Enterprise Risk Management as a Pathway in Enhancing the Organization's Performance and Efficacy: A Case Study of An Indonesian Public Service Organization

Dr. Franciskus Antonius Alijoyo
Faculty of Economics, Parahyangan Catholic University, Indonesia

Abstract

The study aims to analyze the practice of Enterprise Risk Management (ERM) at a large Indonesian public service organization (PSO) and see how it helps them reach their goals and objectives. As the efficacy of ERM is embodied and reflected in risk management maturity level, this study also analyzes the efforts of such PSO to enhance their organization's performance and efficacy through a higher level of risk management maturity. This study observes the assessment of their current risk management maturity level and captures on what and how some recommendations be identified, explored, and proposed to improve its ERM maturity. By applying qualitative approaches (e.g., interviews, questionnaires, and observation), it is found that the current ERM practices of such PSO are not yet integrated with its organizational governance and management. ERMA ISO 31000 RM3 (Enterprise Risk Management Academy - ISO 31000 Risk Management Maturity Model) can determine that their current ERM maturity level is at the initial stage. This reflects that such PSO still uses a silo-based approach in managing risk, and the application of its risk management is only used to cope with a particular risk.

Upon such a result, some room for improvements to increase risk management maturity is proposed to reach a much higher level within four years. As the study is based on real-case, the result can be used as empirical insights to the academic world and comparative references to the risk management practitioners and enthusiasts.

Keywords: Enterprise risk management, risk management maturity, public service organization (PSO), ERMA ISO 31000 RM3.

1. Introduction

The paradigm and the role of enterprise risk management (ERM) are essential for any organization. The significance and importance of ERM have become more apparent since risk is highly interdependent by nature. It had resulted in a situation where the traditional risk management practice (i.e., silo-based approach) would not be sufficient to mitigate risks effectively (Macgillivray et al., 2007). This is undoubtedly the case since most, if not all, organizations operate within a highly complex and interconnected environment. Based on this

circumstance, any organization with an inadequate level of performance, efficacy, and understanding in ERM is more susceptible to get caught by sudden changes that occur within its environment and more vulnerable to the events that can harm its value, financially, or else.

For the public service organization (PSO) in particular, their capability in managing risks is crucial to ensure the output they produce can serve and fulfill the public interest. Implementing effective ERM within the PSOs can further enhance the performance and efficacy of its service delivery and, at the same time, be a tool for accountability (Palermo, 2014). Under this context, the PSOs are directly accountable to the public because they are responsible for delivering the goods and services that link with the public interest and well-being. The PSOs, by default, are exposed to public risk along with the financial, operational, societal, and political risks (Asenova et al., 2015; Carlsson-Wall et al., 2019). Since risks are interdependent, if the PSOs ineffectively manage and mitigate the risk, it can trigger a domino and ripple effect that harms them and the public at large. Consequently, the repercussions from the risk of failure of the PSOs in managing their risks can exceed the private organizations (Lapsley, 2009).

The importance of the PSOs and their relationships with the public have resulted in the ERM paradigm and mechanism being urgently needed in their activities. Adopting the ERM framework within the public sector is now a necessity due to the role of risk management within the respective sector that tends to focus solely on accountability with the greater emphasis on transparency, involvement, proportionality, evidence, and responsibility instead of the strategic and processual risk management (Mahama et al., 2020). Suppose the role of risk management within the public sector is restricted. In that case, it will present the PSOs with a significant challenge in managing the risks effectively and maintaining their performance and efficacy in serving the public. Moreover, if the mentioned restriction exists within the PSOs' activities, it can hinder their opportunities in obtaining an added value through their ERM practice.

Following the brief introduction above, one particular Indonesian PSO has adopted the International Organization for Standardization (ISO) 31000 standard as their reference in managing the risks effectively. However, the respective PSO could not deal with them as expected as they also faced some other problems that made them fail to achieve their performance objectives. Moreover, the coronavirus disease outbreak in early 2020 put more weight on the PSO to have a more effective ERM starting by early 2021 onwards, and their executives have decided to conduct a risk management maturity assessment to understand their current level and map out the road to obtain a higher level of risk management maturity at a later stage. Accordingly, this study aims to understand how ERM is practiced in the particular PSO. More specifically, this study tries to (1) determine the ERM maturity level of the PSO, (2) identify the limitation of the PSO's ERM, and (3) generate a recommendation to improve the PSO's ERM maturity.

As for the remainder of this paper, it is structured as follows. The following section presents the literature review on the relationship between ERM and an organization's performance, the role of risk management within the PSOs, and the ISO 31000 standard. The third section presents the data and the method used to assess the Indonesian PSO ERM maturity. The findings in regards to the PSO's ERM maturity assessment are presented in the fourth section. Lastly, this study's conclusion, limitation, recommendations for future research are presented in the fifth section.

2. Literature Review

2.1 ERM, risk management maturity, and organization's performance

Despite the many views on what constitutes an ERM, there are three consensuses in regards to the matter – namely, (1) ERM manages risks as a portfolio rather than individually, (2) ERM handles not only traditional risks (e.g., accidents) but also consolidates strategic risk within the organization's decision-making process, and (3) the nature of ERM focuses not only on mitigating risk but also on gaining a competitive advantage (Bromiley et al., 2015). At its core, ERM aims to aid the organizations in managing the diverse range of uncertainties and risks that can harm or even endanger their welfare and well-being, enhance and protect their value creation and proposition, and ensure their sustainability through a systemic approach. In that capacity, ERM is also designed to enhance the executives' capabilities in overseeing the risks faced by the organization while simultaneously becoming their source of competitive advantage (Beasley et al., 2005). Under this context, it is worth emphasizing that the effectiveness and efficacy of one's ERM depend on its holistic and integrated implementation, which incorporates all layers of the organization's management and stakeholders to strongly mitigate the risks and gain a higher added value through its activities.

