Contemporary Accounting Case Studies

Vol. 1, No. 1, September 2022 Article 10

EVALUATION OF RISK MANAGEMENT IMPLEMENTATION READINESS IN A MEDIUM-SIZED ENTERPRISE: THE CASE OF PT XYZ

Hendra Ramli
Master of Accounting Program, Faculty of Economics and Business, Universitas Indonesia
ramlihendra2@gmail.com

Chaerul D. Djakman
Master of Accounting Program, Faculty of Economics and Business, Universitas Indonesia
cdjakman@gmail.com

Contemporary Accounting Case Studies,
September 2022, Vol. 1, No. 1, p. 193-212

EVALUATION OF RISK MANAGEMENT IMPLEMENTATION READINESS IN A MEDIUM-SIZED ENTERPRISE: THE CASE OF PT XYZ

***Hendra Ramli*[1]**
***Chaerul D. Djakman*[2]**
Master of Accounting Program, Faculty of Economics and Business, Universitas Indonesia

ABSTRACT

This study aims to evaluate PT XYZ's readiness to implement risk management. The evaluation is based on the "Learn" component of the GRC Capability Model and the "Governance and Culture" component of the COSO ERM 2017 framework. PT XYZ provides integrated security system products in Indonesia and falls within medium-sized enterprise category. Over the next three years, the company intends to expand. However, it must first ensure that it is ready to implement risk management. The literature review focuses on the GRC Capability Model, which is linked to COSO ERM 2017. An interview and observation process was used to collect the data and facts required to conduct the assessment. These were then analyzed using the "Learn" component of the GRC Capability Model. While the basic findings of the study indicate that PT XYZ is ready to implement risk management, several areas also require improvement, as mentioned in the conclusion.

Keywords: COSO ERM 2017, Governance and culture component, GRC Capability Model, Internal element

[1] First author's email: ramlihendra2@gmail.com
[2] Second author's email: cdjakman@gmail.com

1. INTRODUCTION

Nowadays, companies face a growing number of risks as an impact of the changing global environment. Therefore, they need to implement risk management in their daily operations as a preventive action. Large corporations are mostly aware of these matters and practically implement risk management. However, the implementation of risk management in small and medium-sized enterprises appears to be a relatively novel concept. Risk management concerns the process of identifying, analyzing, evaluating, controlling, and attempting to avoid or eliminate unacceptable risks (Moeller, 2011).

Referring to Government Regulation Number 7 (2021), small and medium-sized enterprises are categorized based on their capital or annual sales. Hence, PT XYZ falls within the medium enterprise category with total capital of IDR5,000,000,000 (five billion rupiahs) to IDR10,000,000 (ten billion rupiahs) and annual sales of between IDR15,000,000,000 (fifteen billion rupiahs) and IDR50,000,000,000 (fifty billion rupiahs).

A company is established to pursue certain objectives (OCEG, 2017). As such, it requires a good understanding of both its internal and external context as a crucial step in determining strategies for achieving those objectives (OCEG, 2017). However, PT XYZ seems unable to identify these internal and external contexts and apply them to pursue its objectives.

Moreover, based on preliminary discussions with the board of directors and after focusing exclusively on the government sector, over the next three years, PT XYZ is set to urgently pursue expansion into the private sector. PT XYZ faces several imperatives during that short period, including the need to implement risk management. The consideration is that the company will face greater risks once it begins its expansion plan, including, among others, market risks and financial risks. Thus, to prevent these risks from having a significant impact on the company, it plans to manage them as quickly as possible. In the long term, risk management will help to maintain the sustainability of the company. Accordingly, by using PT XYZ as a research object, this study provides new contributions to medium-sized corporations. As is evident in this case, such corporations rarely concern themselves with risk management implementation as they typically lack the required impetus. Therefore, through this research, medium-sized corporations are expected to understand the exigency and importance of risk management.

Even so, before a company can implement good risk management, it is crucial to have good governance. This aligns with the COSO ERM 2017

framework, which emphasizes that good governance is a prerequisite for a company to identify, assess, and mitigate risks efficiently (COSO, 2017).

Therefore, the company needs to first evaluate its readiness to implement risk management (Lam, 2017). Hence, the researcher generated research questions to use in the process of evaluating medium-sized enterprises' readiness for risk management implementation, employing PT XYZ as a case study. This research aims to answer the question of whether PT XYZ is ready to implement risk management principles. The firm's readiness to implement risk management was evaluated using the COSO ERM 2017 framework as a reference. COSO ERM 2017 comprises a set of principles covering the basic elements needed to implement risk management.

