

November 2021

A REVIEW OF KNOWLEDGE RISK CONCEPTION

Rabih A. El Khatib

PhD Candidate, Department of Business Administration, Faculty of Business Administration, Beirut Arab University, Beirut, Lebanon, r.khatib@bau.edu.lb

AlaaEldine Abbass Ali

Associate Professor, Department of Business Administration, Faculty of Business Administration, Beirut Arab University, Beirut, Lebanon, a.abbas@bau.edu.lb

Nehale Mostapha

Professor – Dean Faculty of Business Administration Beirut Arab University, Beirut, Lebanon, nehale.mostapha@bau.edu.lb

Follow this and additional works at: <https://digitalcommons.bau.edu.lb/csdjournal>



Part of the [Business Commons](#)

Knowledge, knowledge risk, knowledge management, knowledge risk management

Recommended Citation

El Khatib, Rabih A.; Ali, AlaaEldine Abbass; and Mostapha, Nehale (2021) "A REVIEW OF KNOWLEDGE RISK CONCEPTION," *BAU Journal - Creative Sustainable Development*. Vol. 3 : Iss. 1 , Article 9.

Available at: <https://digitalcommons.bau.edu.lb/csdjournal/vol3/iss1/9>

This Article is brought to you for free and open access by Digital Commons @ BAU. It has been accepted for inclusion in BAU Journal - Creative Sustainable Development by an authorized editor of Digital Commons @ BAU. For more information, please contact ibtihal@bau.edu.lb.

A REVIEW OF KNOWLEDGE RISK CONCEPTION

Abstract

Knowledge is regarded as a critical source of sustainable competitive advantage. However, knowledge has a negative aspect as well. Organizations face a variety of risks as a result of a lack of knowledge, its disappearance, incorrect application, or other consequences of knowledge-related use. Various knowledge risk dimensions were reported in the literature. The authors summarized and analyzed the theoretical perspectives on knowledge risks based on certain criteria such as comprehensiveness, clarity and flexibility. This research has provided an extended knowledge risk taxonomy of Durst and Zieba (2018). The taxonomy now includes a strategic knowledge risks group that embraces knowledge loss, knowledge leakage, and knowledge gaps risks. This type of knowledge risks has long-term severe impacts on organizational performance and must be managed by senior management/executives. Further research shall be conducted to empirically test and validate the proposed taxonomy.

Keywords

Knowledge, knowledge risk, knowledge management, knowledge risk management

1. INTRODUCTION

The currency of the modern economy is knowledge. Unlike other resources, the value of knowledge increases when it is applied (Durst & Zieba, 2018; Smits & de Moor, 2004). However, knowledge is not always positive and can be harmful. Organizations will face a variety of risks as a result of a lack of knowledge, its disappearance, its inappropriate utilization, or the consequences of a variety of situations of knowledge usage (Brătianu, Neșțian, Tiță, Vodă, & Guță, 2020; Durst & Zieba, 2020; Durst, Bruns, & Henschel, 2016).

Knowledge risk denotes the risk of causing disturbances in the organizational knowledge field (Brătianu & Bejinaru, 2020). It is comprised of a broad set of knowledge-related threats that a firm might encounter (Durst, Zieba, & Aisenberg Ferenhof, 2018). The risk arises as result of knowledge spillover, leakage, loss, absence, misapplication, or any other event that creates uncertainty (Brătianu *et al.*, 2020; Colemann & Casselman, 2016).

Knowledge risk is an emergent construct in knowledge management (KM) that is related to risk management (Brătianu *et al.*, 2020). According to Neef (2005), knowledge risk management is an integration of two other fields, risk and knowledge management. Bayer and Maier (2007) are among the first researchers to shed light on the negative impact of knowledge risk on knowledge assets. Firms should not continue to ignore knowledge risks, but should instead look for ways to manage those risks (Durst *et al.*, 2016). Thus, organizations' ability to identify, lessen and manage knowledge risks is critical for achieving long-term benefits (Brătianu *et al.*, 2020; Durst & Zieba, 2020; Jurczak, 2017).