In practice, however, there are many challenges that an organization needs to cope with to ensure and maintain the ERM effectiveness. The fundamental challenges in realizing an effective ERM practice revolve around the organization's lack of openness in integrating the ERM concept within its corporate culture, the lack of knowledge about the risk itself, an overly complicated mindset on risk, and unclear objectives and timeframes (Fraser & Simkins, 2016). Following those challenges, some studies (e.g., Arena et al., 2010; Fiksel et al., 2015; Fraser & Simkins, 2016; Nocco & Stulz, 2006) have given some insights on which an organization can apply to increase its performance and efficacy through ERM by: (1) communicating the risks that exist within its environments to its stakeholders, (2) aggregating the common risks across its business segments, (3) becoming adaptive to the changes, (4) achieving active participation among the board members, and (5) seeing the role of ERM beyond compliance tasks. In short, to achieve an effective practice and implementation of ERM, an organization must realize that risk management is critical in enhancing its value creation process, and it must be reflected within its activities, planning, and decisions.

From a different perspective, the organization's characteristics also determine the efficacy, performance, and capabilities level of its risk management initiatives and conduct. Some of the essential characteristics of an organization concerning the ERM implementation are the organization's size, the types of industry, the institutional ownership, and the organization's auditor (Bohnert et al., 2017; Gordon et al., 2009). By considering those characteristics, every organization across all industries has a different level of ERM effectiveness. For instance, a large and wealthy organization has a higher likelihood of having an advanced ERM and more resources to improve its risk management mechanism. Moreover, if the respective organization operates within a highly regulated industry (e.g., financial industry), they are bound by regulations to implement the risk management mechanism in the first place.

Since every organization has a different ERM effectiveness level, the term "risk management maturity" describes the degree of their risk management integration and implementation. Generally speaking, when an organization has low-risk management maturity, it describes that the organization manages risks using a silo-based approach, and its

implementation depends on specific individuals. Whereas, an organization with high-risk management maturity refers to applying systematic, integrated, and holistic ERM mechanisms in coping with risks; at this stage, the concept of risk management has already been embedded within its activities and infused within its decision-making process corporate culture. Such descriptions can be seen in many risk management maturity models, for example, the model of Chapman (2011, 2019), Hillson (1997), Organisation for Economic Co-operation and Development (2021), and Software Engineering Institute (2010). Even though the attributes or aspects used in the mentioned risk management maturity models vary, it still conveys the same purpose of assessing the degree of risk management integration and embeddedness within its activities and culture. Thus, at its peak, an organization that has mature ERM practice has the following nine characteristics. Namely, (1) a dedicated risk executive, (2) highly engage with the stakeholders, (3) fully committed to the ERM implementation at board levels, (4) ERM is included within the strategic decision-making process, (5) ERM as part of the organization's culture, (6) advanced quantitative risk assessment methods, (7) engage in identifying new and emerging risks, (8) transparent risk communication, and (9) integrated information on operational and financial risks (Lindberg & Seifert, 2011).

When an organization can effectively implement the concept of ERM within its operational and business activities or has mature risk management, it can enhance its value, financially, or else. Empirically, it is found that ERM initiatives and tools have the highest efficiency estimation (both in revenue and cost) in improving an organization's value (Grace et al., 2015), and organizations that use ERM is valued higher than the non-ERM users (Farrell & Gallagher, 2015; Hoyt & Liebenberg, 2011). On the other hand, when an organization has an incomplete adoption of ERM, it is estimated that they have either a minimal or no effect on its performance, and it is found that those firms are less profitable within the financial market (Florio & Leoni, 2017). Subsequently, it can be concluded that when an organization has low-risk management maturity, its ERM programs will not be as powerful as expected in enhancing its value (both operationally and financially) and, at the same time, they are at risk of not being able to ensure their sustainability within a complex and highly competitive environment.

2.2 Risk management in PSOs

The role of risk management within the PSOs is not much different from a private organization. However, the fundamental difference between these two lies in two aspects, namely (1) the range and variety of stakeholders and (2) the extent of the organization's decisions impact on the political and social dimensions (Spikin, 2013). To put it into perspective, the PSOs are always facing public risk along with social and organizational risks. When those risks are crystallized, their ramifications go beyond the individuals and their impact permeates within every stratum of society. Due to this situation, if the PSOs applied risk management solely for symbolic insurance, which deviates from the definition and nature of ERM itself, it would not improve its value and the likelihood of delivering the results aligned with the public interest (Hood & Miller, 2009).

The role of risk management within the PSOs has become a necessity and essential in improving a nation's development and sustainability. According to some studies (e.g., Lapsley, 2009; Leung & Isaacs, 2008; Palermo, 2014; Power, 2004), the need and demand for implementing the risk management framework, concept, and system within the PSOs and government institutions are due to external pressure. To be precise, it refers to the competitive

pressure, regulatory changes, and standards that exist within the nationwide and global environments. The growing demand for ERM implementation within the public sector has pushed a higher standard for the PSOs. As a result, the PSOs are now expected to have a holistic perspective and approach in managing risks following their objectives and modernizing their structure and mechanism to better serve the public interest. In a way, such demand can be perceived as an effort to reduce the public's expectation gap on the PSOs' performance and efficacy.

