JOURNAL OF ACCOUNTING AND BUSINESS EDUCATION
P-ISSN 2528-7281 E-ISSN 2528-729X
E-mail: jabe.journal@um.ac.id
http://journal2.um.ac.id/index.php/jabe/

Evaluation of Risk Management Implementation Using COSO ERM 2017 Framework: A Case Study at PT XYZ

Fitria Febriani[1]
Machmudin Eka Prasetya[2]
[1,2] *Master of Accounting Program, Faculty of Economic and Business, Universitas Indonesia, Indonesia*
email: fitria.febriani@ui.ac.id

DOI: http://dx.doi.org/10.17977/jabe.v10i2.63470

Abstract: This study aims to evaluate the implementation of risk management at PT XYZ using the COSO Enterprise Risk Management (ERM) 2017 framework. PT XYZ, a trading and distribution company operating in the industrial equipment sector, faces increasingly complex risks driven by economic uncertainty, supply chain disruptions, and operational vulnerabilities. The study employed a qualitative approach with a case study method, collected data through documentation reviews and semi-structured interviews with seven senior management representatives directly involved in the company's risk management processes. Data analysis used descriptive qualitative methods based on the five components and twenty principles of COSO ERM 2017. The results show that PT XYZ implemented several key aspects of risk management, through its organizational structure, policy guidelines, and processes that support risk management activities. However, several weaknesses remain, such as PT XYZ does not have an audit or risk committee, does not have a formal risk appetite document, incomplete implementation of risk responses, and the lack of a portfolio level risk view. PT XYZ's risk management function also has never been assessed by an independent or external party and does not have whistleblowing system. This research contributes by providing a comprehensive mapping of the implementation of COSO ERM 2017 at PT XYZ and identifying the gap between theory and practice that still occurs in corporate risk management.

Article History
Received:
16 October 2025

Revised:
25 October 2025

Accepted:
1 December 2025

Keywords
COSO ERM 2017; Enterprise Risk Management; Risk Management; Risk Management Implementation

Citation: Febriani, F., & Prasetya, M.E. (2025). Evaluation of Risk Management Implementation Using COSO ERM 2017 Framework: A Case Study at PT XYZ. *Journal of Accounting and Business Education, 10*(2),50-63.

INTRODUCTION

A trading company is generally a form of business organization whose primary activity is purchasing goods from third parties for resale to consumers. This primary activity aims to achieve optimal profit so that the company can continue operating sustainably, maintain its presence in the market, and develop its business towards a more advanced and competitive direction (Wang et al., 2023). In carrying out its operational activities, the company has a structured business process designed to enhance collaboration between business process management, resulting in optimal company performance improvements (Pradabwong et al., 2017).

In facing an increasingly competitive business world, companies are required to manage their resources to achieve strategic goals and optimal performance (Widodo, 2023). Given the dynamic nature

of business development, companies must be more responsive and adaptive to environmental changes and future challenges. Risk management plays a crucial role in identifying, assessing, and managing risks faced by companies, thus providing appropriate strategies for decision making (Ansyari, 2024). Risk management is a coordinated activity related to risk to direct and control a company (Vorst et al., 2018). Meanwhile, risk is the potential for an event that can cause losses due to the uncertainty of an event occurring, which can disrupt operations and decrease financial performance (Yuwono & Ellitan, 2024).

Global business challenges in recent years have been triggered by various factors, including economic instability, commodity price fluctuations, and disruptions to supply chains or procurement of goods and services, leading to new, often conflicting demands from governments, businesses, and the public (Herold & Marzantowicz, 2023). These conditions require companies to adapt to the uncertainties and potential risks that arise in their business activities (Handfield et al., 2020). These risks can originate from both external and internal sources. Effective and well-integrated risk management can improve company performance and value (Tuanakotta, 2019).

Based on data from the Central Statistics Agency (BPS), Indonesian economy is projected to grow by 5.03% in 2024, a decline compared to 5.05% in 2023 (BPS, 2025). Despite stable economic growth at around five percent, the rupiah exchange rate against the US dollar (USD) weakened by approximately 4.8%, from Rp. 15,416 per USD at the end of 2023 to Rp. 16,162 per USD at the end of 2024 (Kemendag, 2025). This weakening rupiah exchange rate puts pressure on import costs and increases financial risks for companies dependent on foreign supplies (Napitupulu et al., 2024).

These economic conditions have a direct impact on PT XYZ's business risks. PT XYZ is a company engaged in the trade and distribution of engineering and industrial equipment, mining and energy, construction, and medical laboratories, with products from well known international brands. Rising import prices due to the weakening rupiah exchange rate can increase the cost of goods sold (COGS) and reduce the company's profit margin. Increased COGS and procurement volumes potentially introduce several types of risks, including financial, market, operational, and fraud risks (Oktalia et al., 2020).

Every business activity carried out by a company faces risks, and risk is inherent in these activities (Lubis & Imsar, 2022). Continuously evolving risks can hamper business activities and company performance. Implementing effective risk management is crucial to mitigate the broad impact of risks, encouraging companies to continuously refine and strengthen their ability to identify and respond to emerging risks (Balaji et al., 2024). Therefore, an enterprise risk management implementation framework is needed, such as Enterprise Risk Management (ERM) Integrating with Strategy and Performance, developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 2017 and widely used in global risk management practices (COSO, 2017). COSO ERM enables companies to integrate risk management into all operational activities, implement strategic decision-making, and improve business performance (Febrianti & Novita, 2021).

