and WT strategies are a systematic framework to optimize the strategy to increase the maturity of the implementation of risk management of PT. XYZ.

Table 2. SWOT Analysis

INTERNAL	**STRENGTH (S)**	**DISADVANTAGES (W)**
EXTERNAL	1. Integrated Risk Reporting Compliance (Q1) 2. Availability of Basic Framework Documents (S2)	1. Weak Risk Culture & Competence (W1) 2. Ineffective Risk Mitigation Execution (W2) 3. Incomplete Governance Infrastructure (W3)
OPPORTUNITY (O)	**S-O STRATEGY**	**W-O STRATEGY**
1. PER-2/MBU/03/2023 requires ERM & maturity assessment (O1) 2. Advanced Analytics, AI, and Automation (O2) Trends 3. Increasing Demands for ESG and Sustainability (O3) Standards	1. Implementation of Self-Assessment of Risk Maturity (S1 + O1) 2. Integration of ESG Indicators into the Monthly Risk Report (S2 + O3) 3. Piloting the Risk Dashboard using BI (S2 + O2)	1. Formation of Risk Committee (W3 + O1) 2. Digitization of Risk Monitoring (W2+O2) 3. Regulation-Based Competency Enhancement (W1 + O1)
THREAT (T)	**S-T STRATEGY**	**W-T STRATEGY**
1. Escalation of Cyberattacks and Digital Crime (Ransomware) (T1) 2. Risk of Sanctions for Fines of the Personal Data Protection Law (PDP Law) (T2) 3. Talent War and High Human Resource Turnover (T3)	1. Strengthening Personal Data Compliance Audit (S1 + T2) 2. Implementation of Cyber Incident Simulation/Ransomware Handling (S2 + T1) 3. Formation of Risk Champions from Operational Units (S1 + T3)	1. Implementation of Periodic Phishing Tests for Employees (W1 + T1) 2. Creation of Knowledge Management System and SOP (W3 + T3) 3. Prioritization of Critical Risk Mitigation (W2 + T1 + T2)

Source: Primary data processed, 2025

The Strength-Opportunity (SO) strategy is an approach that utilizes the internal strengths of the organization to optimally capture opportunities in the external environment. In the context of risk management, this strategy aims to strengthen the organization's position by integrating superior internal resources and capabilities with opportunities arising from the external environment. Based on the strengths and opportunities that have been identified, several SO strategies can be formulated to significantly improve the effectiveness of risk management as follows:

1) Implementation of Regulation-Based Risk Maturity Self-Assessment (S1 + O1).

PT XYZ can utilize the compliance culture of the reporting of the work unit that has been formed (S1) as the main database in conducting a self-assessment of the level of risk maturity.

This strategy is a response to the mandate of PER-2/MBU/03/2023 which requires SOEs to implement standard Enterprise Risk Management (ERM). In its implementation, PT XYZ does not need to build an assessment system from scratch, but it is enough to convert existing risk report data into SOE maturity assessment parameters. This aims to identify capability gaps early and prepare companies to face external assessments with optimal scores.

2) Piloting a Simple Risk Dashboard for Data Visualization (S2 + O2).

The availability of risk data documented in the framework (S2) allowed PT XYZ to start adopting data analytics (O2) technology. As a first step in digital transformation, this strategy focuses on developing an interactive risk dashboard. The goal is to transform the data presentation pattern from a textual/static table format to a dynamic graphical visualization. This is expected to speed up the risk-informed decision-making process because priority risk profiles can be monitored in real-time. By taking advantage of the opportunities of technological advancements, companies not only improve the quality of decision-making, but also strengthen organizational resilience in the face of increasingly rapid and complex risk dynamics. This strategy also helps companies move towards more predictive and future-oriented data-driven ERM practices.

3) Integration of ESG Indicators into the Monthly Risk Report (Q2 + O3).

