

A Study on the Maturity of Risk Management using the RIMS Risk Maturity Model[®] Approach in Investigating Activities at Law Enforcement Agencies for Corruption

Dedy Simanungkalit¹, Agustinus Nicholas L. Tobing²

^{1,2}Faculty of Economics and Business, Universitas Indonesia
dedy.simanungkalit@gmail.com, augie.nicholas@gmail.com

Abstract

This study aims to analyze how to use the RIMS risk maturity model to evaluate the implementation of risk management in a law enforcement agency in Indonesia in investigating corruption and the gap between the existing implementation and the ideal conditions as suggested in the RIMS Risk Maturity Model. This descriptive qualitative research with a case study approach obtained data from external sources of the organization in the form of literature data and internal sources of the organization in direct observations, document analysis, and interviews with related parties within the organization. This research provides a tool for organizations, particularly organizations similar to the object of this research, to assess how to implement risk management processes by following general best practices. The maturity assessment results show that the risk management maturity level in the XYZ agency is in the Tier-2 position, and there is still a large gap between the current condition and the target maturity level. The XYZ agency should immediately start integrating risk management into all business processes and performance management to improve its risk management maturity level.

Keywords

law enforcement, RIMS risk maturity model, public sector



I. Introduction

To carry out the investigation process of a corruption case, investigators have the main task of finding and collecting evidence, which with this evidence can make light of the crime that occurred and locate the suspect. Investigators will carry out a series of investigative activities based on the criminal procedure law and Law Number 31 of 1999 concerning the Eradication of Criminal Acts of Corruption as amended by Law Number 20 of 2001 (Anti-Corruption Law).

As one of the law enforcement agencies formed by the government of the Republic of Indonesia to carry out the main task of preventing and prosecuting corruption, many people believe that the XYZ Agency has various high risks. Call it starting from legal, operational, fraud, and reputation to the risk of physical threats. There are many incidents where the perpetrators of corruption counter-attacks became known as the 'corruptor-fightback' by using various strategies and methods to be free from accusations of corruption (Muttaqin & Susanto, 2018). These risks can undoubtedly be fatal if not managed appropriately, both for individual investigators and the XYZ agency institutionally. Over time, these counter-attacks became more and more varied and began to touch the individual.

In theory, an inadequate risk management process in an organization can indicate that internal controls are still weak in the organization. The more mature the risk management process and framework within an organization, the greater confidence can be

placed in risk assessment by management itself. In the three lines of defense concept, risk control carried out by the organization must include the Risk Owner and the Process Owner, Risk Manager, and Supervisor or Assurance Provider (Alijoyo, 2017).

In this regard, the XYZ Agency already has Principal Regulation Number 9 of 2019 concerning Risk Management Guidelines, which contains policies, guidelines, and risk management procedures and serves as a guide in carrying out risk management for all risk owners. This guideline also stipulates that one of the risk management organs in XYZ agency is the evaluator, the Inspectorate. The evaluator is said to have the following duties: a) carry out risk management supervision; b) evaluate the implementation of the risk management cycle in the work unit; c) provide input on the development and improvement of risk management implementation; d) monitor and review MR reports, and e) assess the maturity level of risk management implementation.

It then motivates the author to examine how the maturity level of risk management implementation in the investigation activities at the XYZ agency. The author finds no research in Indonesia on risk management maturity in law enforcement agencies for corruption using the RIMS Risk Maturity Model. So the results of this study are expected to add to the academic literature on risk management evaluation research, especially with the RIMS RMM approach.

II. Review of Literature

2.1 Risk Management

In particular, the glossary of International Standards for the Professional Practice of Internal Auditing (Standards) defines risk management as a process of identifying, assessing, managing, and controlling the likelihood of an event or situation to provide confidence in the achievement of organizational goals (The Institute of Internal Auditor, 2017). Every organization has the potential to have risks, but an organization that is too conservative to take risks will increase the likelihood of not achieving the organization's strategic goals. On the other hand, organizations that are too progressive towards risk can also cause a crisis danger for the organization. Therefore, with risk management, the expected result is a balance between achieving optimum strategic goals and the risks taken by the organization.

