OCEANIDE: Vol 12, No 3 (2020)
ISSN: 1989-6328
https://oceanidenetne.net/index.php/o

Research Article

Regional Government Management Control in the Implementation of Risk Governance

Dadang Suwanda
Institut Pemerintahan Dalam Negeri (IPDN) Indonesia
Email: dadang_suwanda@ipdn.ac.id

Abstract

This study aims to dig deeper into the effectiveness and consistency of the application of the Three Lines of Defense concept in local governments in the application of a risk management framework. The successful implementation of risk management is inseparable from the role of all individuals in the organization, from the leadership level to the executive level. Optimization of risk also needs to be supported by the implementation of a layered defence system from both the managerial and internal control sides. This study uses qualitative research methods with descriptive reviews. The data collection technique was carried out by in-depth interviews using a "verbal protocol" to research informants, observation and study documentation. Research informants are selected from risk owners and risk leaders who are involved in policy, especially those who are directly involved in the risk management process. After being reduced and classified, data validation was carried out by triangulation of sources, triangulation of theories, and triangulation of methods. The results showed that a risk management structure that describes the division of tasks and responsibilities in risk management had not been established. This research offers novelty, namely that an effective risk management structure, apart from involving three lines of defence, must also apply the fourth line of Defense which is carried out by the external audit function and the fifth line of Defense which is carried out by the part of the law enforcement apparatus.

Keyword: *Risk Governance, Local Government, Management, Management Structure*.

I. INTRODUCTION

The activities of public and business sector organizations are constantly changing and developing along with changes in the internal and external environment of the organization (Christensen, Lægreid, & Rovik, 2020; Finger & Brand, 1999; Senior & Fleming, 2006). Change in the internal environment can usually be controlled by management (Adamec, Rexroad, Leinicke, & Ostrosky, 2002; Langfield-Smith & Smith, 2003; Otley, 1994; Pablo, Reay, Dewald, & Casebeer, 2007). Meanwhile, changes in the external environment, such as changes in the democratic climate and regulations, are outside organizational control (Brief & Aldag, 1981; Guliyeva, 2020; Manz, Mossholder, & Luthanvs, 1987). Demands for change and improvement of organizational capabilities raise risks and opportunities for the organization (Conchúir & Conchúir, 2010). Risk relates to the possibility of failure and loss to the organization. Low-scale chances are not a cause for concern for the organization. However, large-scale risks can have an impact on not achieving the goals and mission of the organization (Rochette, 2009).

The risk of not achieving organizational goals and programs does not only occur in the business sector but also appears in the government sector (Leung & Isaacs, 2008). Therefore, government agencies need to carry out risk management. Failure of goals and missions for public organizations can result in distrust from the public for the services provided (Oulasvirta & Anttiroiko, 2017a). In the worst circumstances and as ever, mistrust can lead to loss of credibility of the organization concerned. Risk management becomes a strategic need (Clarke & Varma, 1999) and determines the performance improvement of the organization (Jan Kopia, Vanessa Just, Wiebke Geldmacher, 2017). The risk that is managed optimally even creates various opportunities for the organization concerned (Purdy, 2010). Risk management is needed to optimize the use of the organization's limited resources (Mearns, Flin, & O'Connor, 2001). The allocation of resources is based on risk priority starting from the highest scale risk. Likewise, existing risk management needs to be evaluated periodically through control activities (internal control) (Pablo et al., 2007).

Government organizations are currently required to have risk management, including government agencies (Saidon & Said, 2020). The many uncertainties faced by government agencies in carrying out their main tasks and organizational functions have caused government agencies to begin to improve by starting to prepare for risk management implementation (Edwards, Griffith, Burton, & Mackey, 2019). Anything that hurts the achievement of organizational goals can be called risk. Risk always affects the achievement of goals which is an event that has not yet happened. If it does happen, it hurts the organization. For that, risk management is needed. The goal is to minimize the risks that will occur. Risk needs to be managed to achieve organizational goals (Guliyeva, 2020; Rockafellar & Uryasev, 2013).

Risk management starts with the awareness of the government to realize that the risk must exist within an organization (McLucas, 2003). The implementation of sound risk management must ensure that the organization can provide proper treatment of troubles that will affect it (Bento, Mertins, & White, 2018). Information on risk management is beneficial for all levels in the government structure, especially for stakeholders to carry out risk analysis so that the expected returns can be met.

Management structure support from every level is significant and essential for an organization to carry out every operation, especially support from top management (Crawford, Crowley, Potter, Saunders, & Johnston, 2018; Hardy, 2014). The form of support can be explicit or implicit, for example, top management supports and participates in formulating/approving the mission and vision, procedures and policies related to risk management (von Hagen & Harden, 1995). Management support can also be demonstrated through management participation in risk management programs (Bartlett & Dibben, 2002). It can be said that the risk management structure is tasked with and is responsible for coordinating, facilitating and overseeing the effectiveness and integrity of risk management processes that are in charge of and are directly responsible for day-to-day risk management and control (Hardy, 2014; Rodríguez Bolívar, Navarro Galera, Alcaide Muñoz, & López Subirés, 2016).

Strengthening management effectiveness in dealing with governance risks through structured, measurable, comprehensive and sustainable implementation needs to be carried out to support increased performance, transparency and accountability of government through management of government administration that is oriented towards sensitivity to all possible events that may hinder the achievement of objectives. The establishment of a risk management structure and risk management process is necessary to support the effectiveness of risk management. These reasons make this study have a high novelty value because it seeks to find other dimensions/factors/variables of support for government structures in the risk governance process in realizing the achievement of government goals itself (Hardy, 2010; Long, 1975; Meyer, Meyer, & Kot, 2017; Power, 2004; Rodríguez Bolívar et al., 2016).

II. LITERATURE REVIEW

1. The Concept of Governance and Risk Governance

Governance and risk governance becomes an integral part of managing the work chain process of an organization. Organizations can run effectively if the governance and risk governance processes carried out by the organization can run optimally (Peters & Pierre, 1998; Rhodes, 1996; Van Asselt & Renn, 2011). Organizational dynamics as a result of dynamic internal and external influences require management that contains governance and risk governance principles, including transparency, accountability and participation. Organizational dynamics also have an impact on the emergence of various potential risks that threaten the achievement of organizational goals (Van Asselt & Renn, 2011). Governance and risk governance is a solution for controlling corporate risk through concrete risk mitigation measures. Governance and risk governance as a whole can be described in more detail in each component, both the governance and risk governance components. The following is an explanation of each element as an element of support for successful governance and risk governance in managing a public organization (Peters & Pierre, 1998; Rhodes, 1996).

Governance is the most prominent central issue in the management of public administration today (Roberts, 2020; Schomaker & Bauer, 2020). Authority arises because of irregularities in governance, thus encouraging the awareness of citizens to create a new system or paradigm to oversee the course of government so that it does not change from its original purpose (Koppenjan & Koliba, 2013; Torfing, Andersen, Greve, & Klausen, 2020). The demand to realize government administration that can support the smooth and integrated implementation of governmental administration duties and functions can be learned by practising good governance (Beeri, Uster, & Vigoda-Gadot, 2019). The concept of governance involves not only the government and the state but also the roles of various actors outside the government and the state so that the parties involved are inclusive (Addink, 2019). It is further argued that governance is a mechanism for managing economic and social resources that consist of the influence of the state sector and the non-government sector in a collective activity (Gisselquist, 2012).

Building good governance is changing work management, making the government accountable and building actors in government to play a role in creating a new system that is generally useful (Gisselquist, 2012; Khouya & Benabdelhadi, 2020). In this context, there is no single development goal that can be well realized only by changing the characteristics and workings of state and government institutions (Basu, Brown, & Devine, 2017). The essence of the concept of good governance as described above is that the strength of the idea of government lies in the activity of the state, public and private sectors to interact. Therefore, good governance, as a social project, must look at the conditions of the sectors outside the country, so that there is an interconnectivity between the sectors that make up governance (Agrifoglio, Metallo, & di Nauta, 2020; Basu, Devine, & Wood, 2017; Bozhikin, Macke, & da Costa, 2019; Jugend, Fiorini, Armellini, & Ferrari, 2020; Pahl-Wostl, 2019)

Governance comes to be a new trend in the management of the public interest by offering a more inclusive format and opening intensive interaction between various actors outside of government, both business people and civil society (Arts, 2014; Borins, 2000, 2001; Leblanc, 2020; G. Li & Wu, 2020; Wu & Walker, 2020). In essence, among the many diversity in the emergence of governance discourse, the basic idea for the emergence of this concept is the existence of economic liberalization that occurred in the United States and Britain which then spread as a new approach in the practice of governance in almost all countries in the world (Abrahamsen, 2004; Hout, 2009). In subsequent developments, the notion of government has become so diverse as a logical consequence of actual products and changes at all levels of public life which are increasingly influenced by two main forces, namely globalization and political democratization. Mention, among others, good governance (Haliah & Nirwana, 2019; Weiss, 2000), collaborative governance (Chris & Alison, 2008), network governance (Kapucu & Hu, 2020; Provan & Kenis, 2008), partnership governance (Righetti, 2020; Vivek, Richey, & Dalela, 2009) and adaptive governance (Chaffin, Gosnell, & Cosens, 2014; Lemos, 2007).