In response to global trends and stakeholder pressures related to Environmental, Social, and Governance (ESG) (O3) standards, PT XYZ needs to update its risk management framework (S2) documents. Companies can make adjustments to risk management documents such as risk taxonomy by including ESG risks in them. Furthermore, companies can align risk reporting mechanisms with sustainability reporting standards. This adjustment does not require drastic changes to the existing system, but rather the expansion of indicators and the addition of data attributes so that risk reports can support the preparation of sustainability reports more consistently. Ultimately, this strategy can provide strategic value for companies as it results in strong integration between ERM and the sustainability agenda. By leveraging the existing ERM policy infrastructure, organizations can accelerate adaptation to sustainability demands without a large cost burden, while increasing the company's capacity to anticipate long-term risks that are increasingly relevant in the era of digital transition and dynamic environments.

The Strength-Opportunity (SO) strategy formulated not only maximizes the company's internal strength, but also takes advantage of external opportunities owned by the company in creating sustainable synergies in improving the quality of company risk management. This approach is in line with the principles of strategic management that focus on the importance of adaptation and innovation processes in dealing with the ever-changing dynamics of the external environment David (2017). Consistent implementation of the SO strategy will strengthen the organization's position in managing risks proactively and responsively, thereby supporting the achievement of organizational goals effectively and efficiently

The Strength-Threat (ST) strategy is an approach that utilizes the organization's internal strengths to face and overcome external threats that have the potential to hinder the achievement of organizational goals. In the context of risk management, this strategy is essential to ensure that the organization is not only able to survive the pressures and challenges that arise, but also can manage risks effectively by leveraging the advantages it has. The following are some ST strategies that can be formulated to strengthen organizational resilience in the face of external threats based on the strength factors and threats that have been identified.

1) Strengthening Personal Data Compliance Audit (S1 + T2).

The discipline of risk reporting that has become the strength of PT XYZ (S1) is directed to mitigate legal risks due to the enactment of the Personal Data Protection Law (PDP Law) (T2). The Risk Management Unit can collaborate with Internal Audit to conduct specific compliance audits on the units that manage customer data. This audit not only checks the completeness of documents, but also remaps the data flow reported by the work unit. The focus of the audit includes verifying the consent of the data owner, the storage mechanism, and the user's access rights. This preventive strategy aims to ensure that there are no procedural loopholes that can trigger administrative and criminal corporate sanctions, which can harm PT XYZ's reputation and finances.

2) Implementation of Cyber/Ransomware Incident Simulation (S2 + T1)

PT XYZ already has the strength in the form of the availability of Risk Management Framework (S2) documents. However, policy documents often become irrelevant when dealing with dynamic cyberattacks such as Ransomware (T1) that require a response in minutes. The policy document needs to be tested for validity through real simulations. Given the massive escalation of cyber threats, policy documents should not just be documents. This strategy ensures that the risk management framework document is actionable and that the results of this simulation will be a feedback loop to update mitigation procedures, thus minimizing operational downtime if an actual attack occurs. This simulation aims to measure the readiness of inter-unit coordination and the speed of system recovery response, so that PT XYZ has a tested and valid Business Continuity Plan (BCP).

3) Formation of Risk Champions from Operational Units (S1 + T3)

The threat of Talent War leads to high difficulties and costs in recruiting competent risk management professionals from external (T3). On the other hand, PT XYZ has internal strength in the form of personnel in the operational unit who are used to and compliant in conducting risk reporting (S1). These personnel are hidden assets that understand the business context as well as the language of risk. Management can formalize the role of a team that performs well in the work unit to become a Risk Champion or Risk Ambassador. They will be given formal mandates, intensive training, and performance incentives as an extension of the Central Risk Management Unit in their respective departments (First Line of Defense). Their duties include early risk identification and mitigation monitoring at the operational level. This strategy is an efficient and sustainable solution to overcome the scarcity of human resources at risk. By empowering internal talent, PT XYZ not only saves on recruitment costs, but also strengthens the risk culture organically from the bottom-up and reduces reliance on external experts.

