MAPPING KNOWLEDGE RISKS AND IMPLEMENTING KNOWLEDGE RISK MANAGEMENT THE CASE STUDY OF INDONESIA'S FINANCIAL AND DEVELOPMENT SUPERVISORY BOARD

Isabella Ishak[1], Djabir Hamzah[2], Nurdjanah Hamid[3]

[1] Magister Management, Faculty of Economics and Business, Hasanuddin University; isabella.ishak@yahoo.com
[2] Faculty of Economics and Business, Hasanuddin University; e-mail@e-mail.com
[3] Faculty of Economics and Business, Hasanuddin University; e-mail@e-mail.com

Abstract

This study aims to describe the framework for implementing knowledge risk management by identifying knowledge risks based on their categories, RM-based KM practice designs and the techniques needed to be able to integrate them. This research uses a case study method with a qualitative approach in one of the government agencies in Indonesia, namely the Financial and Development Supervisory Board (BPKP). After applying KRM implementation techniques in the organization, it is known from the data analysis results that knowledge risk at the organizational level consists of three main categories, further subdivided into several knowledge risks. These three categories are included in the RM-based KM design (also known as knowledge risk management). This research still has limitations because it uses data sources from the 2008 organizational reports. However, this research is expected to be a reference and basis for designing a more effective KRM framework and implementation, adapted to the knowledge risks of public organizations.

Keywords : *knowledge risks; knowledge management; risk management; knowledge risk management*

A. INTRODUCTION

Until recently, Knowledge was a commodity that associations had to manage and use with style (Durst, 2012; Massingham, 2010; Stam, 2009). Similarly, knowledge continues to develop and accumulate within organizations and is used in organizational life. The concept of knowledge management (hereafter referred to as KM) is actually an old concept, as old as the age of mankind in this world. Organizations concentrate on locating and developing the appropriate knowledge to be profitable and accomplish their objectives because the development of KM has expanded beyond propositions to include practices, processes, conditions, tools, and other implicit behaviors (Durst & Zieba, 2019).

KM is considered as a key element in the renewal of corporate risk management (Neef, 2005). In this case, the KM approach is to generate and select the necessary information according to the decisions to be made (Lorenz et.al., 2005). Organizations must restructure their approach to KM in light of the rapid rise of KM hazards (also known as knowledge risk, or KR), in order to take into account potential implicit KR. In comparison to knowledge loss, knowledge leakage, knowledge waste, or knowledge concealment, there hasn't been much debate about knowledge redistribution (KR) in the past (Durst and Zieba, 2019).

In the business sector, KM has been continuously implemented and developed. Rapidly developing and modern companies have effectively applied knowledge risk management (KRM) ways to prevent operational losses and ethical violations. As an illustration, Intel, Novo Nordisk, and Nike have worked hard to develop innovative RM strategies based on knowledge management (Neef, 2005). On the other hand, research on KRM in government agencies is still limited. This paper is a follow-up research referring to the KR taxonomy developed by Durst &

Zieba (2019). The Financial and Development Supervisory Board (BPKP), one of the government organizations in Indonesia, will be used as a case study to examine the applicability of knowledge risk categories at the organizational level. The KRM framework developed by Lorenz et al. (2005) follows the discussion of knowledge risks in organizations, which are divided into human, technological, and operational risks and the KRM implementation techniques created by Neef (2005).

B. LITERATURE REVIEW

Knowledge

Knowledge, which is a dynamic, mortal process (Nonaka & Takeuchi, 1995), provides a specific belief in a reality. The concept of knowledge is not just what is learned from books or mentors; it also includes accumulated experience that a person gains from their surroundings (Davenport & Prusak, 1998). Davenport & Prusak (1998) describe knowledge as a set of combinations of experiences, values, information, and insights that includes an evaluative framework and current information.

According to Nold (2011), data is a collection of meaningless facts, words, sounds, numbers, observations, or images that exist but aren't processed or organized into information that people and organizations can use. Data is transformed into information, which is then transformed into knowledge. The knowledge that results from the ingestion and analysis of information by individuals is defined as "justified beliefs based on personalized information (which may be new or old, unique, useful, or accurate) about facts, observations, interpretations, procedures, ideas, concepts, and judgments" (Nold, 2011). Michael Polanyi (1966) created a well-known model of knowledge that separates information into tacit and explicit sources. Explicit knowledge is recorded, placed into databases, or other easily shareable systems inside businesses (Lee & Choi, 2003). A mix of cognitive and technological processing factors obtained from experience is how tacit knowledge is understood. The technical processing dimension includes knowledge, skills, and expertise acquired from one's experiences over time, the cognitive processing dimension, on the other hand, consists of the mental models, perspectives, and beliefs that are developed over time and selected through individual perceptions (Nold, 2011).