Organizations of all sizes and types face a variety of knowledge-related risks (Durst, Hinteregger, & Zieba, 2019). The risk is caused by knowledge leakage, loss, gaps, concealment, hoarding, or any other event that creates uncertainty (Brătianu *et al.*, 2020). According to Handa, Pagani, and Bedford (2019), the failure rate for knowledge management procedures ranges between 50% and 70%, necessitating the assessment of knowledge risks. Furthermore, the digital transformation altered the way knowledge is transmitted, but it also introduced new knowledge risks (Zeiringer & Thalmann, 2020). Knowledge risks can have a variety of negative consequences, such as operations disruptions, a loss of competitive advantage, or poor performance (Durst *et al.*, 2019). Firms must review their knowledge management approaches to account for potential knowledge risks, according to Durst and Zieba (2018).

The field of knowledge management has received significant attention, and knowledge management has been investigated in a variety of contexts. However, studying knowledge from a risk standpoint is uncommon (Zeiringer & Thalmann, 2020). Knowledge risk is a new topic of study in the field of knowledge management (Durst, 2019), and there has been little research in this area (Brătianu *et al.*, 2020). Knowledge risk is still in its infancy, and the existing literature is primarily composed of conceptual and theoretical papers (e.g., Temel & Durst, 2021; Durst & Zieba, 2019). As a result, there is unquestionably a need for a thorough understanding of how organizations recognize and manage the potential risks of knowledge (Durst, Zieba, & Aisenberg Ferenhof, 2018).

On the other hand, existing research presents a fragmented understanding of the concept of knowledge risk (Durst *et al.*, 2019). Knowledge concealment, knowledge leakage, and knowledge loss are examples of these. Furthermore, there is no agreement on the knowledge risk dimensions or classification of the term. Previous research (Durst & Zieba, 2018; Lambe, 2013) has provided a variety of interpretations of knowledge risk-related concepts. Furthermore, Durst and Zieba (2017) emphasized that existing research is insufficient to describe all potential knowledge risks and that a clear distinction between them is required.

Based on the foregoing, the purpose of this paper is to provide a systematic overview of knowledge risk conception and fill a gap in the existent literature. This task is completed by summarizing and analysing major theoretical conceptions about knowledge risks, and then proposing a new taxonomy of knowledge risks based on existing research, as well as business risks and enterprise risk management literature. This paper offers a more holistic view of knowledge risks and will encourage and guide future research in this field. Also, it will assist firms in identifying their critical knowledge, especially the one that is at risk and develop a knowledge management strategy to address those risks.

The following is how the paper is structured. *First*, definitions of knowledge risk and knowledge risk management are presented, followed by discussion of the various perspectives of knowledge risks that have been presented in the literature. *Then*, a theoretical framework was developed to categorize knowledge risks. The final section summarizes important findings and their implications for further research.

2. KNOWLEDGE RISK FROM A THEORETICAL PERSPECTIVE

2.1 Knowledge Risk and Knowledge Risk Management

In the literature, there aren't many definitions of knowledge risk (KR). Bayer and Maier (2006) defined knowledge risk as “an operational risk caused by reliance on, loss of, unsuccessful deliberate or accidental knowledge transfer resources, resulting in non-exclusivity or scarcity of these resources”.

Perrot (2007) defined knowledge risk as “a likelihood of any loss from an event connected with the identification, storage or protection of knowledge that may decrease the operational or strategic benefit of any party involved in the network”. According to Brătianu (2018), knowledge risk refers to any knowledge action performed under uncertainty. He suggests recognizing the likelihood of those events that head to unfavourable outcomes in knowledge management.

The authors of this paper have elected to adhere to the definition of Zieba and Durst (2018) of knowledge risk as “a measure of the probability and severity of adverse effects of any activities engaging or related somehow to knowledge that can affect the functioning of an organization on any level”. This definition is more comprehensive than the one provided by other scholars which are limited to certain types of risks (e.g., knowledge leakage) or certain conditions (e.g., organizational networks).

Knowledge risk management (KRM) is a new concept to managing different risks associated with knowledge that businesses may face (Durst & Zieba, 2020). It combines two previously separate fields: knowledge management and risk management (Massingham, 2010). This study will adopt Durst et al. (2016) definition of KRM as “a systematic activity devoted to the application of a variety of tools and techniques required to detect, examine and react to risks related to the production, usage, and detainment of knowledge”.

