International Journal of
Economics Development Research, Volume 5(1), 2024
pp. 625-644

Operational Risk Management Design Based on The COSO Enterprise Risk Management Approach : Case Study at TMAP

Arya Prabadaru[1], Yan Rahardian[2]

Abstract:

Every business activity is always filled with uncertainty which can create risks. These risks can have a negative impact on achieving the company's vision, mission and goals. Therefore, handling these risks must be carried out in a comprehensive and integrated manner. Risk management is a system or method for managing, supervising and controlling a company's exposure to risk. This research uses COSO ERM 2017 as a reference for conducting gap analysis and designing a company risk management framework. Apart from that, this research also aims to design a risk management framework according to the COSO ERM 2017 framework. The results of this research show that TMAP has not implemented every risk management principle based on COSO ERM 2017. However, there are several principles that have been implemented by TMAP, namely demonstrating commitment to core values; Attracts, Develops and Retains Capable Individuals; Analyze Business Context, Formulate Business Objectives; Identify Risks. However, these principles have not been implemented completely, but only in part. With this research, it is hoped that it will be able to provide benefits and be useful for the following parties, namely that this research can be input for improving the function and role of risk management in operational activities so that it can increase productivity in accordance with the company's strategy. And academically, this research can be a reference for future research on risk management, especially in companies operating in the chemical trading industry.

Keywords: *Risk management, COSO ERM, Risk, Trading company*

1. Introduction

Every business activity is always filled with uncertainty which can create risks. These risks can have a negative impact on achieving the company's vision, mission and goals. Therefore, risk handling or management must be carried out in a comprehensive and integrated manner. Risk management is a system or method for managing, supervising and controlling a company's exposure to risk (Walburg & Goldman, 1998). Risk management helps companies focus their strategy, goals and company performance and monitor changes that occur (COSO, 2017). One of the

[1] *Universitas Indonesia, Depok, Indonesia. aprabadaru@gmail.com*
[2] *Universitas Indonesia, Depok, Indonesia,*

comprehensive and integrated risk management concepts that is *a best practice* is Enterprise Risk Management (ERM). According to the Committee of Sponsoring Organizations (COSO), ERM is a series of processes that influence an organization starting from the board, management and other personnel, which are practiced in carrying out company strategy, to identify and manage acceptable risks so that company goals can be achieved (Makikui, Morasa & Pinantik, 2017).

Companies that implement COSO ERM-based risk management are able to provide certainty regarding strategy implementation, have sufficient information to make decisions and formulate strategies, and form risk awareness at the managerial level (Aditya & Naomi, 2017). They also believe that implementing risk management with clear guidelines is important, especially for medium to large companies, to maintain the continuity of the company. Even though conceptually and *best practice* shows that risk management is one of the important and main aspects in managing a company to achieve its goals, the facts show that not all companies have and implement risk management, especially risk management that refers to a generally accepted formal framework. One company that has not implemented best risk management practices is TMAP which operates in the trading sector of chemicals.

Based on initial discussions with management, it is known that the Company has identified several general risks but has not been guided by a certain framework of thinking and is not structured. Limitations in risk management are thought to be one of the factors causing the Company not to achieve its targets. For example, the Company's sales growth in the last 10 years (2013-2022) is still very fluctuating or unstable, namely experiencing a drastic decline of up to -17% in 2015, -8% in 2019, and -6% in 2020. In addition, the Company is vulnerable to dependence on chemical suppliers due to the nature of its business as an intermediary.

Currently the Company does not yet have knowledge of a generally accepted formal risk management framework, even though the risks faced by the Company are very diverse and this can hinder the achievement of the Company's objectives. Therefore, the Company needs assistance to design and implement risk management based on a generally accepted framework. This research answers this need by assisting in the first stage of risk management implementation, namely conducting *gap analysis* and designing the Company's risk management framework. This research uses COSO ERM as a reference in conducting gap analysis and designing the Company's risk management framework. This research will apply COSO ERM 2017 as a research framework in assessing the ideal practice of implementing risk management. Later, COSO ERM 2017 will be a comparison tool with field conditions at TMAP companies. From there, this research can see whether what has been carried out by TMAP so far is in accordance with the principles in COSO ERM 2017 or not. After that, COSO ERM 2017 also becomes the basis for designing ideal risk management practices for each existing component.

Implementing optimal risk management is crucial in the company. This is supported by data findings from Leng & Basuki & Setiawan (2022) who conducted a study on 137 company directors. Research shows that 43.5% and 46.6% of companies that

experienced sales growth and increased net profit were companies with optimal ERM implementation. On the other hand, 67% of companies that experienced a decline in sales performance and net profit were companies with weaker levels of ERM implementation. Leng & Basuki & Setiawan (2022). Furthermore, previous research has also proven the positive impact of implementing COSO ERM on risk management in companies. Furthermore, Rikaz, Ulhaq, Mulyono & Cahyaningtyas (2022) stated that companies without risk management guidelines are more likely to implement risk management and be evaluated using COSO ERM. Using the COSO ERM framework can help to identify gaps in internal control and areas of risk management practice that need to be developed. However, different from previous research which generally uses the COSO ERM *framework* (2004), This research uses the latest risk management framework, namely COSO ERM (2017). Therefore, it is very interesting to compare the results of this research with previous studies that used COSO ERM (2004), especially with the research of Rikaz, Ulhaq, Mulyono & Cahyaningtyas (2022) which used a similar research method, namely case studies and used research objects in the form of companies. in the same class and country, namely middle-class companies in Indonesia, even though they are in different industries.

This research uses the single entity TMAP as the unit of analysis. TMAP is a trading company that provides chemicals for the treatment of water and liquid waste in medium scale factories with a turnover of 15 – 50 billion rupiah. Of course, in its operational activities, TMAP faces various challenges including ensuring compliance with strict government regulations including in handling chemical storage and managing distribution transportation, fluctuations in raw material supply and market demand, highly competitive competition, changes in customer preferences and environmental regulations. which is getting tighter.