Research conducted by Vincent & Barkhi (2021) explains that implementing the COSO ERM framework requires adequate consideration of how to manage a collaborative and integrated supply chain ecosystem using blockchain technology. A sound application of ERM in enterprise risk management can achieve business objectives by identifying risks based on the company's risk appetite and risk profile, and taking strategic risk management steps that directly impact company performance (Magradee, 2023). Synergistic alignment by utilizing ERM components can improve overall risk oversight (Stasse et al., 2025). Various ERM practices, such as risk governance, risk culture, risk artifacts, and risk awareness, and the shift from traditional to ERM risk management practices constitute a continuous risk development process to ensure risk management aligns with company strategy (Monazzam & Crawford, 2024).

This research provides a novel contribution to the literature evaluating the implementation of risk management using the 2017 COSO ERM framework in companies engaged in the trading and distribution of industrial equipment, a practice rarely studied compared to the public sector, banking, or manufacturing. In carrying out its business processes, PT XYZ faces increasingly complex challenges, particularly uncertain economic conditions and growing potential risks. This study aims to evaluate the implementation of more effective risk management at PT XYZ and provide recommendations for relevant strategic

improvements according to PT XYZ's conditions to support risk management performance and strengthen the company's resilience in facing various risks to achieve business goals sustainably.

LITERATURE REVIEW AND HYPOTHESES

Risk

Risk can have different meanings for each individual. The word "risk" can connote opportunity, uncertainty, threat, danger, or other negative connotations that could lead to loss (Lam, 2017). Given these negative consequences, risk is an inseparable part of life; in other words, no activity is free of risk (Setiawan, 2024). Therefore, risk is not something that should be completely avoided, but rather how individuals or organizations respond to and manage the risks they face.

Risk is the possibility of an event occurring that impacts the achievement of strategy and business objectives (COSO, 2020). Risk is associated with uncertainty, which can result in gain or loss. This aligns with the business context, where risk has two sides: positive and negative. With risk, there is the opportunity to generate profit (Lam, 2017). However, risk is uncertain, resulting in negative outcomes due to a lack or unavailability of information about what is or will happen (Oktalia et al., 2020). Every action or decision contains a certain level of risk, which must be taken by the organization to achieve its goals, therefore it is important to be able to manage and evaluate risks effectively (Magradee, 2023)

Risk Management

Every organization has various types of inherent risks, requiring a tool mechanism that can support decision-making by considering the risks involved (Moeller, 2011). To manage corporate risk, management needs to take a further step and communicate with the board of directors and stakeholders regarding risk management that can be used to achieve corporate objectives (COSO, 2017). Risk within a company can be managed through the implementation of an organized risk management system that directs and controls the company (Vorst et al., 2018).

Risk management is a comprehensive and continuous process for managing various types of corporate risks, such as strategic, financial, operational, and other risks, with the goal of reducing the likelihood of undesirable events and increasing company value (Shrivastava et al., 2024). Risk management is also a culture, capability, and practice integrated with the strategy-setting and performance processes to manage risk in an effort to create, maintain, and enhance value (COSO, 2017).

COSO Enterprise Risk Management

COSO stated in its 2017 Executive Summary, Enterprise Risk Management – Integrating with Strategy and Performance (COSO ERM) that enterprise risk management plays a crucial role in the strategic planning process and its implementation across the organization, as the risks faced not only affect business activities, but also align strategy and performance across all existing departments and functions, thereby helping the company ensure overall operational effectiveness (COSO, 2017). In addition, COSO ERM framework is based on the latest risk management standards commonly applied to operational business activities to identify risk complexity, the emergence of new risks, and increase the attention and oversight of the board of directors and executives towards enterprise risk management (Prewett & Terry, 2018).

COSO ERM 2017 emphasizes the importance of a flexible enterprise management system that adapts easily to changing situations and dynamic business conditions. This approach is the first step in continuously improving a company's quality and capabilities, enabling the organization to remain competitive and face long-term challenges more effectively (COSO, 2017).

Figure 1. Component of the COSO Enterprise Risk Management
Source: COSO Enterprise Risk Management – Integrating with Strategy and Performance (2017)

COSO ERM framework is a set of organized and interrelated principles comprising five risk management components. Figure 1 shows the relationship between these five components and the organization's vision, mission, and core values. The diagram contains three lines: strategy and objective-setting, performance, and review and revision, representing the overall general processes carried out by the organization. The other two lines, governance and culture, and information communication and reporting, represent the supporting elements of the organization's risk management. The five COSO ERM 2017 components are: (1) Governance and Culture, serve as the foundation for supporting other components of organizational risk management. Governance sets the tone of an organization, reinforces the importance of risk management, and establishes responsibility for oversight of the organization's risk management. Culture relates to the ethical values, behaviors, and understanding of risk that influence management and individual decision-making within the organization. (2) Strategy and Objective-Setting, organizational risk management plays a role in the strategic planning process, collaborating with the organization's established strategy and objectives. Risk appetite is established to align with the organization's strategy, while business objectives in implementing the strategy serve as the basis for identifying, analyzing, and responding to risks. (3) Performance, risks that could impact the achievement of business strategies and objectives must be identified and analyzed. Risk priorities must be determined based on severity, taking into account the organization's established risk appetite. Then, the organization can select appropriate risk management responses and conduct a comprehensive risk assessment. (4) Review and Revision, by reviewing an organization's performance, the organization can evaluate the effectiveness of risk management over time and consider changes that require adjustments or revisions to improve organizational risk management. (5) Information Communication and Reporting, communication is the process of providing, sharing, and obtaining necessary information repeatedly throughout the organization. Organizational risk management requires ongoing communication to gather and convey relevant information from various internal and external sources, flowing across all levels of the organization to support risk management.