According to Scharpf (1997), the existence of democratization in government such as encouraging participation, equality, and more transparent and accountable management also contribute to shifting the format of public service management from government to governance. Various versions of the definition have emerged to make clear what is meant by governance. However, the reference that is often used as the basis for discussing this concept is the World Bank report in 1989, which became known as the Washington Consensus. In essence, governance is the broadest possible involvement of actors outside the government and limits government intervention in the administration of its government (Kaufmann, Kraay, & Mastruzzi, 2003; Shah, 2006). This is also supported by the development of the term governance which continues to change and tends to expand its meaning because, in current products, the government does explain not only the inter-organizational relationships but also administration as a value. This can be seen from the opinion of Rhodes (1996) which defines governance in seven definitions, namely corporate governance, new public management, good governance, interdependence, as a cybernetic social system, as a new political economy approach, and governance as a network (Rhodes, 1996).

Concerning the concept of risk governance, the definition of governance above clearly directs the importance of risk awareness, namely government as the owner of a risk. The keywords of equal position and opportunity in the public policymaking process are in line with the concept of governance as the exercise of political power to manage a nation's affair which is a starting point for understanding governance for several reasons (Leftwich, 1993; Rose & Miller, 1992). Among other things: 1) that good governance is neutral and impartial or shows the domination of certain actors (Weiss, 2000). 2) that good governance also does not take sides explicitly, whether public services should be carried out by the government or by the private sector (S. Li, Park, & Li, 2003). 3) This definition of governance shows that managing public affairs requires a role not only of the government, thus emphasizing the need for the government to build a culture of risk awareness (Koprić, 2012). In another sense, risk governance is a pillar of the achievement of the principles of good government that prioritizes interaction between actors in its realization.

The governance coverage consisting of Internal Control and External Control, as stated in the following figure, emphasizes the importance of risk management. Both internal control and external control emphasize the importance of risk and power for the organization.

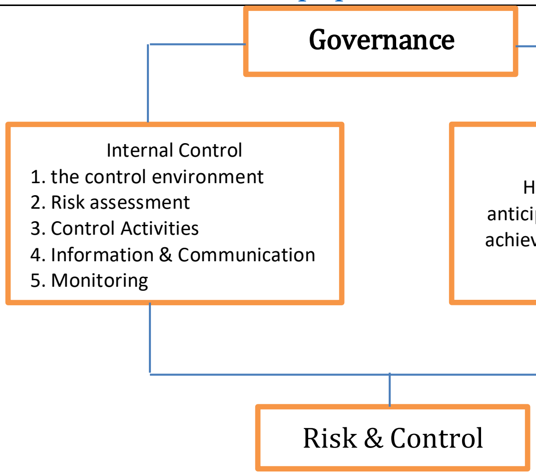

Figure 1 Governance Scope

The concept of public sector governance risk control (GRC) is adopted and developed from the idea of Enterprise Risk Management (ERM) (Arena, Arnaboldi, & Azzone, 2010; Beasley, Branson, & Hancock, 2010; Moeller, 2011; Rochette, 2009). According to the ERM concept, every organization, both profit and non-profit, must provide value to stakeholders. The value must be created through management decisions based on strategy setting to operational policies (Aziz, Manab, & Othman, 2016). In providing this value, the public sector GRC concept discusses a lot of potential future events that create uncertainty. It is essential to do in public sector GRC is a response to risk to reduce the chances of these risks occurring. Based on this figure, organizational goals are seen in 4 (four) categories, namely strategic, operational, reporting and compliance objectives. Thus, ERM divides corporate activities into 3 (three) levels, namely the overall organizational level, division level and business unit processes. Public sector management responds by compiling a risk portfolio at the business unit level and entity level.

The terms risk and risk management have long been recognized in the insurance industry. In this case, the risk is viewed as a loss that is estimated and measured using a direct probability estimation methodology multiplied by the value of the assets exposed to the risk, as the basis for determining the amount of insurance premium to be paid by the insured. In its development, risk management has expanded the scale of activities, not only related to insurance but has and must become an integral part of business management. All members of the organization must have awareness and concern about risks and how to manage risks faced by the organization within the limits of their respective authority. Risk and risk management must be placed in an organization-wide perspective.

Hopkin (2018,) explains that risk management was first developed in the United States, especially in the insurance management function in the 1960s. Then, risk management began to be applied by large companies in the United States in other functions such as taxation, treasury, human resources, procurement of goods/services, and logistics. However, Chapman (2011), explains that in practice, these functions carry out risk management separately without any coordination between parts in one organization. Hopkin (2018), explains that the implementation of risk management that is carried out without coordination between tasks within an organization is called silo-based risk management. The problem that arises from the implementation of silo-based risk management is the presence of risks in a processor unit that is connected to risks in other functions or units or is called interconnected risks so that without coordination between parts it will result in risks that are not mitigated. because there is no clarity of responsibility and coordination (Hopkin, 2018; Hoyt & Liebenberg, 2011)

The limitation of silo-based risk management which is not effective in supporting the achievement of organizational goals is the background for the birth of a more integrated and strategic risk management approach, namely Enterprise Risk Management (ERM), which is a risk management concept that is more strategic in capturing significant organizational risks—from the perspective of achieving strategic objectives, taking into account a comprehensive spectrum of risks and their consequences as a portfolio of interrelated risks to ensure that threats have been analyzed, mitigated and monitored (Bromiley, McShane, Nair, & Rustambekov, 2015; Chapman, 2011; Eaton et al., 2019; Hopkin, 2018; McShane, 2018).

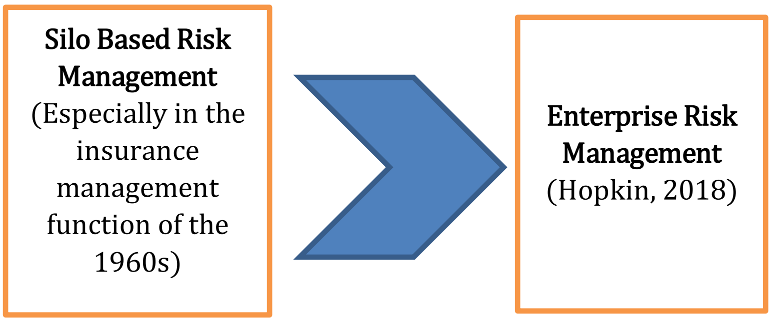

Figure 2 Change In Risk Management

Every organization, whether in the form of a company or a government, has strategic objectives to be achieved. Hardy (2014) explains that both have goals to achieve maximum performance and protect assets and take advantage of current opportunities. Organizations in the private sector use a return-driven strategy (RDS) to achieve their goals. Meanwhile, in the government sector, it is achieved with a mission-driven strategy (MDS). The company has a strategic plan for maximizing shareholder wealth (shareholders' value). This means that the capital provided by shareholders is needed by the company to carry out its business activities. For the provision of capital, shareholders expect a return in the form of a maximum increase of the invested capital with a level of risk that must be faced by shareholders (Chapman, 2011). On the other hand, the MDS approach is initiated from the question "has the organization taken the right steps for the right reasons?" and "has the organization focused on the right initiatives and goals?". In the government sector, government agencies also focus on carrying out their services to internal and external stakeholders (Frigo, 2003; Hardy, 2014).

Although in terms of strategy, there are differences between the private and government sectors, both have similarities in terms of formulating practical strategic goals. This explains that there are still many organizational leaders who do not understand the strategic objectives of their organizations and how they develop these strategic goals (Rodrik, 2001). The task of the organizational leader is to communicate to organizational executives how to set goals, formulate them, and the meaning of each word composed of these goals (Agrawal, Hoyt, & Wilson, 2020). This is important because setting organizational goals and planning activities are the essential steps in the organizational management process. (Doran, 1981) suggested that in a formulation of objectives should refer to the Specific, Measurable, Assignable, Realistic, and Time-related (SMART) indicators. Specific means that the organizational goals must show improvement targets in particular areas; Measurable standards that the organizational goals can be measured in quantity or progress can be calculated; Assignable means that the parties working towards achieving the plans have been precisely determined; Realistic standards that the target of these goals must realistically be achieved by considering the resources owned; Time-related means that there is a time frame to determine when the set goals can be achieved (Doran, 1981; Mathieu, Rennotte, Romain, Vosse, & Al Shehri, 2017; Oulasvirta & Anttiroiko, 2017b).