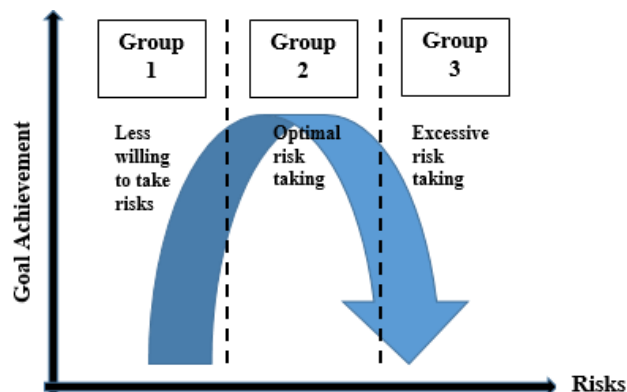


Figure 1. Risk Relationship with Goal Achievement

2.2 Risk Definition

The Big Dictionary of Indonesian (KBBI) defines risk as: "an unpleasant (detrimental, harmful) effect of an act or actions." This context defines risk as something unfavorable. Nevertheless, according to Hopkin (2018), risk can also produce positive

results. ISO 31000:2018 defines risk as "*the effect of uncertainty on achieving a goal*" (Vorst, Priyarsono, & Budiman, 2018). This definition has three keywords: effect, uncertainty, and target. **The effect** is a deviation or deviation of an achievement, which can occur positively or negatively and can be both an opportunity and a threat. **Uncertainty** is a condition of doubt formed due to a lack of information related to how big the impact and possibility of the current decision or action on achieving the goals (Munawar & Aini, 2020). **Targets/Objectives** are plans to be completed.

2.3 Risk Types and Classification

Based on their nature, according to Paul Hopkin (2018), types of risk can be divided into four categories with each explanation as follows: (1) **Pure risks/hazard risks**, namely pure risks that can only produce adverse or harmful impacts and undermine the goals of the organization; (2) **Uncertainty risks/control risks** or uncertain risks; (3) **Opportunity risks/speculative risks**, which are types of risks that are often taken intentionally by organizations in the hope of providing positive returns and increasing (although they can also hinder) opportunities for profit (Hopkin, 2018); and (4) **Compliance risks/mandatory risks**, namely risks related to possible violations of laws and regulations, contract requirements, standards, or internal policies that may result in an organization having to bear a consequence such as direct or indirect financial obligations, civil or criminal penalties, regulatory sanctions or other impacts (SCCE & HACCA, 2020).

Based on the period, Paul Hopkin (2018) also classifies risk into three types: (1) **Short-term risk**, namely risk that can affect the goals and core processes of the organization with a direct impact; (2) **Medium-term risks**, i.e., risks that could affect the organization's ability to effectively and efficiently maintain its core processes related to the management of tactics, projects, and other change programs after a brief delay following the occurrence of an event; and (3) **Long-term risk**, i.e., the risk that can affect the organization sometime after the occurrence of an event.

2.4 Risk Culture, Risk Appetite, and Risk Tolerance

Risk culture is a norm or behavior that every individual and group owns in an organization that will determine the organization's ability to identify and understand, be open to discussing, and act on risks, both current and future (Levy, Lamarre, & Twining, 2010). Organization must have a goal to be achieved by the organizational members (Niati et al., 2021). Risk appetite is an event/action taken, received, monitored, maintained, or maximized to achieve organizational goals. Meanwhile, risk tolerance is how big the amount the organization experience a negative impact in achieving its strategic goals.

2.5 Risk Management Standards

In simple terms, risk management standards contain a description of the risk management process and the framework recommended by each standard to support the success of the process. Some of the most widely used standards by organizations, in general, include ISO 31000 *Risk Management-Principles and Guidelines* (2009 and 2018), COSO ERM (2004 and 2017), AS/NZS 4360 Standard (2009), and *Framework for the Management of Risk Canada* (2010). In Indonesia, the most commonly used standards are ISO 31000 and COSO ERM, even the National Standardization Agency (BSN) has fully adopted ISO 31000 by issuing "SNI ISO 31000:2011 Risk Management – Principles and Guidelines" on October 20, 2011 (Suharso, 2016).

2.6 The Maturity of Risk Management

In an organizational context, maturity can be defined as *"the degree to which an organization implements processes that are explicitly and consistently documented, managed, measured, controlled, and continuously improved that can be measured through assessment"* (Proenca, Estevens, Vieira, & Borbinha, 2017). Meanwhile, in the context of risk management, risk maturity is defined as *"a series of steps in evaluating and assessing the main characteristics of the risk management framework, compared with best practices to determine whether the risk management framework adopted and planned by the organization has been complied with"* (Coetzee & Lubbe, 2013).

There are many risk maturity models designed and published by various international organizations in the field of risk management today, some of which are widely adopted by organizations globally, including (1) Chartered Global Management Accountant/CGMA; (2) The Deloitte Risk Intelligent Enterprises Maturity Model; (3) Aon Risk Maturity Index; (4) The Investor in Risk Management Maturity Model; (5) Capability Maturity Model Integration/CMMI; (6) The IACCM Business Risk Management Maturity Model/BRM3; (7) RIMS Risk Maturity Model; and so on.