The five components of COSO ERM 2017 are supported by twenty principles. These principles cover a wide range of areas, from governance to monitoring, and can be tailored to the needs of organizations of any size, type, or sector. These principles are also flexible, allowing for adaptation to the organization's size, type, and sector. By applying these principles, it is hoped that it will help organizations provide adequate assurance and understand and strive to manage risks related to the organization's strategies and objectives (Abdaljabar et al., 2025).

These 20 principles are a key component of the COSO ERM framework. These principles focus on the need for organizations to develop and implement effective risk management to mitigate risks and ensure

the achievement of business objectives (COSO, 2020). With a systematic approach, COSO ERM helps organizations identify, assess, and respond appropriately to risks (Yuwono & Ellitan, 2024).

Implementation of Risk Management Using COSO Enterprise Risk Management

Effective risk management implementation requires a comprehensive and integrated framework to manage emerging risks so they can be systematically identified, assessed, and controlled (Grebel & Rajmane, 2023). COSO ERM 2017 is a framework that has been widely used in various sectors because it is able to integrate risk with organizational strategy and performance (COSO, 2017). COSO ERM 2017 includes concepts such as risk appetite, tolerance, strategy, and business objectives with a focus on creating, maintaining, and realizing organizational value (COSO, 2020). The implementation of risk management refers to the five components and twenty principles of COSO ERM 2017. Figure 2 illustrates the conceptual framework used in this study to evaluate the risk management implementation at PT XYZ.

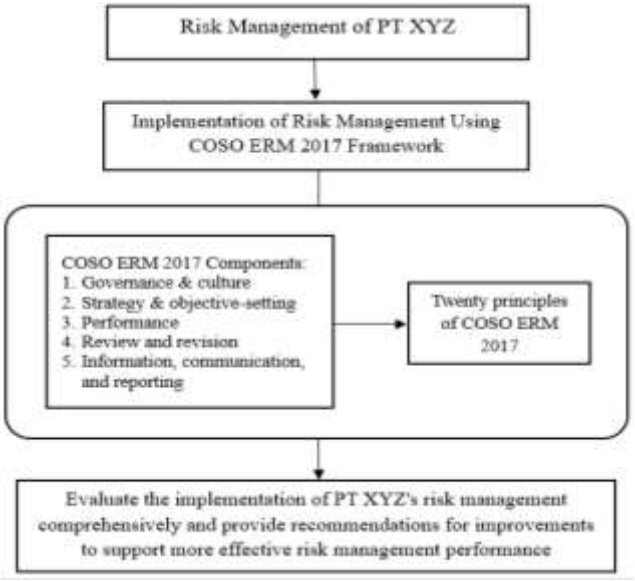

Figure 2. Research Conceptual Framework

Source: Processed Research Results (2025)

METHODS

This study uses a qualitative approach with a case study method to evaluate the implementation of risk management at PT XYZ, specifically using COSO ERM 2017. The qualitative approach can be used to answer existing problems and provide a detailed description of the conditions experienced by the research object (Saunders et al., 2019). The case study method provides a description of the problems related to the circumstances experienced by the research object and provides answers to these problems (Ellet, 2018). A case study approach was employed in this research as it is particularly well suited for conducting an in-depth evaluation of a specific, real world phenomenon, in this instance, the risk management implementation within PT XYZ.

This study uses a combination of secondary and primary data to obtain in-depth and comprehensive information. Secondary data was collection through review and verification of data or documents obtained from PT XYZ, and other documents relevant to the research object. Documentation of these data aims to describe the data that has been collected and as supporting documentary evidence of risk management implementation in PT XYZ.

Primary data collection was carried out through a semi-structured and in-depth interview process. The use of research interviews can help to collect valid and reliable data that is relevant to research questions and objectives (Saunders et al., 2019). In qualitative research, individuals are often referred to as

"informants" because they contribute valuable perspectives and understanding about the subject under investigation (Solarino & Aguinis, 2020). This research interview was conducted with seven relevant respondents related to this research, which are presented in Table 1.