Knowledge Risks (KR)

There are insufficient definitions and descriptions of the issues associated with knowledge risk in the literature (Durst & Zieba, 2019). information risk is the potential for losses that might lower or obstruct an organization's operational or strategic goals as a result of the identification, preservation, or storage of information, according to Perrot (2007). However, it is first required to understand risk in order to proceed with the discussion of KR. The word risk derives from the old Italian verb *risicare*, which means "to dare," where danger is not a matter of fate but rather a decision (Bernstein, 1996). It is beneficial that risk is discussed in business literature, because taking risks is a constructive action that fosters innovation (Schumpeter, 1934). Massingham (2010) explains that risk indicates the possibility of something going wrong. Another view defines risk as the likelihood and severity of adverse impacts/consequences (Haimes, 2009). It's crucial to take into account what went wrong, the possibility of it happening again, and the effects while doing a risk analysis (Kaplan & Garrick, 1981).

An individual's response to risk is a function of the individual's perception of the risk as either completely random or manageable (Massingham, 2010). This view suggests that while risks cannot be eliminated, they can at least be anticipated and then activities can be implemented to reduce their impact. Knowledge risk provides a measure for the likelihood along with severity of adverse consequences resulting from any activity involving or linked to

information that may eventually impede organizational functioning at various levels (Durst and Zieba, 2019). Additionally, knowledge risk is separated into three categories by Durst and Zieba (2019): operational risk, technological risk, and human risk. Human knowledge risk, such as the risk of concealing knowledge, are connected to the management of human resources and include personal, social, cultural, and psychological aspects of an individual. The use of technology, such as information and communication technology (ICT), introduces technological knowledge dangers. Examples include organizations that still use outdated technology and hacking. Finally, operational knowledge risk includes risks from routine operations and organizational functions, such as alliances, mergers, outsourcing, and using incorrect or outdated knowledge.

Knowledge Management (KM)

According to Baskerville and Dulipovici (2006), knowledge management (KM) is a collection of actions for producing, acquiring, sharing, and utilizing information that is based on trust, or for integrating organizational and technology solutions and reusing knowledge to enhance individual and organizational learning (Jennex, 2007 in Massingham et al., 2018). According to Jain and Jeppesen (2013), KM refers to a variety of strategies and tactics used to advance corporate objectives.

Knowledge Risk Management (KRM)

The discussion of KRM is still relatively new in academic research, where this concept combines two previously separate concepts, namely RM and KM (Massingham, 2010). Massingham (2010) further explains that KRM research has focused on two concepts. De Zoysa and Russell's (2003) study on how knowledge can help identify, measure, and respond to risk as well as Verhaegen's (2005) and Otterson's (2005) studies on how knowledge influences decision-making are just a few examples of research that demonstrates the function of knowledge as risk mitigation and leads to more effective RM implementation. Second, scientists have looked at how KM procedures might enhance RM. For instance, research by Marshall et al. (1996) highlighted a variety of KM "generators" as strategies to mitigate the negative consequences of RM, including leveraging knowledge for decision making, enhancing access to knowledge, and developing knowledge-based controls and systems. Numerous research have examined the similarities between risk management and knowledge management, including the need for perception among employees, their sense of values, and their behaviors as a result of lessons learned, and have come to the conclusion that these similarities exist (Neef, 2005). Knowledge mapping, communities of practice, and expert tagging are just a few examples of typical KM approaches that have been recommended by other research (Massingham, 2010).

C. RESEARCH METHOD

Location and Research Design

This research uses a single case study method, which was chosen because it is an appropriate method for conducting management research, especially in the public sector (Riege & Lindsay, 2006; Zainal, 2007). Because the organizational processes discussed in this research about the relationship between risk and knowledge cannot be readily quantified, a qualitative approach was selected (Van Maanen, 1979). The organization used as a case study is one of the government agencies in Indonesia, namely the Finance and Development Supervisory Board. Its primary responsibility is to manage government activities in the areas of national/regional financial supervision and national development. This organization is an internal government supervisory apparatus that reports to and is accountable to the President. This organization was selected for two reasons. First, the Development Finance and Supervision Agency is a

government agency that performs and reports its duties directly to the President, and the majority of its employees are auditors, so knowledge becomes the most important resource to adequately perform its duties, mission, and function. Secondly, the author is an auditor who has been part of the organization for about 10 years, so the author has access to data and information related to this research.

Analysis Method

The case description was developed using a conceptual framework selected based on a literature review, business process observation, and document analysis to understand the KM context and application. The analysis section has three objectives: first, to outline the knowledge risks that may occur in the organization using the knowledge risk framework developed by Durst and Zieba (2019) (see Table 1); second, to describe the KRM framework created by Lorenz et al. (2005), which has been modified (see Figure 1 and Table 2); and third, to explain the KRM integration methods and systems created by Neef (2005) (see Table 3).