Over time, the SMART indicator continues to develop, but in substance, it remains the same. Bogue (2005) and Frigo (2003) establish these indicators to be Specific, meaning that organizational goals must show specific expected results; Measurable means that the organizational goals can be measured in quantity or progress can be calculated; Achievable means that the goals set can be achieved; Realistic means that the target of these goals must be realistically achievable by considering the resources owned and external factors that can and cannot be controlled; Time-based implies that there is a time frame to determine when the set goals can be achieved (Bogue, 2005; Doran, 1981; Frigo, 2003).

McShane (2018) argues that the existence of ERM is not aimed at eliminating all existing risks, but rather provides information to organizations about how organizations allocate risks according to organizational strengths and reduce risk to vulnerable parts of the organization. Fraser & Simkins (2010) added that especially in developing countries, the application of ERM is critical due to several factors such as a more unstable environment, inconsistent policies, uncontrolled growth rates, riskier market environments, and high frequency of corruption.

Governance uses controls to minimize risk. Control is also used to control government and mitigate risk. Right governance processes will result in the optimal achievement of organizational goals through optimal risk control and supervision. In the end, the comprehensive implementation of governance and risk governance will optimize value for the organization while ensuring that organizational goals are achieved (Kim & Lu, 2011; Knechel & Willekens, 2006; Moeller, 2007).

2. Risk Management Structure

Everyone who works for the organization needs to be made aware of their risk management responsibilities. There needs to be a clear statement of responsibility for the management aspects of each risk (Hopkin, 2018). Detailed responsibilities will ensure that the roles of risk owner, process owner, internal audit, risk manager, risk management function, all employees are clear and understandable.

The implementation of risk management is the responsibility of all parties involved in an organization. This principle is the basis for the performance of the three lines of Defense in risk management. Three lines of Defense as a model in addressing how specific tasks, related to risk and control, can be assigned/determined and coordinated within an organization, and this depends on the size and complexity of the organization (Auditors, 2013).

This model deals with the division of roles and responsibilities for implementing risk management and internal control in the organization. Simply put, the three lines of Defense divide the roles and responsibilities of risk management and control into three lines or layers within an organization. The first line is the party who is the core and the main person in charge of operations which must carry out their duties with due regard to risk, control, regulation and the environment. The second line is the function that monitors and maintains compliance and provides input to the first line. The third line is the internal audit function which checks and assesses objectively and then provides feedback so that the first and second lines function correctly. The pattern to be built is when the first line fails it is expected to be detected or backed up by the second line, then if the second line also fails it will be seen by the third line (Anderson & Eubanks, 2015; Kim & Lu, 2011).

The Three Lines of Defense model is a significant effort to provide clear task delegation and reliable communication in the application of risk management (Luburic, Perovic, & Sekulovic, 2015). In the context of risk management, the first line is management as the owner of the risk who is responsible for identifying, assessing, and managing risks in daily activities, including implementing controls. In the second line of Defense, risk management functions such as the Chief Risk Officer (CRO), Risk Manager and Risk Management Unit (RMU) are responsible for formulating risk management guidelines, providing training for the first line, and reporting its implementation to the Board. In the third line of Defense, internal auditors are assigned to provide independent assurance regarding the effectiveness of risk management carried out by the first and second lines of Defense. The Risk Management Committee, as a representative of the Board, oversees the implementation of the Three Lines of Defense (Davies & Zhivitskaya, 2018; Luburic et al., 2015).

In the Three Lines of Defense model, management control is the line of defence risk in risk management, the various control risks and compliance functions defined by the government are the second line of Defense, and assurance is the third. Each of the three "lines" plays a different role in the organization within the broader governance framework (Luburic et al., 2015).

The three lines of the model defence distinguish between the three groups (or lines) involved in the effectiveness of risk management, namely the functions that own and manage risk; The role that oversees risk; and a process that provides independent assurance. As the first line of Defense, managers hold operations and manage risk. They are also responsible for implementing corrective actions to address process and control deficiencies (Auditors, 2013).

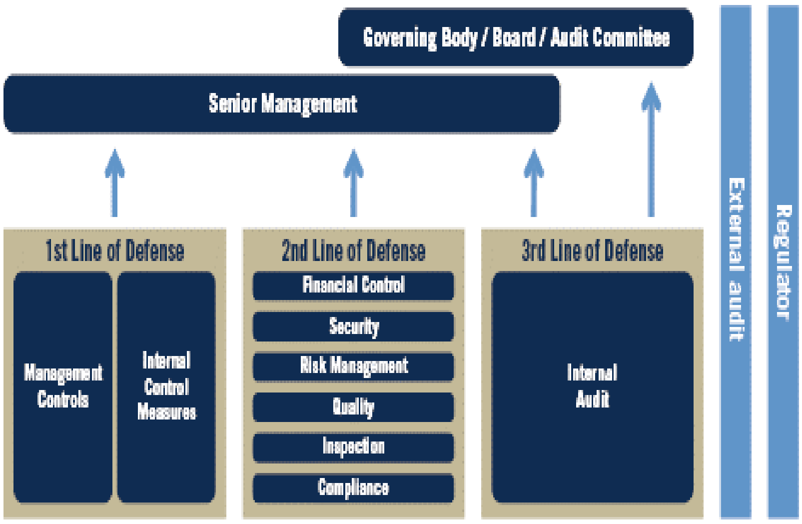

Figure 3 The Three Lines of Defence Model, Institute Of Internal Auditor, 2013

First Line of Defense: Operational Management

Operational management is responsible for maintaining adequate internal controls and for executing risk and control procedures on a day-to-day basis. Active management identifies, assesses, rules, and mitigates risk, guides the development and implementation of internal policies and procedures and ensures that activities are in line with goals and objectives. Through a stratified responsibility structure, middle-level managers design and implement detailed strategies that serve control and oversee the implementation of their procedures by employees (Sadgrove, 2016).

Operational management is naturally the line of the first line of Defense because controls are designed to systems and processes under the guidance of operational management. There must be adequate managerial and supervisory controls in place to ensure compliance and to oversee further clarification of rules, inefficient processes and unforeseen events (Arwinge & Olve, 2017; Potter & Toburen, 2016).

Second Line of Defense: Risk Management and Compliance Function

In a perfect world, perhaps only one line of Defense would be needed to ensure the effectiveness of risk management. In the real world, however, a single line of Defense is often insufficient. Government establishes various risk management and compliance functions to help build and/or monitor the first line of Defense (Auditors, 2013; Luko, 2013). Specific procedures will vary by organization and industry, but typical functions within this second line of Defense include (Arwinge & Olve, 2017; Auditors, 2013; Luko, 2013; Potter & Toburen, 2016; Sadgrove, 2016):

1. The Risk Management function (and/or Committee) that facilitates and monitors the implementation of the effectiveness of risk management practices by operational management and assists risk owners in defining risk targets and adequate reporting of risks related to information throughout the organization.

2. Compliance function to monitor certain risks such as non-compliance with laws and regulations. In this sense, a separate function reports directly to senior management, and in some business sectors, straight to government agencies. Multiple compliance functions often exist within a single organization, with specific responsibility for the type of monitoring compliance.

3. A controllership function that monitors financial risk and financial reporting.

Then, in the second line of Defense, according to JRS Fraser (2016), it is stated that risk management functions such as the Chief Risk Officer (CRO), Risk Manager and Risk Management Unit (RMU) are responsible for formulating risk management guidelines, providing training for the first line, and report the implementation to the head of the agency. The risk management process is not an activity that stands alone but is an integral part of business processes and organizational processes. Everyone who has work goals must apply risk management to ensure the achievement of their work targets better. Thus, the task of risk management is to enable everyone to carry out risk management well to ensure the accomplishment of their work goals. In the aggregate, it is the achievement of the purposes of the organization itself. Following its position in the 2nd line of Defense in the Three Lines of Defense model, it can be argued that the risk management work unit is part of management; the risk management work unit must be independent of other business organizations and operations; the risk management work unit has the function of developing and supervising the implementation of risk management by all business units and other processes; the risk management work unit is responsible for risk management reports, including the effectiveness of the risk management framework, implementation of a risk management roadmap, corporate risk profile, risk management performance and progress of risk planning and risk management work; The risk management work unit must have access to communication and report to the head of the agency.

Third Line of Defense: Internal Audit

Internal auditors provide Government Agencies and senior management with comprehensive assurance based on the highest levels of independence and objectivity in the organization. This high degree of autonomy is not available in the second line of Defense. Internal audit provides assurance of effectiveness in governance, risk management, and internal control, including how the first and second lines of Defense achieve risk management and control objectives (Kim & Lu, 2011).