Table 1. Respondent Codes

No.	Respondent Source Code	Respondent Source Role
1.	R1	Risk Management Director
2.	R2	Head of Business Risk & Analyst Division
3.	R3	Head of Internal Audit Division
4.	R4	Head of Procurement, Logistic, & Warehouse Division
5.	R5	Head of Human Resources Division
6.	R6	Head of Finance, Controlling, & General Affairs Division
7.	R7	Head of Marketing Research, Business, & IT Development Division

Source: Processed Research Results (2025)

Respondents were selected because they are senior management at PT XYZ and have executive and managerial positions that directly influence PT XYZ's risk management process. The primary instrument used in this study was an interview guide developed based on the COSO ERM 2017 framework. This interview guide included structured questions designed to obtain information and an overview of the implementation of risk management using COSO ERM 2017 at PT XYZ.

This study uses descriptive qualitative methods for data analysis. The descriptive qualitative method describes in-depth and detailed research on the object to be researched, and is more flexible in the process of collecting data and information according to conditions in the field (Saunders et al., 2019). The results of the descriptive qualitative analysis are used to answer questions related to how risk management is implemented at PT XYZ and provide recommendations for creating continuous improvements in increasing the implementation of more effective risk management. The categories of the evaluation results of the implementation of risk management at PT XYZ used based on the results of the descriptive qualitative analysis divided them into three categories, namely fulfilled, partially fulfilled, and not fulfilled.

RESULTS AND DISCUSSION

This study aims to evaluate the implementation of risk management at PT XYZ using COSO ERM 2017. This study was conducted with seven respondents who have strategic and core roles in the risk management. The seven respondents are PT XYZ management and hold executive and managerial positions that directly influence the risk management. The purpose of the interviews with the respondents was to explore and obtain in-depth and detailed information regarding the ongoing implementation of risk management, and any obstacles or weaknesses encountered in implementing PT XYZ's risk management.

Interviews with respondents obtained detailed information regarding PT XYZ's implementation of risk management. To analyze and evaluate the implementation of risk management in PT XYZ using five components and twenty princips of COSO ERM 2017 framework, the following implementing of risk management analysis and evaluation is described in Table 2.

Table 2. Analysis and Evaluation of Risk Management Implementation at PT XYZ

No	COSO ERM 2017 Components	COSO ERM 2017 Principles	Analysis and Evaluation	Evaluation Results
1	Governance and Culture	Exercise Board Risk Governance	PT XYZ has a risk management guideline document that clearly outlines the role, structure, and responsibilities of the Board. Executive management responsibilities are also formally defined in the guideline. Furthermore, the company has appointed a risk management officer, the Head of the Business Risk & Analyst Division, to manage risk management. However,	Partially fulfilled

No	COSO ERM 2017 Components	COSO ERM 2017 Principles	Analysis and Evaluation	Evaluation Results
			PT XYZ does not yet have an audit committee or risk monitoring committee formally responsible for risk oversight.	
2		Establishes Operating Structure	PT XYZ has a clear organizational structure documented in the company profile, thus ensuring that all functions run effectively.	Fulfilled
3		Defines Desired Culture	PT XYZ has a code of ethics outlined in company regulations that serves as a guideline for the behavior of all employees. Employee hiring and firing standards have also been formally established through company regulations and Human Resources Division policies, ensuring consistency in human resource management. Furthermore, PT XYZ has developed a risk management philosophy documented in a risk management guideline approved by the Board of Directors and Board of Commissioners in 2023.	Fulfilled
4		Demontrates Commitment to Values	PT XYZ has a good commitment through ethical values training that has been carried out by the Human Resources Division of PT XYZ through new employee orientation by referring to company regulations and the company profile.	Fulfilled
5		Attracts, Develops, and Retains Capable	PT XYZ has undertaken various efforts to develop competent employees through training and development programs organized by the Human Resources Division. The company also provides a formal remuneration policy approved by the Board of Directors and establishes key performance indicators (KPI) for all employees to ensure measurable performance. However, PT XYZ does not yet have a compensation policy specifically designed to align management and shareholder interests.	Partially fulfilled
6	Strategy and Objective-Setting	Analyze Business Context	PT XYZ conducted a SWOT analysis in a joint meeting to find out what factors could influence the business, which would then be used as a basis for compiling next year's work program.	Fulfilled
7		Defines Risk Appetite	PT XYZ does not yet have a formal written document or statement regarding the company's risk appetite, determination of risk appetite, communication of coordination meetings between divisions or departments with top management (board of directors).	Not fulfilled
8		Evaluates Alternative Strategies	PT XYZ has demonstrated efforts to respond to various strategic alternatives, through coordination meetings with root cause analysis (RCA) to consider potential risks and opportunities.	Fulfilled
9		Formulates Business Objective	PT XYZ's performance targets are business objectives stated in the company's vision and mission, and are developed using a top-down approach in the form of KPIs for each individual.	Fulfilled
10	Performance	Identifies Risk	Available in risk identification in PT XYZ's risk management guidelines and risk register.	Fulfilled

