sciendo

Scientific Bulletin
Vol. XXVIII, No. 1(55), 2023

MITIGATING KNOWLEDGE MANAGEMENT INTERNAL AND EXTERNAL RISK FACTORS: A LITERATURE REVIEW OF BEST PRACTICES

Tori Reddy DODLA
ljohnson1@captechu.edu

Laura Ann JONES
lajones@captechu.edu

Capitol Technology University, Laurel, Maryland, USA

ABSTRACT:

Used to store, manage, and leverage information, knowledge management systems are becoming increasingly valuable assets within organizations. Organizations must manage knowledge internally (through knowledge risks) and externally (through reputational risks). We define knowledge risks as internal human, technological, and organizational factors, and reputational risks as the effects of knowledge risks and external perils to reputation, credibility, financial status, and future success. An oversight of either risk type can cause significant damage to an organization. This literature review was a means to analyze, categorize, and offer best practices for mitigating risks within a knowledge management system.

KEYWORDS:

Risk management, information loss, knowledge risks, knowledge management, reputational risks

1. Introduction

Risk is the possibility that actions or events could lead to consequences that impact what people value (Burnap, 2021). Organizations' most-considered risks are knowledge loss and disinformation or unreliable information (Durst & Zieba, 2018). Although awareness could inspire leaders to gather information and suggest proper risk management strategies, researchers have not yet observed the totality of mitigating knowledge management system (KMS) risk across industries. Organizations must ensure that risks are anchored in their risk management to avoid disasters due to neglect (Durst, Hinteregger & Zieba, 2019). Further, there is a need to establish how to conduct, follow, and customize risk management assessments for KMS.

Researchers have focused on risk and knowledge management as separate topics or applied conceptual frameworks to a specific project. Alhawari, Karadsheh, Nehari Talet & Mansour's (2012) attempt to provide a knowledge-based risk management framework for information technology projects provides a foundation but cannot be applied to all fields. Thus, there is limited knowledge

DOI: 10.2478/bsaft-2023-0005

about the relationship between risk management and implementing KMS across a wide range of industries. Despite a knowledge management (KM) implementation failure rate of 50-70% (Rhem, 2015), KM remains unexplored among many organizations in need of risk awareness. In this paper, we present the findings from a literature review to identify risk management components for implementing and maintaining KMS, which can pose a significant risk for organizations.

1.1. Significance of study

Experts and leaders should integrate risk management with KM to achieve the best outcomes for their organizations (Durst et al., 2019). In addition, organizations should be able to identify and understand potential knowledge risks (Durst & Zieba, 2018). This study will provide a significant resource for organizational leaders, policymakers, and researchers on the benefits of mitigating knowledge and reputational risks.

High-level question: What are the best practices for mitigating risks within a knowledge management system?

Q1: Are there risk factors specific to knowledge management?

Q2: Is there a relationship between knowledge and risk?

Q3: Can a knowledge management risk assessment follow a traditional risk assessment flow?

2. Literature review

Knowledge management is the process of sharing, transmitting, distributing, collecting, and documenting knowledge (Abualoush, Masa'deh, Bataineh & Alrowwad, 2018). Leaders use KM to systematically manage organizational knowledge assets to create value and meet organizational objectives. However, managing knowledge also involves managing risk (Yarovenko, Bilan, Lyeonov & Mentel, 2021); therefore, we discuss the KM risk cycle to understand the relationship between knowledge and risk. The KM risk cycle describes the interplay between organizations' KM and risk management activities.

Lipa, Kane & Green's (2022) risk-knowledge infinity cycle shows that KM and quality risk management are synergetic, in that "a robust [quality risk management] program will reduce risk while applying knowledge and creating new knowledge, while and a good KM program will ensure the best possible knowledge is available for risk reduction and to foster continual improvement" (Lipa, 2020). Lipa et al. presented four primary findings: (a) both the input and the outcome of risk management are knowledge; (b) knowledge has an inverse relationship with risk; (c) risk is informed by knowledge that is readily available, while new knowledge is informed by risk; and (d) the risk-knowledge infinity cycle is perpetual.

We now discuss the basic elements of a risk management process and apply KM concepts to each. The risk management process has four stages: risk identification, risk assessment, risk mitigation, and risk monitoring (Dahiya, Solanki & Dhankhar, 2020).

2.1 Risk identification

We start by identifying potential risks associated with KM activities. In this stage, organizational managers discover and document risk factors for future analysis (Dahiya et al., 2020). Organizations can uncover risks by brainstorming from prior personal experiences, consulting with experts, or holding stakeholder meetings.