Briefly, the research process commences with data collection. The data and facts were obtained through interviews and observations and then elaborated further with a literature review. The "Learn" component of the GRC Capability Model was used as the tool of analysis to evaluate PT XYZ's readiness to implement risk management. Later, the result was used to infer whether the company is ready to implement risk management according to the principles included in the "Governance and Culture" component of the COSO ERM 2017 framework.

2. LITERATURE REVIEW

2.1. COSO ERM 2017

The COSO ERM 2017 framework contains guidance to help companies implement risk management principles and practices (COSO, 2017). A company is not obligated to follow the entire framework; instead, it can be customized based on the company's specific needs (COSO, 2017).

COSO ERM 2017 comprises five interrelated components, commencing with Governance and Culture, and Strategy and Objective-Setting, then moving through the ERM process with a focus on Performance (identifying, assessing, prioritizing, and responding to ESG-related risks) and, finally, the Review and Revision, and Information, Communication, and Reporting components (COSO, 2017).

The framework emphasizes the first two principles, Governance and Culture, and Strategy and Objective-Setting (Prewett & Terry, 2018) as they promote the concept of ERM permeating the organization by elevating responsibility for ERM to the highest level of management and creating a corporate-wide culture that is embedded in it.

It can be seen from the COSO ERM 2017 framework that Governance and Culture is the first component and that it affects every other component.

Governance concerns a set of rules or principles that define rights, responsibilities, and expectations between different stakeholders in the governance of corporations. A well-defined corporate governance system can be used to balance or align interests between stakeholders and can work as a tool to support a company's long-term strategy (Ebert & Grifin, 2014). Governance serves to aid in decision-making and helps in setting the tone of the organization from the top to the lower management (COSO, 2017). Culture is associated with the core values, ethics, desired behaviors, and understanding of risk in an entity (COSO, 2017).

The COSO ERM 2017 framework states that good implementation of governance and culture is a requirement for a company to identify, assess, and mitigate risk effectively (COSO, 2017). The Governance and Culture component has the following five associated principles: Exercises board risk oversight; Establishes operating structures; Defines desired culture; Demonstrates commitment to core values; and Attracts, develops, and retains capable individuals in the organization (COSO, 2017).

The principle "Exercises board risk oversight" means that the board of directors provides strategic oversight and holds governance responsibilities to support the management in achieving the organization's strategy and business objectives (COSO, 2017). This principle illustrates the role of the board of directors in monitoring a company's business processes. With proper supervision, a company can be free from conflict. However, the presence of a certain level of conflict within a company can help it to grow (Thompson, Peteraf, Gamble, & Strickland, 2020). The key is to ensure this is a healthy form of conflict that supports the growth of the company.

"Establishes operating structures" means that the organization establishes operating structures in the pursuit of its strategy and business objectives (COSO, 2017). Organizational structure helps the company to demonstrate the tasks and functions performed by each division included in its structure.

"Defines desired culture" means that the organization defines a set of behaviors that characterize its desired culture (COSO, 2017). An organizational culture is a set of values, principles, traditions, and ways of working that are shared and also influence the behavior and actions of employees within an organization (Robbins & Coulter, 2015).

"Demonstrates commitment to core values" relates to the organization demonstrating a commitment to its core values, while "Attracts, develops, and retains capable individuals" means that the organization is committed to building human capital in alignment with its strategy and business objectives.

It is very important to apply human resources management in a company because good human resources can be the source of a firm's competitive advantage and are a crucial part of the company while also influencing its performance (Robbins & Coulter, 2015).

2.2. GRC Capability Model

While GRC officially denotes governance, risk management, and compliance, it connotes much more than the assemblage of those three terms into an acronym. It is important to remember that organizations have been governed, and risk and compliance have been managed, for a long time; as such, GRC is nothing new (OCEG, 2017). However, many organizations have not approached these activities maturely, nor have their efforts necessarily supported each other to enhance the likelihood of achieving organizational objectives (OCEG, 2017).

Integrating GRC capabilities does not mean creating a mega-department of GRC and doing away with decentralized or programmatic approaches to risk and compliance management. Nor does it necessarily call for the use of only one GRC technology system. Rather, it is about establishing an approach that ensures the right people get the appropriate and correct information at the right times, that the right objectives are established, and that the right actions and controls required to address uncertainty and act with integrity are put in place (OCEG, 2017).

An organization that strives to achieve Principled Performance will have several integrated capabilities (OCEG, 2017). Hence, the GRC Capability Model consists of four components: Learn, Align, Perform, and Review (OCEG, 2017).

The Learn component examines and analyzes context, culture, and stakeholders to ascertain what the organization needs to know to establish and support its objectives and strategies (OCEG, 2017). Understanding the external and internal contexts within which an organization operates, along with the organizational culture, is a critical first step in determining organizational objectives, strategies, and structures (OCEG, 2017).