2.2 Knowledge Risk Perspectives

The term "knowledge risk" refers to a wide range of dangers linked to knowledge that a firm can encounter (Durst *et al.*, 2018). There was a lack of knowledge risk perspectives in the existing literature. Jamieson and Loeng (2003) identified several risks associated with knowledge management systems, including the risk of declining organizational creativity and innovation, a lack of end-user buy-in or usage, and the risk of poor knowledge quality. Other risks included a lack of proper knowledge base maintenance, poorly structured knowledge repositories, knowledge theft, poor management of user perception of the usefulness of knowledge management, organizational change and power shifts, and cultural barriers to knowledge transfer.

According to Neef (2005), firms are adopting a mix of risk management and knowledge management procedures and methods. Perrot (2007) emphasized the negative impact of knowledge gap risk on a firm's ability to achieve its goals. Massingham (2010) created a revised knowledge risk management conceptual model that integrates knowledge management tools and strategies into organizational risk management. Trkman and Desouza (2012) investigated the knowledge risk associated with knowledge sharing in network structures.

Knowledge outsourcing risks, knowledge acquisition risks, knowledge continuity risks, and knowledge articulation risks are the four major types of knowledge risk identified by Lambe (2013). Knowledge leakage, knowledge attrition, knowledge loss, knowledge leaking, knowledge concealment, and other knowledge dangers were later added to Lambe's (2013) list by Durst and Zieba (2017). They divided the risks into two groups: internal and external risks. Durst and Zieba (2017) also suggested categorizing the risks based on their source, such as competitors, collaborators, or employees.

Brătianu (2018) proposed that knowledge risk should comprise spiritual, emotional, and rational KR because their effects and significance differ. Durst and Zieba (2018) suggested a knowledge risk map that divides hazards into three categories: human, technological, and operational. Knowledge hoarding, hiding, unlearning and forgetting, and missing/inadequate abilities of organizational members are all human risks.

Cybercrime risks, hazards associated with older technology, risks associated with digitalization, and dangers associated with social media are all part of technological risks (Durst & Zieba, 2018). Whereas merger and acquisition risks, knowledge transfer risk, knowledge acquisition risks, communication risks, continuity risks, espionage, risk of improper knowledge application, risk of using obsolete/unreliable knowledge, knowledge waste, knowledge outsourcing risks, relational risks, and knowledge gaps are all operational risks (Durst & Zieba, 2018). According to Handa et al. (2019), the risks associated with knowledge assets and the risks associated with knowledge capabilities and functions, are the two ways to investigate knowledge risk.

This study is grounded on a thorough examination of the literature so that to comprehend what has been explored about knowledge risk and knowledge risk management so far. The aim is to identify different knowledge risks classifications and to critically discuss and analyse those classifications based on certain criteria such as comprehensiveness, clarity of distinction between different categories and flexibility in accommodating additional risks. Table 1 below outlines various knowledge risk/ knowledge risk management perspectives available in the literature. It will details the authors’ name, journal name, objective of the study, main findings and discussions.

Table 1: Dimensions and conceptualizations of knowledge risk (KR) and knowledge risk management (KRM)
Reference: The author

Authors (Year)	Journal	Purpose	Findings	Discussions
Jamieson & Loeng (2003)	Conference paper	Explore current perceptions of knowledge management and learn about the different forms of risks and challenges that are now preventing knowledge management implementation	The major finding was the identification of certain risks related to knowledge management systems and environments: <ul style="list-style-type: none"> • <i>A lack of effective knowledge base maintenance</i> • <i>Lack of end-user buy-in or adoption</i> • <i>Poor quality knowledge risk</i> • <i>Inadequately structured knowledge repositories</i> • <i>Knowledge stealing</i> • <i>Risk of declining organizational creativity and innovation</i> • <i>Ineffective management of user perceptions of KM's utility</i> • <i>Organizational change and power shift</i> • <i>Cultural hindrances to knowledge transfer</i> 	This paper is among the first studies to address the subject of knowledge risks. Yet, this paper just highlighted a few risks and did not provide a classification of knowledge risks.
Neef (2005)	The Learning Organization	Describe how forward-thinking businesses are combining knowledge and risk management processes and approaches	The author argued that knowledge risk management, knowledge and risk management integration is booming and sound. Moreover, in view of the risk management worldwide importance, KRM might offer knowledge management a necessary and stimulating momentum.	This paper emphasized the necessity of identifying vital knowledge and suggested a technique for managing it properly. It did not, however, specifically mention any knowledge risk.
Bayer &Maier (2006)	Conference paper	Identify knowledge risk in inter-organizational knowledge transfer	Because engineers and middle managers, in alliances, interact with their counterparts on a daily basis, the authors believe that knowledge transfer risks are concentrated at the level of operational business practices.	The authors offered a definition for the term knowledge risk, which was primarily concerned with operational risk. As a result, this definition is neither comprehensive nor flexible in terms of accommodating various types of knowledge risks.
Perrot (2007)	Business Horizons	Learn more about the challenges that good knowledge management faces in contemporary organizations	The author highlighted the significant impact of knowledge gap risk, which may hinder the company in fulfilling its objectives.	Perrot provided a different definition of KR. He distinguished strategic knowledge from operational knowledge. In his paper, the focus of knowledge risk was mainly on