Within the context of the public sector, the issues are not lies in the implementation of risk management but are oriented on the PSOs' complex nature. More specifically, due to a public organization which is highly bureaucratic by nature, any attempt to implement the risk management initiatives and approaches is more likely to be difficult (Ahmeti & Vladi, 2017). In some cases, implementing risk management within a public organization is more complicated than the private organization due to the existence of the seven challenges within the public sector, namely, (1) the separation between the operating and program budgets, (2) the unavailability of clear risk metrics, (3) complicated procedural requirements, (4) narrow mindset of risk, (5) senior officers who lack knowledge on risk management and business, (6) frequent changes and vacancies of leadership positions, and (7) goals that nullify other considerations (Braig et al., 2011).

Despite the complexities in implementing risk management in the public sector, many PSOs and government institutions have adopted and integrated the ERM mechanism within their activities. For instance, following the findings of Collier and Woods (2011), Legislation primarily drives the risk management practice and implementation within the United Kingdom and Australian local authorities, which contributes to the enhancement in managing the resource dependence of the two respective local authorities through the inclusion of external monitoring. In the United States, the Food and Drug Administration applies risk management to identify and assess the potential risks that reside within the medical products after it is made available to the public (Hardy, 2010). Additionally, following the case study of Woods (2009) on the Birmingham city council, the applied risk management framework and the system are shaped by the government's expectation, where it is developed under the existing standards (e.g., ERM integrated framework of the Committee of Sponsoring Organizations of the Treadway Commission) and its application is supported by the professional organizations (e.g., the Institute of Risk Management).

In conclusion, the demand for ERM framework and mechanism within the PSOs is due to the public's pressure. The ERM formalization within the PSOs is expected to at least the same as the private organizations since the professional organization can support the PSOs in developing its ERM system and mechanism. Furthermore, the consequence from the risk of failure within the context of PSOs can be much greater than the private organizations. This happens due to the differences in the range of stakeholders and the scale of its impact on the societal and political aspects.

2.3 ISO 31000 standard and its adoption

Due to the increasing demand and need for integrated ERM within the enterprise level, the International Organization for Standardization (ISO) has issued the ISO 31000 standard. The first edition was released in 2009 entitled "risk management – principles and guideline" and also known as the ISO 31000:2009 (ISO, 2009). The ISO 31000:2009 standard aims to

aid organizations in implementing integrated risk management within their activities, infusing the principles of ERM within its governance structure and mechanism, and enhancing its value through its decision-making process.

The second and current edition was released in 2018 (i.e., ISO 31000:2018) and renamed to "risk management – guideline" (ISO, 2018). Within the ISO 31000:2018 standard latest edition, the primary changes that have taken place revolve around the emphasis on the continual nature of risk management and the revision of the risk management principles. It also concentrates on the open system model to accommodate the organization's numerous needs and context and focuses on the leadership aspect and the integration of risk management that begins from the organization's governance (ISO, 2018). Even though the respective standard is updated, its purpose remains unchanged: to enhance the organization's value creation and protection through the application of risk management, continual improvement, and risk-oriented decision making. Similar to its predecessor, within the latest ISO 31000:2018 standard, there are three fundamental components in building and implementing a practical, efficient, and integrated ERM, namely (1) the principles, (2) the framework, and (3) the process of risk management. Furthermore, these three components are interdependent. To have effective risk management, the organization has to ensure that the risk management principles are reflected within its activities and governance structure.

Following the relationship between the three components of integrated ERM under the ISO 31000:2018, the component of risk management principles is considered the most critical aspect in realizing effective and integrated ERM. By design, the risk management principles dictate the organization's culture and attitude in implementing an integrated ERM concentrated in creating and protecting its value by establishing and improving its ERM mechanism and its capacity and capability in dealing with risks.

As for the component of the risk management framework under the ISO 31000:2018, it is oriented on the foundations and organizational arrangements for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the organization. Accordingly, the organization's executives are required to define the level of leadership and commitment needed in using the ERM framework in the first place. Hence, the organization has to align its ERM mechanism with its strategic decision-making process and culture to operate under the risk management perspectives to achieve objectives. Furthermore, the organization is also required to guarantee its continual improvements to ensure its ERM effectiveness in the long term and establish an agenda to regularly communicate the ERM role within every layer of its management level to ensure the common understanding of the necessity in applying risk management.

Lastly, the risk management process under the ISO 31000:2018 revolves around the implementation and practice of the established procedures and policies in identifying and assessing risk, along with communicating the role and ERM function on every management layer within the organization. Following the relationship between the risk management principles, framework, and process defined by ISO (2018), ERM process effectiveness of an organization reflects the its ERM framework quality and the engagement level in enforcing the principles of ERM within its activities. Concerning the previous edition of the respective standard, the ISO 31000 focuses on harmonizing the purpose and function of the risk management principles, framework, and process rather than purely enforcing the best practice of ERM (Dali & Lajtha, 2012). Therefore, the implementation of ERM under the ISO 31000

standard is not entirely concentrating on coping with risks but also ensuring the compatibility between the three components defined by ISO (2018) to seamlessly operate under the organization's distinct characteristics and culture.

The adoption of the ISO 31000 standard gains broad acceptance in many countries and large corporations as it is practical and business-oriented. Although there are still some challenges that need to be addressed, the ISO 31000 standard tries to harmonize risk management practices and attempts to achieve the position as a global benchmark for risk management (Almeida et al., 2019; Leitch, 2010; Purdy, 2010). The ISO 31000 standard has established the risk management principles, framework, and process in managing the enterprise risks, which is relevant and appropriate to any organization (Choo & Goh, 2015). Thus, the ISO 31000 standard captures ERM as an integrated way of managing risk rather than merely an ERM framework. Furthermore, its universal characteristics make them applicable for any organization.