The Align component relates to aligning performance, risk, and compliance objectives, strategies, decision-making criteria, actions, and controls with the context, culture, and stakeholder requirements. Principled Performance requires alignment. Decisions about how to address opportunities, threats, and requirements must align with the context, organizational culture, and decision-making criteria (OCEG, 2017).

The Perform component focuses on addressing threats, opportunities, and requirements by encouraging desired conduct and events, and preventing what is undesired, through the application of proactive, detective, and responsive actions and controls. To achieve Principled Performance, an organization must employ actions and controls to ensure it is addressing uncertainty and acting with integrity while pursuing its objectives. It must proactively encourage the type of conduct and events that support its objectives and try to prevent anything that threatens those objectives (OCEG, 2017).

The Review component pertains to explaining activities to monitor and improve the design and operating effectiveness of all actions and controls, including their continued alignment to objectives and strategies (OCEG, 2017). From these four components, Learn is fundamental to the GRC Capability Model.

The Learn component consists of four elements: external context, internal context, culture, and stakeholders. Internal context is the most important element as it affects the processes involved in pursuing the organizational objectives. Therefore, this research focuses more on the Learn component (internal context) as its tool of analysis. Understanding the internal context, as it continually evolves and changes, is crucial in designing appropriate objectives, strategies, and capabilities (OCEG, 2017). The internal context should be adaptive to every single possible change. Thus, if changes occur, the company can proactively adjust its internal context to pursue its strategies for achieving organizational objectives (OCEG, 2017).

2.3. Connection between COSO ERM 2017 and the GRC Capability Model

The COSO ERM 2017 framework offers guidance to help companies implement the practice and principles of risk management (COSO, 2017). It is the first (and only) open-source standard that integrates the various sub-disciplines of governance, risk, audit, compliance, ethics/culture, and IT into a unified approach (OCEG, 2017).

This research uses the first component of the COSO ERM 2017 framework, Governance and Culture, along with internal context from the Learn component of the GRC Capability Model. In terms of the linkage between COSO ERM 2017 and the GRC Capability Model, the internal context element from the Learn component of the GRC Capability Model was utilized as the tool of analysis to evaluate PT XYZ's readiness to implement risk management. Later, the result of this research is used to analyze whether the company is ready to

implement risk management according to the principles outlined in the Governance and Culture component of the COSO ERM 2017 framework.

3. RESEARCH METHOD

3.1. Research Approach

Five types of methods can be used in conducting research: experiments, surveys, case studies, grounded theory, and action research (Sekaran & Bougie, 2019). This research employs the case study method, which focuses on gathering information related to a particular object, event, or activity. Cases can be based on individuals, groups, business units, or companies. As an empirical research method, various data collection approaches are required to gather the necessary data for the research.

The case study model is based on an in-depth investigation of a single individual, group, or event that is related to the reality faced by the research object and aims to answer the research question (Ellet, 2018). This method was chosen since the objective of the research is to evaluate the risk management implementation readiness of a medium-sized enterprise, namely PT XYZ. The researcher is therefore using the evaluation method, as one type of case study, to determine the firm's readiness to implement risk management. This case study is expected to uncover sufficient knowledge about the present state of PT XYZ and whether it is ready to implement risk management in its present situation.

3.2. Research Object

PT XYZ was established in 1998 and is based in Jakarta. It provides integrated digital security systems and offers, for example, the installation of automatic doors, surveillance cameras, fire alarms, and security sensors. Uniquely, all of the company's projects are based on requirements from the government. These have included the installation of CCTV and a perimeter system at the Ministry of Transportation of the Republic of Indonesia and the installation of CCTV, a perimeter system, x-ray screening, road blockers, and access control at North Sumatera Regional Police. To date, PT XYZ has not undertaken many projects on behalf of private parties.

3.3. Data Collection

Data collection is the process of gathering and measuring information on variables of interest, in an established systematic procedure, to enable the research to answer the stated research questions, develop hypotheses, and

evaluate outcomes (Kabir, 2018). In this study, the data and facts were obtained through a literature review, interviews, and observation. The literature review focuses on the Governance and Culture component of the COSO ERM 2017 framework and the Learn component of the GRC Capability Model. The interview questions were developed with reference to the GRC Capability Model and the interviews were conducted with a total of 16 people comprising employees, managers, and directors of PT XYZ. In addition, observations were made to collect relevant information about the current situation at PT XYZ.

Literature Review

A literature review surveys reliable sources such as books, scholarly articles, journals, reports, and newspapers, and in so doing, provides a description, explanation, and summary concerning the research problem under investigation (Sekaran & Bougie, 2019). The purpose of a literature review is to gain an understanding of the existing research related to a particular topic or area of study. A literature review also helps us to explore similar research topics (Kuncoro, 2018). In this research, the literature review examined the COSO ERM 2017 framework, the GRC Capability Model, and other supporting sources. When referring to a literature review, researchers expect to fully exploit all of the available information, thus enabling them to achieve a qualified result.