Table-1: Knowledge Risk at Organisational Level

No	Knowledge Risks Categories	Examples of Knowledge Risk Categories
1	The Risks of Human Knowledge	a. Knowledge hiding b. Knowledge hoarding c. Unlearning d. Forgetting e. Organizational members' lack of or insufficient competencies
2	Technology Risk	a. Risks related to cybercrime b. Risk related to old technologies c. Digitalization risks d. Risk related to social media
3	Operatios Risks	a. Knowledge waste b. Risks related to knowledge gaps c. Relational risks d. Knowledge outsourcing risks e. Risk of using obsolete/unreliable knowledge f. Risk of improper knowledge application g. Espionage h. Continuity risks i. Communication risks j. Knowledge acquisition risks k. Knowledge transfer risks l. Merger & acquisition (M&A) risks

D. RESULTS

Human knowledge risks
Knowledge hiding and knowledge hoarding

According to Nere, Hernaus, Dysvik, and Kerlavaj (2017), knowledge hiding is the willful conduct of an employee who, for whatever reason, does not want to divulge his or her information and purposefully hides it. The process of gathering knowledge that may (or may not) be shared in the future is known as knowledge hoarding, on the other hand (Connelly et al., 2012).

Organizations have built knowledge management systems (KMS) that can accommodate employees who want to share knowledge, but the risk of knowledge hiding and knowledge hoarding remains a potential problem that may occur. Lack of financial rewards, egotism, and anger with the organization are a few factors that might be to blame for this occurrence (Leonard, 2014). In addition, the risk may occur because there is no embedded knowledge sharing culture in the organization. Employees do not feel compelled to share knowledge because the organization has not implemented a reward and punishment system so that employees who do or do not share knowledge are still treated equally in the organization.

Unlearning

According to De Holan (2011), unlearning is a sort of purposeful (confused) forgetting that involves leaving behind beliefs, principles, and/or behaviors that are viewed as outmoded within an organization. Although purposeful forgetting is seen as a good thing, it may sometimes result in unintended knowledge loss, which can be harmful (Durst & Zieba, 2019). In government agencies, such as the Financial and Development Supervisory Agency, this risk is less likely to occur because the organization is in the process of becoming a learning organization. According to Jabeen and Dari (2023), organizational learning is a process that enables an organization to change through time via innovation and learning from failures.

Forgetting

According to De Holan (2011), forgetting can be inadvertent (caused by a poor memory) or purposeful (done to break undesirable habits). Durst & Zieba (2019) explained that the possibility of forgetting knowledge occurs because this knowledge is rarely used, even though it is relevant to the job, so there is a need for a knowledge repository to ensure that explicit knowledge has been properly captured. In contrast, organizations may purposefully overlook specific information that impedes or delays the process of making decisions. Because the business is in the process of becoming a learning organization, there is little chance that information that is important to accomplishing the organization's goals will be forgotten.

Organizational members' lack of or insufficient competencies

According to Durst & Zieba (2019), this risk is related to organizational members who have little training, experience, competence, or competency, which might interfere with their ability to do their duties. Missing/minimal competencies can be the result of inadequate (lost) succession planning within the organization, which can lead to the loss of knowledge (Durst & Wilhelm, 2012). Additionally, organizational members' inexperience and carelessness can lead to knowledge-related hazards including the negligent disclosure of confidential firm data and knowledge (Durst & Zieba, 2019). This risk has a low probability of occurrence because the organization has currently implemented talent management, where all training, experience, and skills of all members of the organization have been documented in a system to support succession success in the organization.

Technological risks
Risks related to cybercrime

For organization, reports on the results of state / regional financial supervision and reports on the results of state / regional financial investigations are sensitive and confidential information. The risk of cybercrime will have a serious impact, especially with the risk of hacking. Hacking is an attempt by outsiders to break into an organization's computer system (especially to obtain confidential information). This attack can change data and content and damage its authenticity, which can result in the disruption or even termination of organizational processes (Durst & Zieba, 2019).

Risk related to old technologies

Durst & Zieba (2019) explain that this risk is a difficulty for public and private organizations to keep up with the enormous development of ICT. The current state of the organization has built a system that can be accessed through intranet and Internet networks, but the systems built are not fully connected to each other. So it adds time to the completion of work and the decision-making process.

Digitalization risks

The company may suffer from any overreliance on technology that disregards the human element (Durst & Zieba, 2019). This risk cannot be separated from the organization, which has

built several applications related to the financial accountability of local governments in the course of performing its duties and functions. Currently, organizations that are moving towards digital business processes must be able to face the risks of digitization.

Risk related to social media

Social media-related dangers are associated with user-generated data and material that is disseminated and supported by automated tools and bots that distribute disinformation and alternative information (Durst & Zieba, 2019). Organizations such as open and accountable government agencies also use social media to disseminate information about government oversight programs and other important information, and they may receive fake comments or content related to their duties and functions.

Operational risks
Knowledge waste

Knowledge waste is the act of intentionally not using potential and available knowledge within the organization (Durst & Aisenberg Ferenhof, 2016). By not using existing knowledge, the organization has wasted valuable resources (such as money and human labor).The higher the potential for waste of knowledge, the more it means that it is not being used within the organization (Durst & Zieba, 2019). This risk can occur in organizations seeing that the knowledge documented in the KMS is not used in the daily work.