Since the ISO 31000 standard has the universal trait, it is applicable for any type of organization, even for the government institutions. For instance, within the Asian region in general and South East Asia (SEA) region in particular, the study noted that five Asian countries are members of the G20 (i.e., China, India, Japan, South Korea, and Indonesia). South Korea confirmed that they had adopted ISO 31000 standard since 2014 relatively across most of their PSOs general government extensively. This adoption was pre-initiated by the crisis management guidelines for public organizations in 2007 (Kim, 2014).

Indonesia as the only G20 country in the SEA region had adopted ISO 31000 as their national risk management standard, namely SNI ISO 31000 (*Standar Nasional Indonesia* ISO 31000 in Indonesian) in 2011. However, the implementation of ISO 31000-based integrated risk management in their PSOs just started in 2018 in the Indonesian Ministry of Finance. Afterward, there were some other general government bodies announced their initiatives in 2019 to adopt ISO 31000 standards, such as the Financial Services Authority, the Central Bank of Indonesia, and the Supreme Audit Board.

3. Research methodology

The subject of this study is an Indonesian logistics PSO. The respective PSO's mission is to assure the logistics and manage the supply and demand of primary foods across Indonesia's archipelago. Thus, PSO's primary objective is to manage the availability of primary foods and maintain its price at a reasonable level. If there is an over-supply or shortage of primary foods, they will intervene in the market to maintain equilibrium. By which, when there is an over-supply, the PSO will buy and pull the primary foods in some quantity to prevent its prices drop in the market. In contrast, they will release the primary foods stocks when there is a deficit of supply to maintain the primary food's market price. As previously mentioned in the introduction section, the mentioned PSO uses the ISO 31000 standard as their primary reference in managing risks.

3.1 Data

The study is qualitative that used surveys through questionnaires and supported by interviews with senior and middle management. In addition, some observations are also conducted to validate the data from the questionnaire and interviews.

The questionnaire was given to all 24 Heads of Headquarters Divisions and all 26 Heads of Regional Offices. Interviews were done with all Heads of headquarters and 3 Heads of Regional Offices representing Western, Central, and Eastern Indonesia. The assessment results are discussed with the Strategic Planning and Research Division as the Counterpart Team and then presented to the Director of Procurement in charge of risk management.

3.2 Method

The model to assess the PSO's risk management maturity is ERMA ISO 31000 RM3 (Risk Management Maturity Model) which provides five Maturity levels based on six attributes, 22 indicators, 52 parameters, and 168 test factors.

The model is known as ERMA ISO31000 RM3, which provides five maturity levels:

1. Initial;
2. Repeatable;
3. Defined;
4. Managed; and
5. Optimized

The following table describes the interpretation of the respective maturity level:

Table 1. Maturity level ERMA 31000 RM3

Maturity level	Interpretation
1. Initial	Risk management is still ad-hoc, relies on individual initiative. It is silo or limited to a particular risk aspect and used to manage only certain risks, and relied on corrective actions.
2. Repeatable	Risk management starts systematically implemented. However, it is not integrated with organizational governance and organizational management. Competency, leadership, and commitment to risk management are not evenly distributed.
3. Defined	Risk management has been implemented systematically and consistently practiced as per ISO 31000 Risk Management Guideline or Standard. It is starting to be integrated with organizational governance and most of the organizational management. Competency, leadership, and commitment to risk management have been evenly distributed. However, positive behavior in managing risk remains limited.
4. Managed	Risk management has been integrated with organizational governance and organizational management systematically and consistently practiced as per ISO 31000 Risk Management Guideline or Standard. It becomes a culture that includes the strong support of competency, leadership, and commitment to risk management. Positive behavior in managing risk is prevalent throughout the organization and consistently supported with reviews, corrective actions, and improvements as needed.
5. Optimized	Risk management is an integral part of organizational governance and organizational management, systematically and consistently practiced as per ISO 31000 Risk Management Guideline or Standard. It has been internalized and rooted as an organizational culture with strong competency, leadership, and commitment to risk management. Positive behavior in managing risk has been manifested throughout and at all levels of the organization, supported consistently with reviews, corrective actions, and improvement as needed. It becomes the strong pillar of business resiliency and sustainability.

Source: ERMA ISO 31000 RM3

To determine the level of a particular organization's risk management maturity, ERMA ISO31000 RM3 suggests an assessment of the following six attributes presented in table 2:

Table 2. ERMA ISO 31000 attributes and descriptions

Attribute	Description
1. Risk culture	Measuring the extent to which corporate values have strengthened the risk management culture, whether the adequacy of competencies to take advantage of risk management is optimal or positive behavior in dealing with risks has become a significant element of the organization culture.
2. Risk management framework	Measuring the extent to which a strong leadership and commitment level have supported implementing an integrated risk management framework through the design, implementation, evaluation, and improvement of risk management effectiveness.
3. Risk management process	Measuring the extent to which the risk management process has been used as a technical approach to implement the risk management integration into all organizational processes.
4. Management process	Measuring the extent to which the management process includes risk-based strategic planning and its execution following the principles of managing risk as suggested by ISO 31000 Risk Management Guidelines.
5. Performance management	Measuring the extent to which performance management has been planned, implemented, monitored, reviewed, improved, and enhanced on a risk-based basis.
6. Resilience and sustainability	Measure the extent to which the organization's resilience and sustainability have been planned, implemented, monitored, reviewed, improved, and enhanced on a risk basis.

Source: ERMA ISO 31000 RM3

The assessment ultimately produces the achievement value in terms of scoring. Based on such achievement value, the risk management maturity level is determined through the conversion matrix, as shown in Table 3 below:

Table 3. The achievement value and maturity level

	Initial	Repeatable	Defined	Managed	Optimized
Risk management framework					
Risk management process					
Management process					
Performance management					
Risk culture					
Resilience and sustainability					

	Completely fulfilled
	Partially fulfilled
	Not fulfilled

Source: ERMA ISO 31000 RM3

The risk management maturity (RMM) score could be determined by applying equation (1):

$$RMM\ Score = Average\left(\sum_{i=1}^{n}\sum_{j=1}^{m} x_{i,j}\right) \quad (1)$$

Where:

RMM score = Risk management maturity score.