Lundqvist (2014), compiles four pillars that support the implementation of risk management, namely the first two pillars are general prerequisites for implementing risk management within an organization; one pillar is a holistic infrastructure of risk management. The last pillar is a specific risk management process, namely, identification and risk assessment. Lundqvist (2014), also emphasizes that the third pillar, namely the holistic risk management organization, is the central pillar which is the infrastructure of risk management implementation. This pillar consists of several sub-pillars, including those related to the parties within the organization who are responsible for implementing risk management.

A board-level committee in charge of overseeing risk management. Beasley, Branson, & Hancock (2010), state that to optimize supervision, the Board can delegate supervision by forming a committee that oversees the implementation of risk management explicitly and receives direct reports from the government regarding the risk management process. One of the backgrounds of the delegation is based on the importance of knowledge. Comprehensive risk management Moeller (2011), argues that many risk management activities are essential for organizations so that decisions and planned actions must be supervised and approved by the risk management committee.

Risk management. To provide support in the implementation process through specific competencies related to risk management, local governments appoint a risk manager who is supported by a particular risk management unit for large-scale local governments and only a risk manager for small-scale local governments. At the level of monitoring the implementation of risk management and assessing its effectiveness, responsibility is given to internal auditors (Arena et al., 2010).

III. METHOD

This study uses a descriptive study research method. The data collection technique was carried out by in-depth interviews using the "verbal protocol" to research informants, observation and study documentation. Research informants were selected from the actors (risk owners and risk leaders) involved in policies, especially those directly involved in the risk management process. After being reduced and classified, data validation was carried out by triangulation of sources, triangulation of theories, and triangulation of methods.

IV. RESULT AND DISCUSSION.

The application of risk management will not run effectively without a risk culture (Roeschmann, 2014). Positive risk culture is that all parties in the organization, from the leadership to the executor, understand their respective roles in implementing risk management (Bento et al., 2018). The implementation of risk management requires control and supervision, so it is necessary to establish a risk management structure (Brown & Osborne, 2013; Oulasvirta & Anttiroiko, 2017a). Within the organization, there are boundaries between activities related to an internal audit, risk management, and compliance which are not always well defined. So that it seems that they overlap and sometimes rely on each other so that the implementation of risk management is not practical, for this reason, clear responsibilities must be defined, so that each group understands their role in addressing risks, controls, aspects for which they are responsible, and how they coordinate with other parties. So that there are no gaps in addressing risks and controlling or duplicating unnecessary or unintentional efforts.

Responsibilities in risk management make it clear that everyone who works for the organization needs to be informed about their risk management responsibilities. There needs to be a clear statement of responsibility for the management aspect of each risk. Detailed responsibilities will ensure that the roles of risk owner, process owner, internal audit, risk manager, risk management function, all employees are clear and understandable (Hopkin, 2018). The implementation of risk management should be the responsibility of all parties involved in an organization. This principle is the basis for the implementation of the three lines of Defense in risk management. The latest trend regarding risk management which is best practice is the three lines of Defense as a model in addressing how specific tasks, related to risk and control, can be assigned/determined and coordinated within an organization, and this depends on the size and complexity of the organization. The three lines of Defense are a model that has an essential component in working together, where the first line of Defense is carried out by front line staff and operational management. The systems, internal controls, control environment, culture developed and implemented by the business unit are very important in anticipating and managing operational risk. The second line of Defense is carried out by the risk management unit and compliance function. These functions provide the necessary oversight, tools, systems and advice to support first-line risk identification, management and monitoring. The internal audit function carries out the third line of Defense. This function provides an adequate level of independent assurance that the risk management and internal control framework is working as designed.

First Line of Defense

Implementation of internal government control through the application of risk management, especially in the risk management structure within local governments, in the context of risk management, on the first line, namely administration as a risk owner who is responsible for identifying, assessing and managing risks in daily activities, including implementing the control, not yet fully implemented effectively. The implementation of a risk management structure consisting of policies, guidelines, risk management committees, job descriptions and reporting has not met expectations. In general, respondents think that policies, procedures, risk management committees, job descriptions and reporting have not been fully implemented because there is still a significant gap between expectations and reality, this gap shows that the implementation of internal government control through the application of risk management, especially in the management structure. Risks in local government circles still need to be increased to meet respondents' satisfaction expectations. Based on research through document reviews, the provincial government already has a regulatory basis related to the application of risk management within the local government, namely a risk management policy which states that in the context of controlling and supervising control over the implementation of risk management in the local government, a risk management structure has been established consisting of: 1) local government risk management committees, which control the level of local government policies; 2) OPD Head, who controls the operational level; 3) the local government inspectorate as a risk management compliance unit, which supervises control over the implementation of risk management.

Besides, some local governments in Indonesia already have guidelines for the implementation of risk management, which state that the performance of a risk management process includes communication and consultation activities, setting the context, risk identification, risk analysis, risk evaluation, risk mitigation, and monitoring and review. However, up to the time of the research, the regulation had not been implemented in a structured, measurable, comprehensive and sustainable manner following the stipulated policy.

A risk management policy is a statement of intention and commitment of agency leaders to implement risk management and contains an overview of its application (Hood & McGarvey, 2002; Power, 2004; Sadgrove, 2016). There are two types of risk management policies. 1) a statement supported by a separate Risk Management Handbook, 2) a book containing a risk management policy statement followed by details of risk management procedures and governance. Risk management policies must be disseminated to all levels of agency employees, as well as to all relevant stakeholders (Hood & McGarvey, 2002; McShane, 2018).

Second Line of Defense

Following the function and position of the risk management work unit, the scope of work of the risk management work unit includes: 1) designing risk management policies to be approved by the head of the agency: 2) preparing manuals and risk management procedures for approval by the head of the agency; 3) compile a risk management implementation plan to obtain permission from the head of the agency and carry out a detailed description of the project for implementation; 4) compiling risk criteria, including criteria for risk appetite, risk limits and risk tolerance for approval by the agency leadership; 5) designing the appointment of risk owner and risk control owner as well as risk officer/champion at the structural level and if necessary at lower levels, to be approved by the head of the agency; 6) planning and conducting tiered training on risk management from the head of the agency to the executive level in the field. Special training for risk officers/champions to become trainers for their work units; 7) assisting the implementation of risk management in all agencies in stages according to the plan, capability and competence of the unit to implement risk management; 8) monitoring and reviewing the risk management implementation process according to the predetermined road map. Also monitoring and examining the effectiveness of the risk management framework and risk management performance, as well as the progress of existing risk handlers; 9) assisting the integration of risk management in business and organizational processes to obtain optimal benefits from the application of risk management; 10) carry out risk management reports to agency leaders regularly and take corrective actions on the findings of monitoring and review results; 11) establish an internal risk management communication forum to improve communication and exchange of information and risk management techniques, as well as to foster a risk awareness culture; 12) developing organizational capabilities in risk management through the preparation of a risk information system, capacity building on risk assessment techniques, risk database preparation (risk library), benchmarks and comparative studies, short in-house seminars, and others; 13) specifically designing a risk awareness culture fostering program in the organization in conjunction with a regulatory and regulatory compliance program.

Regarding the application of risk management in this second line of Defense, local governments do not have a legal umbrella that forms the basis for its implementation explicitly. The risk management policy has not regulated the risk management structure in the second line of Defense. It has not regulated the existence and role of the second line of Defense, namely the function of the risk management unit, so it cannot be implemented yet. Even though the part of the risk management unit is essential because generally, the competencies related to risk management between one unit and another unit in the organization are not the same, so it is necessary to have a unit specifically responsible for developing a risk management system and assisting functional units within the organization.

Based on the results of interviews with key informants as described above, they believe that there is no need for a permanent risk management organization formation process. In comparison, Collier & Woods (2011), argues that at the local government level, the implementation of risk management should be supervised by a risk management committee. To provide support in the implementation process through specific competencies related to risk management, local governments appoint a risk manager who is supported by a particular risk management unit for local governments. At the level of monitoring the implementation of risk management and assessing its effectiveness, responsibility is given to the internal auditor. The previous efforts have not been fully implemented by local governments, even though a culture of awareness has been developed, even though risk management awareness has been understood and understood through socialization and supported by the decision of the regional head regarding the application of risk management in local governments. Still, at the OPD level, it has not been fully implemented; this is due to different perceptions about risk management.

All informants gave almost similar answers that establishing a clear structure and pattern of responsibility related to risk management and control within the organization was deemed to have not resolved the problem. Because there is already an internal control system in each OPD, it is not necessary if the risk management function is to be used as an ad hoc unit or a unit that is formed permanently within the organizational structure.