Risks related to knowledge gaps

The knowledge gap is the gap between a term that the organization should know and whether it is really understood, and it has the ability to hinder the achievement of the objectives of the organization (Perrot, 2007). According to Durst & Zieba (2019), organizations implementing modern ICT advances run the risk of having insufficient expertise to assess the potential and usefulness of available ICT tools. Furthermore, when individuals leave an organization, previously accessible skills may no longer be available, resulting in knowledge gaps.

Relational risks, Knowledge outsourcing risks, Espionage, and Merger & acquisition (M&A) risks

The author does not discuss this risk because the relationship between this risk and the operational activities of the organization as a government agency cannot be determined.

Risk of using obsolete/unreliable knowledge, risk of improper knowledge application, and knowledge acquisition risks

When using obsolete or erroneous information, there is a risk since certain knowledge might quickly become outdated (Tan et al., 2006). Because of this, information must constantly be updated and renewed. Otherwise, an organization faces the danger of applying outdated or invalid knowledge in its operations (Durst & Zieba, 2019). This risk can occur in organizations especially if the knowledge in the KMS is not always updated, so knowledge and information must always be validated and reviewed before decisions are made.

When an organization misinterprets particular knowledge (which can happen due to a lack of capacity and abilities to critically assess this knowledge), it increases the risk of making wrong decisions (Zieba & Durst, 2018). The challenge for organizations is to be able to use knowledge appropriately when the amount of knowledge available is very large and therefore skills and abilities are needed to apply all of this knowledge (Durst & Zieba, 2019). This risk can occur when organizational resources do not make efforts to improve skills and competencies, which can lead to misinterpretation of knowledge or incorrect analysis, resulting in inappropriate decision making.

The danger of utilizing knowledge that is out-of-date or unreliable and the risk of employing the wrong knowledge are all strongly connected. According to Durst & Zieba (2019), knowledge acquisition risk is connected to the organization's capacity to acquire new knowledge required to follow new strategic orientations. New knowledge is needed for innovation or

continuous development of skills and competencies to ensure that the organization can meet current and future challenges. Organizations must be able to ensure that outdated/unreliable knowledge is not used in decision making, continuously update knowledge, and improve competencies and skills so that new knowledge and knowledge that is still relevant can be used to achieve organizational goals.

Continuity risks

The capacity of the company to retain its performance and competitiveness over time when human resources arrive and depart is referred to as continuity risk (Lambe, 2013, in Durst & Zieba 2019). This calls for a strategy involving personnel replacement and succession planning (Durst & Wilhelm, 2012). Organizations that are currently dealing with a steady stream of employees quitting have developed a procedure by putting in place a mentoring process so that knowledge that was previously present is preserved when employees depart through resignation (due to personal matters, receiving offers elsewhere, or other circumstances), retirement, and dismissal.

Communication risks

Communication plays an important role in KM to enable knowledge practice (Durst & Zieba, 2019), so this risk has a high probability/potential to occur and organizations need to implement effective communication in every activity meeting/agenda.

Knowledge transfer risks

Knowledge transfer within an organization is a process in which the experience of one unit/group/department/division) influences other units (Argote & Ingram, 2000) and there is a reward for exchanging knowledge with other assets (or other knowledge) (Durst & Zieba, 2019). According to Tangaraja, Rasdi, Samah, and Ismail (2016), barriers to effective knowledge transfer are influenced by organizational and personal factors including organizational culture, management commitment to resource and time availability, incentives offered, and the category of knowledge itself. Personal factors include motivation, trust, competence, knowledge absorptive capacity, and language similarity.