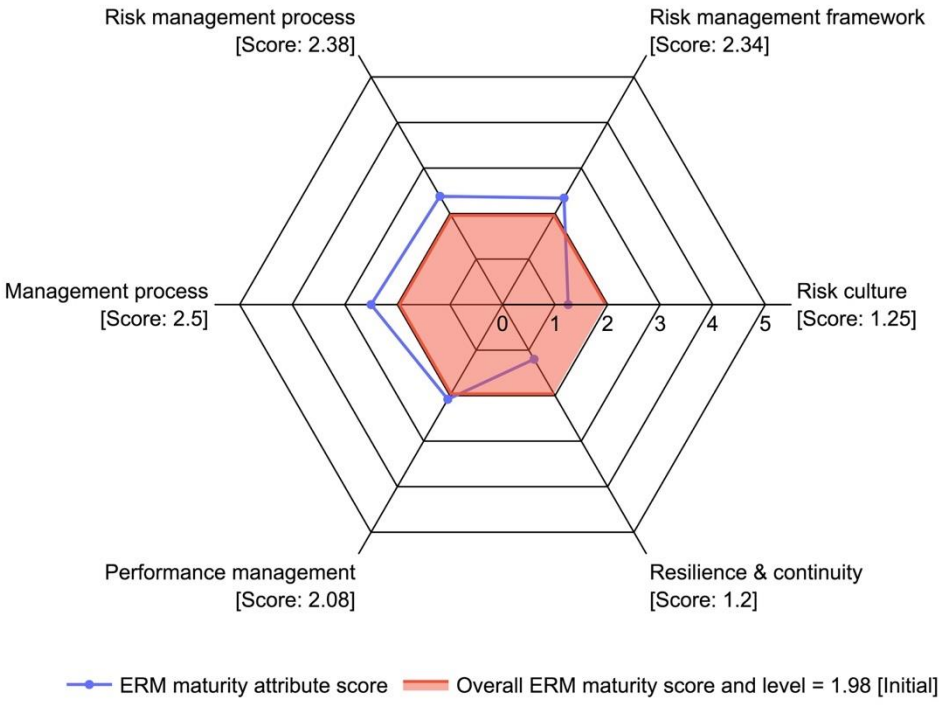
$x_{i,j}$ = Value of indicator j of attributes i.

4. Findings and discussions

4.1 ERM maturity assessment

The risk management practice is not integrated with organizational governance and organizational management. This result is in line with the result of risk management maturity assessment which produces maturity level at the initial stage (i.e., score at 1.96 within 0-5 scale). This value is the result of the respective score aggregation of each six attributes, as seen in Figure 1.

Figure 1. ERM maturity attributes' score and overall ERM level



This value is derived from some supporting evidence collected through document reviews, questionnaires, interviews, and observations as follows:

Attribute 1: Risk management framework	
RMM Score	2.34
Positive indicators and evidence	• There is a directors' regulation number: PD- 23/DU300/07/2017 concerning the implementation of integrated risk management practices. This document demonstrates an explicit responsibility of BOD for the implementation of risk management through the establishment of policies and procedures.

	• There has been an establishment of a "Corporate Governance Monitoring Committee" at the supervisory board level. • Some efforts of the plan-do-check-act (PDCA) cycle in the risk management framework have been documented but ineffective as there is not any evidence about the improvement and enhancement by corporate leaders. In this case, the Risk Management Unit merely conducted the PDCA efforts as part of their internal routine activities.
Shortcomings of the PSO's ERM, its root causes, and implications	• Leadership and commitment from the risk leaders are very minimal as no distinct and regular tone from the top, no structured and systematic risk-based decisions applied, and no monitoring on the follow-up of any evaluation result. • As a result, risk management integration has not been carried out by the risk leaders independently. It is seen in the activities of the PDCA, which the Risk Management Unit dominates more.

Attribute 2: Risk management process	
RMM Score	2.38
Positive indicators and evidence	In this case, the standard operating procedures (SOP) is available for risk owners to carry out the risk management process, which includes: • The main process of risk management to cover the scope, context, criteria, risk assessment stage, risk treatment stage, and monitoring and review stage. • The support process of risk management to cover communication and consultation along with recording and reporting.
Shortcomings of the PSO's ERM, its root causes, and implications	• There is not any operational plan for the risk management process. As a result, an evaluation cannot be conducted as there is not any comparison that can be made between the implementation plan versus the actual implementation. • The risk identification was not based on the mapping of their internal and external context. As a result, there is not any clarity of the risks source and track to identify which risks were related to which context. Therefore, the risk root cause and the related risk control effectiveness are hardly known. • The risk communication and consultation were not carried out in a measured and controlled manner due to the absence of a clear risk management implementation plan. As a result, evaluation and improvement of the ERM process are not possible.

Attribute 3: Management process	
RMM Score	2.50

Positive indicators and evidence	• The strategic and operational plans availability to fulfill their public obligation and assignments which were set out in the regulations that the government makes. • The management contract availability between board of directors with all business unit heads (BUH) based on their respective key performance indicators (KPIs). This showed a strong commitment to excel in their business process and management in general.
Shortcomings of the PSO's ERM, its root causes, and implications	• The objectives are unclear, unmeasurable, and potentially ambiguous as they do not meet SMART (Specific, Measurable, Achievable, and Time-bound) criteria. Since risk is the effect of uncertainty on objectives, no-SMART, and ambiguous objectives will only cause ineffective risk assessment in particular and the whole risk management process in general. • No clear strategies, initiatives, or work programs address risks that might hinder the organization in achieving its mission, goals, and objectives. Their plans do not have any focus on identifying and mitigating the effect of threats on the organization's goals and objectives – both strategic and operational objectives, or neither identifying nor exploiting opportunities to create value.