The Weakness-Opportunity (WO) strategy focuses on efforts to overcome the internal weaknesses of the organization by taking advantage of opportunities that exist in the external environment. This approach is very important to improve aspects that are still obstacles in the implementation of risk management, while taking advantage of opportunities that can increase the effectiveness and efficiency of risk management. Based on the weaknesses and opportunities that have been identified, several WO strategies can be formulated as follows:

1) Establishment of Risk Committee as a Governance Mandate (W3 + O1)

The identification of weaknesses shows that the governance infrastructure at PT XYZ is incomplete (W3), especially the absence of specific supervisory organs at the strategic level. Using the momentum of the issuance of regulation PER-2/MBU/03/2023 (O1). The structure

needed by the company is the Risk Management Committee. The company already has a risk management unit that carries out the function of coordinating and facilitating the ERM process, the risk governance structure required by PER-2/MBU/03/2023 is still not fully fulfilled. The regulation requires the existence of a Risk Management Committee at the director/commissioner level as an organ that provides strategic direction, conducts supervision, and ensures that the risk management process is integrated with business decision-making. The absence of the committee causes the strategic risk escalation process to not run optimally and important decisions do not have a challenge-and-review mechanism as standard for SOEs. The existence of the PER-2/MBU/03/2023 (O1) regulation provides an opportunity for companies to immediately improve this structure with a clear legal basis. Therefore, the most relevant strategy is to form a Risk Management Committee, so that weaknesses in the governance aspect (W3) can be overcome while improving the alignment of the ERM process with SOE requirements. The implementation of this strategy will strengthen the role of existing risk management units, create stronger oversight mechanisms, and ensure that strategic risks are managed consistently and accountably across the company's lines.

2) Digitization of Risk Monitoring (W2+O2)

One of PT XYZ's biggest operational obstacles is the ineffectiveness of risk mitigation (W2) execution, which is often caused by manual monitoring processes. The use of automation (O2) technology is the solution to this problem. PT XYZ can develop an Early Warning System (EWS) based on automatic notifications that is integrated with the corporate email platform. Technically, this system will work by tracing the due date of each mitigation plan in the risk register. The system will send automated reminders in stages to the Risk Owner. If the mitigation status has not been updated until the deadline has been exceeded, the system automatically escalates the notification to the direct supervisor or Risk Management Unit as a form of control mechanism. This system functions to collect mitigation status updates from risk owners before the deadline ends, thereby increasing execution discipline and minimizing the risk of unhandled residues. The implementation of this strategy can drastically reduce the number of overdue mitigations. With transparency in the mitigation status monitored by the system, the accountability of risk owners will increase. This ensures that residual risks can be reduced to an acceptable level according to the company's risk appetite.

3) Regulation-Based Competency Enhancement (W1 + O1)

Weak risk culture and competence in employees (W1) is addressed by adopting competency standards required by regulations (O1). PT XYZ can make risk management professional certification obligations mandatory for key officials and organize SOE curriculum-based training for operational staff. With this strategy, PT XYZ can change the paradigm of risk management training from voluntary to mandatory. This program can be divided into two tiers (tiering). First, for the strategic and managerial level, companies require the possession of a nationally recognized risk management professional certification. Second, for the operational staff level, periodic in-house training will be held with a curriculum that is aligned with SOE standards. In addition, the risk competency parameter will be included as one of the Key Performance Indicators (KPIs) in individual assessments.

The Weakness-Threat (WT) strategy aims to minimize internal weaknesses while avoiding or reducing the impact of external threats that can hinder the achievement of organizational goals. In the context of risk management, this strategy is essential to strengthen

organizational resilience by improving weak internal aspects and anticipating challenges from the potentially detrimental external environment. Based on the weaknesses and threats that have been identified, some WT strategies can be formulated as follows:

1) The most fundamental weakness in PT XYZ's cyber defense is not in the software, but in the people aspect. Low employee risk culture and competence (W1) create a massive vulnerability gap to Social Engineering and Ransomware (T1) attacks. Conventional socialization methods are not effective in building vigilance. Therefore, an educational approach that is an active simulation is needed to build awareness. This strategy can change the mindset of employees from passive to alert. A decrease in click-through success rates on phishing simulations will be a quantitative indicator of the success of improving the cyber risk culture. This significantly reduces the probability of successful cyberattacks entering through user negligence.
2) The threat of Talent War (T3) results in a high risk of losing key personnel (key person risk). On the other hand, PT XYZ has weaknesses in the form of uneven competence (W1) and incomplete governance infrastructure. If an expert employee leaves the company without leaving a neat documentation trail, PT XYZ will experience a loss of business processes from key persons where technical and historical knowledge risks being lost along with the employee's departure. Management creates a strategy by converting repetitive knowledge into written documents. This strategy is realized through the development of a centralized Knowledge Management System (KMS). Each work unit is required to prepare a detailed Standard Operating Procedure (SOP) and Work Instructions (IK) for each critical process. In addition, any troubleshooting or risk mitigation should be documented in the Lesson Learned report uploaded to KMS. This policy affirms that knowledge is a company asset, not an employee's personal asset. This system ensures business continuity despite high labor turnover. New hires can learn the work process and related risks more quickly through the resources available in KMS, so that the learning curve can be trimmed and dependence on specific individuals can be minimized.
3) One of PT XYZ's biggest obstacles is the ineffectiveness of mitigation execution (W2) which is often caused by limited resources (budget, time, and effort). In situations where companies are not able to handle all risks at once, the Pareto principle should be applied. Top Management can set budget policies. Mitigation resources will be locked and fully prioritized for high-value risks in the enterprise. Other operational risks whose impact is in the form of minor inefficiencies will be lowered to handle them. This policy must be formalized in the Decree of the Board of Directors so that there is no conflict of interest between divisions in the budget fight. With this strategy, PT XYZ can ensure that weaknesses in internal execution do not lead to catastrophic incidents or damage the company. This ensures that the company remains operational and avoids heavy legal sanctions, giving management time to gradually fix other internal issues.

Managerial Implications

1. PT XYZ needs to emphasize the role of the risk management unit as a second line independent of operational functions, with direct reporting channels to the President Director/Risk Committee and the establishment of a Risk Committee at the

Director/Commissioner level are crucial to ensure that strategic risk discussions are carried out regularly and documented, in line with the demands of PER 2/MBU/03/2023.

2. Low scores on the Culture & Capability dimension indicate the need for a structured risk competency development program (certification, periodic training, coaching to risk owners). The culture of risk needs to be integrated into KPIs and performance appraisal processes, so that staff are encouraged to see risk as part of the job, not just an additional document.
3. The limitations of data models and risk technologies indicate the need for an integrated risk management information system that is able to store risk data centrally, support the Early Warning System, and present a risk dashboard for management.

CONCLUSION

PT XYZ had adopted a risk management framework aligned with ISO 31000:2018 and the regulations of the Ministry of SOEs, as reflected in the availability of policies, guidelines, procedures, and the Three Lines Model structure; however, its implementation remained largely compliance-driven, focusing more on documentation and reporting than on integration with business decision-making and performance management. The Risk Maturity Index measurement based on PER-2/MBU/03/2023 and SK-8/DKU.MBU/12/2023 indicated an average score of 1.6, placing the company in the Early phase, with only the Risk Process and Control dimension reaching an evolving stage, while the other dimensions—Risk Culture and Capabilities, Risk Governance and Organization, Risk and Compliance Framework, and Risk Data and Technology Model—remained at a foundational level. This highlighted a gap between the relatively comprehensive design of the risk management system and its effectiveness in practice. Based on SWOT and TOWS analyses, several strategic initiatives were identified, including establishing a Risk Committee, strengthening the Three Lines Model, enhancing risk culture and competencies, digitizing risk monitoring and reporting, and improving data governance and information security to address regulatory demands and cyber risks. The implementation of these strategies was expected to elevate ERM maturity from the Initial to Developing phase and toward best practice standards for SOEs. Future research is recommended to examine the longitudinal impact of these strategies on ERM effectiveness and organizational performance, as well as to explore comparative studies across SOEs to identify best practices in advancing risk maturity.