KRM Framework

The RM process is a systematic application of management policies, processes, and actions through the steps of creating the context, identifying, analyzing, assessing, managing, monitoring, and communicating risks. It is based on the Australian/New Zealand Standard AS/NZS 4360 (2004). The first four elements are risk assessment steps, while the fifth element is risk control in handling the risks that will occur. Meanwhile, the process of communication and consultation (learning) as well as monitoring and review is carried out throughout the risk assessment and risk control process to ensure that changes in the situation do not change the priority of risks according to the management plan. The Lorenz et al. (2003) framework for knowledge management in risk management demonstrates how knowledge management (KM) supports risk-based decision-making by giving information. The first step in analyzing what should be done in implementing KM-based RM is to establish KM as the cornerstone of RM implementation (see Figure 1).
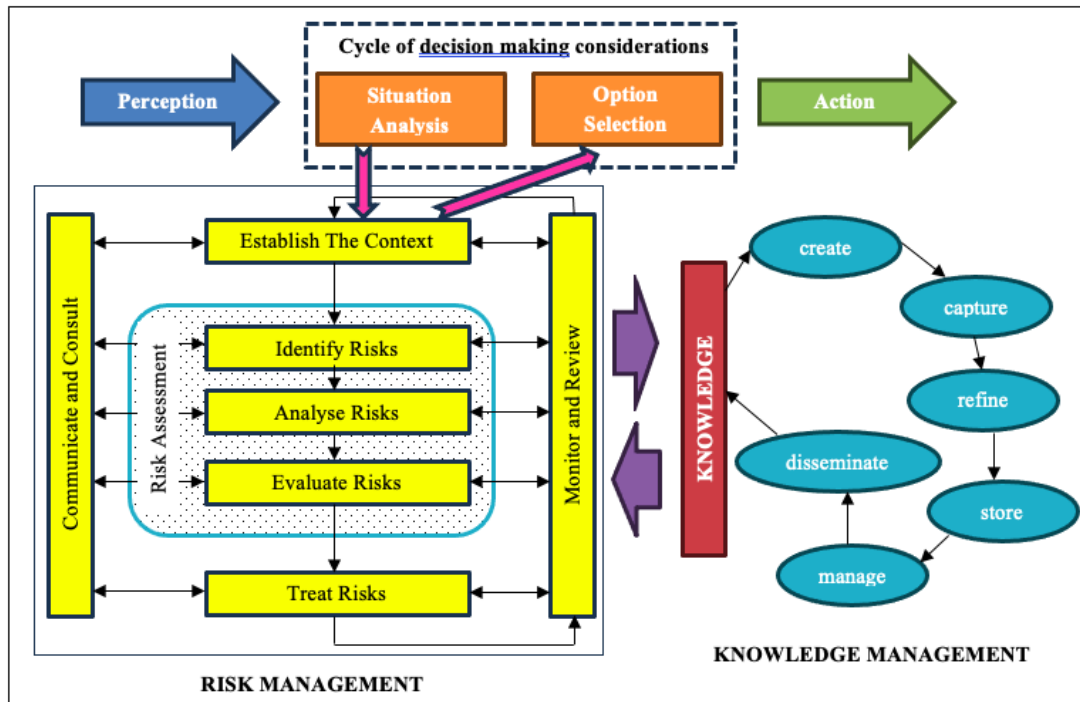
Figure 1 Modification of the KRM model by Lorenz et al. (2003)

The work unit of the Supervisory Research and Development Center as part of the organization has conducted research related to the implementation of KM-based RM as shown in Table 2.

Table-2 : Knowledge Management Based RM Process

No	RM Phases	Source	KM Process
1	Establish The Context		
	-Strategic	- Organization leaders - Knowledge repository	Knowledge related to this stage is obtained from interviews with organizational leaders (the transformation of implicit information into explicit knowledge) or from the knowledge repository, if the information has been systematically stored in a medium that can be accessed by organizational members (KM stages from the create to disseminate stage).
	-Organization	- Leaders, employees, community of practice - Knowledge repository	If the information has been systematically stored in a medium that is accessible to members of the organization, then knowledge related to organizational policies, systems, and procedures is taken from the knowledge repository. Knowledge related to expectations is obtained from interviews with leaders, employees, and the community of practitioners (implicit knowledge transformation into explicit knowledge), starting with Create, Capture, and Refine.
2	Identify Risks The process includes - Events that affect the risk assessment structure, - Potential impact, - How it happens and why it happens	Every employee	Risk identification must be obtained from the risk owners. At this stage, a questionnaire or focus group discussion is conducted with employees at all levels, areas and departments (exploring the experience/tacit knowledge of employees in performing daily tasks along with the identification of risks and impacts that may occur). If this stage is carried out without the knowledge of the risk owner, misidentification may occur. The MR task force/team also communicates MR information with workers at this level to facilitate

No	RM Phases	Source	KM Process
			knowledge transfer and employee acceptance in recognizing hazards in each employee's activity.
3	Analyse Risks It is the frequency of risk occurrence and how much negative impact (magnitude) it has on the achievement of organizational goals that determines the risk rating.	- MR Team - Knowledge repository	The MR team processes and analyzes the data mining findings from risk identification. The refining and storing of information takes place as a process.
4	Evaluate Risks The results of the analysis create a risk register that describes risks that exist in the organization	- MR Team - Knowledge repository - Employees	The results of the analysis are then mapped. In this process, there is communication/validation of the risk map and a knowledge sharing process between the MR team and the employees as risk owners.
5	Treat Risks Treatment options list created	- MR Team - Knowledge repository - Employees	Risk handling is consulted and socialized with risk owners (employees) and the community of practice, and a handling list is created. The process that occurs is store, manage, and disseminate.

Source: Research report risk management based on knowledge management and implementation efforts at BPKP (2008)

KRM integration techniques and systems

The process of integrating KM in the context of KM-based RM carried out by organizations with several techniques and systems, as developed by Neef (2005), is outlined in Table 3.