2.2 Risk factors

Our discussion of possible KM risk factors has two categories: knowledge risks and reputational risks. Knowledge risks can be any activities related to internal KM, such as human, technology, and operational vulnerabilities (Durst et al., 2019). We propose that once knowledge leaves the confines of an organization and enters the general public, knowledge risks become reputational risks. Sickler (2021) identified reputational risk as

the potential harm to an organization's reputation, leading to negative perceptions and a loss of credibility, customers, and finances. Internal knowledge risks can turn into reputational risks when information becomes public or is disclosed to external parties, especially if the information is negative or damaging. Because 70-80% of a company's market value comes from intangible assets such as brand and intellectual capital (Su, 2014), it is necessary to understand the best practices of mitigating knowledge and reputational risks.

2.2.1 Knowledge Risks (Internal)

Knowledge risks relate to an organization's day-to-day operations (Durst et al., 2019). An ideal approach to knowledge risks is to focus on the organization's personnel and information technology mechanisms. Here, we outline knowledge risks at the organizational and individual levels.

Knowledge Hoarding. With knowledge hoarding, individuals accumulate and keep knowledge to themselves rather than sharing it with others (Durst et al., 2019). Knowledge hoarding leads to a lack of collaboration and knowledge sharing, which could hinder innovation. Although some employees perceive that knowledge developed on the job is their personal intellectual property, the knowledge belongs to the organization (Bilginoğlu, 2019). Knowledge hoarding can be intentional or unintentional. Individuals might resist knowledge sharing due to a lack of training or understanding of the KMS (Friedrich, Becker, Kramer, Wirth & Schneider, 2020). They could also be resistant due to the inconvenience and time or because they do not want to share. Because knowledge sharing is considered an essential activity (Ahmad & Karim, 2019) directly linked to organizational expansion (Rumanti, Wiratmadja, Sunaryo, Ajidarma & Ari Samadhi, 2019), we conclude that knowledge hoarding is a risk factor that could hinder the growth of an organization.

Data Quality/Knowledge Quality. Data quality risks stem from potential issues or problems affecting data accuracy, completeness, and reliability (Cichy & Rass, 2019). These risks can arise from various sources, including data entry errors, data definition inconsistencies, lack of proper validation checks, and insufficient data management processes. Data quality is a crucial aspect of knowledge quality because the quality of knowledge is only as good as the quality of the data it is based on. Poor data quality can lead to missed business opportunities and poor decision-making (Cichy & Rass, 2019); therefore, ensuring quality data is essential to achieving high knowledge quality and making informed decisions. Practitioners and researchers recognize the value of data quality.

Intellectual Property. In a knowledge-driven economy, knowledge assets are essential to gain a competitive edge (Oladejo, 2022). These assets, called intellectual property, can include trademarks, copyrights, patents, trade secrets, and other proprietary information. In the context of KM, intellectual property risks refer to potential legal and financial problems arising from asset infringement or misappropriation. In the past, organizations dismissed the need to protect their knowledge and intellectual property rights (Ali & Tang, 2022). Now, newer research shows that intellectual property in the context of KM is an important component of an organization's day-to-day activities.

Cyberattacks. Cyberattacks include unauthorized access to or malicious attacks on computer systems and networks, including malware, phishing, man-in-the-middle, and denial of service (Li & Liu, 2021). Cyber hacks pose a significant threat to an organization's knowledge assets. Knowledge assets, such as confidential business information, trade secrets, and customer data, can be valuable targets for cybercriminals. Cyberattacks have many risks, including the theft of information, financial data, and trade secrets. They can also cause disruptions to critical business

operations, computer systems damage, and revenue loss.

Cyber risks can harm a company's reputation and credibility, leading to a loss of customers and decreased trust in the organization. When a cyberattack breaches a company's external boundaries, it becomes a reputational risk.

2.2.2. Reputational Risks (External)

Reputational risks are serious organizational issues, especially regarding financial stability and operational longevity (Jones, 2020). Reputational risks can damage KM and lead to the loss of customers, revenue, and operation status (Jones, 2020). In this section, we outline the risk factors that qualify as knowledge risks; however, these risks, affecting thousands of people, extend well beyond the organization's day-to-day operations. According to Jones (2020), "*While concerns related to reputation vary, the outcome of a negative reputation risk event can be damaging*".