COSO ERM research in the water and wastewater treatment chemicals trade industry has not been widely carried out. This research uses a qualitative descriptive research method. This research will use primary data sources through semi-structured interviews based on the COSO ERM 2017 framework with directors, production and warehouse managers, and management representatives. As well as additional secondary data coming from internal TMAP documents. Data that has been collected from interviews and document studies is categorized and linked to the concepts used to answer the research problem formulation. Categorization is done by coding and to simplify the data processing process, coding is done by forming categories from the data. Key words or phrases used as data categorization are based on the concepts used in the research, namely risk, risk management, and the five components of COSO ERM (2017), namely Governance and Culture; Strategy and Objective Setting; Performance; Review and Revision; as well as Information, Communication, and Reporting. Furthermore, this research analyzes and reviews the data and links it to the research formulation, namely comparing risk management practices in TMAP with the COSO ERM framework and designing risk management in companies based on COSO ERM. Analysis was carried out using COSO ERM 2017.

Overall, this research is interesting research to carry out. First, conceptually the existence of risk management according to *best practices* is an essential thing that a

company should have. Second, empirically there has not been much previous research on COSO ERM in the context of the water and wastewater treatment chemical trade industry. Third, practically this research, which carries out *gap analysis* and designs a risk management framework, has a high contribution to companies which until now do not have a structured risk management framework.

This research aims to help companies conduct *a gap analysis* of current risk management practices compared to the COSO ERM framework. Apart from that, this research also aims to design a risk management framework according to the COSO ERM framework, taking into account the results of gap analysis.

Problem Formulation : How does TMAP implement formal and structured risk management in order to mitigate risks in the field that may arise?
Research Questions :
1. How do current risk management practices in TMAP compare to the COSO ERM framework?; And
2. How is risk management designed in TMAP based on the COSO ERM framework?

2. Theoretical Background

Risk
According to the Committee of Sponsoring Organizations Enterprise Risk Management (COSO ERM), risk is the possibility of an event occurring that affects the achievement of organizational goals (COSO ERM, 2017). Furthermore, Rahardjo, 2018 divided risk categories based on Financial Services Authority Regulation (POJK) No. 18/POJK.03/2016, namely into eight categories, namely: credit risk, market risk, operational risk, liquidity risk, compliance risk, legal risk, reputation risk and strategic risk. Meanwhile Anderson & Schoeder (2010) divides risk into four categories, namely: disaster risk, economic risk, operational risk and strategic risk. The combination of these approaches produces the following risk categories:

1. Disaster risk (*hazard*)
   Disaster risk is a concern for organizational leaders and is negative with the source of the risk originating from outside the company.
2. Economic *risk*
   Economic risk focuses on the financial side, is negative, and can originate from inside and outside the company.
3. Operational risk (*operational risk*)
   Operational risks result from inadequate or non-functioning internal processes, system failures, human errors and external events that can affect company operations. Constraints caused by operational risk originate from non-compliance or limitations in the system.
4. Strategic risk (*strategic risk*)
   Strategic risks are caused by future threats or possibilities and have far-reaching impacts that are often difficult to identify. Every strategic risk decision is related to the assumptions, estimates, and measurement methodologies used.

Risk management

According to Chapelle (2019), in non-financial industries, risk is a series of causes-events-impacts. This structure is generally used by companies in the energy and technology sectors, but currently other financial and non-financial companies have also adopted it. Chapelle, 2019 presents a sequence of risk management, starting from risk exposure and its causes to financial and non-financial impacts when a risk occurs. Before carrying out mitigation actions, it is very important to see the importance of the magnitude of risk exposure and its causes. Currently, companies are more focused on preventing incidents rather than overcoming them because basically the principle of prevention is better and more profitable than correcting the impact of risks that have occurred.

Integrated Risk Management (Enterprise Risk Management)

The term Enterprise Risk Management (ERM) is a framework issued by COSO. In a 2017 publication, COSO defined ERM as a risk management approach in the form of company practices, policies and frameworks responding to the various risks faced. This approach is important because it can prevent losses or unexpected negative outcomes. Furthermore, ERM can help determine company plans to mitigate risks strategically and in an applicable manner. This framework is intended for boards and management at all sizes of entities (Hayes, 2022). Lam, 2011 states that ERM as a comprehensive and integrative framework for companies is very useful in managing credit risk, market risk, operational risk and risk transfer to maximize company value.

Risk Management and COSO ERM Standards

In its development, there are several risk management guidelines from various institutions. Each guide has different concepts, standards and approaches. COSO is one of the institutions that publishes guidelines regarding risk management and is generally accepted or considered best practice. COSO ERM functions to help companies integrate risk management into all aspects of company operations. This framework has become an international standard used by almost all types of companies in both the public and private sectors to manage risk holistically.

Figure 1 COSO ERM 2017

3. Methodology

This research aims to carry out a gap analysis of risk management practices in the research object compared to the COSO ERM framework and to help design a risk management framework for the company that is the research object according to the COSO ERM framework by considering the results of the gap analysis. To achieve this goal, this research requires in-depth and real information about risk management practices currently running in the company that is the object of research. The appropriate approach to achieve the research objectives is a qualitative approach using the case study method. A qualitative approach is an approach that attempts to understand or see social conditions from the perspective of the subject (including individuals or groups) who wish to be researched (Neuman, 2014). A qualitative approach allows this research to explore in depth the understanding of stakeholders regarding current risk management practices at TMAP. Qualitative will help understand how TMAP's organizational context, culture, and operational environment influence the implementation of risk management practices. In addition, this case study method will allow research to describe in detail how TMAP handles risks and where there are gaps compared to COSO ERM 2017 that may not be detected by quantitative surveys.