Table-3 : RM-based KM Integration Stages by Neef (2005)

No	Stages	Description
1	Knowledge mapping	The technique through which businesses map the knowledge of their human resources is known as knowledge mapping. It can take the form of a skills map, which is a list of each employee's expertise and work experience, created as a database that can be accessed through the KM portal. Knowledge mapping in the KM phase is capture. The firm will be aware of the experience and competence of its personnel as well as any gaps thanks to knowledge mapping. The mapping data is then developed in the form of an accountability matrix, in which decision-makers are mapped and electronically linked through databases and related software applications. Responsibility for a project or a crisis resolution idea can be promptly evaluated when a crucial decision must be made.
2	Communities of Practice	Employees who share or complement one other's interests, experiences, and areas of competence naturally develop networks called "communities of practice" to explore new problems. In KM-based RM, these communities are encouraged to discuss potential ideas (create), capture knowledge (capture), and provide feedback (refine). The presence of this community of practice will encourage an organizational culture of knowledge sharing, allowing for the open exchange of ideas between work units. Incidents involving lower-level management can be prevented if they are detected early and formally addressed at the top management level. Early detection of the sensitivity and responsiveness of lower-level management to potential incident signals. As a result, a formal method for exchanging ideas and communicating must be established by the company.
3	Hard-taging experts	Hard-tagging is a knowledge management procedure that combines formal mentorship with knowledge mapping. Employee experience is recognized and classified, much like the knowledge and skill mapping process, to create a database that is accessible when necessary to foresee certain events. In addition to experience, new knowledge is contextualized. In this case, someone must be able to understand it (tacit knowledge) and express it as explicit knowledge. The knowledge is then stored (store and manage) in a reliable format so that it becomes a collection of knowledge (knowledge repository) that can be accessed by others in the organization. This knowledge can be used by organizational leaders when a potential incident or crisis occurs during decision making in the RM phase. The technical team (charged with managing incidents) should be consulted before making any decisions on the upcoming RM phase. This team should be made up of subject matter experts and a network of knowledge practitioners or practitioners who can provide the necessary analysis and assistance for implementation (action). With input from the right people, experienced

No	Stages	Description
		experts and able to provide solutions, the decision making process becomes informative and appropriate.
4	Learning	A very important proposition in KM is that employees need to share (disseminate) experiences with each other. So the process of knowledge sharing and continuous and dynamic learning is well positioned. After the review process (post-mortem incidents), it is then learned what was done right and what went wrong. Making errors and learning from them is one of the advantages of learning. Hard labeling, community of practice gatherings, and the availability of best practices not only enhance HR data but also strengthen corporate memory to prevent recurrence of incidents.
5	Encouraging knowledge sharing	An important aspect of a successful KM-based RM framework is values in the form of ethical behavior that are effectively communicated throughout the organization. Integrity is required as part of the organizational culture in the short term, where values and knowledge sharing behaviors are continuously communicated when a risk is identified.
6	Performance monitoring and reporting	When non-financial performance data (such as organizational capital and intellectual capital) is utilized to forecast future organizational success based on the measurement and monitoring of organizational performance, knowledge-based resource management (RM) is considered to be effective. International standards and reporting guidelines should be used in the management process to statistically measure and publish HR performance and organizational integrity.
7	Community and stakeholder involvement	The key to the success of KM is communication and knowledge sharing, which applies not only to all employees of the organization, but also to stakeholders involved in the organization's policies. An information system, such as e-mail and electronic bulletins, is needed to provide information to stakeholders and organizational leaders so that they can sense and respond to suggestions from parties outside the organization.
8	Business research analysis	The present KM revolution has given organizations unprecedented access to the findings of research and analysis, which is its ultimate advantage. Organizations must acquire information capacity, knowledge research and analytical skills, and the ability to find, organize, and disseminate information from internal and external sources linked to policy, culture, and legislation as part of a KM-based RM process. This calls for the capacity to carry out in-depth formal research on legal/regulatory policies, corporate violations and non-compliance, political, social, and local regulations, corporate performance, social performance, and supplier reputation, as well as the ability to record best practices and lessons learned both internally and among rivals.

Source: Research report risk management based on knowledge management and implementation efforts at BPKP (2008)

E. DISCUSSION

As described in Table 1, public sector organizations (government agencies in Indonesia, especially the Indonesian Development and Finance Agency) have the potential to be exposed to different types of knowledge risks. These risks include the risks associated with human knowledge, operational knowledge, and technical knowledge. These risks are further subdivided into several risk kinds, and the majority of the knowledge risks fall under the operational risk category since they are associated with the daily operations of the company. The risks identified have a high probability of occurrence, so organizations must closely analyze and monitor these risks. It is important to understand the details of these knowledge risks so that organizations can prepare strategies to reduce negative impacts that have the potential to interfere with the achievement of organizational goals.

The next step after identifying organizational risks is to analyze KM-based RM, or also known as KRM, using the conceptual framework shown in Figure 1 and explained in more detail in Table 2. In order to start implementing KM-based RM, it is necessary to first build commitment among organizational members, especially organizational leaders. Then proceed with building a KM system and developing risk awareness in the organization. Extracting tacit knowledge into explicit knowledge can be used in every decision consideration at every stage of RM in the organization. In addition, the culture of knowledge sharing is a key that cannot be abandoned. Thus, identifying, analyzing, evaluating, and managing risks based on the knowledge of the risk owner, the RM task force or risk manager, and the community of practitioners in the field of RM

will result in decisions with the least risk. Organizations can be said to be successful when they effectively implement RM by integrating KM as the main foundation and using it as a management tool. The reason is simple: an organization cannot effectively manage its risks if it does not manage its knowledge.