2.7 RIMS Risk Maturity Model®

In 2022 The Risk Management Society released the latest version of the RIMS Risk Maturity Model®. This version redefines the elements (pillars) and characteristics (attributes) that are most important for every organization to achieve the desired risk management maturity level. Five pillars have varying weights based on the experience of practitioners to replace the seven attributes in the previous model (The Risk Management Society, 2022). Each pillar consists of several attributes totaling 35 attributes (replacing 25 components in the previous version), which are as follows:

Table 1. Pillars and Attributes RIMS RMM 2022

Description of Pillars	No	Attributes
Pillar 1: Strategy Alignment (25%)		
Degree that decisions integrate risk of the strategy itself, those resulting from the strategy, and threats to the strategy. The extent to which leaders understand the connection and act on potential consequences of identified risks with the organization's strategy.	1	Process for integrating risk with decision making
	2	The extent of forward-looking considerations
	3	The extent of risk evaluation for strategic initiatives or investment
	4	Consistency of risk appetite (risk and reward) and tolerance (acceptance of uncertainty or loss used in decision making
	5	View of enterprise risk management capabilities within an organization
	6	Risk considerations of and to the business model
Pillar 2: Culture and Accountability (30%)		
Risk considerations are pervasive from the governing body to the front-line personnel. Risk owners understand and take action commensurate with their responsibility. Risk competencies are evident throughout the organization. The risk	1	The extent that results of risk assessments directly affect changes in initiatives, projects, or strategy
	2	The extent of the direct contribution of employees and other stakeholders in the collection of risk information
	3	The degree to which risk considerations influence leadership
	4	Demonstration of risk culture oversight and accountability
	5	The connection between performance evaluation and managing risk
	6	Demonstration of leadership's understanding and

Description of Pillars	No	Attributes
management discipline reflects its stated cultural and ethical values/principles.		accountability for managing top known risks
	7	The extent to which leaders actively participate in enterprise or organization-wide risk assessments
Pillar 3: Manage Organizational Risk Capabilities (20%)		
The degree of organizational and individual learning and development concerning managing risk, alignment, integration, and engagement with the stakeholders.	1	Considerations in evaluating risk treatments
	2	Level of analytical capabilities of organization and individuals in assessing risk
	3	Level of technical competencies of the organization's risk management leaders
	4	Assessment of emerging risks
	5	The span of developing and sharing risk information
	6	The extent of and criteria used in conducting enterprise risk assessments
	7	How the organization's risk profile understood
Pillar 4: Risk Governance (13%)		
The degree to the risk management discipline influences and interacts within an organizational risk ecosystem. Organization's ability to apply its governance and risk management principles for accountability in managing risk in creating and protecting value, including assessment, execution, and process improvement.	1	The extent that organizational oversight responsibilities for risk management are established at the board or governing body level
	2	The extent is the commitment and appreciation of senior-level leadership to fostering value from risk management
	3	The degree that the risk data process informs long term spending plans/decisions by leadership
	4	Development of a risk management function or framework
	5	Development of risk management policies or statements
	6	The extent to that established operational or specialized (e.g., legal, insurance, safety) risk functions align with enterprise risk management function or framework
	7	Use of risk appetite considerations (e.g., risk-return tradeoffs)
Pillar 5: Technology and Analytics (12%)		
The degree to which an organization uses technology and analytics to establish, collaborate, gain insight, and maintain connections with stakeholders. The extent to which an organization uses varied and innovative techniques to report insights, monitor actions, and escalate to the appropriate management level.	1	Consistency of qualitative and quantitative analyses
	2	To what extent are data and analytics utilized to inform risk decisions
	3	To what extent are insights extracted from external sources and expertise used to complement internal assessment data
	4	How does the organization believe that it has considered the effect of bias in its risk assessment
	5	To what extent does the organization use a combination of methodologies or techniques to identify and assess risks?
	6	The thoroughness of assessing sources or causes of risk
	7	Availability of risk data to decision-makers
	8	Depth and integration of risk reporting and communication within the organization

There are five levels ranging from Tier-1 to Tier-5 to show the position of the risk management program in the organization. A holistic explanation of each tier is as follows:

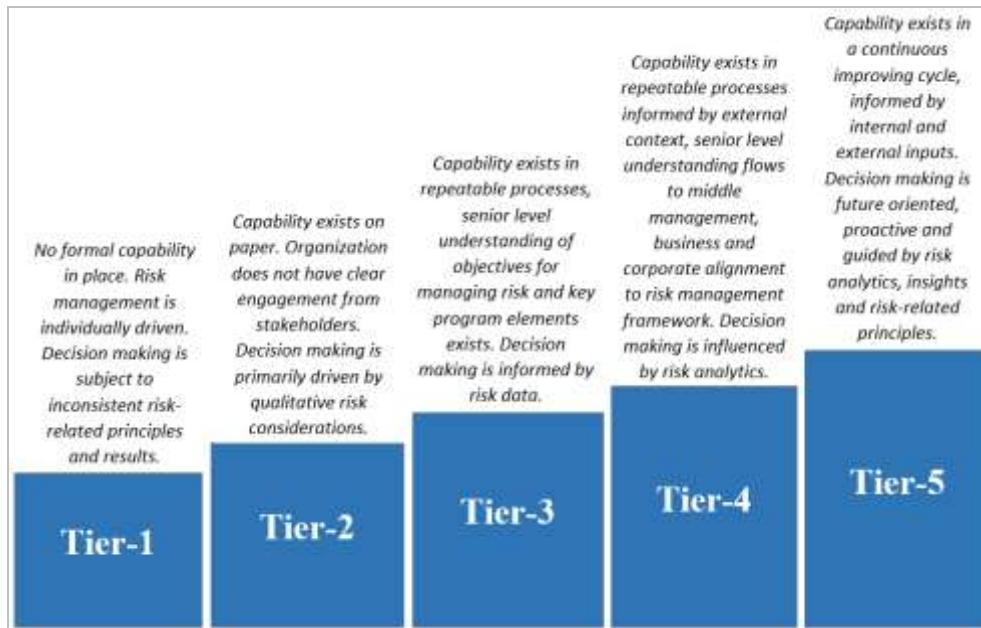


Figure 2. Tiers of RIMS RMM

2.8 Previous Research

Based on a literature search, the author found that previous studies on the maturity of organizational risk management using the RIMS RMM model were still little done. Indeed, several studies examine the maturity of risk management in organizations in the public and private sectors that use the RIMS RMM model. Still, the authors have not found any research on risk management maturity in law enforcement agencies, especially in corruption, which uses the RIMS RMM®. The following are several previous studies related to risk management maturity, ERM, and corruption:

Table 2. Previous Research on Risk Management

No	Researcher Name and Research Year	Research Results	Similarities/Differences
1	Coetzee, Lubbe (2013) <u>Title:</u> <i>The risk maturity of South African private and public sector organizations</i>	The risk maturity of the participating organizations was assessed based on an adapted risk maturity score for organizations in South Africa. The results showed that the private sector organizations that were sampled on average already had risk management maturity. In contrast, none of the public sector organizations tested had RM maturity.	Similarities: <ul style="list-style-type: none"> - Assess the maturity level of the organization's risk management - Use RIMS RMM in measuring maturity. - The object of research includes organizations in the public sector Differences: Do not use law enforcement agencies as the object of research.

No	Researcher Name and Research Year	Research Results	Similarities/Differences
2	Farrell, Gallagher (2014) <u>Title:</u> <i>The Valuation Implications of Enterprise Risk Management Maturity</i>	This study indicates that companies that have been fully involved and are considered mature in the ERM approach have a significant increase in company value of around 25 percent.	<u>Similarities:</u> <ul style="list-style-type: none"> - Assess the maturity level of the organization's risk management. - Use RIMS RMM data as a reference for research analysis. <u>Differences:</u> The research object does not cover the public sector, especially law enforcement agencies in corruption.
3	Sumi, Lalicic (2015) <u>Title:</u> <i>Risk Analysis of Corruption Within Law Enforcement</i>	Improvement of employment procedures (recruitment) and promotion (career development), mentoring, training and education on ethics and integrity, and exemplary will positively impact the professionalism of Law Enforcement Officials.	<u>Similarities:</u> <ul style="list-style-type: none"> - Use the public sector as the research object - Review the analysis of the risk of fraud-corruption, which occurs in law enforcement agencies, especially the police. <u>Differences:</u> <ul style="list-style-type: none"> - Not reviewing the maturity of risk management and RIMS RMM - The specific type of risk studied is only corruption; there are no other types of risk.
4	Muttaqin, Susanto (2018) <u>Title:</u> <i>Mengkaji Serangan Balik Koruptor Terhadap KPK dan Strategi Menghadapinya</i>	The counter-attack of corruptors is real, whose emergence is still very likely to occur. The methods are very creative in carrying out the fightback against the KPK. The results of this study indicate that the KPK has not been able to keep up with the incessant counter-attacks it faces.	<u>Similarities:</u> The object and subject of the research are the same, namely the risk of handling cases in law enforcement agencies in corruption. <u>Differences:</u> Research subjects do not cover risk management and organizational risk management maturity.

III. Research Method

The research method used in this research is descriptive qualitative research with a single case (embedded) design case study approach. The data collection method used in this research is semi-structured interviews with parties directly involved in the risk management process at XYZ Agency, including (1) Head of the Center for Strategic Planning for Corruption Eradication; (2) Head of Performance and Risk Management Division; and (3) Specialist in Youth Corruption Eradication Strategic Planning. To strengthen the validity of the analysis and conclusion, the author also conducted a semi-structured interview with one of the Heads of the Audit Team at the XYZ agency Inspectorate.