Although there is no standard model or guide in the preparation of organizational infrastructure in risk management, the most important thing is the clarity of accountability and responsibility to encourage the implementation of risk management based on an exact and designated function. Each organization must prepare the risk management organization infrastructure according to the needs and types of risks faced.

Therefore, the risk management culture encourages policymakers in the public sector to implement proactive risk management. Risk has always been an important focus, evaluated periodically, and its impact on the objectives of the entity is measured. Starting from employees, executives, stakeholders, to regulators, they must understand that risk is an essential factor that needs to be considered in every action and decision making.

However, some of the Regional Government OPDs do not fully understand the position of the risk management organization. They only know that risk management is essential, but not with an adequate structure. Risk management is designed to be able to identify, analyze and control risks that may occur in every activity process carried out. If government agencies already have and implement effective risk management, the risks faced by the government have been identified and managed in such a way to a certain level that is acceptable to the government.

Third Line of Defense

In the third line of Defense, the internal auditors are assigned to provide adequate independent assurance regarding the effectiveness of risk management carried out by the first and second lines of Defense. Besides, the Risk Management Committee as a representative of the head of the agency is assigned to oversee the implementation of the Three Lines of Defense (Luburić, 2017). The core task of the internal auditor concerning risk management is to assure that risk management activities are carried out effectively in providing reasonable assurance of the achievement of organizational goals. Two important ways to carry out its duties are to ensure that the principal risks of the organization are appropriately handled and ensure that risk management and internal control activities are carried out effectively.

The core role of internal audit in risk management is the service-related activity of providing confidence in the design and effectiveness of risk management processes; provides assurance that the risks are appropriately evaluated; evaluate risk management processes; evaluate reporting on the status of critical risks and their controls; review the management of critical risks, including the effectiveness of controls and other responses to those risks. Different additional roles that may be performed in consulting services coupled with adequate safeguards for independence and objectivity include initiating the establishment of a risk management structure within the organization; develop risk management strategies for approval by agency leaders; facilitate risk identification and evaluation; management training on responding to risks; coordinating the risk management process activities; consolidate reports on risks; maintaining and developing a risk management framework.

The role in risk management that should not be performed by internal auditors is to manage risk interests, implement risk management processes; guarantee risk management; make decisions on risk responses; implement response and risk management on behalf of the government; risk management accountability. To maintain the effectiveness of internal audit activities, the responsibility given to internal auditors regarding risk management activities must be designed so as not to interfere with their independence. This is because internal audit has a vital role in supervising, monitoring and assessing the effectiveness of organizational risk management. Assigning responsibility to internal auditors to determine risk appetite, establish a risk management process, etc. can create a clash of interest that has the potential to interfere with their assessment of the effectiveness of risk management.

Based on risk management policies within local governments in Indonesia, it is stated that the local government Inspectorate has been appointed as the Compliance Office for Risk Management as the internal auditor. This is following the concept of The Three Lines of Defense Model, namely the critical function of the internal auditor concerning risk management, is to provide adequate confidence to management regarding the effectiveness of risk management. This function is realized, among others, by:

1. Monitoring and reviewing the risk management process, both at the local government level and the OPD level;

2. Assessing the maturity level of risk management implementation, both at the regional government level and at the OPD level;

3. An audit of the risk management process, both at the local government level and at the OPD level;

4. We are providing consulting services and assistance for the application of risk management within local governments when requested.

However, in practice, there is still confusion at the leadership level regarding the differences between the particular risk management unit and the internal auditor. One of the interviewees said that the risk management unit should be at the Provincial Inspectorate as the government's internal auditor. This is not appropriate because, in the risk management process, internal auditors should not play several roles, such as designing risk management, making decisions about risk responses and setting risk appetite.

Fourth Line of Defense

Based on the research results, the variable of risk management structure in local governments is not only influenced by three lines of Defense as a model, but the implementation of risk management should be the responsibility of all parties involved in an organization so that the role of other parties is needed. The informants revealed this that it is necessary to define and clarify roles, authorities, responsibilities and accountability related to the implementation of risk management, namely the presence of an agency leader who has full accountability for risk management; there is a risk management work unit that is independent of other functions; there is a risk owner unit whose responsibility has been firmly determined; there is a unit that ensures the effectiveness of risk management implementation; There is a unit that supervises the implementation of the risk management process so that risk management can improve performance, encourage innovation and support the achievement of the agency's strategic goals. The application of risk management is risk management which is an inseparable part of the leadership and governance of an institution where there must be clarity on the roles and responsibilities of each position in risk management and oversight as well as the establishment of a work unit in a risk management structure consisting of three layers of Defense accordingly. With its accountability, namely the risk owner unit, the risk management unit, the internal audit unit and even the capacity of its responsibility to be increased to a five-layer defence, by involving all other related parties, namely the external auditor unit and the law enforcement unit, so that risk management can create and protect objectives. And agency strategic objectives.

Based on this fact, it is the basis for the novelty, which was originally from three lines of Defense to five lines of Defense as a model. The five lines of Defense serve as a model that has an essential component in working together, in which the fourth line of Defense is carried out by the external audit function / external supervisor, either carried out by the Audit Board of the Republic of Indonesia and/or Government Internal Supervisory Apparatus outside local government agencies. This function provides adequate assurance (assurance) on the effectiveness of risk management implementation. As the Fifth Line, Defense is carried out by Law Enforcement Officials (APH) both by the Corruption Eradication Commission (KPK), the Attorney General's Office of the Republic of Indonesia, the Indonesian Police. This function provides limited assurance on the effectiveness of risk management and internal control frameworks to prove illegal acts that may cause state financial losses and/or potential financial losses, as shown in the following figure:

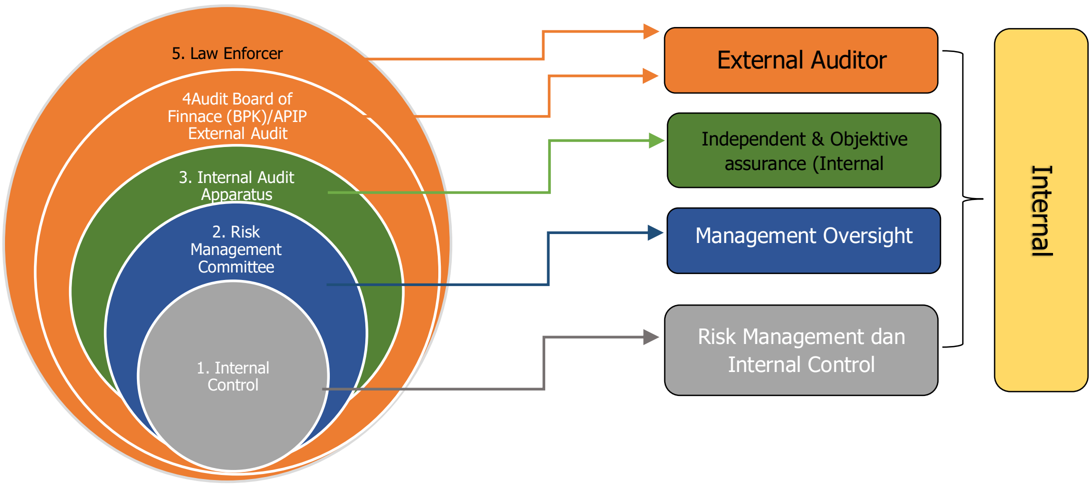

Figure 4 Five Lines of Defence

As the fourth layer of The Five Lines Of Defense Model, the role of external auditors carried out by the Supreme Audit Agency (BPK) of the Republic of Indonesia and/or APIP outside the APIP local government agencies, including the Inspectorate General of the Ministry in managing risks, especially fraud risk can only be achieved by using a systematic and methodological approach to assess and improve the effectiveness of the risk management process through assurance assignments, primarily through fraud risk assessments and providing recommendations for fraud risk mitigation.

The duties and powers of the BPK include examining the management and accountability of state finances at the central government, local governments, other state institutions, Bank Indonesia, state-owned enterprises, public service agencies, regional-owned enterprises, and other institutions or agencies that manage state finances. And can report criminal elements found during the examination to the competent authority following the provisions of laws and regulations. Its role as oversight is carried out to ensure that government entities carry out good state financial governance and comply with applicable laws and regulations and also play a role in preventing fraud, fraud, waste, abuse and mismanagement in the management and responsibility of state finances. This function is carried out by encouraging efforts to eradicate corruption, increase transparency, ensure the implementation of accountability, and increase the economy, efficiency, ethics, the value of justice and effectiveness.

Its role as insight is expected to provide opinions on programs, policies, and operations that are performing well; suggest best practices to serve as a reference; means institutional efforts to improve cross-sectoral relations within government as well as in better and more suitable match between government and non-governmental partners to achieve meaningful outcomes for the state and society. This function is carried out by exploring public policies and issues.