In comparing TMAP's current risk management practices and the COSO ERM framework, this research will establish the scope of gap analysis in operational activities at TMAP. Then use the COSO ERM 2017 framework and describe each component and principle that will be used as a standard. After collecting data with stakeholders, this research identified assessment criteria based on the main components of COSO ERM 2017. Furthermore, this research will then compare current risk management practices with the established criteria. Then we will identify and describe any gaps in current practice that are not in accordance with COSO ERM standards.

Unit of Analysis and Research Period

The unit of analysis is the individual or group that is the main object of research which provides information that is analyzed based on the study topic (Sedgwick, 2014). In this research, the unit of analysis that is the object is TMAP and its management. The main reason this research chose TMAP as the unit of analysis is because the company does not yet have a structured risk management framework. The absence of a risk management framework is thought to be one of the reasons why the Company's revenue has not met the target. By choosing TMAP as the unit of analysis, this research can explore from the starting point a company without a risk management framework so that it can comprehensively analyze the needs, challenges and opportunities in implementing COSO ERM on TMAP. TMAP also operates in industries that have a high level of risk, namely trading in liquid chemicals, both in terms of operations, regulations and work safety. To that end, TMAP provides a rich context for evaluating how COSO ERM can be applied and useful in the industry. TMAP management has also recognized the need for their risk management practices which creates an opportunity to implement the new framework.

Research Instrument

The data used in this research are primary data and secondary data. Primary data is obtained through interviews where the interview method can also create a more relaxed atmosphere so that information gathering is much deeper because people tend to be more open when interacting directly rather than filling out surveys (Bryman, 2012), while secondary data is obtained from company performance reports, information on websites, and other relevant documents to be able to understand the context of the implementation of risk management in the company that is the subject of research. Apart from that, the results of the documentation study are also used to verify data obtained from other sources, namely interviews.

Seeing that the size of the TMAP company is not too big because it has 15 members, this research decided to conduct interviews with 3 crucial informants. Among them are company directors, production and warehouse managers, as well as marketing managers and representative management. The criteria for selecting the informants interviewed were based on the director still being involved hands-on in operational activities, the production and warehouse manager directly managing the company's operational activities, and the marketing manager and representative management who are work safety supervisors. Interview questions were formulated based on ideal risk management criteria from COSO ERM 2017 which were then adapted into questions in order to collect comprehensive information.

In conducting research, there will of course be limitations related to data collection methods, including the possibility of bias in interviews. For this reason, this research uses semi-structured questions which create impartial questions to encourage informants to provide honest and in-depth answers. The researcher also made sure to maintain a non-judgmental attitude throughout the interview. In avoiding challenges to the validity of secondary data, this research will consider the context of the data's origin, and document all secondary data sources used. This research will also carry out data triangulation using various data sources to confirm findings and reduce bias.

4. Empirical Findings/Result

COSO Components	COSO Principles	Activities within the Company	Recommendation
Governance and Culture	Exercises Board Risk Oversight	1. There is no clear separation of roles between directors and commissioners. 2. The Director understands the company's main risks, is involved in scenario simulation activities (APAR training and work safety) and currently only plays a supervisory and advisory role on K3 reports and quality management.	*A framework* design was created in chapter 5
	Establish Operating Structures	1. TMAP has artifacts to promote a risk awareness culture related to occupational safety. 2. Conduct monthly briefings to instill awareness of work safety risks.	
		1. TMAP has an operational structure with company work guidelines for each division. 2. Risk management supervision is carried out informally with the board of directors being more involved in daily decision making through reporting made by the marketing PIC.	1. Companies must create a comprehensive organizational structure complete with roles, responsibilities and hierarchies and integrate risk management into this organizational structure. This formation is expected to make risk management a unified function so that each team can manage relevant risks effectively. 2. Companies must choose risk management methods and frameworks that suit the company's needs and characteristics. Based on this and previous studies (Umannath & Kumar, 2019), this research recommends companies use the COSO ERM approach (2017). 3. The company appointed a main director who also doubles as *Chief Risk Officer* (CRO) who is responsible for supervising and implementing risk management. The reason only 1 person is the executor is because human resources are limited because the number of employees is only 15 people.