In addition to the interview method, the author also makes direct observations and analyzes the documents collected during the study. The types of data used are: (a) primary data obtained directly from officials and employees who are directly involved and have a good understanding of the risk management process and the investigation process at the XYZ agency; (b) secondary data obtained from the results of literature studies and other sources such as books, journals, laws and regulations, and others. To ensure the validity of the research content and the objectivity of the opinions expressed by the parties involved, the authors use several criteria stated by Sari Wahyuni (2015). The criteria include (1) internal validity in the form of source triangulation, member checking, peer debriefing, and prolonged engagement; (2) external validity; and (3) reliability, namely through a case study protocol that includes the core questions of each observed variable.

IV. Results and Discussion

4.1 Implementation of Risk Management in XYZ Agency

The XYZ agency is one of the state institutions in the executive power clump in Indonesia, which is independent and free from the influence of any power in carrying out its duties and authorities, namely the prevention and prosecution of criminal acts of corruption. The XYZ agencies have initiated the risk management since 2012, namely with the issuance of Principle Regulation (Perpim) number 6 of 2012 concerning the Implementation of the Internal Control System in the XYZ Environment (SPIK). In 2019, Regulation number 9 of 2019 was issued on November 28, 2019, concerning Guidelines for Risk Management at XYZ Agencies which later became the legal basis for implementing risk management at XYZ agencies. In general, the Regulation contains several main matters: (a) determination of risk management organs and the duties of each organ; (b) determining the scope, context, and risk criteria; (c) risk assessment which includes risk identification, risk analysis, and risk evaluation; (d) risk management; (e) monitoring and review; and (f) recording and reporting.

Based on Perpim number 9 of 2019, the risk management organs in the XYZ agency consist of: **(1) Leaders; (2) Supervisory Board; (3) The Risk Management Committee; (4) Unit in charge of Risk Management**, in this case, PPSPK; **(5) Risk Owners**; and **(6) The Evaluator**, in this case, is the Inspectorate. There is another role related to risk management but not included in the above risk management organs, namely the Risk Management Agent (formerly Risk Champion), an employee appointed annually by the Risk Owner in each work unit to support the implementation of risk management activities and formally determined through the Decree of the Secretary-General of the XYZ Agency.

4.2 Assessment Method

In calculating the maturity level, the author uses the average rating method with the following details:

- a. The first step is to assess each attribute in each pillar according to the selected tier. For example, if attribute A is considered suitable as tier-3, we will give a score of 3. If we consider attribute B qualified as tier-1, we will give a score of 1.
- b. After completing the assessment of the attributes, the next step is to find the score for each pillar by averaging the attribute values in each pillar and then positioning them to each tier. For example, if the average score for the *Strategy Alignment* pillar is 1.9, then this pillar will be positioned at *tier-1*.
- c. The next step is to multiply the average score by the weighted score of each pillar. Then add up the weighting results of each pillar to get the total score of all pillars.

- d. Then use the total score as a reference in positioning which tier is the maturity level of risk management in the XYZ organization.

Table 3 Value Range of Each Tier

<i>Tiering</i>	<i>Value Range</i>
Tier-1	$1,0 \leq \text{Score} < 2,0$
Tier-2	$2,0 \leq \text{Score} < 3,0$
Tier-3	$3,0 \leq \text{Score} < 4,0$
Tier-4	$4,0 \leq \text{Score} < 4,5$
Tier-5	$\text{Score} \geq 4,5$

4.3 Risk Management Maturity Assessment



Figure 3. Assessment Result Score

Based on the assessment results, XYZ agency's overall risk management maturity level gets a total score of **2.32** and is in the Tier-2 position. The lowest score and the only pillar in the Tier-1 category is the *Culture and Accountability* pillar, with a score of 1,43. The *Culture & Accountability* pillar is the pillar that has the most significant weight, which is 30%. Without this pillar, the effectiveness of risk management can be minimal. With a more substantial risk awareness culture and maintained accountability, organizational performance can improve further.