The steps of integrating KM-based RM in the organization by following the steps designed in Table 3. The three main components of KM are people, place, and content. KM requires competent people, a place for discussion, and the content of the discussion itself. In the context of supporting RM, the competent people are the risk owners, the risk manager / MR task force, and the community of RM practitioners. While the place of discussion, among others, in the form of MR discussion forums for a place/means of sharing knowledge that will be used in RM. While the content includes tacit and explicit knowledge of each individual organization, which will be the strength of the organization in managing RM.

The implication of this research for academics is to provide an example of the practice of identifying organizational knowledge risks and the KRM framework. On the other hand, public organizations can use the results of this research as a reference and basis for designing a more effective KRM framework and implementation with adaptations to the knowledge risks of each organization. This research is a development of the previous research conducted by Durst & Zieba (2019).In the previous research, the risk taxonomy was only discussed theoretically and not applied in a practical context. This research still has limitations where the research report used is the organizational unit report in 2008. At that time, the implementation of KRM in the organization was still in the form of a design and was still in the early stages of implementing KRM. Of course, currently the implementation of KRM has progressed with the existence of a comprehensive KMS and KM architecture by applying risk awareness in every operational implementation of the organization. For future research, research can be developed on the taxonomy of knowledge risks in different organizations (both private and public organizations) by developing a conceptual framework that can reduce the negative impact of these risks and design KRM modifications according to the conditions and objectives of each organization.

REFERENCE

Argote, L., & Ingram, P. (2000). *Knowledge transfer: A basis for competitive advantage in firms. Organizational Behavior and Human Decision Processes*, 82(1), 150–169. DOI : https://doi.org/10.1006/obhd.2000.2893

Australia/New Zealand Standard AS/NZS 4360:2004. (2004). RM Guidelines, Companion to AS/NZS:2004. (Standards Australia and New Zealand: December 2004).

Baskerville, R., & Dulipovici, A. (2006). *The theoretical foundations of knowledge management. Knowledge Management Research & Practice*, 4(2), 83–105. DOI : https://doi.org/10.1057/palgrave.kmrp.8500090

Bernstein, P.L. (1996). *Against the Gods: The Remarkable Story of Risk.* New York, NY : John Wiley & Sons, p. 383.

Černe, M., Hernaus, T., Dysvik, A., & Škerlavaj, M. (2017). *The role of multilevel synergistic interplay among team mastery climate, knowledge hiding, and job characteristics in stimulating innovative work behavior. Human Resource Management Journal*, 27(2), 281–299. DOI : https://doi.org/10.1111/1748-8583.12132

Connelly, C. E., Zweig, D., Webster, J., & Trougakos, J. P. (2012). *Knowledge hiding in organizations. Journal of Organizational Behavior*, 33, 64–88. DOI : https://doi.org/10.1002/job.737

Davenport, T and Prusak, L. (1998). *Working Knowledge: How Organizations Manage What They Know.* Harvard Business School Press, Boston.

De Holan, P. M. (2011). *Agency in voluntary organizational forgetting. Journal of Management Inquiry*, 20(3), 317–322. DOI : https://doi.org/10.1177/1056492611408265

De Zoysa, S. and Russell, A.D. (2003). *Knowledge-based risk identification in infrastructure projects. Canadian Journal of Civil Engineering*, Vol. 30 No. 3, pp. 511-22. DOI : https://doi.org/10.1139/l03-001

Durst, S. (2012). *Innovation and intellectual capital (risk) management in small and medium-sized enterprises. International Journal Transitions and Innovation Systems*, 2(3/4), 233–246. DOI: https://doi.org/10.1504/IJTIS.2012.051531

Durst, S., & Aisenberg Ferenhof, H. (2016). *Competitive strategies for small and medium enterprises knowledge risk management in turbulent times*. In K. North & G. Varvakis (Eds.), Competitive strategies for small and medium enterprises (pp. 195–209). Cham: Springer International Publishing.

Durst, S., & Wilhelm, S. (2012). *Knowledge management and succession planning in SMEs. Journal of Knowledge Management*, 16(4), 637–649. DOI : https://doi.org/10.1108/13673271211246194

Durst, Susanne & Zieba, Malgorzata. (2019). *Mapping knowledge risks: towards a better understanding of knowledge management, Knowledge Management Research & Practice*, 17:1, 1-13, DOI: https://doi.org/10.1080/14778238.2018.1538603

Haimes, Y. Y. (2009). *On the complex definition of risk: A systems-based approach. Risk Analysis*, 29(12), 1647–1654. DOI : https://doi.org/10.1111/j.1539-6924.2009.01310.x

Jabeen, Fauzia & Dari, Taghreed AI. (2023). *A framework for integrating knowledge management benefits in the UAE organisations, Knowledge Management Research & Practice*, 21:2, 277-291, DOI: https://doi.org/10.1080/14778238.2020.1780966

Jain, Ajay & Jeppesen, Hans. (2013). *Knowledge Management Practices in a Public Sector Organization: The Role of Leaders´ Cognitive Styles. Journal of Knowledge Management.* 17. 347-362. DOI: https://doi.org/10.1108/JKM-11-2012-0358.