Attribute 4: Performance management	
RMM Score	2.08
Positive indicators and evidence	• Organizational goals, performance units, and work plans have been clearly articulated before developing a performance plan. • Each performance unit has a KPI that guides the success of achieving organizational goals. • Each KPI has a target value to be used in evaluating performance achievement.
Shortcomings of the PSO's ERM, its root causes, and implications	• All KPIs do not have any leading indicators in the form of key risk indicators (KRI). • There is not any early warning system that could be applied as KRI is not in place. • Consequently, there are not any performance improvements that could be made based on the monitoring of the KRI's dynamics.

Attribute 5: Risk culture	
RMM Score	1.25
Positive indicators and evidence	• The risk appetite framework has been put in place, but it has been determined that the criteria for risk-based decision-making are not optimal. • The Board of Directors Regulation Number: PD-23/DU300/07/2017 concerning the Implementation of

	Integrated Risk Management Practices has established risk governance based on a three-layer defense model.
Shortcomings of the PSO's ERM, its root causes, and implications	• Although there is a very simple risk appetite framework, the elements and criteria are not clear. As a result, such a framework is ineffective to be used as the basis of risk-based decision-making. • There is not any evidence of cultural reinforcement and change management program in place. As a result, the current culture remains the same, which tends to be reactive rather than to become as per their expectation (i.e., to be more anticipatory and proactive toward risks). • Although there is a Board of Directors Regulation Number: PD-23/DU300/07/2017 concerning the Implementation of Integrated Risk Management Practices based on a three-lines-of-defense model, it remains just as a silent document as order parameters are not verified. In this case, there is not much evidence to see how it is being practiced across the organization.

Attribute 6: Resilience and sustainability	
RMM Score	1.20
Positive indicators and evidence	• Financial risks affecting company earnings have been written in a risk register and are managed according to appropriate financial procedures. • Disaster risk has been mentioned in the risk list, followed up with a disaster response plan in the K3 management system by the provisions of the regulation, namely the Government Regulation Number 50 of 2012.
Shortcomings of the PSO's ERM, its root causes, and implications	• Although there are two documents that use nomenclatures of resilience and sustainability in their risk register, they refer to some basic financial risks and a provision defined by Government Regulation Number 50 / 2012 concerning K3. As a result, their efforts are limited to manage the financial risks through financial ratio management and only have a "disaster response plan" that refers to what action needs to be done only if there are fatalities due to accidents at the working place. • There is not any evidence found that says risk management must support the organization's efforts to reduce the environmental risks, and therefore enable them to sustain. As a result, the organization does not have any referential plan in dealing with its potential consequences and costs, especially on how to remain resilient if such consequences lead to a disaster situation. • There is not any evidence found that says risk management must support the organization's efforts to reduce social risks, and therefore enable them to sustain in a longer term. As a result, the organization does not have any referential plan in dealing with

	its potential consequences and costs, especially on how to remain resilient if such consequences lead to a disaster situation. • There is not any evidence found that says risk management must support the organization's efforts to reduce environmental risks and enable them to sustain in the longer term. As a result, the organization does not have any referential plan in dealing with its potential consequences and costs, especially on how to remain resilient if such consequences lead to a disaster situation. • There is not any evidence found that says risk management must support the organization's efforts to reduce risk exposures that potentially affect their critical value chain and business models. As a result, the organization does not have any referential plan in dealing with its potential consequences and costs, especially on how to remain resilient if such consequences lead to a disaster situation.

4.2 Solutions for improving the PSO's ERM maturity

The paper result is used as input to identify which ERM aspects could be strengthened to improve the organization's performance. Those inputs were wrapped into a recommendation list that would help the organization increase the effectiveness of their ERM and forward to the organization's performance, including their resilience and sustainability. Those recommendations are

a. To complete the integration of the ERM process into all organizational processes and activities. The risk leaders should demonstrate their leadership and commitment through the following but not limited to:
   - Adapting and implementing all components of the risk management framework.
   - Ensuring the availability of the right resources both in quality and quantity, in terms of people and currency or financial budget.
   - Building risk management competencies across the organization and continuously updating and leveraging them.
   - Providing necessary facilities and infrastructure such as risk management information system which could provide symmetric information for recording and reporting risks that are efficient, reliable, and safe.
   - Ensuring that each Risk Owner has a high level of concern for risks and drive them to manage those risks according to their authority, responsibility, and accountability.
   - Ensuring the supervision of risk management integration by carrying out regular evaluation of risk management performance and monitoring its follow-up effectively.

b. To strengthen the risk governance based on the three lines model to work effectively and efficiently. As such, the following are recommended but not limited to:
   - Line One: carrying out the Risk Control Self-Assessment (RCSA) competency development program to all risk owners in line one. Upon completing the program,

we may hope that risk owners will have the better capability and bigger capacity to manage risks that may affect their respective business process objectives.