Data Breach. A data breach is the unauthorized access, use, disclosure, alteration, or destruction of sensitive or confidential information. Data breaches can occur for various reasons, including "*cyber-attacks, theft or loss of devices, theft or leak of the employee data, such as security credentials, and human errors*" (Algarni, Thayananthan & Malaiya, 2021).

The consequences of a data breach can be significant and long-lasting and include knowledge loss, financial losses, reputational damage, legal liabilities, and the loss of customer trust (Jones, 2020). Data breaches are reputational risks that can affect external stakeholders and customers and ruin a company's reputation. Following a data breach, companies lose more money in the stock market, customers, and court settlements than from the actual event.

Compliance Failure Risks. Compliance risks refer to an organization's potential to face legal or regulatory consequences for failing to adhere to laws and regulations, such as those related to data privacy, anticorruption, and health and safety (Gressgård, 2014). Effective KM can help organizations mitigate compliance risks by ensuring that employees can access accurate and up-to-date information on relevant laws and regulations and understand their obligations under these rules. A well-designed KM system can provide employees guidance on ethical and compliant behavior, help organizations track and manage regulatory changes, and provide a secure repository for storing sensitive information.

Fraud Risks. Fraud risks stem from an organization's potential for financial losses and reputational damage because of fraudulent activity, such as embezzlement, false invoicing, identity theft, or false information (Brasel, Hatfield, Nickell & Parsons, 2019). Effective KM can help organizations mitigate fraud risks by promoting transparency, accountability, and a strong culture of ethics. A well-designed KMS allows employees to locate and understand the organization's policies and procedures for preventing and detecting fraud, provides access to training and guidance on fraud-related issues, and fosters open communication and collaboration among employees to identify and prevent fraudulent activity. Additionally, a KMS can provide an audit trail of decisions and actions, making it easier to detect fraudulent behavior and track the sources of fraudulent activity. With the help of technology advancement and more sophisticated knowledge management software, losses from fraud activity may be reduced over time. Table no. 1 presents a sample of companies, risk factors, and outcomes.

Table no. 1
Fraud Outcomes

Year	Company	Risk factor	Result
2017	Equifax	Data breach	$425 million+ settlement
2016	Uber	Data loss	$100,000 payoff
2016–18	Wells Fargo	Fraud risk	12% decline in profits, 77% operational loss, damaged reputation
2015	Chipotle	Compliance risk	$278 stock fall
2017	Merck	Ransomware attack	$870 million loss
2017	FedEx	Ransomware attack	$400 million loss
1987	Chrysler	Fraud risk	Class action lawsuit: 15 felonies, $7.6 million in fines, $16 million loss of awards, damaged reputation

Note. Created from summarized information from reputational risks involving KM risk factors. (Source: Jones, 2020)

Accessing risks entails analyzing and evaluating risks' severity and probability (Dahiya et al., 2020). Determining the risk impact, properties, and classifications also occurs during the assessment. A risk assessment can help organizations understand the risks associated with managing knowledge assets, such as confidential information, intellectual property, and sensitive data. By conducting a risk assessment, organizations can identify the potential consequences of data breaches or critical knowledge loss and develop strategies to mitigate those risks, such as implementing security measures, backup plans, and contingency plans. Acting on the information gained from a risk assessment could enhance KM effectiveness, ensuring that knowledge assets are protected and effectively used to support the organization's goals. Table no. 2 shows risk likelihood and risk consequence definitions.

Table no. 2
Risk Likelihood and Risk Consequence

Description	Definition
Risk likelihood	
Frequent	Will happen more than once or one many occasions
Probable	Has happened and likely to happen, again
Occasional	Infrequent but possible
Remote	Low chance of occurring
Improbable	Very low chance of occurring
Risk consequence	
Catastrophic	Will cause grave damage and suffering
Critical	Will cause adverse damage
Major	Will cause serious damage
Minor	Will cause slight damage

Note. Created from summarized information from Knowledge Risk Management: A Framework. (Source: Massingham, 2010)

Using a standard hazard severity chart, organizational leaders can quantify a risk factor's potential impact and compare scores for other hazards to determine the most important ones requiring immediate attention.

Specialized risk assessments could provide a more detailed and tailored evaluation of specific risks and vulnerabilities, allowing for the development of more effective risk management strategies. Here, we discuss possible KMS risk assessments.

Information Security Risk Assessment: This type of assessment focuses on the security of an organization's data and information. The assessment will cover a range of topics, including threat analysis, data gathering, and cloud security (Landoll, 2021).