Interview

Interviews are used to obtain data related to the research questions. Interviews entail asking open-ended questions to converse with respondents and collect relevant data from them. They can be held individually or in groups, depending on the supporting condition, and can be conducted in person, by telephone, or online (Sekaran & Bougie, 2019). Researchers should select the method that best answers their research question, taking into account that the greater the accuracy of the collected data and subsequent analysis, the more accurate the outcomes will be (Sekaran & Bougie, 2019).

In this research, interviews were deemed necessary for obtaining information as they offered an effective means of gathering detailed data from the employees of PT XYZ, as the research object. The interviews were conducted directly with the individuals working in PT XYZ's office building.

The questions were taken from the Learn component of the GRC Capability Model and could be developed into much more detailed questions regarding the internal condition of the company as the interviews were conducted. Each face-to-face interview lasted for between 20 to 25 minutes; a total of 16 people were interviewed out of the total workforce of 35, comprising three directors of PT XYZ, five managers, and eight employees representing each division of the company, as shown in Table 1.

Table 1. Interview Participants

Number	Codes	Position	Tenure	Interview Duration	Interview Mode
1	Mr. A	President Director	8 years	35 minutes	Face to face
2	Mrs. B	Director of Finance and Marketing	7 years	30 minutes	Face to face
3	Mr. C	Director of IT and Operations	2 years	30 minutes	Face to face
4	Mr. D	Supply Chain Management Manager	3 years	20 minutes	Face to face
5	Mr. E	Operations and Distributions Manager	3 years	20 minutes	Face to face
6	Mr. F	Project and Marketing Manager	2 years	35 minutes	Face to face
7	Mr. G	Services Manager	6 years	20 minutes	Face to face
8	Mr. H	General Manager	5 years	35 minutes	Face to face
9	Ms. I	Supply Chain Management Employee	1 year	20 minutes	Face to face
10	Mr. J	Operation and Distributions Employee	1 year	25 minutes	Face to face
11	Mr. K	Project and Marketing Employee	3 years	20 minutes	Face to face
12	Mr. L	Services Employee	4 years	20 minutes	Face to face
13	Mr. M	Product Technology and Development Employee	2 years	25 minutes	Face to face
14	Mrs. N	Human Resources Department Employee	3 years	25 minutes	Face to face
15	Ms. O	Accounting and Finance Employee	2 years	30 minutes	Face to face
16	Mr. P	General and Administration Employee	2 years	20 minutes	Face to face

The researcher asked questions related to the company's internal condition. The interview process was estimated to be completed within eight working days, with an average of two people interviewed per day, followed by observation at the company.

Observation

Observation is a way of gathering data by monitoring, recording, analyzing, and interpreting behavior, actions, or events in their natural setting. It can be distinguished based on whether or not control is exerted during the observation process, whether or not the observation is structured, and whether or not those being observed are informed that this is happening (Sekaran & Bougie, 2019). The goal of an observational study is usually to draw conclusions about the corresponding population or differences between two or more populations (Peck, Olsen, & Devore, 2018). However, this research was spontaneous as the researcher wished to assess the reality at PT XYZ. Hence, no control was exerted over the observation process undertaken. However, while it was not structured, the employees involved were notified that they were being observed.

Aside from the interviews that had previously been conducted, the researcher used the observation method to enrich the data as needed to pursue the objective of this research. This included observation of meetings held in the company; for example, the tender offer process begins with a study and the appointment of the person in charge before progressing to the bidding process and monitoring whether the responsibilities are appropriate for the job description ordered.

The main focus of this observation was the company's internal condition during those main activities in its business process. The observation process

lasted for two weeks, with each week comprising five working days. During the observation, the observer attempted to act as a passive observer as far as possible to minimize their impact on the observed activities.

The greatest challenge posed by the observation method is the possibility of bias between the observation that takes place and the reality of the company's situation. Indeed, a company may seek to show only the best side of its business flow during the observation. Throughout the observation process in this study, the researcher was present at tender meetings with the government.

During the observation, the researcher learned about the system that the company used in its tender offer process. It begins with the submission of a proposal in response to a government tender offer. If the proposal is accepted, the process moves to negotiations on price and various other terms that cannot be explained here. Once everything is settled, the company obtains a loan from the bank to purchase all of the products required for the tender.

3.4. Data Analysis

The data and facts were obtained through a literature review, interviews, and observation. After the interviews were completed and added to the observation results, they were analyzed, linked, and interpreted with reference to the theory discussed in the literature review, as a basis from which to evaluate the readiness to implement risk management at PT XYZ.