			4. The board of commissioners, chief director (CRO), management and representatives of each team need to design a written risk mitigation strategy based on the results of risk identification. The strategy contains concrete steps that can be taken before the risk occurs and when the risk has become an incident to enable the risk to occur and reduce the impact of the risk. 5. Companies need to set performance metrics and indicators through simple *Key Performance Indicators* (KPI) for each team to evaluate the success of the risk management program. That way, it is hoped that the company can make effective decisions regarding risks. 6. Companies need to provide training and education to the chief director (CRO) before starting to implement risk management practices.
	Defines Desired Culture	1. There is no company's own core values. 2. These values are not listed in the company profile, website, or artifacts around the office but are only communicated verbally during meetings or during briefings.	1. Determine the company's main values and principles that will shape the expected risk management culture. If a company wants to adopt the 5S values from Japan, the company needs to adapt them to the company's circumstances and in accordance with risk management principles. 2. Companies need to instill these values at every level of the company through socialization and education, compiling them in writing in company reports and putting up posters in the corners of each team's office regarding the company's cultural values. This is done to increase awareness of the company's risk culture and risk management. 3. Companies also need to integrate risk management values into business processes and company decision making. Every company decision and action related to risk management needs to reflect the culture stated in these values.
	Demonstrates Commitment to Core Values	1. The company makes efforts to demonstrate some of the company's values through the practice of installing artifacts in the warehouse and carrying out weekly cleanliness controls. 2. They have not implemented their commitment to practice the core values of other companies because they do not yet exist.	1. Conduct morning *briefings* every day via online applications or in offline activities to read out the vision, mission, organizational cultural values that have been explained previously and discuss daily business strategies. 2. Ensure risk reporting is carried out honestly and fairly. 3. Ensure that every ethical decision making and action is in accordance with norms in managing and dealing with risk consequences. 4. Insert company core values into every risk management policy.
	Attracts, Develops and Retains Capable Individuals	1. The company wants to facilitate the training required by its employees in accordance with the company's needs so that competent individuals can increase their competitiveness in the market. But not yet about risk management. 2. There is no supporting evidence to show whether the company has been able to recruit candidates who fit the risk-aware culture, desired behavior and who have the competencies for the proposed role.	1. When recruiting for a job as a CRO or to become a risk management team, companies need to create a clear and comprehensive job profile containing the qualification criteria, roles and tasks they will carry out. 2. Implementing employee knowledge development programs on an ongoing basis through training or courses related to risk management aspects such as how to recognize risks, risk analysis methodology, risk management technology and others. 3. Companies also need to implement a transparent and fair performance evaluation system and provide rewards and recognition to employees who are successful in carrying out risk management.
Strategy and Objective-Setting	Analyze Business Context	1. New companies analyze the business context of external stakeholders who are influenced by the company, namely its competitors. However, the way they carry out business context analysis is not to predict by making a list of risks but rather to learn from past performance. 2. TMAP has only just made analyzes related to *legal* or regulatory components related to chemicals and *social* or market trend analysis.	1. Companies need to prepare reports related to elements that influence business operations regarding internal and external factors. 2. Companies also need to identify stakeholders related to the company. This includes buyers, suppliers, business partners, employees, regulators and other stakeholders 3. Companies also need to assess and pay attention to changes related to the business context such as technological changes, market shifts or government policies and assess how this impacts the company's risk management. 4. Companies can also use analysis techniques such as SWOT (Strengths, Weaknesses, Opportunities, Threats) and PESTEL (Political, Economic, Social, Technological, Environmental, Legal) analysis to analyze the business context. 5. After conducting a business context analysis, companies need to evaluate the impact of the business context on achieving strategic goals and business initiatives. 6. Business context analysis is also used for consideration when making company strategic decisions 7. Companies also need to regularly update their business context analysis considering the dynamic business environment.
	Define Risk Appetite	1. TMAP has not implemented ideal practices in determining risk appetite, including setting acceptable risk limits for the company. 2. The Board of Directors has indeed determined the company's most strategic risk, namely business continuity, but for other risks, the risk limits that the company can accept are not explained.	*A framework* design was created in chapter 5
	Evaluates Alternative Strategies	1. Most evaluations of alternative strategies are carried out only verbally without making special reports or lists to understand the implications of the chosen strategy. 2. The company has evaluated alternative strategies using a SWOT analysis approach. However, there has been no specific report regarding this matter.	1. Companies need to identify various business strategies as several alternative strategies. Companies also need to analyze potential risks that may occur when taking alternative strategies as well as the potential impacts that may occur. Researchers try to map several strategies that companies can take based on the results of interviews, namely: 2. Companies also need to determine *key risk indicators* (KRI) which aim to monitor and provide warnings when risks arise during implementing alternative strategies. In determining KRI, companies need to know what the company's goals are and what risks have the potential to hinder achieving targets. Next, determine the most significant risks that will determine the achievement of targets. Then the company needs to look for the triggers for the risk to appear and the indicators that need to be used to assess how big the influence of the risk is. Of the many risk indicators, companies need to choose the key risk indicators and those that are most relevant to the causes of the risk.
	Formulates Business Objectives	1. TMAP has determined their *business objectives* , namely to obtain maximum profits and maintain business continuity. 2. They have not set a risk appetite so there is no alignment with business goals and strategic decisions.	1. Companies need to have an understanding of what the company's business goals are. This includes what the short-term and long-term goals are, the company's vision, mission and strategy. Because the company says it has business goals, the company needs to prepare a report regarding business goals. For example: • Business goal: achieve revenue growth through increased sales of chemicals and services. • Short-term goal: achieve company profits and financial efficiency by managing costs effectively and managing cash properly. • Long term goal: the company wants to increase its business presence in the domestic market (all over Indonesia) and internationally through chemical exploration and the services offered. 2. Companies also need to formulate how the business context and external environment of the company can influence the achievement of business goals. Companies can carry out a SWOT analysis (Strengths,