Authors (Year)	Journal	Purpose	Findings	Discussions
				knowledge gap. As a result, no KR classification is provided.
Massingham (2010)	Journal of Knowledge Management	Verify the validity of decision tree methods for managing organizational risk; and to develop an alternative KRM	The author developed a modified knowledge risk management (KRM) conceptual model that consider KM tools and techniques to the management of organizational risk.	The study offered an alternative risk management strategy based on knowledge management frameworks. The paper is tackling organizational risks in general and highlighting knowledge transfer risks. As a result, there is no KR classification.
Trkman & Desouza (2012)	Journal of Strategic Information Systems	Study knowledge risks with knowledge sharing in network structures	<p>The authors proposed a framework for classifying knowledge risks according to five dimensions:</p> <ul style="list-style-type: none"> • <i>Nature of collaboration (asymmetric, symmetric)</i> • <i>Network nature (innovative, risk hedging, agile, and functional)</i> • <i>Proximity (non-proximate, proximate)</i> • <i>Action type (non-deliberate, deliberate–individual, deliberate–company)</i> • <i>Range of risk.</i> <p>The effect on knowledge transfer, network impact, and probable mitigation strategies were explored for each component of knowledge risk.</p>	The authors of this paper presented a taxonomy of knowledge risks that are mostly related to network structures. This classification is narrow and does not include all kinds of KR.
Lambe (2013)	iKNOW Magazine	Identify forms of KR in organizations	<p>In organizations, Lambe identified four main types of knowledge risks:</p> <ul style="list-style-type: none"> • <i>Knowledge articulation risks</i> • <i>Knowledge outsourcing risks</i> • <i>Knowledge acquisition risks</i> • <i>Knowledge continuity risks</i> 	The author defined four sorts of risks, all of which are primarily operational concerns. As a result, this classification is limited and rigid in terms of accommodating extra risks.
Durst & Aisenberg Ferenhof, (2016)	Book Chapter	Present a KRM framework in the context of SMEs	<p>The authors highlighted a number of knowledge risks:</p> <ul style="list-style-type: none"> • <i>Outsourcing of business functions risks</i> • <i>Knowledge gaps risks</i> • <i>Relational risk</i> • <i>Knowledge waste</i> • <i>Knowledge leakage</i> • <i>Knowledge loss</i> • <i>Risks related to human resources</i> 	The authors identified several knowledge hazards that SMEs face. Nonetheless, the suggested classification was not clear, and it was not stated where knowledge waste, leakage, and loss will fit.
Durst & Zieba (2017)	International Journal of Business Environment	Identify, describe, analyze, and classify KR.	<p>The authors identified the knowledge risks, namely:</p> <ul style="list-style-type: none"> • <i>Knowledge hoarding</i> • <i>Knowledge hiding</i> • <i>Knowledge waste</i> • <i>Knowledge spillover</i> • <i>Knowledge leakage</i> • <i>Knowledge attrition</i> • <i>Knowledge loss</i> • <i>Knowledge risks due to unlearning</i> • <i>Knowledge risks due to forgetting</i> • <i>Knowledge outsourcing</i> • <i>knowledge continuity risks</i> • <i>knowledge acquisition risks</i> • <i>knowledge articulation risks</i> • <i>Relational risks</i> • <i>Risks related to knowledge gaps</i> <p>Then, they assembled the above risks into two categories: internal and external. External risks originate from outside the organization, while the internal ones originate from inside the organization.</p> <p>The authors also suggested to divide the risks according to their origin, i.e., employees, co-operants or competitors.</p>	The authors identified a diverse set of KR. However, this is not an exhaustive list. They created a taxonomy of knowledge risks. The extent of each group, however, was unclear. The limits of each category were not clearly specified since certain risks can be recognized at the crossing of several groups.