4. ORGANIZATION PROFILE

4.1. General Description

PT XYZ is a company based in Jakarta that offers a wide range of state-of-the-art communication and security system products to meet the varying needs of customers. It claims that its products are durable and reliable due to the strict monitoring undertaken through quality control before the products reach the customer. PT XYZ targets the local market in Indonesia and to date has not expanded to sell its products abroad. Having been established in 1998, the company's vision is to provide high-end quality products to its customers. Its current focus leans toward the provision and installation of integrated security systems in transportation, industry, banks, airports, and harbors. The company's strategic projects have included the installation of a CCTV and perimeter system at the Ministry of Transportation of the Republic of Indonesia and CCTV, a perimeter system, x-ray for people screening, road blocker, and access control for the North Sumatera Regional Police.

4.2. Company Structure

In the more than 20 years since its establishment, PT XYZ has strived to provide the best security system products from suppliers to ensure the satisfaction of its customers. At the same time, it has continually made adjustments and improvements to its internal aspects to ensure it operates optimally. To date, the company has modified its organizational structure on several occasions. In 2008, it reduced the size of the board of directors, from five people to three people, in a move that was known to cut operational expenses.

The company now has three directors, five managers, and eight divisions. The latter comprise supply chain management, operations and distribution, project and marketing, services, product technology and development, human resources, accounting and finance, and the general and administration division.

5. RESULT AND DISCUSSION

5.1. Internal Context (GRC Capability Model) Analysis on PT XYZ

Internal Strengths and Weaknesses (as part of SWOT)

Strength analysis focuses on the advantages or things that can provide benefits for the company and highlights several aspects that constitute a strength for PT XYZ. First, the company offers high-end products, with its quality control process helping to ensure that it sells only the best-quality products. This strict quality control, which the company combines with the use of the latest technology, ensures a high degree of reliability and durability.

As stated by a supply chain management employee, “PT XYZ believes that if the products that are offered to the consumers is the best-quality product, it will generate trust from consumers.”

Therefore, good relationships are created with customers that will lead to new opportunities in the future. In addition, as a form of responsibility, PT XYZ provides a guarantee covering damage during the first year after installation. This is a critical part of maintaining consumers’ trust in both the company and the products themselves.

Second, the company faces low competitor risk as it is the sole distributor of the products offered.

A service employee stated, “PT XYZ is also becoming the sole franchise holder of security systems under the brand of ‘X’ in Indonesia. Hence, PT XYZ is superior compared to other competitors in the same industry. As a sole distributor, PT XYZ is given priority over other companies when it comes to the installations of security systems.”

Third, PT XYZ pays great attention to the quality of its human resources. To improve the quality of these human resources, the company provides frequent training to existing employees based on their roles in the company. However, it also believes that the quality of human resources is one of the factors that can contribute to its further evolution. With appropriate training, PT XYZ is confident that its human resources will be able to compete with others. The information in this section was obtained from interviews with a human resources department employee

Meanwhile, weaknesses analysis focuses on aspects that may be potential obstacles in terms of hindering the company from achieving its objectives. First, the organizational structure of PT XYZ does not fully reflect the employees' actual roles. Thus, while there is a clear division of tasks and functions between the different divisions, in practice, some tasks continue to be allocated to individuals that fall outside their responsibilities.

For example, employees from the services department may be responsible for the distribution of the company's products. Second, according to the interviews with accounting and finance employees, "the company is less concerned about the welfare of its own employees. If the employees are obligated to work overtime due to an unfinished job, PT XYZ does not give compensation for the overtime worked. Hence, it seems detrimental and ends up reducing employee morale."

Third, PT XYZ operates with fairly large profit margins of almost 200% across its entire product range. In this respect, the company benefits from its status as the sole franchise holder of security systems under the "X" brand in Indonesia through its ability to set higher prices. However, this also creates a new threat in that the prices of the products render them less competitive in the market.

Existing Strategic Plan

After focusing exclusively on the government sector, one of PT XYZ's strategic plans concerns its decision to expand into the private sector over the next three years. However, during that short period, PT XYZ must address various imperatives, including the implementation of risk management. The consideration is that the company will face higher risks once it begins to expand, including market risks and financial risks, among others. Thus, before those risks can have a significant impact on the company, it plans to manage them as quickly as possible.

PT XYZ considers that risk management should be implemented once it begins to expand into the private sector. By expanding in this way, the company is moving outside its more traditional comfort zone. The implementation of risk

management will thus help it to identify the risks it might face or the opportunities that it should pursue over the longer term (Ebert & Grifin, 2014).

Existing Operating Plan

PT XYZ's operational planning focuses on two main areas: sales (including product installations) and servicing provision. For sales, when the company receives an invitation to tender in the government sector, various requirements must be met before it can take part. In contrast, working in the private sector will tend to be less complicated and quicker than in the government sector.