			Weakness, Opportunities, Threats) and compile documents when determining business goals. 3. After determining business objectives, the company needs to recognize what possible risks may arise from these business objectives. For example, financial risk, competitor risk and operational risk.
Performance	Identify Risk	1. TMAP has identified risks that are often experienced by the Company. 2. The approach currently used by the Company is only through a review of past performance which is then discussed and resolved on the spot.	*A framework* design was created in chapter 5
	Assesses Severity of Risk	1. TMAP has assessed the level of risk *severity* according to the categories and is only related to K3, not overall risk management. 2. The company has not used qualitative (through interviews, workshops, *benchmarking*) and quantitative (through modeling and decision trees) approaches to assess the severity *of* risk impacts.	1. Companies need to assess risks to measure the level of risk *severity* through several methods including: a. Impact: the result or result of a risk. There are various possible impacts associated with a risk. The impact of a risk may be positive or negative on business strategies and objectives. b. Likelihood: the possibility of a risk occurring. This can be expressed in terms of probability or frequency of occurrence. Possibilities can be expressed in various ways
	Prioritises Risk	1. Companies can prioritize risks. However, because companies have not shown their risk inventory, risk appetite and risk *severity level* , it cannot be ascertained whether they assess the level of risk priority based on these three things as suggested by COSO ERM.	1. After assessing the level of risk *severity* , companies need to determine risk priorities based on several criteria: a) Adaptability: what is the company's capacity to respond to certain risks. For example, responding to changes in market trends and their impact on business goals regarding product innovation. b) Complexity: how the nature of risk and its scope affect the success of the company. Risks can be interdependent which can increase the complexity of their impacts. For example, raw materials that no longer meet buyers' needs and low sales meet the business goal of becoming a leading company in the chemical trading industry market. c) Velocity: the speed of risk impact on the company. The speed of risk can disrupt company performance. For example, the risk of disruption due to strikes at chemical producing factories.
	Implementing Risk Responses	1. The company will respond to a risk by resolving it immediately. The company does not yet have a list of categorized risk responses 2. The company still adheres to the principle of overcoming risks that have become incidents and learning from these incidents, rather than identifying risks before they occur.	1. After identifying all company risks, management needs to implement risk responses while considering *severity level* , risk priority, and business context.
	Develops A Portfolio View	1. They have not implemented *the portfolio view principle* . This can be seen from the fact that they have only just identified and not yet assessed and managed various risks that could affect the overall achievement of company goals.	1. Minimal Integration-Risk View: in a *risk-centric view* , companies need to identify and assess risks in a closed manner. The main focus of this level is the underlying risk event, not the objective. For example, the risk of violating regulations which could impact the company's compliance with state laws. 2. Limited Integration-Risk Category View: this level uses information from *the risk universe* and organizes risks by category. Risk categories often describe the company's operating structure and also inform roles and responsibilities. For example, a representative management team has responsibility for managing risks related to K3. 3. Partial Integration-Risk Profile View: integrating risk information at each level of the company to provide a comprehensive view and how risks in various parts can be interconnected. For example, raw material supply risks related to sustainability with a supplier can impact delivery and finances. 4. Full Integration-Portfolio View: at this level the focus needs to shift to overall business strategy and goals. This level also refers to combining risk information from the entire integrated business portfolio. For example, supply and distribution risks will also include information regarding the availability of raw materials, chemical quality risks, changes in logistics regulations, and risks to the distribution process.
Review and Revision	Assesses Substantial Change	1. The company currently does not have a specific list of substantial changes that have the potential to affect the running of the company. 2. Any changes they experience will be communicated directly either through meetings or short messages.	*A framework* design was created in the chapter 5
	Reviews Risk and Performance	1. The company has no risk management guidelines at all, which of course means that there is still no review of their performance in this regard.	1. To review a company's risk management performance it is necessary to answer the questions below: a) Has the company performed in line with expectations and achieved targets? b) What risks occur and might affect performance? c) Is the company taking enough risks to achieve company targets? d) Is the estimate of the amount of risk in *the risk universe* accurate? 2. If performance does not meet company expectations, management needs to: a) Review business goals b) Review business strategy c) Review company culture d) Revise performance targets
	Pursues Improvement in ERM	1. The company has not implemented risk management. For this reason, they have not made adjustments or improvements to the ERM process.	1. Companies need to carry out a comprehensive evaluation regarding the maturity of their risk management system by identifying SWOTs that influence the company's ability to manage risk 2. Companies also need to determine specific and measurable improvement goals. For example, improving *the risk universe* or speed of response to a risk. 3. Companies need to take corrective steps that have been explained in the previous principles and study the successful experiences of other companies.
Information, Communication, and Reporting	Leverages Information Systems	1. The company has not used an integrated risk management system in any form. This is caused by companies that have not implemented risk management with COSO ERM.	*A framework* design was created in chapter 5

Communicates Risk Information	1. The company has a transparent communication culture to ensure that risks are known to management and will be resolved by the field team.	1. Companies need to communicate to every level of management regarding the importance, relevance and value of corporate risk management. Apart from that, characteristics, desired behavior and *core values* determine company culture. Furthermore, companies also need to socialize the entity's business strategy and objectives, risk appetite and tolerance, and overall expectations regarding company risk and management performance. 2. Communication methods can be used according to the company's convenience. Such as conducting face-to-face meetings, training and seminars, written internal documents, and electronic messages. 3. Companies also need to use clear, non-technical language and use data visualization to avoid misunderstandings by those who do not have a risk management background.
Reports on Risk, Culture and Performance	1. In terms of reports regarding risk and risk management, the company does not yet have a structure guided by risk management standards. The reports they carry out still only cover risk requirements related to K3 and quality management.	1. Companies need to prepare reports related to risk management which include the following attributes: a) Portfolio view of risk b) Risk profile view c) Analysis of the root of the problem 2. Companies also need to prepare culture reporting which is manifested in: a) Analyze cultural trends b) *Benchmarking* other companies as a business context analysis c) Compensation scheme 3. Companies also need to determine the frequency period used to prepare each risk report. This determination needs to be adjusted to the amount of risk borne by the company. Considering the company is still at the middle level. Quarterly risk reporting would be better to reduce the possibility of inaccurate reports.

5. Discussion

A. Gaps in Corporate Risk Management Practices with COSO ERM

The problem formulation and first objective of this research is to evaluate risk management practices at TMAP. The following are the results of data findings related to the comparison between risk management practices in TMAP with the reference for ideal risk management practices, namely the Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management (COSO ERM) in 2017.

1. Governance and Culture

Exercises Board Risk Oversight

Based on the evaluation results, it can be concluded that the TMAP company has not implemented the principles of board risk oversight exercises as a whole. The Board of Directors (especially the main director) has been actively involved in identifying and understanding strategic risks, simulating risk scenarios, and providing the training needed by employees. However, this is only related to K3. Apart from that, there are no structured policies and procedures regarding how to recognize and manage risks and this shows that the board of directors has not carried out its role in being involved in determining these policies and procedures.

Establish Operating Structures

Based on the evaluation results, it can be concluded that the TMAP company has implemented some of the principles of Establishing Operating Structures. This can be seen from those who claim to have work procedures for each division and have a complete organizational structure in accordance with the data on the company website. However, risk management monitoring activities are still carried out informally and do not fully follow COSO ERM 2017 recommendations, namely by having a clear and structured reporting system.