Kaplan, S., & Garrick, B. J. (1981). *On the quantitative definition of risk. Risk Analysis*, 1(1), 11–27. DOI : https://doi.org/10.1111/j.1539-6924.1981.tb01350.x

Lee, H & Choi, B. (2003). *Knowledge management enablers, processes, and organizational performance: an integrative view and empirical examination. Journal of Management Information Systems* 20(1), 179–228. DOI : https://doi.org/10.1080/07421222.2003.11045756

Leonard, D. (2014). How to prevent experts from hoarding knowledge. *Harvard Business Review.* Retrieved from https://hbr.org/2014/12/how-to-prevent-experts- from-hoarding-knowledge

Lorenz, Martin & Gehrke, Jan & Hammer, Joachim & Langer, Hagen & Timm, Ingo. (2005). *Knowledge Management to Support Situation-aware Risk Management in Autonomous, Self-managing Agents.* 114-128.

Marshall, C., Prusak, L. and Shpilberg, D. (1996). *Financial risk and the need for superior knowledge management. California Management Review*, Vol. 38 No. 3, pp. 77-102. DOI : https://doi.org/10.2307/41165844

Massingham, P. (2010). *Knowledge risk management: A framework. Journal of Knowledge Management*, 14(3), 464–485. DOI : https://doi.org/10.1108/13673271011050166

Massingham, P., Massingham, R., & Pomering, A. (2018). *Designing a knowledge management system for social services not-for-profit organisations. International Journal of Knowledge Management*, 14(3), 69–81. https://doi.org/10.4018/IJKM.2018070105

Neef, D. (2005). *Managing corporate risk through better knowledge management. The Learning Organization,* 12, 112-124. DOI : https://doi.org/10.1108/09696470510583502

Nold, Herbert A. (2011). *Making knowledge management work: tactical to practical, Knowledge Management Research & Practice*, 9:1, 84-94, DOI: https://doi.org/10.1057/kmrp.2010.27

Nonaka I and Takeuchi H. (1995). *The Knowledge-creating Company: How Japanese Companies Create the Dynamics of Innovation*. Oxford University Press, New York.

Otterson, S. (2005). Transferring catastrophe risk management knowledge. Risk Management, Vol. 52 No. 5, p. 46.

Perrott, B. E. (2007). *A strategic risk approach to knowledge management. Business Horizons*, 50(6), 523–533. DOI : https://doi.org/10.1016/j.bushor.2007.08.002

Polanyi, Michael. (1966). *The Tacit Dimension*. Routledge and Kegan Paul, London.

Riege, A., & Lindsay, N. (2006). *Knowledge management in the public sector: Stakeholder partnerships in the public policy development. Journal of Knowledge Management*, 10(3), 24–39. DOI : 10.1108/13673270610670830

Schumpeter, J.A. (1934). *The Theory of Economic Development*. Harvard University Press, Cambridge, MA (Oxford University Press, New York, NY, 1961) (first published in German, 1912).

Stam, C. D. (2009). *Intellectual liabilities: Lessons from the decline and fall of the Roman Empire. The Journal of Information and Knowledge Management Systems*, 39(1), 92–104. DOI : https://doi.org/10.1108/03055720910962470

Tangaraja, G., Rasdi, R. M., Samah, B. A., & Ismail, M. (2016). *Knowledge sharing is knowledge transfer: A misconception in the literature. Journal of Knowledge Management*, 20(4), 653–670. DOI : https://doi.org/10.1108/JKM-11-2015-0427

Van Maanen, J. (1979). *Reclaiming qualitative methods for organizational research: a preface. Administrative Science Quarterly*, Vol. 24, pp. 520-6. DOI : https://doi.org/10.2307/2392358

Verhaegen, T. (2005). Knowledge makes risks manageable. Business Insurance: Industry Focus, Vol. 3, pp. 16-17.

Zainal, Z. (2007). *Case study as a research method*. *Jurnal Kemanusiaan*, 9, 1–6. https://jurnalkemanusiaan.utm.my/index.php/kemanusiaan/article/view/165

Zieba, Malgorzata & Durst, Susanne. (2018). *Knowledge Risks in the Sharing Economy*. E.M. Vătămănescu & F. Pînzaru, Eds., Knowledge management in the sharing economy (pp. 253–270). Cross-Sectoral Insights into the Future of Competitive Advantage, Springer.