- Line Two: getting four-eyes principles implemented thoroughly and consistently by keeping the Risk Management Unit - as line two is able to support the risk-based business processes effectiveness conducted by risk owners in line one. In so doing, it requires competency development for all members of the Risk Management Unit to obtain a certain level of risk management professional qualification.
- Line three: Implementing regular management reviews by the Board of Directors and the Board of Commissioners to evaluate the performance of integrated risk management conducted by line one and line two, respectively. The review is supported by the Internal Auditor and Governance Monitoring Committee who must obtain a certain competency level to be competent and work according to schedule.

c. To develop early warning systems based on KRI as leading indicators towards the accomplishment of KPI. Upon having KRI in place, we may hope that obstacles in accomplishing KPI could be detected earlier. Hence, the probability of successful performance is increased.

d. To adopt a risk-based sustainability approach, henceforth with the implementation of a relevant management system for its consistency and effectiveness. As such, it is recommended that the organization adopt and implement ISO 22301 Standard - Business Continuity Management System.

e. To strengthen risk culture that fosters people in the organization to manage the downside risk (i.e., protect value) and up-side risk (i.e., creating value). It may include but not limited to:
   - Enforcing risk appetite framework-based decision making,
   - Adopting recruitment, placement, and promotion arrangements that require risk management expertise,
   - Setting reasonable rewards and penalties for risk management achievements, etc.
   - Creating critical masks across the organization through massive risk management competency development programs across the organization and at all levels.
   - Getting risk management process as a routine scheduled of corporate culture rite and ritual.

5. Conclusion

This study concludes that the higher effectiveness of ERM as embodied in a higher maturity level could be expected to improve the organization's performance and efficacy. A higher ERM maturity level means a higher capacity and capability to increase the probability of an organization accomplishing the organization's goals and objectives, i.e., better performance than otherwise. Further, this study also shows how the current practices of ERM in a large PSO are conducted, and how a road map is built and proposed to increase their ERM maturity level. As such, the road map does not only recognize the issues and challenges that may face organization to increase their ERM maturity level from their current base of 1.96 to 4.00 within four years, but it also provides some recommendations steps which could be used as empirical

insights into how ERM is implemented as a pathway in enhancing the organization's performance and efficacy. Hopefully, such empirical insights would enrich academic literature and become valuable lessons to learn for risk management practitioners and/or enthusiasts.

Despite some useful deep understandings and insights about how ERM is being practiced in a large PSO, and about how risk management maturity is being conducted, this paper has limitations in the sense of generality and comparability with other PSOs in general. Therefore, it is strongly recommended to conduct further research through a similar case study approach in some other PSO organizations either in the same country or in different countries.

References

Ahmeti, R., & Vladi, B. (2017). Risk management in public sector: A literature review. *European Journal of Multidisciplinary Studies*, *2*(5), 323–329. https://doi.org/10.26417/ejms.v5i1.p323-329

Almeida, R., Teixeira, J. M., Mira da Silva, M., & Faroleiro, P. (2019). A conceptual model for enterprise risk management. *Journal of Enterprise Information Management*, *32*(5), 843–868. https://doi.org/10.1108/JEIM-05-2018-0097

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society*, *35*(7), 659–675. https://doi.org/10.1016/j.aos.2010.07.003

Asenova, D., Bailey, S. J., & McCann, C. (2015). Public sector risk managers and spending cuts: mitigating risks. *Journal of Risk Research*, *18*(5), 552–565. https://doi.org/10.1080/13669877.2014.910683

Beasley, M. S., Clune, R., & Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy*, *24*(6), 521–531. https://doi.org/10.1016/j.jaccpubpol.2005.10.001

Bohnert, A., Gatzert, N., Hoyt, R. E., & Lechner, P. (2017). The relationship between enterprise risk management, value and firm characteristics based on the literature. *Zeitschrift Für Die Gesamte Versicherungswissenschaft*, *106*(3), 311–324. https://doi.org/10.1007/s12297-017-0382-1

Braig, S., Gebre, B., & Sellgren, A. (2011). *Strengthening risk management in the US public sector* (McKinsey Working Papers on Risk Number 28). https://www.mckinsey.com/business-functions/risk/our-insights/strengthening-risk-management-in-the-us-public-sector

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long Range Planning*, *48*(4), 265–276. https://doi.org/10.1016/j.lrp.2014.07.005

Carlsson-Wall, M., Kraus, K., Meidell, A., & Tran, P. (2019). Managing risk in the public sector – The interaction between vernacular and formal risk management systems.

Financial Accountability & Management, *35*(1), 3–19. https://doi.org/10.1111/faam.12179

Chapman, R. J. (2011). *Simple tools and techniques for enterprise risk management* (2nd ed.). John Wiley & Sons. https://doi.org/10.1002/9781118467206

Chapman, R. J. (2019). Exploring the value of risk management for projects: Improving capability through the deployment of a maturity model. *IEEE Engineering Management Review*, *47*(1), 126–143. https://doi.org/10.1109/EMR.2019.2891494

Choo, B. S.-Y., & Goh, J. C.-L. (2015). Pragmatic adaptation of the ISO 31000:2009 enterprise risk management framework in a high-tech organization using Six Sigma. *International Journal of Accounting & Information Management*, *23*(4), 364–382. https://doi.org/10.1108/IJAIM-12-2014-0079

Collier, P. M., & Woods, M. (2011). A comparison of the local authority adoption of risk management in England and Australia. *Australian Accounting Review*, *21*(2), 111–123. https://doi.org/10.1111/j.1835-2561.2011.00126.x

Dali, A., & Lajtha, C. (2012). ISO 31000 Risk Management — "The Gold Standard." *EDPACS*, *45*(5), 1–8. https://doi.org/10.1080/07366981.2012.682494

Enterprise Risk Management Academy (2020). *ISO 31000 Risk Management Maturity Model.* Singapore: Enterprise Risk Management Academy.