Defines Desired Culture

Based on the evaluation results, it can be concluded that the TMAP company has not implemented the Defines Desired Culture principle, which can be seen from the fact

that the company's core values have not been formulated and ratified. If a company really wants to adapt the 5S culture from Japan, the company must adapt to the culture the company wants.

Demonstrates Commitment to Core Values
Based on the evaluation results, it can be concluded that the TMAP company has implemented some of the principles of Demonstrating Commitment to Core Values. The company shows its commitment by actively encouraging all employees at every level to identify and improve work safety practices through artifact installation practices, verbal outreach and work safety training. However, they have not implemented their commitment to practice the core values of other companies because they do not yet exist.

Attracts, Develops and Retains Capable Individuals
Based on the evaluation results, it can be concluded that the new TMAP company implements some of the principles of Attracts, Develops and Retains Capable Individuals. There is no evidence to support that the company has recruited talented workers. Meanwhile, regarding training, the company has tried to meet the needs of employees to develop their skills. However, this is only limited to worker safety and halal supervisor training, not yet related to overall risk management training.

2. Strategy and Objective-Setting
Analyze Business Context
Based on the evaluation results, it can be concluded that the TMAP company has only implemented some of the principles of business context analysis. TMAP has followed COSO ERM (2017) recommendations, namely learning from the past to create risk profiles and analyze legal or regulatory components in the PESTLE (Politics, Economics, Socials, Technologies, Law and Environment) method recommended by COSO ERM (2017). However, TMAP has not paid attention to other stakeholders, future aspects, as well as analysis of other PESTLE components.

Define Risk Appetite
Based on the evaluation results, it can be concluded that TMAP has not implemented the principle of defining risk appetite. The Board of Directors has indeed determined the company's most strategic risk, namely business continuity, but for other risks, the risk limits that the company can accept are not explained. The company has not used a risk matrix, Key Performance Indicator (KPI), or risk evaluation using other methods when setting risk limits.

Evaluates Alternative Strategies
Based on the evaluation results, it can be concluded that TMAP has only implemented some of the principles of evaluating alternative strategies. TMAP has evaluated strategic options, but only regarding the purchase of chemical raw materials. In addition, TMAP has used the SWOT method as recommended by COSO ERM (2017), although it is not supported by related documentation.

Formulates Business Objectives
The evaluation results show that TMAP has implemented the principles of formulating business objectives. The company has determined business objectives using a best practices approach, namely SWOT analysis as stated in ISO 9001 Quality Management System. However, this research cannot verify the application of the SWOT.

3. Performance
Identify Risk
The evaluation results show that the new TMAP implements some of the Identify Risk principles. The company is able to identify risks that can affect company performance, especially those related to K3. Meanwhile, for risks outside K3, the Company only responds to risks that have occurred based on past performance, and has not yet estimated the potential risks that could be faced. TMAP has not properly described the risk and identified the causes of the risk, the potential impact of the risk, or the impact of poor risk implementation. The company also has not used an approach that is embedded in daily operational activities such as budgeting, business planning and performance reviews.

Assesses Severity of Risk
The evaluation results show that TMAP has not implemented the principle of Assessing the Severity of Risk. The company has not used qualitative (through interviews, workshops, benchmarking) and quantitative (through modeling and decision trees) approaches to assess the severity of risk impacts. If varying impacts result in different severity assessments or require different risk responses, management determines whether additional risks need to be identified and assessed separately.

Prioritises Risk
The evaluation results show that TMAP has not implemented the principle of Prioritizing Risk. This is shown by the absence of supporting documents regarding risk priorities. Companies have only been able to identify the most crucial risk, namely bankruptcy, but have not been able to identify risks with other priority levels. TMAP also has not determined risk priorities based on certain criteria, such as adaptability, complexity, velocity, persistence and recovery. Risk prioritization must take into account the level of risk severity compared to risk appetite.

Implementing Risk Responses
The evaluation results show that TMAP has implemented the principles of Implementing Risk Responses. However, the Company's response to risk is carried out in a traditional manner, namely the Company responds to a risk by resolving it immediately. The company does not yet have a list of categorized risk responses as discussed previously. The company has not selected and implemented risk responses by considering factors such as business context, costs and benefits, obligations and expectations, risk priorities, risk appetite, and risk severity level.

Develops A Portfolio View
The evaluation results show that TMAP has not implemented the Portfolio View principle. TMAP has not implemented risk management with a framework guide and does not have a risk inventory document so that the Company does not yet have a portfolio view and divides the levels of integration (from minimum to maximum), namely minimal integration (risk view), limited integration (risk category view), partial integration (risk profile view), and full integration (portfolio view).

4. Review and Revision
Assesses Substantial Change
The evaluation results show that TMAP has not implemented the principles of Assessing Substantial Change as a whole. Based on interviews, TMAP has indeed been able to identify substantial but only verbal changes. Until now there are no documents to support this statement. The company has not reported any substantial changes, evaluated their impact, and responded to changes which are an iterative process and can affect several components of the company's risk management.

Reviews Risk and Performance
The evaluation results show that TMAP has not implemented the Risk and Performance Reviews principle. The company has not implemented risk management so a review of risk management has certainly not been carried out. The company has not periodically reviewed its performance in responding to risks. The company has not reviewed business objectives, corporate strategy, corporate culture, revised performance targets, reassessed the severity of risk impacts, reviewed how risks are prioritized, and revised risk appetite when performance is below the target risk profile.

Pursues Improvement in ERM
Companies need to ensure that ERM improvements and improvements are carried out across all functions, operating units and teams systematically, periodically and continuously to identify areas of improvement and improvement. Because the company has not carried out a performance and risk review, the ERM improvement stages have certainly not been carried out. TMAP management has also not made continuous improvements throughout the entity to increase risk management efficiency.