Intellectual Property Risk Assessment: The assessment will identify potential threats to the intellectual property, such as theft, misappropriation, or infringement, and assess the threats' impact on the organization (Oladejo, 2022).

Compliance Risk Assessment: A compliance risk assessment focuses on ensuring that an organization complies with applicable laws and regulations, including data protection laws and industry standards (Gressgård, 2014).

Continuity Risk Assessment: A continuity risk assessment aims to identify potential threats and vulnerabilities and develop contingency plans to minimize the impact of disruptions. Continuity risk assessment is a critical component of overall risk management and essential for ensuring long-term stability and sustainability (Torabi, Giahi & Sahebjamnia, 2016).

2.3 Risk Mitigation

The third stage of the risk management process is risk mitigation. Mitigating risks entails taking action to reduce a risk's adverse effects and the likelihood of its occurrence (Ahmed, 2017). Risk mitigation can involve the development of risk management plans and the implementation of risk mitigation strategies. Incorporating risk mitigation strategies before launching a new technology can minimize the impact of risks and bring about a competitive advantage. Effective risk mitigation helps organizations avoid or reduce harm, protect their assets, and maintain the stability of their operations. The following paragraphs present common risk responses.

Risk control actions are means to reduce or eliminate the probability or impact of a negative event (Battisti, 2020). Risk control is separate from risk mitigation, with measures taken to minimize the adverse effects of events (Ahmed, 2017). An example of risk control is diversification, which, in KM, entails spreading the sources of knowledge and expertise across the organization. A risk diversification strategy includes knowledge integration, cross-training, collaboration, and documenting knowledge and processes. By diversifying, an organization can mitigate the risk of losing valuable information and expertise and increase its overall resilience. Unrelated diversification refers to knowledge-sharing across groups in dissimilar teams (Li, 2020). In a crisis, firms that practiced unrelated diversification were less likely to need external resources.

Risk transfer entails transferring all or part of a risk to another entity (Battisti, 2020), such as an insurance company. Cyber insurance can protect an organization from losses due to cybercrime (such as a cyberattack or data breach) or malfunction (Romanosky, Ablon, Kuehn & Jones, 2019). Cyber insurance is a type of risk transfer because it transfers the financial consequences of a potential cyberattack from the policyholder (the organization) to the insurance company. Organizations pay insurance premiums in exchange for the company's promise to cover the policyholder's financial losses from a cyber incident specified in the policy (Romanosky et al., 2019). However, "*Firms that have cyber insurance may not be as protected as they think*" (Granato & Polacek, 2019). Cyber insurance policies might include first-party expenses that reimburse a company for a cyberattack that directly affects their business and third-party liability coverage that reimburse the costs incurred by customers for

data breaches. Many organizations lack silent cyber risk insurance, which reimburses a company for indirect damage to physical assets caused by a cyberattack (Granato & Polacek, 2019).

Risk avoidance means eliminating the risk before it occurs by not engaging in the activity that generates it (Battisti, 2020). An example of risk avoidance is a policy prohibiting personal identification information in a KMS (Granato & Polacek, 2019).

Risk acceptance entails adapting to risks without attempting to control them (Battisti, 2020). With risk acceptance, organizations acknowledge that some activities hold uncertainty and unpredictability that is impossible to avoid.

2.4 Risk Monitoring

Risk monitoring, the final stage of the risk management process, involves ongoing monitoring and evaluating the risks to ensure they are managed effectively (Dahiya et al., 2020). During this stage, an organization updates risk mitigation strategies and plans as needed.

3. Method

We used a modified version of Dahiya, Solanki & Dhankhar's (2020) risk assessment framework to outline this article using the following steps: 1. Identification; 2. Assessment; 3. Mitigation; 4. Monitoring. We conducted a systematic literature review to identify strategies for mitigating risks within KM. First, we formulated a clear and concise research question:

High-level question: What are the best practices for mitigating risks within a KMS?

Next, we identified three follow-up questions:

Q1: Are there risk factors specific to KM?

Q2: Is there a relationship between knowledge and risk?

Q3: Can a KM risk assessment follow a traditional risk assessment flow?