Authors (Year)	Journal	Purpose	Findings	Discussions
			Also, KR can be divided according to the source; i.e., one situation-specific or number of factors.	
Brătianu (2018)	Management Dynamics in the Knowledge Economy	Introduce a comprehensive KR grounded on knowledge field theory	<p>Brătianu gives more emphasis on <i>knowledge spillover, knowledge leakage, and knowledge loss</i>. He mentioned other KR found in the literature for instance: <i>knowledge waste, knowledge forgetting, knowledge hoarding, knowledge hiding and knowledge attrition or obsolescence risk</i>.</p> <p>He proposed that KR should comprise spiritual, emotional, and rational knowledge risks. Though, these components differ in their consequences and magnitude.</p> <ul style="list-style-type: none"> • From the rational side, KR might exhibit as obsolete knowledge, knowledge gaps, knowledge outsourcing, knowledge spillover, knowledge leakage, and knowledge loss. • Emotional KR normally come across in firms as soon as anxiety of the unknown is a result of transformations in firms, or in changes their management. • When there are substantial transformations in corporate governance, the shift in top management's values system is referred as spiritual KR. 	The author's list of knowledge risks is not comprehensive. The author contended that knowledge had three aspects, and that literature focuses solely on rational knowledge. Individual knowledge risk follows the same pattern, with three basic forms. The proposed classification is based on a different context and theoretical foundation than earlier studies. However, it treats all knowledge risks in the same way, with no clear distinction.
Durst & Zieba (2018)	Knowledge Management Research and Practice	Discuss the probable consequences of knowledge risks and offer a concept map for these risks and a new classification	<p>The authors proposed a KR map and classify knowledge risks into three groups namely: operational, technological and human KR.</p> <p>A. Operational risks Operational KR stem from the ordinary activities of organizations.</p> <ul style="list-style-type: none"> • <i>Merger and acquisition risks</i> • <i>Knowledge transfer risk</i> • <i>Knowledge acquisition risks</i> • <i>Continuity risks</i> • <i>Espionage</i> • <i>Communication risks</i> • <i>Risk of improper knowledge application</i> • <i>Risk of using obsolete/unreliable knowledge</i> • <i>Knowledge outsourcing risks</i> • <i>Relational risks</i> • <i>Risks related to knowledge gaps</i> • <i>Knowledge waste</i> <p>B. Technological risks Technological KR are related to the utilization of different kinds of technologies by firms</p> <ul style="list-style-type: none"> • <i>Risk related to social media</i> • <i>Digitalization risks</i> • <i>Risk related to old technologies</i> • <i>Risks related to cybercrime</i> <p>C. Human knowledge risks Human KR concern individual elements, such as psychological, cultural, social, and personal, in addition to human resources management.</p> <ul style="list-style-type: none"> • <i>Missing/inadequate competencies of organizational members</i> • <i>Forgetting</i> • <i>Unlearning</i> • <i>Knowledge hoarding</i> • <i>Knowledge hiding</i> 	The authors expanded on their prior work. They included new knowledge risks to their prior list and proposed a new knowledge risk classification that included the vast majority of knowledge risks. They explicitly identified each category of knowledge risks. This classification, however, did not include knowledge loss or leakage. In terms of having additional risks in each category, this taxonomy is the most comprehensive, clear, and flexible.

Authors (Year)	Journal	Purpose	Findings	Discussions
Mueller and Mueller, (2019)	Conference Paper	Outline the fundamentals of KRM and propose procedures to avoid or prevent knowledge loss risk	The authors mentioned that knowledge risks are composed of personnel and structural knowledge risks. <i>Personnel risks</i> include: missing knowledge carriers, disqualified employees, restrained knowledge, and knowledge carriers at risk of leaving. <i>Structural knowledge risks</i> include: organizational knowledge risks, factual-technical knowledge risks, and market-based risks.	The authors presented a new categorization of knowledge risks. They did not, however, provide definitions for each group or mention any specific KR. As a result, it is difficult to proceed with the distribution of KR to each category.