5. Information, Communication, and Reporting
Leverages Information Systems
TMAP does not yet have reports and data that can support risk management practices. This includes information regarding cultural governance practices, strategy and goal-setting related practices, performance-related practices, review and revision practices related to operational operations practices.

Communicates Risk Information
The evaluation results show that TMAP has only implemented some of the Communicates Risk Information principles. TMAP already has a transparent communication culture to ensure that risks are known to management and will be resolved by the field team. However, because the company has not implemented risk

management, the company cannot maximize communication channels to convey the importance, relevance and value of the company's risk management, characteristics, desired behavior and core values determined by the company's culture.

Reports on Risk, Culture and Performance

The evaluation results show that TMAP has not implemented the principles of Reports on Risk, Culture and Performance. TMAP has not produced management reports and culture reports in accordance with COSO ERM recommendations (2017). TMAP also does not have risk data and reports, risk appetite and other documents related to risk management.

B. Risk Management Design Based on the COSO ERM Framework

Based on the results of the gap analysis, this research then helps design an ERM framework model for TMAP based on the COSO ERM Framework (2017). However, because the company showed a significant gap analysis, the design of the ERM framework model for TMAP was carried out in stages. In this research, the design of the ERM framework model is focused on one of the principles of each component. Determining the principles for creating the ERM framework design is based on considerations of urgency for the company in implementing ERM. The five principles above were chosen because they influence the implementation of other principles. The exercise board risk oversight principle was chosen because it influences the implementation of overall risk management. Define risk appetite was chosen because although the TMAP business context is quite clear, management does not yet have a risk appetite to determine the level of risk acceptance. Meanwhile, the design of identify risks, assesses substantial changes, and leverages information systems was chosen because it influences the implementation of the following principles.

1. Exercises Board Risk Oversight

Governance and risk culture must start from the supervision and influence of the supervisory board so that they must have the knowledge, experience and skills to carry this out. For this reason, this research describes a design that can be implemented in companies to fulfill this principle based on COSO ERM (2017).

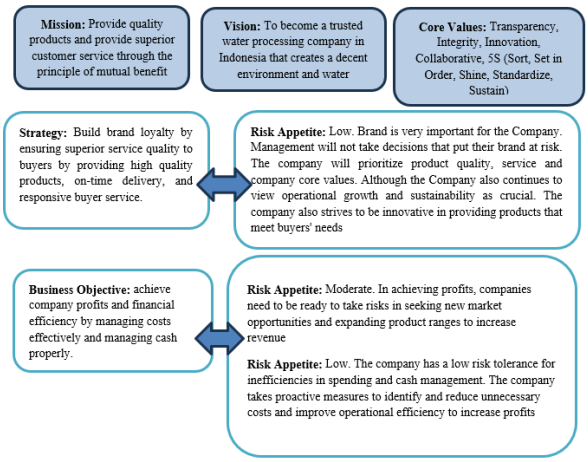
Responsibilities of the Board of Commissioners	Directors' Responsibilities
1. Supervise and provide input to ensure the company can manage risks effectively in achieving its long-term goals. 2. Supervise and provide input to the company's risk management, including in the identification, evaluation, mitigation and monitoring stages of the risks faced. 3. Supervise and provide input on the company's risk management performance reports prepared by the	1. Has responsibility for establishing company direction and targets in the preparation of policies, strategies and guidelines for implementing risk management, as well as changes if necessary. 2. Assess the effectiveness of the implementation of the risk management framework. 3. Ensure that significant risks are identified, measured, monitored and managed appropriately.

Responsibilities of the Board of Commissioners	Directors' Responsibilities
board of directors periodically and ensure that the risk management system continues to be updated and improved in accordance with the company's needs. 4. Conduct discussions with the Board of Directors, senior management and other stakeholders regarding significant risks and risk management strategies and provide approval for the risk management strategic plan.	4. Ensure that directors have knowledge related to risk management and ensure that human resources in the company also have knowledge related to risk management. 5. Conduct performance assessments regarding company risk management periodically and ensure that the risk management system is continuously updated and improved. 6. Communicate with company stakeholders regarding significant risks facing the company and risk management strategies. 7. Take company strategic decisions by considering relevant risk factors.

Source: Researcher data processing

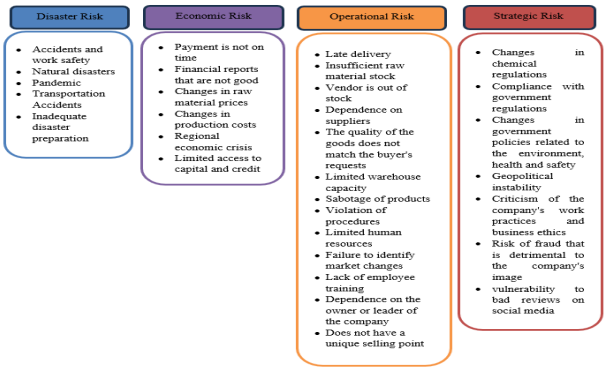
2. Define risk appetite

Defining the company's risk appetite is done when determining strategy by discussing it with management and the board of directors. For this reason, researchers tried to develop a risk management design based on this principle in accordance with COSO ERM guidelines (2017).



Source: Researcher data processing

3. Identify risks



Source: Researcher data processing

Researchers develop a management design on the principle of identifying risk by creating a risk universe based on the results of interviews with informants or performance reviews. as follows: Companies must implement data tracking methods from past events so they can predict future events. This data can also be used to develop predictive and causal models. As has been done by companies, they need to conduct brainstorming sessions to track the risks faced by the Company. This can be done at the end of year meeting.

4. Assess Substantial Change

When monitoring substantial changes, it is necessary to insert them into business operational processes to avoid a decline in performance and business strategy.