Guided by these questions, we searched Elicit and Google Scholar for relevant literature using the keywords risk management, knowledge management, systematic literature review, and mitigation strategies. We screened the articles in the search results and identified those most relevant to the research question. Next, we evaluated the quality of the selected literature, including the research design, sample size, data collection methods, and conclusions, then synthesized the studies' findings to identify common themes, best practices, and knowledge gaps. Here, we present a synthesis of the systematic literature review, highlighting key findings, best practices, and recommendations for future research. This literature review contributes a comprehensive and evidence-based understanding of the best practices for mitigating risks within a KMS.

4. Results

High-level question: What are the best practices for mitigating risks within a KMS? From our literature review, we summarized the best practices for mitigating risks within a KMS. All findings directly apply to a KMS or a subcomponent of a KMS. We also listed the corresponding risk factor the studies addressed and the risk mitigation strategy type (see Table no. 3).

Table no. 3

Risk Assessment Best Practices

Best practice	**Risk factor addressed**	**Risk mitigation strategy**	**Authors, years**
Identify the goals and scope of data quality in the planning phase	Data quality	Risk controlling	Cichy & Rass, 2019
Promote unrelate diversification as a knowledge strategy.	Knowledge hoarding	Risk controlling (diversification)	Li et al., 2020

Best practice	Risk factor addressed	Risk mitigation strategy	Authors, years
Create models for knowledge sharing. Include professional development courses as a part of corporate learning. Reward those who teach others how to do their job.	Knowledge hoarding	Risk controlling	Bilginoğlu, 2019
Establish an intellectual property management system for formal IP and train users	Intellectual property risks	Risk controlling	Cheung et al., 2013
Ensure cyber insurance premium has a 'business interruption" coverage for data breaches	Cyber attack	Risk transfer	Romanosky et al., 2019
Become educated on implicit silent cyber coverage and add to cyber insurance coverage if needed	Cyber attack	Risk transfer	Granato & Polacek, 2019
"Reputational risk can be controlled by managing other risk categories."	Reputational risks	Risk controlling/risk acceptance	Jones, 2020
"Not all consumers consume messages in the same place: diversify."	Reputational risks	Risk controlling (diversification)	Jones, 2020
Recruit and retain a full-time, highly skilled chief risk officer who gains support while advocating for a focus on reputation risk	Reputational risks	Risk controlling	Jones, 2020
Create policies and procedures to prevent the storage of personal information about employees or confidential business information	Data breach	Risk avoidance	Algarni et al., 2021
"Practice inward-directed skepticism through repeated risk assessments. Perform timely fraud inquiries of operational-level employees."	Fraud risk	Risk controlling	Brasel et al., 2019
"Practice inward-directed skepticism through repeated risk assessments. Perform timely fraud inquiries of operational-level employees."	Fraud risk	Risk controlling	Brasel et al., 2019

Q1: Are there risk factors specific to KM?

Our research indicated six risk factors related to KM: data breach, data/knowledge quality, knowledge hoarding, compliance, cyberattacks, and intellectual property. We divided the factors into two categories: knowledge risks (Durst et al., 2019), which are internal to a KMS, and reputational risks (Jones, 2020), which happen as a result of internal risk and external.

Q2: Is there a relationship between knowledge and risk?

According to Lipa et al. (2022), "*Risk is informed by knowledge that is readily available, while new knowledge is informed by risk*". We started the literature review by analyzing the relationship between knowledge and risk, finding that risk management's input and output are knowledge and create a perpetual cycle.

Q3: Can a KM risk assessment follow a traditional risk assessment flow?

We used a modified version of Dahiya et al.'s (2020) risk assessment framework to outline this article. However, customized risk assessments considering specific factors relevant to the evaluated organization should produce more accurate results. The literature showed several risk assessments that could offer a more tailored approach to KMS: intellectual property, information security, continuity, and compliance.

5. Conclusion

Risk mitigation is vital to KM, as it protects against potential losses, increases stakeholder confidence, and supports long-term sustainability. Organizations must identify, assess, and mitigate the risks associated with KMS to ensure long-term success and sustainability. The goal of this study was to outline best practices for mitigating risks in KMS. Additionally, we

identified the components of a risk assessment to include risk factors, likelihood, and consequences.

This article has a few limitations. We found minimal research on methods to enhance or mitigate data and knowledge quality. No scholarly articles in recent years have addressed best practices for risk avoidance or acceptance regarding KMS or relevant topics. A suggestion for research is to explore the best practices of mitigation strategies focused on risk avoidance and acceptance for mitigating risks within a KMS. There is a need for more extensive study of technology's role in mitigating risks in KMS. Future research could focus on the impact of technology-based solutions, such as artificial intelligence and machine learning, in reducing risks in KMS.