3. PROPOSED KNOWLEDGE RISKS TAXONOMY

Based on the existing literature, it appears that there is currently no agreement among researchers regarding the dimensions of knowledge risks. Lambe (2013) and Durst and Zieba (2018) classifications of knowledge risks are the most widely used. However, Durst and Zieba (2018) developed a more comprehensive and clear classification that divided knowledge risks into three categories: operational, technological, and human knowledge risks. This study will extend Durst and Zieba's taxonomy based on existing research and business risks and enterprise risk management literature.

Sadgrove (2016) distinguished six kinds of business risks, namely: human, operational, strategic, technological, financial, and compliance risks. Compliance risks include stock exchange, tax, environmental laws, accounting standards, etc. Accordingly, this type is inapplicable to knowledge. The same holds true for financial risks. As a result, the authors of this study propose a new knowledge risk taxonomy divided into four categories: strategic, operational, human, and technological. This taxonomy will supplement Durst and Zieba's (2018) classification, which includes three groups: risks associated with human, technological, and operational knowledge.

According to Burkholder, Golas, and Shapiro (2007), employee risks are divided into two categories: strategic risk and operational risk. Management input varies between operational and strategic risks (Sadgrove, 2016). While strategic risks necessitate the attention of top management, operational risks may be resolved at a lower level of management. According to Burkholder et al. (2007), strategic risks include all risks to an organization's growth. Strategic risks are more difficult to detect, evaluate, and deal with because they have a long-standing effect, a large number of interconnecting variables, and are more abstract. (Bayer & Maier, 2007). Operational risks arise from an organization's day-to-day operations (Durst & Zieba, 2018; Sadgrove, 2016; Burkholder *et al.*, 2007).

Moreover Perrot (2007) identified differences between operational and strategic knowledge. While strategic knowledge is essential for an organization to make major decisions, operational knowledge focuses on the day-to-day operations of the company. Since the literature on risk and knowledge management contains a strategic category, and extant research indicates that knowledge risk management is a combination of knowledge management and risk management, strategic knowledge risk could be added to the knowledge risks taxonomy.

Knowledge risks with long-term impact that require senior management/executive involvement are classified as strategic knowledge risks (Bayer & Maier, 2007). For both technology and human knowledge risks, this study will use Durst and Zieba's (2018) description. Individual variables including psychological, cultural, social, and personal characteristics, in addition to human resource management, are all considered in human KR. Technological KR are related to the utilization of different kinds of technologies by firms (Durst & Zieba, 2018).

Brătianu (2018) noted that when an organizational culture encourages sharing of knowledge, knowledge hiding might be considered a risk. Furthermore, he stated that knowledge waste cannot be regarded as a knowledge risk. It is, rather, the outcome of an ineffective knowledge management. The authors of this research agree with Brătianu (2018) on knowledge waste, but because knowledge sharing is so important in organizations, knowledge hiding will be treated as a risk in this study.

Gaghman (2019) argued that knowledge loss is a strategic risk that affect firm's overall strategy. The loss of knowledge resources is irreversible, resulting in a void that has a negative impact on business activities execution (Bayer & Maier, 2007). Olander and Hurmelinna-Laukkanen (2015) stated that as a result of knowledge leaking and leaving, knowledge can be lost. According to Dalkir (2005), strategic capabilities are aggregated to organizational competencies and are things that an individual is skilled at. He went on to say that the more valuable a capability is, the less likely it is to be shared among many individuals, making the company more vulnerable if those employees quit.

Although Durst and Zieba (2018) considered knowledge loss and leakage to be consequences of knowledge risk, Durst et al. (2019) treated both as knowledge risks when analysing the link between KRM and organizational performance. Furthermore, Brătianu et al. (2020) stated that knowledge risk is generated by knowledge loss and leakage, and their study focused solely on knowledge loss among other hazards. On the other hand, leaking confidential knowledge to rivals has negative impact on an organization's performance and competitive advantage (Vafaei-Zadeh, Hanifah, Foroughi & Salamzadeh, 2019).

It's worth noting that most knowledge loss research looks to NASA as a classical example of knowledge loss. Knowledge loss had a long-term influence on NASA's operations and performance (Jennex, 2014), demonstrating that knowledge loss is a strategic risk. As a result, knowledge loss and leakage may be regarded as strategic knowledge risks.