Internal Environment	Risk implications	External Environment	Risk Implications
Higher level of operational activity	Human resources that cannot adapt to higher levels of operational activity add new personnel	Changes in regulations related to freight transportation regulations throughout the industry	Affects chemical delivery logistics
New innovation by implementing an integrated risk management system	HR who cannot adapt to the company's new innovations. So training must be provided to improve performance	New technology related to liquid waste cleaning	Can incur large operational costs
Changes in company management	Changes in management can also affect the company's risk management. So there is a need for socialization regarding company culture and philosophy	Disruption in the supply chain	Causes an increase in business operational costs due to additional shipping costs or more expensive alternative chemicals

5. Leverages Information Systems

Using information system technology can provide companies with information and data that will support the implementation of ERM including market needs, competitor criteria and their relationship to costs and benefits.

Source	Example Data	Structured	Unstructured	Storage Location
Directors and management meetings	MoM and notes on potential transactions		✅	Google Docs in Google Drive 'TMAP'
Buyer satisfaction survey	Feedback from priority buyers regarding service	✅	✅	Google Forms in Google Drive 'TMAP'
Due diligence activities	Reduction and addition of employees due to management restructuring	✅		Google Docs in Google Drive 'TMAP'
E-mail	Information related to decision making and company performance		✅	Outlook in Microsoft Office
Manufacturing report	Reports regarding competitors' superior products		✅	Google Docs in Google Drive 'TMAP'
Marketing reports from website tracking services	Number of website visits, duration on website pages and conversion into buyer interest	✅		Google Docs in Google Drive 'TMAP'
Social media and blogs	Feedback and the number of negative and positive comments regarding the company's services	✅	✅	Spreadsheets in Google Drive 'TMAP'

5. Conclusions

Risk management that adheres to certain standard guidelines is very important for companies operating in the chemical trading sector. For this reason, this research aims to conduct a gap analysis of current company risk management practices compared to the COSO ERM 2017 framework and assist companies in designing risk management based on COSO ERM 2017. The results of this research interview show that TMAP has not implemented every component and principle of risk management based on COSO ERM 2017. Several principles have been implemented by TMAP, namely *demonstrating commitment to core values; Attracts, Develops and Retains Capable Individuals; Analyze Business Context, Formulate Business Objectives; Identify Risk.* However, these principles have not been implemented completely, but only in part. There is not yet much supporting evidence that can determine with certainty whether they have implemented the principles they claim to have implemented. Therefore, the

next step taken by researchers is to design a risk management design based on COSO ERM 2017 for TMAP.

References:

Aditya, O., & Naomi, P. (2017). Implementation of corporate risk management and company value in the construction and property sector.

Alawattegama, K. (2018). The impact of enterprise risk management on firm performance: Evidence from Sri Lankan banking and finance industry. *International Journal of Business and Management, 13*(1), 1-15. https://doi.org/10.5539/ijbm.v13n1p225

Altanashat, M., Bataineh, H., Khasawneh, M., & Bataineh, A. (2019). The impact of enterprise risk management on institutional performance in Jordanian public shareholding companies. *International Journal of Business and Social Science, 10*(3), 113-123. https://doi.org/10.30845/ijbss.v10n3p13

Anderson, T., & Schroeder, P. (2010). *Strategic risk management practice: How to deal effectively with major corporate exposures*. Cambridge University Press.

Bryman, A. (2012). *Social research methods* (4th ed.). Oxford University Press.

Chapelle, A. (2019). *Operational risk management: Best practices in the financial services industry*. John Wiley & Sons.

COSO. (2017). *COSO enterprise risk management: Integrating with strategy and performance*. Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Hayes, A. (2022). Enterprise risk management (ERM): What is it and how it works. *Investopedia*. Retrieved from https://www.investopedia.com/terms/e/enterprise-risk-management.asp

Lam, J. (2011). *Risk management: The ERM guide from AFP*. Association for Financial Professionals, Inc.

Leng, P., Basuki, B., & Setiawan, R. (2022). Implementation of enterprise risk management in medium-sized priority sector companies in East Java. *Journal of Accounting and Finance, 24*(2), 80–90. https://doi.org/10.9744/jak.24.2.80-90

Lokobal, A. (2014). Risk management in construction services companies in Papua Province (Case study in Sarmi Regency).

Makikui, L. E., Morasa, J., & Pinatik, S. (2017). Analysis of the internal control system for inventory management based on COSO at CV. Tendean Manado combo. *Going Concern: Journal of Accounting Research, 12*(2), 1222–1232.

Neuman, W. L. (2014). *Social research methods: Qualitative and quantitative approaches* (7th ed.). Pearson Education Limited.

Perera, B. A. K. S., Rameezdeen, R., & Chileshe, N. (2014). Enhancing the effectiveness of risk management practices in Sri Lankan road construction projects: A Delphi approach. *International Journal of Construction, 14*(1), 1–19. https://doi.org/10.1080/15623599.2013.875271

Rahardjo, S. S. (2018). *Ethics in business & the accountant profession and corporate governance*. Salemba Empat.

Rikaz, M. M., Yahya, M. M., & Fadil, N. (2022). Designing COSO enterprise risk management for publishing and printing companies (Case study at CV. Gema Insani Press).

Sedgwick, P. (2014). Unit of observation versus unit of analysis. *BMJ, 348*, g3846. https://doi.org/10.1136/bmj.g3846

Umanath, B., & Kumar, A. (2019). Enterprise risk management framework for small and medium enterprises.

United States Environmental Protection Agency (EPA). (2022). Understanding water treatment chemical supply chains and the risk of disruptions. *U.S. Environmental Protection Agency*. Retrieved from https://www.epa.gov/system/files/documents/202303/Understanding%20Water%20Treatment%20Chemical%20Supply%20Chains%20and%20the%20Risk%20of%20Disruptions.pdf

Warburg, S. C., & Goldman, Sachs. (1998). *The practice of risk management*. Euromoney Institutional Investor.