REFERENCES

Belal Dahiam Saif Ghaleb. (2024). The importance of using SWOT analysis in business success. *International Journal of Applied Business and Management (IJABM), 3*(4), 557–564. https://doi.org/10.55927/ijabm.v3i4.10857

Bongomin, G., Ntayi, J., Munene, J., & Malinga, C. (2017). The relationship between access to finance and growth of SMEs in developing economies: Financial literacy as a moderator. *Review of International Business and Strategy, 27*(4), 520–538.

Brandt, T. (2021). *Enterprise risk management maturity model*.

BSN. (2018). *SNI ISO 31000:2018 manajemen risiko—Prinsip dan pedoman*.

Coetzee, G. P., & Lubbe, D. (2013). The risk maturity of South African private and public sector organisations. *Southern African Journal of Accountability and Auditing Research, 14*, 45–56.

CRMS Indonesia. (2019). *Survei nasional manajemen risiko 2019*.
David, F. R. (2017). *Strategic management: Concepts and cases* (11th ed.). Prentice Hall.
David, F. R., Kate, S., Thomas, H., & Idalia, M. (2019). Integrating risk, strategy, and performance to enhance decision-making. *The Journal of Government Financial Management, 68*(2), 12–16.
Deloitte. (2023). *Considerations for maturity model selection*.
EY, & Institute of International Finance. (2024). *EY/IIF global bank risk management survey*. Ernst & Young.
Ghani, E. K., Hassin, N. H. N., & Muhammad, K. (2019). Effect of employees' understanding on risk management process on risk management: A case study in a non-profit organisation. *International Journal of Financial Research, 10*(3), 144–152.
Gürel, E. (2017). SWOT analysis: A theoretical review. *Journal of International Social Research, 10*(51), 994–1006. https://doi.org/10.17719/jisr.2017.1832
Hopkin, P. (2018). *Fundamentals of risk management: Understanding, evaluating, and implementing effective risk management*. Kogan Page.
Iswajuni, I., Manasikana, A., & Soetedjo, S. (2018). The effect of enterprise risk management (ERM) on firm value in manufacturing companies listed on Indonesian Stock Exchange year 2010–2013. *Asian Journal of Accounting Research, 3*(2), 224–235. https://doi.org/10.1108/AJAR-06-2018-0006
Leng, P., Basuki, B., & Setiawan, R. (2022). Implementation of enterprise risk management in medium-sized priority sector companies in East Java. *Jurnal Akuntansi dan Keuangan, 24*(2), 80–90.
Leng, P., Basuki, B., & Setiawan, R. (2023). The maturity level of enterprise risk management implementation in medium-sized priority sector companies in East Java. *International Journal of Financial and Investment Studies, 3*(2), 79–93. https://doi.org/10.9744/ijfis.3.2.79-93
Phadermrod, B., Crowder, R. M., & Wills, G. B. (2019). Importance-performance analysis based SWOT analysis. *International Journal of Information Management, 44*, 194–203. https://doi.org/10.1016/j.ijinfomgt.2016.03.009
Sasmita, A. K., & Suhaimi, H. (2020). Implementation of enterprise risk management (ERM) to improve risk culture awareness in Alienco Photo. In *Proceedings of the International Conference on Business and Management Research (ICBMR 2020)* (pp. 233–238).
Sprčić, D. M., Pećina, E., & Orsag, S. (2017). Enterprise risk management practices in listed Croatian companies.
Suhaimi, A. (2020). Analisis manajemen risiko UMKM batik Bangkalan Madura di tengah pandemi COVID-19. *Jurnal Manajemen Risiko, 1*(2), 141–148.
Tjahjono, S. (2017). Enterprise risk management implementation maturity in non-bank and financial companies. *Etikonomi, 16*(2), 173–186. https://doi.org/10.15408/etk.v16i2.5440
Van der Vegt, G. S., Essens, P., Wahlström, M., & George, G. (2015). Managing risk and resilience. *Academy of Management Journal, 58*(4), 971–980. https://doi.org/10.5465/amj.2015.4004
World Economic Forum. (2025). *The global risk report 2025* (Edition 1.0). Forum Publishing.