Based on the results of the BPK's research, it has not carried out a specific objective examination of the effectiveness of risk management in local governments. However, the BPK annually conducts a financial audit of the fairness of the financial statements of all regional governments. One of the scopes of the financial audit is an examination of the effectiveness of the internal control system reliability. BPK is the Government Internal Supervisory Apparatus (APIP) outside the APIP of local government agencies. The scope of supervision is independent and objective in assurance activities and consulting activities, which are designed to add value and improve the operations of an organization. These activities help the organization achieve its objectives by using a systematic and orderly approach to assess and improve the effectiveness of the risk management process. Supervision of the point of risk management is an integral part of the implementation of BPK's role both as a supervisor for the performance of internal control.

The role of BPK as APIP is to carry out internal supervision which includes auditing, reviewing, evaluation, monitoring and other maintenance. Meanwhile, the role of BPK as a supervisor of the government's internal control system is manifested in the formulation of technical guidelines for risk management implementation; risk management socialization; risk management education and training; risk management guidance and consulting; and increasing competence related to risk management and having the task of carrying out government affairs in the field of state / regional financial supervision and national development. In carrying out these tasks, one of the functions of the BPK is to carry out internal supervision of state / local financial accountability and national development including cross-sectoral activities, state general treasury activities based on stipulations by the Minister of Finance as State General Treasurer and other activities based on assignments from the President.

The risk management evaluation conducted by the BPK is to ensure that the risk management framework is running effectively. From the results of this evaluation, improvements can also be made to increase the effectiveness of the risk management framework. The risk management evaluation process can be carried out in three types of evaluation, namely whether all elements of the standard are present and functioning correctly, meaning that the principles, frameworks and risk management processes are already in practice and functioning (Conformance Assessment); whether all these components have functioned and operated as an integrated risk management unit in the process of government administration so that the maturity level of the implementation of risk management can be assessed effectively following the previously established specifications (Control Effectiveness Assessment).

In maintaining state / regional financial accountability towards excellent and clean governance, according to the concept of The Three Lines Of Defense. APIP can carry out educational, preventive, and repressive activities. In the educational pillar, actions can be carried out to build an anti-corruption culture in society and at the apparatus level through a series of programs for understanding, strengthening, and empowering APIP. As for preventive activities, which focus on creating synergy in good Governance, Risk and Control (GRC), APIP in developing quality assurance activities for priority programs and activities of local governments, encourages the implementation of spip, fraud control. plan, risk management based on fraud risk assessment, bureaucratic reform, and integrity zone. Whereas in the repressive pillar, APIP can play an active role in the implementation of investigative audits, auditing the calculation of state financial losses, state / regional financial loss recovery programs, and monitoring of fraud risk mitigation.

Furthermore, to achieve optimal results, APIP needs to resolve obstacles in implementing these programs which include the dilemma of political will versus conflict of interest, limited resources including the number and quality of auditors, lack of guidance for repressive tasks, lack of experience, and not yet or lack of application of the reward system. In supporting the spirit of the government in development programs for the realization of public welfare, related to the problems that arise, it is necessary to have an early warning system which demands the role of APIP in the form of prevention, detection, investigation and recovery towards better accountability in carrying out the main tasks and functions of government agencies.

External APIP has a push for performance and risk-based planning, updating audit charters to accommodate commitments for repressive actions, establishing regulations related to audit procedures for specific objectives including investigative auditing, mapping auditor competence, and running a quality assurance improvement program (QAIP) in activities supervision.

Fifth Line of Defense

Law enforcement apparatus is an institution or agency that is authorized by law to enforce the law concerning the judicial process which is defined as the process of displacing legal norms as a code of conduct in the life of the community, nation and state to create a safe and orderly situation. for the success of national development to create a just and prosperous society as mandated in the 1945 Constitution.

In carrying out countermeasures to prove that there are acts against the law that can cause state financial losses and/or potential financial losses, it means discussing a comprehensive criminal justice system, meaning that it can be seen from the normative system, namely as a set of legal rules that reflect illegal values. Against wrong or despicable actions. On the other hand, it can also be approached as an administrative system that demonstrates the law enforcement mechanism carried out by the state apparatus or law enforcement apparatus. To realize the effectiveness and efficiency of the implementation of the internal audit function, both internal and external APIs need to collaborate and coordinate with Law Enforcement Officials (APH) following the prevailing laws and regulations.

The Internal Control System is a necessary process for actions and activities carried out continuously by the leadership and all employees to provide adequate confidence in the achievement of organizational goals through effective and efficient workouts, reliability of financial reporting, safeguarding state assets, and compliance with laws and regulations. Invitation. As a necessary process, SPIP includes elements that regulate human behaviour (soft control) and activity procedures (rigid control). Therefore, SPIP implemented in government agencies will be able to minimize and eliminate employee motivation (smooth control) and opportunities (rigid control) to commit fraud (fraud) in achieving organizational goals. Thus, APH is a useful tool in efforts to prevent fraud which is essentially an effort to eliminate and minimize motivation and opportunities for committing fraud.

V. CONCLUSION

The risk management structure that describes the division of tasks and responsibilities in risk management, using the three lines of defence model approach has not been established; this can be seen from 1) the risk management structure has not played a role as stipulated in the risk management policy. 2) The existence and role of the particular risk management unit are still not understood, both in terms of regulations and understanding by the leaders of regional apparatus organizations. 3) The novelty of the research results that affect the risk management structure, namely the fourth line of Defense carried out by the audit function external either carried out by BPK RI and / or BPK and as the Fifth Line of Defense carried out by Law Enforcement Officials (APH) either by the KPK, Attorney General's Office, Police.

Apart from involving the Three Lines of Defense, an effective risk management structure also affects all other related parties, namely the Fourth line of Defense which is carried out by the external audit function and the fifth line of Defense which is carried out by the role of the Law Enforcement Officials (APH). With the involvement of stakeholders adequately, it will make them willing to share their knowledge, views and perceptions for consideration. The result of this process is increased awareness of the parties involved and the application of mature risk management.

If designed and implemented accountably, the risk management structure will be able to ensure that the risk management process will become an integral part of all government management processes, including the decision-making process and will be able to capture changes that occur in the internal and external context.

ACKNOWLEDGEMENTS

Researchers would like to thank several local governments in Indonesia who are willing to be the object of research as well as leaders of regional work units who are willing to conduct interviews.

REFERENSI

1. Abrahamsen, R. (2004). The power of partnerships in global governance. *Third World*

Quarterly, *25*(8), 1453–1467. https://doi.org/10.1080/01436590420003084 65

2. Adamec, B. A., Rexroad, W. M., Leinicke, L. M., & Ostrosky, J. A. (2002). Internal reflection: management's self-assessment of its performance can be an effective and powerful way to enhance an organization's control processes. *Internal Auditor*, *59*(6), 56–63.
3. Addink, H. (2019). *Good governance: Concept and context*. Oxford University Press.
4. Agrawal, D. R., Hoyt, W. H., & Wilson, J. D. (2020). Local Policy Choice: Theory and Empirics. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3545542
5. Agrifoglio, R., Metallo, C., & di Nauta, P. (2020). Understanding Knowledge Management in Public Organizations through the Organizational Knowing Perspective: a Systematic Literature Review and Bibliometric Analysis. *Public Organization Review*, 1–20. https://doi.org/10.1007/s11115-020-00480-7
6. Anderson, D. J., & Eubanks, G. (2015). Leveraging COSO across the three lines of Defense. *Committee of Sponsoring Organizations of the Treadway Commission*.
7. Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society*, *35*(7), 659–675.
8. Arts, B. (2014). Assessing forest governance from a 'Triple G'perspective: Government, governance, governmentality. *Forest Policy and Economics*, *49*, 17–22.
9. Arwinge, O., & Olve, N.-G. (2017). 12 Three Lines of Defense for Organizing Risk Management. *Bank Regulation: Effects on Strategy, Financial Accounting and Management Control*, 284.
10. Auditors, I. of I. (2013). *The three lines of Defense in effective risk management and control*.
11. Aziz, N. A. A., Manab, N. A., & Othman, S. N. (2016). Sustainability Risk Management (SRM): An extension of Enterprise Risk Management (ERM) concept. *International Journal of Management and Sustainability*, *5*(1), 1–10.
12. Bartlett, D., & Dibben, P. (2002). Public sector innovation and entrepreneurship: Case studies from local government. *Local Government Studies*, *28*(4), 107–121. https://doi.org/10.1080/714004159
13. Basu, I., Brown, G. K., & Devine, J. (2017). Governance, rights and the demand for democracy: Evidence from Bangladesh. In *Politics and Governance in Bangladesh: Uncertain Landscapes* (pp. 86–106). Routledge.
14. Basu, I., Devine, J., & Wood, G. (2017). Politics and governance in Bangladesh: Uncertain landscapes. In *Politics and Governance in Bangladesh: Uncertain Landscapes*. https://doi.org/10.4324/9781315201337
15. Beasley, M. S., Branson, B. C., & Hancock, B. V. (2010). Developing key risk indicators to strengthen enterprise risk management. *ERM Initiative at North Carolina State University and the Committee of Sponsoring Organizations of the Treadway Commission, Raleigh, NC*.
16. Beeri, I., Uster, A., & Vigoda-Gadot, E. (2019). Does Performance Management Relate to Good Governance? A Study of Its Relationship with Citizens' Satisfaction with and Trust in Israeli Local Government. *Public Performance and Management Review*, *42*(2), 241–279. https://doi.org/10.1080/15309576.2018.1436074
17. Bento, R. F., Mertins, L., & White, L. F. (2018). Risk management and internal control: A study of management accounting practice. In *Advances in Management Accounting* (Vol. 30, pp. 1–25). https://doi.org/10.1108/S1474-787120180000030002
18. Bogue, R. L. (2005). Use SMART goals to launch management by objectives plan. *Retrieved November 15*, 2010.
19. Borins, S. (2000). What border? Public management innovation in the United States and Canada. *Journal of Policy Analysis and Management*, *19*(1), 46–74. https://doi.org/10.1002/(SICI)1520-6688(200024)19:1<46::AID-PAM4>3.0.CO;2-Z
20. Borins, S. (2001). Public management innovation: Toward a global perspective. *American Review of Public Administration*, *31*(1), 5–21. https://doi.org/10.1177/02750740122064802