The discrepancy between what a company needs to know and what it actually knows is referred to as the knowledge gap, and it is a strategic gap (Zack, 1999). The larger the knowledge gap, the more likely it is that timely strategies and capabilities will not be available for implementation (Perrot, 2007). Thus, this study consider knowledge gaps as strategic knowledge risk in congruence with Zack (1999).

Following the logic of the above arguments, the proposed knowledge risk taxonomy and its components are as follows: (1) *human knowledge risks*: insufficient or missing competencies, forgetting, unlearning, knowledge hoarding, knowledge hiding; (2) *technological knowledge risks*: risk associated with social media, risk associated with old technologies, risks associated with cybercrime, digitalization risks; (3) *strategic knowledge risks*: knowledge loss, knowledge leakage, and knowledge gap risks; and (4) *operational knowledge risks*: risk of improper knowledge application, risk of using obsolete/unreliable knowledge, knowledge continuity risks, knowledge articulation risk, relational risks, knowledge outsourcing risks, espionage, communication risks, merger and acquisition risks, knowledge transfer risk.

4. CONCLUSION

This paper has examined current research on knowledge risks and knowledge risk management. The concept of knowledge risks is still in its infancy, and existing research provided a fragmented understanding of the topic. This study provided a thorough theoretical overview and assessment of knowledge risk concept. As a result, the theoretical viewpoints on knowledge risks were collated and analysed. Durst and Zieba (2018) classification was chosen because of its comprehensiveness, clarity, and flexibility when compared to others such as Lambe (2003) or Trkman & Desouza (2012). A new knowledge risk taxonomy has been established as an extension of this knowledge risk classification. The strategic knowledge risk group has been added to the taxonomy. This study argued that some knowledge risks, such as knowledge loss and knowledge leakage, which are not included in Durst and Zieba (2018)'s classification, as well as risks associated with knowledge gaps, can be classified as strategic knowledge risks. A new holistic taxonomy is provided by adding strategic knowledge risks as a new group, which may motivate and guide future study in this field. Strategic knowledge risks have long-term consequences for operations and performance. This study is the first to distinguish between operational knowledge risks, which must be controlled by functional/operational managers, and strategic knowledge risks, which must be managed by top management/executives. The field of knowledge risks has immense research potential, and the suggested taxonomy lays the groundwork for future research. The taxonomy has not been empirically validated, which is the study's main limitation. Next step will be to test this taxonomy within certain group of firms such as knowledge-intensive firms, whose performance is largely dependent on effective knowledge management.