No	COSO ERM 2017 Components	COSO ERM 2017 Principles	Analysis and Evaluation	Evaluation Results
11		Assesses Severity of Risk	Available in the risk likelihood and impact criteria for PT XYZ. Risk assessment has been applied in assigning a score to each risk in the risk register.	Fulfilled
12		Prioritizes Risks	The risk management policy is outlined in PT XYZ's risk management guidelines. Each risk is assessed based on the likelihood and impact of its occurrence. The risk level is then measured using a risk matrix and risk management is implemented accordingly.	Fulfilled
13		Implements Risk Responses	PT XYZ has a risk response policy listed in the risk management guidelines, but it has not been fully implemented in the company's activities.	Partially fulfilled
14		Develops Portfolio View	The implementation of PT XYZ's risk management is still carried out at the department level, and has not yet reached the company's overall portfolio level.	Not fulfilled
15	Review and Revision	Assesses Substantial Change	PT XYZ collects risk data from each department through a structured survey annually, in conjunction with the development of work programs. Risk updates are conducted annually, and any changes to the risk are reported to the board of directors or management. However, if no such reporting occurs, significant risks could arise.	Partially fulfilled
16		Review Risk and Perfomance	PT XYZ conducts regular risk monitoring and reviews, particularly regarding risk mitigation agreed upon by each department. This involves appointing a person in charge (PIC) to complete the mitigation. However, PT XYZ's risk management function has never been assessed by an independent or external party.	Partially fulfilled
17		Pursues Improvement in ERM	PT XYZ's internal audit process uses risk based audits, thus helping company management create continuous improvement.	Fulfilled
18	Information, Communication and Reporting	Leverages Information and Technology	PT XYZ utilizes technology and information systems by developing a risk management dashboard to increase the effectiveness of the risk-based decision-making process.	Fulfilled
19		Communicates Risk Information	PT XYZ's communication pattern is top down, with the Human Resources Division conducting risk awareness through training, new employee onboarding, and town hall meetings. PT XYZ utilizes several communication channels, including inter divisional coordination meetings, official company email, Microsoft Teams, and an ERP system. External communication is communicated through official letters, email, and business meetings and virtual meetings.	Fulfilled
20		Reports on Risk, Culture, and Performance	Each department and division produces quarterly reports on business process risk control and security risk management activities, which are then consolidated by the BRNA Division into a Quarterly Risk Management Report and	Partially fulfilled

No	COSO ERM 2017 Components	COSO ERM 2017 Principles	Analysis and Evaluation	Evaluation Results
			submitted to the Board of Directors and Commissioners. However, PT XYZ does not yet have a whistleblowing system for reporting violations of laws, regulations, or other irregularities.	

Source: Processed Research Results (2025)

Based on Table 2, the implementation of risk management at PT XYZ shows that the company has implemented most of the principles adequately, although there are still aspects of risk management that have not been met according to the COSO ERM 2017 criteria. In the Governance and Culture component, PT XYZ has a risk management guideline that explains the roles and responsibilities of the Board and executive management. The Business Risk & Analyst Division (BRNA) has also been appointed as the person responsible for risk management. However, the company still does not have a formally functioning audit committee or risk monitoring committee. This condition has been explained by the respondent.

> "…we have implemented a three-line model within the structure of PT XYZ, which defines roles and responsibilities according to their functions. In the future, we may establish a special committee, such as a risk monitoring committee, to jointly identify risks and their impact on the company.*"* (R1, 2025).

The absence of an audit committee or risk monitoring committee weakens the formal risk oversight function and control system at the strategic level. The establishment and strengthening of both committees is crucial to ensuring effective risk governance and protecting the organization from strategic and operational risks (Soobaroyena et al., 2019).

On the other hand, PT XYZ has met the principles related to organizational structure, desired culture, commitment to core values, and employee development efforts through training and competency improvement programs. However, the company still lacks a compensation policy that directly aligns the interests of management and shareholders. This has the potential to reduce the effectiveness of goal alignment between management and shareholders, increase the risk of opportunistic behavior, and decrease the company's value (Park & Byun, 2021).

In the Strategy and Objective-Setting component, PT XYZ has conducted a formal business context analysis through a SWOT analysis, which serves as the basis for developing its annual work program. The company has also established business objectives through its vision, mission, and derived key risk indicators (KPI) for each individual. Meanwhile, risk limits have not been formalized and require internal dissemination, as some divisions or departments are not yet aware of risk appetite, as explained by respondents.

> "There are no tolerance limits in the risk management guidelines yet. Going forward, my team and I will try to coordinate further on this so that it can be formalized in the guidelines." (R2, 2025).
>
> "... we usually receive guidance on what is permitted and what is not permitted from the board of directors. As for risk appetite, I can't confirm whether it exists yet." (R4, 2025).

These unformalized risk boundaries can result in inconsistencies in risk acceptance or avoidance across departments, and potentially hinder the effectiveness of overall risk management (Ullah et al., 2022).

For the Performance component, PT XYZ has successfully identified, assessed, and prioritized risks systematically based on applicable guidelines. The risk register is used as a tool to monitor risks, and risk assessments are conducted using likelihood and impact criteria. However, the implementation of risk responses has not been fully implemented in daily business activities, as explained by respondents in interviews.

> "Although the risk response policy is in place, its implementation is not yet fully underway. We are currently remapping the main risk areas and determining the most realistic and efficient mitigation measures." (R2, 2025).

> "...although the risk response policy has been established, its implementation is still in the socialization stage..." (R4, 2025).

In addition, the implementation of enterprise risk management is still limited to the departmental level and has not yet formed a portfolio view of risk at the company level, which can reduce the effectiveness of ERM as a whole (Balaji et al., 2024).