Meanwhile, based on field observations and interviews with several informants, the corporate culture at XYZ agency still shows low-risk management accountability. Some work units still consider risk management to meet compliance only. Even though there has been an assignment as a Risk Management Agent (*Risk Officer/Risk Champion*) in each work unit, in its implementation, it is only in compliance with filling out and updating the risk list. In fact, from observations, it is still found that there are work units that have not consistently carried out these obligations. The following are the details of the results of the maturity level assessment of risk management at the XYZ agency:

No	Attributes	Questions	Score
Pillar I: Strategy Alignment			
1	How is risk considered in strategic decision-making	How is risk considered in strategic decision-making?	3

No	Attributes	Questions	Score
2	The extent of forward-looking considerations	How forward-looking is the risk management horizon?	2
3	The extent of risk evaluation for strategic initiatives or investment	How are the risks for a strategic initiative or investment (e.g., major acquisition, new product, new geography) evaluated?	2
4	Consistency of risk appetite (risk and reward) and tolerance (acceptance of uncertainty or loss used in decision making	How consistently are risk appetite (risk/reward) and tolerance (acceptance of uncertainty/loss) expectations used to guide decision making?	3
5	View of enterprise risk management capabilities within an organization	To what extent does the organization view its risk management capabilities?	2
6	Risk considerations of and to the business model.	Describe how the organization considers risk (e.g., new competitive entrants, technology disruptors, unique advantages) to its business model (products, services, target market, distribution channels, resources, and expenses)?	2
Average score of Strategy Alignment Pillar			2,33
Weighted Score (25%)			0,58
Pillar II: Culture and Accountability			
1	The extent to that results of risk assessments directly affect changes in initiatives, projects, or strategies.	To what extent do risk assessment data/output results directly affect initiatives, projects, or strategy changes?	2
2	How the contribution of employees and stakeholders in gathering information about risks.	To what extent do employees and other stakeholders contribute directly to collecting risk information?	2
3	The degree to which risk considerations influence leadership.	To what extent do risk considerations influence leadership?	2
4	Demonstration of risk culture oversight and accountability	How are risk culture oversight and accountability demonstrated in the organization?	2
5	The connection between performance evaluation and managing risk	What type of connection exists between performance evaluation and managing risk?	2
6	Demonstration of leadership's understanding and accountability for managing top known risks	How well do leaders within the organization demonstrate understanding and accountability for managing the top risks in the enterprise?	2
7	The extent to which leaders actively participate in enterprise or organization-wide risk assessments	How actively do leaders participate in enterprise or organization-wide risk assessments	2
The average score of Culture & Accountability Pillar			2,00
Weighted score (35%)			0,70
Pillar III: Manage Organizational Risk Capabilities			
1	Considerations in evaluating risk treatments	How are risk treatments evaluated?	2
2	Level of analytical capabilities of organization and individuals in assessing risk	What is the level of analytical capabilities of organizations and individuals in assessing risk?	2
3	Level of technical competencies of the	What are the technical competencies of the	2

No	Attributes	Questions	Score
	organization's risk management leaders	organization's risk management leader(s)?	
4	Assessment of emerging risks	To what extent does the organization assess emerging risks?	2
5	The span of developing and sharing risk information	How is information about risks developed and shared in the organization?	3
6	The extent of and criteria used in conducting enterprise risk assessments	To what extent and criteria does the organization use to conduct enterprise risk assessments?	3
7	Understanding of organization's risk profile	How well is the organization's risk profile understood?	2
Average score of Manage Organizational Risk Capabilities Pillar			2,29
Weighted Score (20%)			0,46
Pillar IV: Risk Governance			
1	The extent that organizational oversight responsibilities for risk management are established at the board or governing body level	To what extent have organizational oversight responsibilities for risk management been established at the board or governing body level?	3
2	The extent to which senior-level leadership is committed, incented, and rewarded for fostering value from risk management	To what extent is senior-level leadership committed, incented, and rewarded for fostering value from risk management?	2
3	The degree to the risk data process informs leadership's long-term spending plans/decisions.	How is risk data used to inform leadership's long-term spending plans/decisions?	1
4	Development of a risk management function or framework	Has the organization developed an enterprise risk management function or framework?	2
5	Development of risk management policies or statements	To what extent have risk management statements or policies been established?	4
6	The extent to which established operational or specialized (e.g., legal, insurance, safety) risk functions align with enterprise risk management function or framework	To what extent are operational or specialized (e.g., legal, insurance, safety) risk functions aligned with enterprise risk management function or framework?	2
7	Use of risk appetite considerations (e.g., risk return tradeoffs)	How does your organization address risk appetite (e.g., risk return tradeoffs)	2
Average score of Risk Governance Pillar			2,29
Weighted Score (13%)			0,30
Pillar V: Technology & Analytics			
1	Consistency of qualitative and quantitative analyses	How consistently does the organization apply qualitative and quantitative analysis?	2
2	The extent to which data and analytics are utilized to inform decisions about risk	To what extent are data and analytics utilized to inform risk decisions?	2
3	The extent that insights extracted from external sources and expertise used to complement internal assessment data	To what extent are insights extracted from external sources and expertise used to complement internal assessment data?	4
4	Organizational confidence level regarding the effect of bias in risk assessment	How does the organization believe it has considered the effect of bias in its risk assessment?	2