REFERENCES

- Abdul Manab, N., & Abdul Aziz, N. A. (2019). Integrating knowledge management in sustainability risk management practices for company survival. *Management Science Letters*, 9, 585-594.
- Bayer, F., & Maier, R. (2006). Knowledge risks in inter-organizational knowledge transfer. *Proceedings of I-KNOW '06 Graz*, Austria, 200-208.
- Bayer, F., & Maier, R. (2007). Governing knowledge risks –design and results of an empirical study. *Proceedings of I-KNOW '07 Graz*, Austria, 76-84.
- Brătianu, C. (2018). A holistic approach to knowledge risk. *Management Dynamics in the Knowledge Economy*, 6 (4), 593-607.
- Brătianu, C., & Bejinaru, R. (2020). Knowledge dynamics: A thermodynamics approach. *Kybernetes*, 49 (1), 6-21.
- Brătianu, C., Neșțian, A.Ș, Tiță, S.M., Vodă, A.I., & Guță, A.L. (2020). The impact of knowledge risk on sustainability of firms. *Amfiteatru Economic*, 22 (55), 639-652.
- Burkholder, N. C., Golas, S., & Shapiro, J. P. (2007). *Ultimate performance: Measuring human resources at work*. John Wiley & Sons.
- Coleman R., & Casselman, M. (2016). Optimizing decisions using knowledge risk strategy. *Journal of Knowledge Management*, 20 (5), 936-958.
- Dalkir, K. (2005). *Knowledge management in theory and practice*. Elsevier Butterworth–Heinemann, Burlington, MA 01803, USA.
- Durst, S. (2019). How far have we come with the study of knowledge risks? *VINE Journal of Information and Knowledge Management Systems*, 49 (1), 21-34.
- Durst, S., & Aisenberg Ferenhof, H. (2016). *Knowledge risk management in turbulent times*. In North, K. and Varvakis, G. (Eds), *Competitive Strategies for Small and Medium Enterprises Increasing Crisis Resilience, Agility and Innovation in Turbulent Times*, Springer International Publishing, Cham, 195-209.
- Durst, S., & Zieba, M. (2017). Knowledge risks - towards a taxonomy. *International Journal of Business Environment*, 9 (1), 51-63.
- Durst, S., & Zieba, M. (2018). Mapping knowledge risks: Towards a better understanding of knowledge management. *Knowledge Management Research and Practice*, 17, 1-13.
- Durst, S., & Zieba, M. (2020). Knowledge risks inherent in business sustainability. *Journal of Cleaner Production*, 251, 119670.
- Durst, S., Bruns, G., & Henschel, T. (2016). The management of knowledge risks: What do we really know? *International Journal of Knowledge and Systems Science*, 7 (3), 19-29.
- Durst, S., Zieba, M., & Aisenberg Ferenhof, H. (2018). Knowledge risk management in organizations. *Proceedings IFKAD 2018*, Delft, Netherlands.
- Durst, S., Hinteregger, C., & Zieba, M. (2019). The Linkage between knowledge risk management and organizational performance. *Journal of Business Research*, 105, 1-10.
- Gaghman, A. A. (2019). The Impact of Knowledge Behavioural Factors on Tacit Knowledge Retention: Empirical Study in Oil and Gas Industry in Economies of the Balkan and Eastern European Countries. *KnE Social Sciences*, 34-53, DOI 10.18502/kss.v4i1.5976.
- Handa, P., Pagani, J., & Bedford, D. (2019). Managing risks of knowledge assets, knowledge assets and knowledge audits (working methods for knowledge management). *Emerald Publishing Limited*, 169-182.
- Jamieson, R., & Loeng, D. (2003). An exploratory study of risks and issues in knowledge management. *14th Australasian Conference on Information Systems*, Perth, Western Australia.
- Jennex, M. E. (2014). A proposed method for assessing knowledge loss risk with departing personnel. *The Journal of Information and Knowledge Management Systems*, 44 (2), 185-209.
- Jurczak, J. (2017). Intellectual capital risk management for knowledge-based organizations. In: Raczkowski K. (eds) *Risk Management in Public Administration*, 257-282. Palgrave Macmillan, Cham.
- Lambe, P. (2013). Four types of knowledge risk, 1-3 [online]. Retrieved from www.greenchameleon.com/uploads/Four_Types_of_Knowledge_Risk.pdf.
- Massingham, P. (2010). Knowledge risk management: a framework. *Journal of Knowledge Management*, 14 (3), 464-485.

- Mueller, F., & Mueller, A. (2019). Knowledge risk management – how to manage future knowledge loss. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 5673-5680.
- Neef, D. (2005). Managing corporate risk through better knowledge management. *The Learning Organization*, 12 (2), 112-124.
- Olander, H., & Hurmelinna-Laukkanen, P. (2015). Perceptions of employee knowledge risks in multinational, multilevel organizations – Managing knowledge leaking and leaving. *International Journal of Innovation Management*, 19 (3), 1540006, 1-28.
- Perrot, B. E. (2007). A strategic risk approach to knowledge management. *Business Horizons*, 50, 523-533.
- Sadgrove, K. (2016). *The complete guide to business risk management*. New York: Routledge.
- Smits, M., & de Moor, A. (2004). Effective knowledge management in knowledge-intensive organizations. *Proceedings of Organizational Knowledge, Learning and Capabilities*, Innsbruck.
- Temel, S., & Durst, S. (2021). Knowledge risk prevention strategies for handling new technological innovations in small businesses. *VINE Journal of Information and Knowledge Management System*, 51 (4), 655-673.
- Trkman, P., & Desouza, K. (2012). Knowledge risks in organizational networks: An exploratory framework. *Journal of Strategic Information Systems*, 21, 1-17.
- Vafaei-Zadeh, A., Hanifah, H., Foroughi, B. and Salamzadeh, Y. (2019). Knowledge leakage, an Achilles' heel of knowledge sharing. *Eurasian Business Review*, 9, 445-461.
- Zack, M. (1999). Developing a knowledge strategy. *California Management Review*, 41 (3), 125-145.
- Zeiringer, J. P., & Thalmann, S. (2020). Knowledge risks in digital supply chains: A literature review. *15th International Conference on Wirtschaftsinformatik*, Potsdam, Germany.