In terms of its role as a servicing provider, as the sole official distributor of the products that it sells, PT XYZ holds the right to provide servicing to products under the "X" brand for which there are problems. PT XYZ has a service department that is responsible for these duties.

Existing Organizational Structure

PT XYZ's organizational structure reveals that the finance and marketing director does not appear to be linked to the chief executive officer. This connection should be indicated in the organizational structure, along with that of the IT and operational director.

The organizational structure also shows that middle managers have direct communication with the chief executive officer, thus bypassing the IT and operational director. If the middle management communicates directly with the chief executive officer, then the board of directors is not functioning optimally and the chief executive officer will be too dominant.

Based on Constitution Law No. 40 in 2007 on Limited Liability Companies, the board of directors should be monitored by the board of commissioners, both generally and specifically. Meanwhile, the organizational structure of PT XYZ shows that it does not have commissioners. Without commissioners, there can be no optimal monitoring of the board of directors.

Existing Incentives (Appropriate or Inappropriate) For Performance

An employee of PT XYZ stated, "the company is less concerned about the welfare of its own employees. Incentives that are given by the company are not suitable for the performance of the employees. For example, if the employees are obligated to work overtime due to an unfinished job, PT XYZ does not give compensation for the overtime worked. Hence, it seems detrimental and leads to reduced employee morale."

It can be concluded that not all employees are satisfied with the incentives offered by PT XYZ. The company should be concerned about this issue as it will generate new problems in the near future. For example, it will affect the loyalty of employees to the company.

Existing Key Processes and Resources (People, Financial, Process, and Technology)

PT XYZ always emphasizes the importance of responsibility to its employees and if any employees are not responsible for the tasks assigned to them, they will be issued a penalty. The human resources at PT XYZ come from different educational backgrounds. The company seeks to provide opportunities for people who strive to improve in terms of their skills, experience, and competence. Reflecting this, PT XYZ provides frequent training to employees based on their roles in a bid to boost their capacity. Investing in the quality of its human resources gives the company confidence to pursue its objectives more effectively and efficiently.

At the same time, however, the company is also considered to be less concerned about the welfare of its existing employees. Based on the interviews, if employees are obliged to work overtime due to an unfinished job, the company does not compensate them for the overtime worked. This can be detrimental and end up damaging employee morale. From the interviews with the directors, the explanation for this is that if there are employees who are dissatisfied with the company's system and decide to leave, they can be easily replaced. However, PT XYZ must also consider the cost of training its employees.

Based on the information obtained, PT XYZ is in good financial health. It should be noted that the company's financial cash flow is heavily dependent on project tenders in the government sector. When it wishes to begin an installation project in the government sector, it must first apply for a loan from the bank to purchase the required products.

The first stage in the existing business process at PT XYZ is participation in the tender offer process. However, the company must fulfill various requirements before it can take part. After winning a tender, PT XYZ will deliberate on the products to use. Soon after this, given that it does not store large quantities of products in a warehouse, an order will be placed with suppliers for the products required. Once these products arrive, PT XYZ will commence the installation process based on the stated agreement. Following completion of the installation process, the company will be responsible for the products for one year, including the maintenance.

While the technology that PT XYZ uses evolves periodically, the company works in integrated digital security systems, which means that technology sophistication remains a priority. The COVID-19 pandemic also promoted the more rapid development of and transition toward touchless technology.

To counterbalance these technological changes, companies must ensure they have the correct human resources in place that understand the latest innovative technology set to enter use. PT XYZ anticipates this by delegating

employees to attend training on the related technology before it is applied to the company's products. This solution helps employees to understand the new technology that will be applied.

Existing Information and Gaps or Conflicts in Information

Conflict was found to occur at PT XYZ that involved communication and information at the top management level. The conflict arose due to poor communication among the top management, one member of which was also relatively new, meaning that knowledge of the system at PT XYZ was considered to still be minimal. This resulted in a discrepancy in terms of communication and information delivery.

Conflicts that occur repeatedly can disrupt a company's performance (Thompson et al., 2020). To avoid this type of situation, PT XYZ should be more selective regarding its process for hiring individuals to join the top management. New individuals should be given training and develop a good understanding of how things work in the company before they are assigned responsibilities.

5.2. Readiness Analysis About Risk Management Implementation (COSO ERM 2017)

The first component of the COSO ERM 2017 framework (Governance and Culture) consists of five related principles. The results of the analysis of the internal context derived from the Learn component of the GRC Capability Model aid in determining whether the company is compliant with the principles under the Governance and Culture component of COSO ERM 2017.