In the Review and Revision component, PT XYZ collects risk data annually and provides a reporting mechanism for changes in risk. However, the frequency of risk updates, which is only once a year, and the reliance on manual reporting from departments, means significant risks may not be detected in a timely manner. This is consistent with the explanations of several interview respondents.

> "...we see that the risk management process at PT XYZ is still carried out by department. There is no system that combines all risk profiles into a single, comprehensive view." (R3, 2025).
>
> "Currently, there is no mechanism to link these risks to risks in other divisions. So, PT XYZ does not yet have a comprehensive risk view at the company level." (R7, 2025).

BRNA Division periodically monitors and reviews risk mitigation, and each department then reports on its progress. This aligns with the statement from respondent R1 in the interview.

> "...evaluate the effectiveness of risk management through a periodic monitoring and review process of the risk mitigation plans agreed upon with each department. We monitor the progress of each identified risk against the established timeline..." (R1, 2025).

Although a risk mitigation monitoring process has been implemented internally, PT XYZ has never engaged an independent or external party to assess its risk management function. This situation can limit the ability to assess the extent to which the risk management system is integrated with the company's performance (Feitosa et al., 2021). The following are some explanations from interview respondents regarding the lack of an independent or external assessment at PT XYZ.

> "To date, no risk management assessments or audits have been conducted by external parties. All evaluation processes are still managed internally by our team." (R2, 2025)
>
> "...but for formal assessments of the risk management function itself, we have never engaged an independent or external party. This internal audit is part of internal monitoring, while the external audit provides additional confirmation that risk management is up to standard and effective." (R3, 2025).

In the Information, Communication, and Reporting component, PT XYZ has utilized technology through the development of a risk management dashboard and established a structured and hierarchical risk communication model. To strengthen understanding among all employees, the Human Resources Division conducts risk awareness campaigns through training, new employee onboarding, and town hall meetings.

> *"*We, at the Board of Directors, emphasize that risk management is not solely the responsibility of one division, but of all employees. Our communication flows from the Board of Directors to Division Heads, then down to managers and staff." (R1, 2025).
>
> "Human Resources is tasked with acting as a liaison in communicating the importance of risk management to all employees, through training, new employee onboarding, and town hall meetings with the Board of Directors." (R5, 2025).

Risk reporting is also conducted quarterly and consolidated to the Board of Directors and Commissioners. In terms of risk culture, interviews indicate that PT XYZ has begun to instill risk awareness at all levels of the organization through the Internal Audit Division and the Human Resources Division. Both divisions strive to ensure that the values of compliance, integrity, and responsibility are part of daily work behavior. However, weaknesses remain in the risk culture aspect, namely the lack of a formal communication channel for reporting violations of laws, regulations, or other irregularities (a whistleblowing system).

> "PT XYZ does not yet have a formal whistleblowing system. This is a concern for us because such a reporting channel is crucial for maintaining integrity and a healthy risk culture." (R3, 2025).

> "...we acknowledge that the lack of a reporting channel for violations presents a challenge. Moving forward, HR will coordinate with the Risk Management Directorate and Internal Audit to establish such a mechanism so that employees have a safe space to report irregularities without fear." (R5, 2025).

The lack of a whistleblowing system indicates that there are still gaps in the violation reporting system and the strengthening of an integrity culture. The absence of these channels can result in low transparency and an increased risk of undetected irregularities (Gao et al., 2015).

CONCLUSION

This study aims to evaluate the implementation of more effective risk management at PT XYZ and provide recommendations for relevant strategic improvements according to the conditions of PT XYZ to support risk management performance and strengthen the company's resilience in facing various risks to achieve business goals sustainably. The results of the evaluation of the implementation of risk management at PT XYZ based on the COSO ERM 2017 framework can be categorized as "partially fulfilled". PT XYZ has demonstrated a commitment to implementing risk management through organizational structures, policy guidelines, and processes that support risk management activities. However, the evaluation results indicate that there are still several aspects of risk management that have not been met according to the COSO ERM 2017 criteria.

The main weakness identified in this study relates to the absence of an audit committee or risk monitoring committee formally responsible for the risk oversight function. The absence of a risk appetite document also indicates that the company lacks clearly defined risk boundaries, potentially leading to inconsistent decision making across departments. Suboptimal implementation of risk responses, and risk management that remains at the departmental level rather than the portfolio level, also have a strategic impact on the company's inability to view and address risks holistically. Furthermore, the one time risk update process can lead to significant risks not being detected in a timely manner. The absence of external review or a whistleblowing system also weakens the company's ability to maintain objectivity in risk evaluation and management.

The implications of these shortcomings indicate that PT XYZ has the potential to face strategic, operational, and compliance risks that may not be optimally managed. Without clear risk boundaries and a robust oversight structure, the company may experience a mismatch between its business strategy and the risks it can actually bear. Similarly, the lack of dynamic risk updates can result in risk surprises, the sudden emergence of major risk events due to lack of regular monitoring. This situation indicates that although the basic elements of risk management are in place, the effectiveness of their implementation has not reached the ideal level.