Farrell, M., & Gallagher, R. (2015). The valuation implications of enterprise risk management maturity. *Journal of Risk and Insurance*, *82*(3), 625–657. https://doi.org/10.1111/jori.12035

Fiksel, J., Polyviou, M., Croxton, K. L., & Pettit, T. J. (2015). From risk to resilience: Learning to deal with disruption. *MIT Sloan Management Review*, *56*(2), 79–86. http://mitsmr.com/1uOW55d

Florio, C., & Leoni, G. (2017). Enterprise risk management and firm performance: The Italian case. *The British Accounting Review*, *49*(1), 56–74. https://doi.org/10.1016/j.bar.2016.08.003

Fraser, J. R. S., & Simkins, B. J. (2016). The challenges of and solutions for implementing enterprise risk management. *Business Horizons*, *59*(6), 689–698. https://doi.org/10.1016/j.bushor.2016.06.007

Gordon, L. A., Loeb, M. P., & Tseng, C.-Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy*, *28*(4), 301–327. https://doi.org/10.1016/j.jaccpubpol.2009.06.006

Grace, M. F., Leverty, J. T., Phillips, R. D., & Shimpi, P. (2015). The value of investing in enterprise risk management. *Journal of Risk and Insurance*, *82*(2), 289–316. https://doi.org/10.1111/jori.12022

Hardy, K. (2010). *Managing risk in government: An introduction to enterprise risk management*. IBM Center for The Business of Government. http://www.businessofgovernment.org/report/managing-risk-government-introduction-enterprise-risk-management

Hillson, D. A. (1997). Towards a risk maturity model. *International Journal of Project and Business Risk Management*, *1*(1), 35–45.

Hood, C., & Miller, P. (2009). Public service risks: What's distinctive and new? In *Risk and Public Services* (pp. 2–3). The London School of Economics and Political Science. https: //www.lse.ac.uk/accounting/assets/CARR/documents/S-R/RiskAndPublicServices.pdf

Hoyt, R. E., & Liebenberg, A. P. (2011). The value of enterprise risk management. *Journal of Risk and Insurance*, *78*(4), 795–822. https://doi.org/10.1111/j.1539-6975.2011.01413.x

Indonesian Ministry of Finance. (2016). *Penerapan manajemen risiko di lingkungan kementerian keuangan*. Indonesian Ministry of Finance. https://jdih.kemenkeu.go.id /fulltext/2016/12~PMK.09~2016Per.pdf

International Organization for Standardization. (2009). *Risk management - Principles and guidelines* (ISO 31000:2009). International Organization for Standardization. https://www .iso.org/standard/43170.html

International Organization for Standardization. (2018). *Risk management - Guidelines* (ISO 31000:2018). International Organization for Standardization. https://www.iso.org /standard/65694.html

Kim, E. (2014). How did enterprise risk management first appear in the Korean public sector? *Journal of Risk Research*, *17*(2), 263–279. https://doi.org/10.1080/13669877.2013 .808685

Lapsley, I. (2009). New public management: The cruellest invention of the human spirit? *Abacus*, *45*(1), 1–21. https://doi.org/10.1111/j.1467-6281.2009.00275.x

Leitch, M. (2010). ISO 31000:2009 - The new international standard on risk management. *Risk Analysis*, *30*(6), 887–892. https://doi.org/10.1111/j.1539-6924.2010.01397.x

Leung, F., & Isaacs, F. (2008). Risk management in public sector research: approach and lessons learned at a national research organization. *R&D Management*, *38*(5), 510–519. https://doi.org/10.1111/j.1467-9310.2008.00529.x

Lindberg, D. L., & Seifert, D. L. (2011). Enterprise risk management (ERM) can assist insurers in complying with the Dodd-Frank Act. *Journal of Insurance Regulation*, *30*(13), 319–337.

Macgillivray, B. H., Sharp, J. V., Strutt, J. E., Hamilton, P. D., & Pollard, S. J. T. (2007). Benchmarking risk management within the international water utility sector. Part I: Design of a capability maturity methodology. *Journal of Risk Research*, *10*(1), 85–104. https: //doi.org/10.1080/13669870601011183

Mahama, H., Elbashir, M., Sutton, S., & Arnold, V. (2020). New development: Enabling enterprise risk management maturity in public sector organizations. *Public Money & Management*, 1–5. https://doi.org/10.1080/09540962.2020.1769314

Nocco, B. W., & Stulz, R. M. (2006). Enterprise risk management: Theory and practice. *Journal of Applied Corporate Finance*, *18*(4), 8–20. https://doi.org/10.1111/j.1745-6622.2006

.00106.x

Organisation for Economic Co-operation and Development. (2021). Enterprise risk management maturity model. *OECD Tax Administration Maturity Model Series*. http: //www.oecd.org/tax/forum-on-tax-administration/publications-and-products/enterprise-risk-management-maturity-model.htm

Palermo, T. (2014). Accountability and expertise in public sector risk management: A case study. *Financial Accountability & Management*, *30*(3), 322–341. https://doi.org/10.1111 /faam.12039

Power, M. (2004). The risk management of everything. *The Journal of Risk Finance*, *5*(3), 58–65. https://doi.org/10.1108/eb023001

Purdy, G. (2010). ISO 31000:2009 - Setting a new standard for risk management. *Risk Analysis*, *30*(6), 881–886. https://doi.org/10.1111/j.1539-6924.2010.01442.x

Software Engineering Institute. (2010). *CMMI for development, version 1.3*. https://doi.org/10 .1184/R1/6572342.v1

Spikin, I. C. (2013). Risk Management theory: The integrated perspective and its application in the public sector. *Estado, Gobierno y Gestión Pública*, *21*, 88–126. https://boletincorteidh .uchile.cl/index.php/REGP/article/view/29402/31180

Woods, M. (2009). A contingency theory perspective on the risk management control system within Birmingham city council. *Management Accounting Research*, *20*(1), 69–81. https: //doi.org/10.1016/j.mar.2008.10.003