The first principle is "Exercises board risk oversight." Based on the analysis of "existing information and gaps or conflict in information" conducted on PT XYZ, the researcher identified conflicts among the board of directors. PT XYZ's directors should be able to set an example of behavior to those who work at the lower management level. However, the current conflict between the company's directors is considered a bad example for other employees, especially at the lower management level.

The conflict also illustrates that the board of directors may include incompetent and inexperienced people. PT XYZ must immediately resolve this problem and ensure there is no reoccurrence as it can lead to a fall in the employees' trust in the board of directors.

PT XYZ currently lacks a commissioner, as can be seen from the organizational structure. With no commissioner, there is no supervision of the board of directors as no one else in the company can perform this role. The commissioner can also provide oversight of the tone at the top of the company.

From the description above, the researcher concludes that PT XYZ has failed to properly implement and exercise board risk oversight.

The second principle is "Establishes operating structures." The existing operating structure at PT XYZ has been well defined, from the tender offer to the installation process carried out once the company has won a tender. This statement is in line with the results of the analysis of the GRC Capability Model's internal component "existing operating plan."

Based on the analysis of the "existing organizational structure" as an internal element of the GRC Capability Model, the organizational structure of PT XYZ indicates that the finance and marketing director does not appear to be linked to the chief executive officer. The organizational structure should indicate this connection, along with that for the IT and operational director.

PT XYZ's organizational structure also shows that middle management has direct communication with the chief executive officer, thus bypassing the IT and operational director. If the middle management communicates directly with the chief executive officer, then the board of directors is not functioning optimally, and the chief executive officer will be too dominant.

However, PT XYZ also needs to consider that the implementation of tasks does not strictly align with the company's stated organizational structure. Various employees perform duties that fall outside their previously defined job descriptions. The company also needs to consider the addition of coordination lines, as outlined by the researcher in the previous section.

If the company's organizational structure is based solely on a command line, then the board of directors does not need to coordinate with management to go through to employees. The lines connecting the different divisions should be based on coordination and not command lines, thereby illustrating the lines of coordination between divisions.

The third principle is "Defines the desired culture." PT XYZ emphasizes to employees a culture of being responsible and the obligation to finish what they have started. The company also issues penalties in the event of violations by employees. Based on the analysis of the "existing key process and resources (people, financial, process, and technology)" internal component of the GRC Capability Model, all employees at PT XYZ successfully follow the responsible work culture, with no exception.

Regarding its code of ethics and company regulations, PT XYZ does not have a written code of ethics. Instead, the code is conveyed orally to the lower positions by the board of directors and is understood by all employees. However, a code of ethics should be written and not only delivered orally (Robbins & Coulter, 2015).

In contrast, PT XYZ has a set of written regulations that are posted on the company wall. Nevertheless, the researcher concludes that PT XYZ has not fully implemented the "Defines desired culture" principle because certain things are only conveyed orally.

The fourth principle is "Demonstrates commitment to core values." One of PT XYZ's core values is to provide only the best-quality products to consumers. This is evident from the dedication in the company's internal discussions, where the company directors strongly emphasize the importance of ensuring product quality for consumers. As such, other employees will uphold this value and ensure that consumers do not receive poor quality products.

Based on the internal element of the GRC Capability Model, "internal strengths and weaknesses (as part of SWOT)," PT XYZ makes various efforts to ensure product quality, including employee training and development programs, strict quality control, and the use of technology innovation in the products offered to consumers. This demonstrates the company's integrity and commitment to implementing the core values that have been set. The researcher therefore concludes that PT XYZ has implemented the principle of "Demonstrates commitment to core values" well.

The fifth principle is "Attracts, develops, and retains capable individuals." Here, PT XYZ performs its function to improve the quality of human resources in the company through the provision of various training programs. In addition, the company accepts employees from a range of different backgrounds, and all new employees who join the company receive appropriate training based on their role in the company.

However, PT XYZ is unable to maintain its existing human resources as it assumes that employees who leave can be easily replaced; as such, there is an assumption among certain employees that the company does not highly value employee welfare. This requires more attention from the company.

The assumption that the company does not pay attention to the welfare of employees can be interpreted as employee dissatisfaction with the incentive system in place. PT XYZ must therefore pay closer attention to retaining existing employees. While it is true that employees who leave can be replaced, companies still need to consider the costs associated with training new employees.

Based on analysis using the internal component of the GRC Capability Model, as elaborated above, the researcher assessed the readiness of PT XYZ to apply risk management based on the COSO ERM 2017 framework, especially regarding the Governance and Culture component. This analysis implies that the internal context of PT XYZ is not yet ready for the company to

apply risk management. It is not yet following all of the Governance and Culture principles, as stated by COSO ERM 2017. The company needs to make improvements regarding the main issues explained in the previous section, including conflict among the board of directors, the organizational structure that is not operating optimally, and employees' dissatisfaction with their remuneration. Hence, the researcher proposes recommendations to respond to these issues in the next section.