No	Attributes	Questions	Score
5	The extent of varying methodologies or techniques used to identify and assess risks	To what extent does the organization use a combination of methodologies or techniques to identify and assess risks?	3
6	The thoroughness of assessing sources or causes of risk	How thoroughly does the organization assess sources or causes of risk?	2
7	Availability of risk data to decision-makers	How available is risk data to decision-makers?	2
8	Depth and integration of risk reporting and communication within the organization	How is risk reported or communicated within the organization?	2
Average score of Technology & Analytics Pillar			2,38
Weighted Score (12%)			0,29
Total Weighted Score (1 -5)			2,32
Tier Classification			Tier-2

Current condition:

There is no formal process for integrating risk into decision-making. The XYZ agency still uses the experience of past losses as the primary basis for measuring current risk exposure. The XYZ agency has not considered the risks of strategic initiatives or investments. Risk appetite and risk tolerance are not used or do not exist. Most of the leaders in XYZ Agency do not have the ability related to risk management, and some even consider it a negative thing. Most leaders do not consider business model risks in organizations.

Report the assessment results to the initiative, project, or strategy owners but generally do not affect change. Contributions to the collection of risk information are limited to risk-related functions. Risk considerations affect leadership only after an event has occurred or a problem has arisen. There is no evidence of commitment or accountability to managing risk. There is no direct relationship between evaluating individual or organizational performance and managing risk. Most leaders still show little or no understanding of the relationship between risk and achieving objectives. Most leaders choose not to participate in organizational risk assessments.

Ideal condition according to Tier-4:

Formal processes are used to consider risks after, during, and before a decision, i.e., assessing the associated risk before a decision, such as before proceeding with a strategic initiative, launching a new program or policy, and others. Execution is tracked, and progress is also reported. There is an analysis of resilience to extreme scenarios and disruptive forces (e.g., recession, epidemic or pandemic, changes to regulatory laws, political instability). Risks for strategic initiatives or investments are evaluated continuously from the start of the approval process with the risk management plan. Risk appetite and tolerance are formally stated and considered part of the planning process. Risk management skills have been viewed as essential by most leaders. Business model risks are analyzed and tested to verify or incrementally revise the underlying assumptions and strategies.

Assessment results are reported and followed up by the initiative, project, or strategy owner. Organizational leadership, policy-making, compliance, and evaluation functions have been fully engaged. Other contributions are also broadly sought. Risk considerations mainly occur in decisions related to the organizational strategy and operations (e.g., issuing

new programs, reorganization, new initiatives, and large-scale projects). The commitment to risk culture is strategic, pervasive, and observable at different levels of the organization. The board or other governance body holds top management individually accountable for managing risk in achieving objectives. Most leaders already have themselves and their employees responsible for managing the top risks in the organization, and those risks that arise can affect the organization's goals. Most leaders actively participate in organizational risk assessment by volunteering information, offering different perspectives, and providing regular feedback.

V. Conclusion

The maturity assessment results using the RIMS RMM® model show that the risk management maturity level in the XYZ agency is in the Tier-2 position. With this level, risk management capabilities at XYZ agency are already on paper. Still, there is no clear and active involvement of stakeholders related to XYZ agency, both internal and external contexts. Decision-making is still primarily driven by qualitative risk considerations. Risk management is also still considered to add to the existing workload.

In addition, there is still a large gap between the current condition and the target maturity level (tier-4), namely a condition where risk management capabilities in the organization have become an iterative process supported by internal and external contexts, situations where the comprehension at the senior management level has also flowed to the middle management level. There is an alignment between the business processes and the risk management framework, and every decision considers risk analysis.

The XYZ agency should immediately start integrating risk management into all business processes and performance management to improve its risk management maturity level to overcome these issues. They also need to evaluate and properly document it formally and periodically, especially those related to the Directorate of Investigation activities. The risks at the institutional level need to be compiled and determined, not just limited to the Directorate's work unit level. Competencies related to risk management must be a requirement at every selection stage, including assessing the promotion and recruitment of structural officers.

References

- Alijoyo, A. (2017, April 6). *Pertahanan 3 Lapis (The 3 lines of defence) – Konteks ERM Perusahaan Publik Di Indonesia*. Retrieved August 2, 2021, from Website Kompasiana Beyond Blogging: <https://www.kompasiana.com/crmsindonesia/pertahanan-3-lapis-the-3-lines-of-defence-konteks-erm-perusahaan-publik-di-indnesia?page=all>
- Coetzee, G. P., & Lubbe, D. (2013). The risk maturity of South African private and public sector organizations. *Southern African Journal of Accountability and Auditing Research*, 14, 45-56.
- Creswell, J. W. (1994). *Research Design Quantitative & Qualitative Approach*. London: Sage Publication.
- Hopkin, P. (2018). *Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management* (5th ed.). The Institute of Risk Management.
- Indrayana, D. (2016). *Jangan Bunuh KPK - Kajian Hukum Tata Negara Penguatan Komisi Pemberantasan Korupsi* (Revisi ed.). Malang: Intrans Publishing.