To improve the effectiveness of risk management implementation, PT XYZ needs to take several strategic steps, including establishing an audit committee or risk monitoring committee to strengthen risk governance at the Board level. Preparing a formal risk appetite statement is crucial to ensure that every decision is aligned with the company's risk capacity. Implementation of risk responses also needs to be strengthened with an integrated monitoring system. Furthermore, the company is advised to develop risk management at the portfolio level to comprehensively assess risk correlations across business units. Risk updates should be conducted more frequently, utilizing technology, so that changes in risk can be identified in real time. PT XYZ also needs to involve an independent party to evaluate its ERM function and develop a whistleblowing system to increase transparency and early detection of violations.

This study provides an important contribution in evaluating the effectiveness of risk management implementation at PT XYZ using the COSO ERM 2017 framework, resulting in a comprehensive picture of the company's readiness level in managing risk in an integrated manner. This study shows how non financial companies in Indonesia implement COSO ERM principles, thus presenting a gap between formal guidelines and operational implementation that can affect the effectiveness of the risk management system. This approach has practical value for practitioners and can be adapted across various non-financial

companies. More broadly, these findings support efforts to improve risk management implementation by integrating it into strategy and performance in a comprehensive manner.

REFERENCES

Abdaljabar, W. M., Zakuan, N., Saman, M. Z., & Setapa, D. M. (2025). The Effect of Enterprise Risk Management Implementation on Non-Financial Performance in Jordan Manufacturing Firms: A Review. *Information Management and Business Review, 17*(1(I)), 148-157. doi:https://doi.org/10.22610/imbr.v17i1(I).4361

Ansyari, S. (2024). Implementation of Risk Management in Strategic Decision Making. *Journal of Scientific Interdisciplinary, 1*(1), 35-44. doi:https://doi.org/10.62504/t7c2r379

Balaji, S., Shreshta, L., & Sujatha, K. (2024). A Study on Risk Management in Corporate Business. *Involvement International Journal of Business, 1*(3), 197-209. doi:https://doi.org/10.62569/iijb.v1i3.26

BPS. (2025). *Berita Resmi Statistik.* Badan Pusat Statistik. Retrieved from https://www.bps.go.id/id/pressrelease

COSO. (2017). Enterprise Risk Management - Integrating with Strategy and Performance Executive Summary. Committee of Sponsoring Organizations of the Treadway Commission.

COSO. (2020). Compliance Risk Management: Applying The COSO ERM Framework. Committee of Sponsoring Organizations of the Treadway Commission.

Ellet, W. (2018). *The Case Study Handbook A Student's Guide.* Harvard Business Review Press.

Febrianti, I., & Novita, N. (2021). COSO's Enterprise Risk Management Framework in Agriculture Startup to Support the Achievement of SDGs Pillars. *5*(1), 18-36. doi:https://doi.org/10.20473/tijab.V5.I1.2021.18-36

Feitosa, I. S., Carpinetti, L. C., & Almeida-Filho, A. T. (2021). A supply chain risk management maturity model and a multi-criteria classification approach. *Benchmarking: An International Journal, 28*(9), 2636–2655. doi:https://doi.org/10.1108/BIJ-09-2020-0487

Gao, J., Greenberg, R., & Wong-On-Wing, B. (2015). Whistleblowing Intentions of Lower-Level Employees: The Effect of Reporting Channel, Bystanders, and Wrongdoer Power Status. *Journal of Business Ethics, 126*(1), 85-99. doi:https://doi.org/10.1007/s10551-013-2008-4

Grebel, P. V., & Rajmane, S. (2023). Proposed Framework and Method for Integrating Risks into an Organizational Setting. *Journal of Enterprise and Business Intelligence , 3*(3), 126-134. doi:https://doi.org/10.53759/5181/JEBI202303013

Handfield, R., Sun, H., & Rothenberg, L. (2020). Assessing Supply Chain Risk for Apparel Production in Low Cost Countries Using Newsfeed Analysis. *Supply Chain Management: An International Journal, 25 (6)*, 803–821. doi:https://doi.org/10.1108/SCM-11-2019-0423

Herold, D. M., & Marzantowicz, Ł. (2023). Supply chain responses to global disruptions and its ripple effects: an institutional complexity perspective. *Operations Management Research*. doi:https://doi.org/10.1007/s12063-023-00404-w

Junaedi, U. A., Saroh, S., & Trianti, K. (2025). Analisis Proses Manajemen Risiko Operasional (Studi Kasus Pada Cv. Indo Pratama). *Jiagabi, 14*(2), 458 – 469.

Kemendag. (2025). Nilai Tukar Mata Uang Asing Terhadap Rupiah. *satu data perdagangan*. Pusat Data dan Sistem Informasi Kemendag RI. Retrieved from https://satudata.kemendag.go.id/data-informasi/perdagangan-dalam-negeri/nilai-tukar

Lam, J. (2017). *Implementing Enterprise Risk Management: From Methods to Applications.* John Wiley & Sons, Inc.

Lubis, M. D., & Imsar. (2022). Analisis Manajemen Risiko Operasional Berdasarkan Pendekatan Enterprise Risk Management (Erm) Pada Ud. Anugrah Cabang Rantauprapat. *JMBI UNSRAT (Jurnal Ilmiah Manajemen Bisnis Dan Inovasi Universitas Sam Ratulangi)*, 1492-1504. doi:https://doi.org/10.35794/jmbi.v9i3.44457

Magradee, P. (2023). Enterprise Risk Management Case Study : PTT Exploration and Production Public Company Limited. Thammasat University, Faculty of Commerce and Accountancy. Retrieved from http://ethesisarchive.library.tu.ac.th/thesis/2023/TU_2023_6502022111_17958_28016.pdf

Moeller, R. R. (2011). *COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes* (2nd ed.). John Wiley & Sons, Inc.