6. CONCLUSION AND DISCUSSION

This section elaborates the conclusions and recommendations obtained through the evaluation and analysis in Section 5. This section also elaborates the limitations of the research and provides recommendations for future research regarding risk management.

6.1. Conclusion

Based on the analysis in the previous section, this research derives the following conclusions. Based on the five principles of the Governance and Culture component in the COSO ERM 2017 framework, PT XYZ is not ready to implement risk management. Moreover, many aspects require improvement, notably regarding conflicts among the board of directors. Specifically, improvement is needed in the delegation of tasks to employees. The company's organizational structure does not reflect the role of the financial director and there is no board of commissioners as regulated in constitutional law. The interview results also revealed that the employees are not satisfied with their incentives.

6.2. Recommendations

Based on the analysis and conclusions obtained in this research, various recommendations are proposed to PT XYZ. These are elaborated as short-term and long-term recommendations.

Short-term Recommendations:

Improvement is needed to PT XYZ's organizational structure, including the delegation of tasks to employees and the recruitment of a board of commissioners to monitor the activities of the board of directors of PT XYZ. PT XYZ needs to emphasize the lines of responsibility through its organizational chart.

Furthermore, PT XYZ needs to address the issues surrounding employee satisfaction based on concerns with the existing incentive scheme. The company needs to consider employees' opinions regarding the remuneration system. Ignoring the issue will only bring the risk of more significant issues in the future.

PT XYZ also needs to resolve the conflicts within the board of directors. These cannot be neglected as doing so would affect the image of the directors. PT XYZ can hold a meeting to further discuss this issue.

Long-term Recommendations:

PT XYZ needs to ensure that forum group discussions are held regularly to discuss the issues facing employees. In this way, the company can endeavor to minimize dissatisfaction among employees.

PT XYZ must also act to prevent the same issues regarding conflicts in the board of directors. It needs to ensure that the employees it recruits are suitable based on their experience and competency. The company also needs to provide appropriate training if this is required.

6.3. Research Limitation

The limitation of this research concerns the analysis section, which focuses heavily on the Learn component of the GRC Capability Model and the Governance and Culture component of the COSO ERM 2017 framework.

6.4. Suggestion

Based on the conclusion, recommendations, and limitation of this research, the researcher makes the following suggestions for future studies.

1. The next study should seek to obtain a more comprehensive result by using every component in the COSO ERM 2017 framework and the GRC Capability Model.
2. Future research could use a different approach in the literature review and conceptual framework, such as ISO 31000.

ACKNOWLEDGEMENTS

The author is grateful to PT XYZ for consenting to become the research object for this study. The author would also like to thank all of PT XYZ's employees for their participation in this research.

REFERENCES

Alshenqeeti, H. (2014). Interviewing as a data collection method: A critical review. *English Linguistics Research, 3*. doi:10.5430/elr.v3n1p39.

COSO (2017). *COSO Enterprise Risk Management 2017*.

Ebert, R. J., & Grifin, R. W. (2014). *Pengantar Bisnis*. Jakarta: Penerbit Erlangga.

Ellet, W. (2018). *The case study handbook: A student's guide*. Boston, MA: Harvard Business Review Press.

Kabir, S. M. S. (2018). *Basic guidelines for research: An introductory approach for all disciplines*. Chittagong, Bangladesh: Book Zone Publication.

Kuncoro, M. (2018). *Metode riset untuk bisnis & ekonomi.* Jakarta: Penerbit Erlangga.

Lam, J. (2017). *Implementing enterprise risk management.* Hoboken, NJ: Wiley.

Moeller, R. R. (2011). *COSO Enterprise Risk Management: Establishing effective governance, risk, and compliance processes*. Hoboken, NJ: Wiley.

OCEG (2017). *GRC Capability Model Version 3.0 (Red Book)*.

Peck, R., Olsen, C., & Devore, J. (2008). *Introduction to statistics & data analysis.*

Peraturan Pemerintah Republik Indonesia Nomor 7 Tahun 2021 Tentang Kemudahan, Pelindungan, dan Pemberdayaan Koperasi dan Usaha Mikro, Kecil, dan Menengah (2021).

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), 16–23. doi:10.1002/jcaf.22346

Robbins, S. P., & Coulter, M. (2015). *Manajemen*. Jakarta: Penerbit Erlangga.

Sekaran, U., & Bougie, R. (2019). *Research methods for business: A skill building approach* (7th Ed.). Chichester, UK: Wiley.

Thompson, A., Peteraf, M., Gamble, J., & Strickland, A. J. (2020). *Crafting and executing strategy.* New York: McGraw-Hill Education.