21. Bozhikin, I., Macke, J., & da Costa, L. F. (2019, July 20). The role of government and key non-state actors in social entrepreneurship: A systematic literature review. *Journal of Cleaner Production*, Vol. 226, pp. 730–747. https://doi.org/10.1016/j.jclepro.2019.04.076
22. Brief, A. P., & Aldag, R. J. (1981). The "Self" in Work Organizations: A Conceptual Review. *Academy of Management Review*, *6*(1), 75–88. https://doi.org/10.5465/amr.1981.4288006
23. 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
24. Brown, L., & Osborne, S. P. (2013). Risk and Innovation: Towards a framework for risk governance in public services. *Public Management Review*, *15*(2), 186–208. https://doi.org/10.1080/14719037.2012.707681
25. Chaffin, B. C., Gosnell, H., & Cosens, B. A. (2014). A decade of adaptive governance scholarship: synthesis and future directions. *Ecology and Society*, *19*(3).
26. Chapman, R. J. (2011). Simple tools and techniques for enterprise risk management. 2006. *John Wiley&Sons*.
27. Chris, A., & Alison, G. (2008). Collaborative Governance in Theory. *Journal of Public Administration Research and Theory* , *18*(4), 917–946. https://doi.org/10.1093/JOPART
28. Christensen, T., Lægreid, P., & Rovik, K. A. (2020). *Organization theory and the public sector: Instrument, culture and myth*. Routledge.
29. Clarke, C. J., & Varma, S. (1999). Strategic risk management: The new competitive edge. *Long Range Planning*, *32*(4), 414–424. https://doi.org/10.1016/s0024-6301(99)00052-7
30. 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.
31. Conchúir, D. Ó., & Conchúir, D. Ó. (2010). Risk Management Processes. *Overview of the PMBOK® Guide*, 1–1. https://doi.org/10.1007/978-3-642-11188-4_11
32. Crawford, M. H., Crowley, K., Potter, S. H., Saunders, W. S. A., & Johnston, D. M. (2018). Risk modelling as a tool to support natural hazard risk management in New Zealand local government. *International Journal of Disaster Risk Reduction*, *28*, 610–619. https://doi.org/10.1016/j.ijdrr.2018.01.011
33. Davies, H., & Zhivitskaya, M. (2018). Three Lines of Defence: A Robust Organising Framework, or Just Lines in the Sand? *Global Policy*, *9*, 34–42. https://doi.org/10.1111/1758-5899.12568
34. Doran, G. T. (1981). There's a SMART way to write management's goals and objectives. *Management Review*, *70*(11), 35–36.
35. Eaton, K., Faguet, J.-P., Harbers, I., Schakel, A. H., Hooghe, L., Marks, G., … Shair-Rosenfield, S. (2019). Measuring and theorizing regional governance. *Territory, Politics, Governance*, *7*(2), 265–283.
36. Edwards, I., Griffith, J. N., Burton, D., & Mackey, B. (2019). Implications of emergent risk for application of risk transfer mechanisms by local governments in Queensland. *Environmental Science and Policy*, *96*, 1–8. https://doi.org/10.1016/j.envsci.2019.02.006
37. Finger, M., & Brand, S. B. (1999). The concept of the learning organization applied to the transformation of the public sector: Conceptual contributions for theory development. *Organizational Learning and the Learning Organization: Developments in Theory and Practice*, 130–156.
38. Fraser, J. R. S. (2016). The role of the Board in risk management oversight. *The Handbook of Board Governance: A Comprehensive Guide for Public, Private, and Not-for-Profit Board Members*, *283*.
39. Fraser, J., & Simkins, B. (2010). *Enterprise risk management: Today's leading research and best practices for tomorrow's executives* (Vol. 3). John Wiley & Sons.
40. Frigo, M. L. (2003). Mission-driven strategy. *Strategic Finance*, *85*(2), 8.
41. Gisselquist, R. M. (2012). *Good governance as a concept, and why this matters for*

development policy. WIDER Working Paper.
42. Guliyeva, S. (2020). Enterprise Risk Management Strategy. In *55 the International Scientific Conference on Economic and Social Development-Baku*.
43. Haliah, H., & Nirwana, N. (2019). The development of good governance model for performance improvement. *International Journal of Excellence in Government*, *1*(1), 21–36. https://doi.org/10.1108/ijeg-09-2018-0004
44. Hardy, K. (2010). *Managing risk in government: An introduction to enterprise risk management*. IBM Center for the Business of Government Washington, DC.
45. Hardy, K. (2014). *Enterprise risk management: A guide for government professionals*. John Wiley & Sons.
46. Hood, J., & McGarvey, N. (2002). Managing the risks of public-private partnerships in Scottish local government. *Policy Studies*, *23*(1), 21–35.
47. Hopkin, P. (2018). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*. Kogan Page Publishers.
48. Hout, W. (2009). Development and governance: An uneasy relationship. *Governance and the Depoliticisation of Development, London: Routledge*, 29–43.
49. 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
50. Jan Kopia, Vanessa Just, Wiebke Geldmacher, A. B. (2017). Organization Performance and Enterprise Risk Management. *Ecoforum*, *6*(1), 0–0.
51. Jugend, D., Fiorini, P. D. C., Armellini, F., & Ferrari, A. G. (2020). Public support for innovation: A systematic review of the literature and implications for open innovation. *Technological Forecasting and Social Change*, *156*, 119985. https://doi.org/10.1016/j.techfore.2020.119985
52. Kapucu, N., & Hu, Q. (2020). *Network Governance: Concepts, Theories, and Applications*. Routledge.
53. Kaufmann, D., Kraay, A., & Mastruzzi, M. (2003). *Governance matters III: Governance indicators for 1996–2002*. The World Bank.
54. Khouya, M., & Benabdelhadi, A. (2020). Good Governance And Its Impact On Economic Development: A Systematic Literature Review. *Finance, Auditing, Management and Economics*, *1*(1), 47–67. https://doi.org/10.5281/zenodo.3936217
55. Kim, E. H., & Lu, Y. (2011). CEO ownership, external governance, and risk-taking. *Journal of Financial Economics*, *102*(2), 272–292.
56. Knechel, W. R., & Willekens, M. (2006). The role of risk management and governance in determining audit demand. *Journal of Business Finance & Accounting*, *33*(9-10), 1344–1367.
57. Koppenjan, J., & Koliba, C. (2013). Transformations towards new public governance: Can the new paradigm handle complexity? *International Review of Public Administration*, *18*(2), 1–8. https://doi.org/10.1080/12294659.2013.10805249
58. Koprić, I. (2012). Managing Public Affairs in South-Eastern Europe: Muddled Governance. *Governance: Is It for Everyone*, 25–47.
59. Langfield-Smith, K., & Smith, D. (2003). Management control systems and trust in outsourcing relationships. *Management Accounting Research*, *14*(3), 281–307. https://doi.org/10.1016/S1044-5005(03)00046-5
60. Leblanc, R. (2020). *The handbook of board governance: A comprehensive guide for public, private, and not-for-profit board members*. John Wiley & Sons.
61. Leftwich, A. (1993). Governance, democracy and development in the Third World. *Third World Quarterly*, *14*(3), 605–624. https://doi.org/10.1080/01436599308420345
62. Lemos, M. C. (2007). Drought, governance and adaptive capacity in North East Brazil: A case study of Ceará. *Occasional Paper for UNDP*, *2008*.
63. 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