- Kaplan, R. S., & Mikes, A. (2012, Juni). *Managing Risks: A New Framework*. Retrieved from Harvard Business Review: <https://hbr.org/2012/06/managing-risks-a-new-framework>
- Kitab Undang-Undang Hukum Pidana*. (n.d.).
- Komisi Pemberantasan Korupsi. (2019). *Peraturan Pimpinan KPK RI Nomor 9 tahun 2019 tentang Pedoman Manajemen Risiko*.
- Levy, C., Lamarre, E., & Twining, J. (2010). *McKinsey Working Paper On Risk: Taking Control of Organizational Risk Culture*. McKinsey&Company.
- Minsky, S. (2021). *ERM Program Audit Guide: Risk Maturity Model, Assessing the Adequacy and Effectiveness of Risk Management*. LogicManager.
- Munawar, Y., & Aini, R. F. (2020). *Ketidakpastian, Risiko, Masalah, Krisis, dan Bencana*. Retrieved January 23, 2022, from Website LSP MKS: <https://lspmks.co.id/2020/08/07/ketidakpastian-risiko-masalah-krisis-dan-bencana/>
- Muttaqin, L., & Susanto, M. E. (2018). Mengkaji Serangan Balik Koruptor Terhadap KPK dan Strategi Menghadapinya. *INTEGRITAS Volume 4 Nomor 1 - Juni 2018*.
- Niati, D. R., Siregar, Z. M. E., & Prayoga, Y. (2021). The Effect of Training on Work Performance and Career Development: The Role of Motivation as Intervening Variable. *Budapest International Research and Critics Institute (BIRCI-Journal): Humanities and Social Sciences*, 4(2), 2385–2393. <https://doi.org/10.33258/birci.v4i2.1940>
- Proenca, D., Estevens, J., Vieira, R., & Borbinha, J. (2017). Risk Management: A Maturity Model based on ISO 31000. *IEEE Computer Society*, 99-108. doi:10.1109/CBI.2017.40
- RIMS, Risk and Insurance Management Society Inc. (2006). *RIMS Risk Maturity Model (RMM) for Enterprise Risk Management: Executive Summary*. Risk and Insurance Management Society, Inc. Retrieved from Website of The Risk Management Society.
- Sawyer, L. B. (2018). *Sawyer's Internal Auditing: Enhancing and Protecting Organizational Value* (7th ed.). The Institute of Internal Auditors.
- SCCE & HACCA, S. H. (2020). *Compliance Risk Management: Applying The COSO ERM Framework*. Committee of Sponsoring Organizations of the Treadway Commission (COSO).
- Suharso. (2016). *Pilihan Standar Manajemen Risiko di Indonesia*. Retrieved January 25, 2022, from www.klikharso.com.
- The Institute of Internal Auditor. (2017). *Standards Glossary*. Retrieved January 23, 2022, from Website IIA North America: <https://na.theiia.org/standards-guidance/mandatory-guidance/pages/standards-glossary.aspx>
- The Institute of Internal Auditors. (2016). *International Standards For The Professional Practice Of Internal Auditing (STANDARDS)*. Florida, USA.
- The Risk Management Society. (2022). *RIMS Risk Maturity Model*. Retrieved May 15, 2022, from Website of RIMS - The Risk Management Society: <https://www.rims.org/Tools/risk-maturity-model>
- Tuanakotta, T. (2019). *Audit Internal Berbasis Risiko*. Jakarta: Penerbit Salemba Empat.
- Undang-Undang Republik Indonesia Nomor 19 tahun 2019 tentang Perubahan Kedua Atas Undang-Undang Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi*. (2019).
- Undang-Undang Republik Indonesia Nomor 20 Tahun 2001 tentang Perubahan Atas Undang-Undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi (UU Tipikor) oleh Pemerintah*. (2001).

- Undang-Undang Republik Indonesia Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi.* (2002).
- Undang-Undang Republik Indonesia Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi.* (1999).
- Vorst, C. R., Priyarsono, D., & Budiman, A. (2018). *Manajemen Risiko Berbasis SNI ISO 31000.* Jakarta Pusat: Badan Standardisasi Nasional.
- Wahyuni, S. (2015). *Qualitative Research Method: Theory and Practice* (2nd ed.). Jakarta: Penerbit Salemba Empat.
- Yin, R. K. (2018). *Case Study Research and Applications Design and Method* (6th ed.). California: SAGE Publications, Inc.