Monazzam, A., & Crawford, J. (2024). The role of enterprise risk management in enabling organisational resilience: a case study of the Swedish mining industry. *Journal of Management Control, 35*(1), 59-108. doi:https://doi.org/10.1007/s00187-024-00370-9

Napitupulu, B. E., Rajagukguk, J. S., & Siswono, S. (2024). The Managerial Economics Implications Of Rupiah Exchange Rate Fluctuations On Investment And Corporate Growth. *International Journal of Informatics, Economics, Management and Science, 3*(2), 174-187. doi:https://doi.org/10.52362/ijiems.v3i2.1528

Oktalia, R. D., Nafiah, S. I., & Kusuma, D. (2020). Analisa Dan Mitigasi Risiko Pada Proses Pengadaan Barang Menggunakan Metode House Of Risk. *Prosiding Industrial Engineering National Conference (IENACO)*, 318-323.

Park, W., & Byun, C. (2021). Effect of SME's Managerial Ability and Executive Compensation on Firm Value. *Sustainability, 13*(21), 1-16. doi:https://doi.org/10.3390/su132111828

Pradabwong, J., Braziotis, C., Tannock, J. D., & Pawar, K. S. (2017). Business process management and supply chain collaboration: effects on performance and competitiveness. *Supply Chain Management: An International Journal, 22*(2), 107–121. doi:https://doi.org/10.1108/SCM-01-2017-0008

Prewett, K., & Terry, A. (2018). COSO's Updated Enterprise Risk Management Framework—A Quest For Depth And Clarity. *Journal of Corporate Accounting & Finance, 29*(3). doi:https://doi.org/10.1002/jcaf.22346

Saunders, M. N., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students* (8th ed.). Research Methods for Business Students.

Setiawan, T. (2024). Evaluasi Penerapan Manajemen Risiko pada RSUD XYZ. Program Magister Akuntansi Fakultas Ekonomi dan Bisnis Universitas Indonesia. Retrieved from https://lib.ui.ac.id/detail?id=9999920549127&lokasi=lokal

Shrivastava, V. K., Balasubramanian, J., Katyal, A., Yadav, A., & Yogananthan, S. (2024). Understanding the significance of risk management in enterprise management dynamics. *Multidisciplinary Reviews, 6*(2023), 1-8. doi:https://doi.org/10.31893/multirev.2023ss093

Solarino, A. M., & Aguinis, H. (2020). Challenges and Best-practice Recommendations for Designing and Conducting Interviews with Elite Informants. *58*(3), 649-672. doi:https://doi.org/10.1111/joms.12620

Soobaroyena, T., Ntimb, C. G., Broadb, M. J., Agrizzia, D., & Vithana, K. (2019). Exploring the Oversight of Risk Management in UK Higher Education Institutions: The Case of Audit Committees. *Accounting forum, 43*(4), 404-425. doi:https://doi.org/10.1080/01559982.2019.1605872

Stasse, L. J., Hilhorst, C. A., & Rouwelaar, J. A. (2025). Enterprise risk management revisited: a study to identify the elements of ERM. *Journal of Risk Research, 28*(7), 768–793. doi:https://doi.org/10.1080/13669877.2025.2553846

Tuanakotta, T. M. (2019). *Audit Internal Berbasis Risiko* . Salemba Empat.

Ullah, S., Mufti, N. A., Saleem, M. Q., Hussain, A., Lodhi, R. N., & Asad, R. (2022). Identification of Factors Affecting Risk Appetite of Organizations in Selection of Mega Construction Projects. *Buildings, 12*(1), 1-19. doi:https://doi.org/10.3390/buildings12010002

Vincent, N. E., & Barkhi, R. (2021). Evaluating Blockchain Using COSO. *Current Issues in Auditing, 15*(1), A57–A71. doi:https://doi.org/10.2308/CIIA-2019-509

Vorst, C. R., Priyarsono, D., & Budiman, A. (2018). Manajemen Risiko Berbasis SNI ISO 31000. Badan Standardisasi Nasional. Retrieved from https://perpustakaan.bsn.go.id/repository/ca09e618c360ecd38f4f0ccfc828a2ff.pdf

Wang, W., Zhang, D., Wang, H., Zhu, Q., & Heravi, H. M. (2023). How do businesses achieve sustainable success and gain a competitive advantage in the green era? *Kybernetes, 52*(9), 3241–3260. doi:https://doi.org/10.1108/K-07-2021-0614

Widodo, S. (2023). *Manajemen Strategik: Keunggulan Bersaing Berkelanjutan.* Penerbit NEM.

Yuwono, M. A., & Ellitan, L. (2024). Evaluating the application of components governance and culture based on COSO ERM at PT. Agro. *Journal of Business Management and Accounting, 14 (2)*, 307-338. doi:https://doi.org/10.32890/jbma2024.14.2.5