64. Li, G., & Wu, Z. (2020). Research on Innovation and Governance of Local Government. *International Public Management Journal*, *23*(3), V–IX.
65. Li, S., Park, S. H., & Li, S. (2003). The great leap forward: The transition from relation-based governance to rule-based governance. *Organizational Dynamics*, *33*(1), 63–78.
66. Long, J. (1975). The Impact of Scale on Management Structures and Processes. *Local Government Studies*, *1*(2), 45–59. https://doi.org/10.1080/03003937508432647
67. Luburic, R., Perovic, M., & Sekulovic, R. (2015). Quality Management in terms of strengthening the "Three Lines of Defence "in Risk Management-Process Approach. *International Journal for Quality Research*, *9*(2), 243–250.
68. Luko, S. N. (2013). Risk management principles and guidelines. *Quality Engineering*, *25*(4), 451–454.
69. Lundqvist, S. A. (2014). An Exploratory Study of Enterprise Risk Management. *Journal of Accounting, Auditing & Finance*, *29*(3), 393–429. https://doi.org/10.1177/0148558X14535780
70. Manz, C. C., Mossholder, K. W., & Luthanvs, F. (1987). An Integrated Perspective of Self-Control in Organizations. *Administration & Society*, *19*(1), 3–24. https://doi.org/10.1177/009539978701900101
71. Mathieu, A., Rennotte, C., Romain, F., Vosse, B., & Al Shehri, S. (2017). Strategic asset management implementation (SAMI) at National Grid, Saudi Arabia. *2017 Saudi Arabia Smart Grid (SASG)*, 1–6. IEEE.
72. McLucas, A. C. (2003). *Decision making: risk management, systems thinking and situation awareness*. Argos Press P/L.
73. McShane, M. (2018). Enterprise risk management: history and a design science proposal. *Journal of Risk Finance*, *19*(2), 137–153. https://doi.org/10.1108/JRF-03-2017-0048
74. Mearns, K., Flin, R., & O'Connor, P. (2001). Sharing' worlds of risk'; improving communication with crew resource management. *Journal of Risk Research*, *4*(4), 377–392. https://doi.org/10.1080/13669870110063225
75. Meyer, N., Meyer, D., & Kot, S. (2017). The development of a process tool for improved risk management in local government. *Calitatea*, *18*(S1), 425.
76. Moeller, R. R. (2007). *COSO enterprise risk management: understanding the new integrated ERM framework*. John Wiley & Sons.
77. Moeller, R. R. (2011). *COSO enterprise risk management: establishing effective governance, risk, and compliance processes* (Vol. 560). Wiley Online Library.
78. Otley, D. (1994). Management control in contemporary organizations: Towards a wider framework. *Management Accounting Research*, *5*(3–4), 289–299. https://doi.org/10.1006/mare.1994.1018
79. Oulasvirta, L., & Anttiroiko, A. V. (2017a). Adoption of comprehensive risk management in local government. *Local Government Studies*, *43*(3), 451–474. https://doi.org/10.1080/03003930.2017.1294071
80. Oulasvirta, L., & Anttiroiko, A. V. (2017b). Adoption of comprehensive risk management in local government. *Local Government Studies*, *43*(3), 451–474. https://doi.org/10.1080/03003930.2017.1294071
81. Pablo, A. L., Reay, T., Dewald, J. R., & Casebeer, A. L. (2007). Identifying, enabling and managing dynamic capabilities in the public sector. *Journal of Management Studies*, *44*(5), 687–708. https://doi.org/10.1111/j.1467-6486.2006.00675.x
82. Pahl-Wostl, C. (2019). Governance of the water-energy-food security nexus: A multi-level coordination challenge. *Environmental Science and Policy*, *92*, 356–367. https://doi.org/10.1016/j.envsci.2017.07.017
83. Peters, B. G., & Pierre, J. (1998). Governance Without Government? Rethinking Public Administration. *Journal of Public Administration Research and Theory*, *8*(2), 223–243. https://doi.org/10.1093/oxfordjournals.jpart.a024379

84. Potter, P., & Toburen, M. (2016). The 3 lines of Defense for risk management. *Risk Management*, *63*(5), 16–18.
85. Power, M. (2004). *The risk management of everything: Rethinking the politics of uncertainty*. Demos.
86. Provan, K. G., & Kenis, P. (2008). Modes of network governance: Structure, management, and effectiveness. *Journal of Public Administration Research and Theory*, *18*(2), 229–252.
87. Purdy, G. (2010, June 1). ISO 31000:2009 - Setting a new standard for risk management: Perspective. *Risk Analysis*, Vol. 30, pp. 881–886. https://doi.org/10.1111/j.1539-6924.2010.01442.x
88. Rhodes, R. A. W. (1996). The New Governance: Governing without Government. *Political Studies*, *44*(4), 652–667. https://doi.org/10.1111/j.1467-9248.1996.tb01747.x
89. Righetti, T. K. (2020). *Collaborative Pipeline Risk Governance: A Response to Professor Gosman*.
90. Roberts, A. (2020). *Strategies for Governing: Reinventing Public Administration for a Dangerous Century*. Cornell University Press.
91. Rochette, M. (2009). From risk management to ERM. *Journal of Risk Management in Financial Institutions*, *2*(4), 394–408.
92. Rockafellar, R. T., & Uryasev, S. (2013). The fundamental risk quadrangle in risk management, optimization and statistical estimation. *Surveys in Operations Research and Management Science*, *18*(1–2), 33–53. https://doi.org/10.1016/j.sorms.2013.03.001
93. Rodríguez Bolívar, M. P., Navarro Galera, A., Alcaide Muñoz, L., & López Subirés, M. D. (2016). Risk Factors and Drivers of Financial Sustainability in Local Government: An Empirical Study. *Local Government Studies*, *42*(1), 29–51. https://doi.org/10.1080/03003930.2015.1061506
94. Rodrik, D. (2001). *The global governance of trade: as if development really mattered* (Vol. 58). UNDP New York.
95. Roeschmann, A. Z. (2014). Risk Culture: What It Is and How It Affects an Insurer's Risk Management. *Risk Management and Insurance Review*, *17*(2), 277–296. https://doi.org/10.1111/rmir.12025
96. Rose, N., & Miller, P. (1992). Political Power beyond the State: Problematics of Government. *The British Journal of Sociology*, *43*(2), 173. https://doi.org/10.2307/591464
97. Sadgrove, K. (2016). *The complete guide to business risk management*. Routledge.
98. Saidon, I. M., & Said, R. (2020). *Ethics, Governance and Risk Management in Organizations*. Springer.
99. Scharpf, F. W. (1997). Economic integration, democracy and the welfare state. *Journal of European Public Policy*, *4*(1), 18–36.
100. Schomaker, R. M., & Bauer, M. W. (2020). Public Governance in the MENA Region: Reform Trends and Patterns. *International Journal of Public Administration*, *43*(5), 378–391. https://doi.org/10.1080/01900692.2019.1669179
101. Senior, B., & Fleming, J. (2006). *Organizational change*. Pearson Education.
102. Shah, A. (2006). *Corruption and decentralized public governance*. The World Bank.
103. Torfing, J., Andersen, L. B., Greve, C., & Klausen, K. K. (2020). *Public Governance Paradigms: Competing and Co-existing*. Edward Elgar Publishing.
104. Van Asselt, M. B. A., & Renn, O. (2011). Risk governance. *Journal of Risk Research*, *14*(4), 431–449. https://doi.org/10.1080/13669877.2011.553730
105. Vivek, S. D., Richey, R. G., & Dalela, V. (2009). A longitudinal examination of partnership governance in offshoring: A moving target. *Journal of World Business*, *44*(1), 16–30. https://doi.org/10.1016/j.jwb.2008.03.017
106. Von Hagen, J., & Harden, I. J. (1995). Budget processes and commitment to fiscal discipline. *European Economic Review*, *39*(3–4), 771–779. https://doi.org/10.1016/0014-2921(94)00084-D

107. Weiss, T. G. (2000). Governance, good governance and global governance: Conceptual and actual challenges. *Third World Quarterly*, *21*(5), 795–814. https://doi.org/10.1080/713701075
108. Wu, J., & Walker, R. M. (2020, May 3). Public management in China: reform, innovation and governance. *International Public Management Journal*, Vol. 23, pp. v–ix. https://doi.org/10.1080/10967494.2020.1784646