REFERENCES

Abualoush, S., Masa'deh, R., Bataineh, K., & Alrowwad, A. (2018). The role of knowledge management process and intellectual capital as intermediary variables between knowledge management infrastructure and organization performance. *Interdisciplinary Journal of Information, Knowledge, and Management, Vol. 13,* 279–309, available at: https://doi.org/10.28945/4088.

Ahmad, F., & Karim, M. (2019). Impacts of knowledge sharing: A review and directions for future research. *Journal of Workplace Learning, Vol. 31, Issue 3,* 207–230, available at: https://doi.org/10.1108/jwl-07-2018-0096.

Ahmed, R. (2017). Risk mitigation strategies in innovative projects. *INTECH - Key issues for management of innovative projects*, 83–100, available at: https://doi.org/10.5772/intechopen.69004.

Algarni, A.M., Thayananthan, V., & Malaiya, Y.K. (2021). Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems. *Applied Sciences, Vol. 11, Issue 8, Article 3678*, available at: https://doi.org/10.3390/app11083678.

Alhawari, S., Karadsheh, L., Nehari Talet, A., & Mansour, E. (2012). Knowledge-based risk management framework for information technology project. *International Journal of Information Management, Vol. 32, Issue 1,* 50–65, available at: https://doi.org/10.1016/j.ijinfomgt.2011.07.002.

Ali, S., & Tang, H. (2022). Is intellectual property beneficial to knowledge management? Literature review on organizational knowledge protection. *Journal of the Knowledge Economy*, available at: https://doi.org/10.1007/s13132-022-00904-3.

Battisti, E., Shams, S.M.R., Sakka, G., & Miglietta, N. (2020). Big Data and risk management in business processes: Implications for corporate real estate. *Business Process Management Journal, Vol. 26, Issue 5,* 1141–1155, available at: https://doi.org/10.1108/bpmj-03-2019-0125.

Bilginoğlu, E. (2019). Knowledge hoarding: A literature review. *Management Science Letters, Vol. 9*, 61–72, available at: https://doi.org/10.5267/j.msl.2018.10.015.

Brasel, K.R., Hatfield, R.C., Nickell, E.B., & Parsons, L.M. (2019). The effect of fraud risk assessment frequency and fraud inquiry timing on auditors' skeptical judgments and actions. *Accounting Horizons, Vol. 33, Issue 1*, 1–15, available at: https://doi.org/10.2308/acch-52349.

Burnap, P. (2021). Risk management & governance Knowledge Area Version 1.1.1. *The National Cyber Security Center*. Available at: https://www.cybok.org/media/downloads/Risk_Management_Governance_v1.1.1.pdf.

Cheung, C.F., Yang, W.M., Tse, Y.L., & Ma, R. (2013). Knowledge-based intellectual property management for technology development industry. *Journal of Knowledge Management Practice, Vol. 14, Issue 2.*

Cichy, C., & Rass, S. (2019). An overview of data quality frameworks. *IEEE Access, Vol. 7*, 24634–24648, available at: https://doi.org/10.1109/access.2019.2899751.

Dahiya, O., Solanki, K., & Dhankhar, A. (2020). *Risk-based testing: Identifying, assessing, mitigating & managing risks efficiently in software testing*, available at: https://doi.org/10.31224/osf.io/3w5v8.

Durst, S., & Zieba, M. (2018). Mapping knowledge risks: Towards a better understanding of knowledge management. *Knowledge Management Research & Practice, Vol. 17, Issue 1,* 1–13, available at: https://doi.org/10.1080/14778238.2018.1538603.

Durst, S., Hinteregger, C., & Zieba, M. (2019). The linkage between knowledge risk management and organizational performance. *Journal of Business Research, Vol. 105*, 1–10, available at: https://doi.org/10.1016/j.jbusres.2019.08.002.

Friedrich, J., Becker, M., Kramer, F., Wirth, M., & Schneider, M. (2020). Incentive design and gamification for knowledge management. *Journal of Business Research, Vol. 106*, 341–352, available at: https://doi.org/10.1016/j.jbusres.2019.02.009.

Granato, A., & Polacek, A. (2019). The growth and challenges of cyber insurance. *Federal Reserve Bank of Chicago*. Available at: https://www.chicagofed.org/publications/chicago-fed-letter/2019/426.

Gressgård, L.J. (2014). Knowledge management and safety compliance in a high-risk distributed organizational system. *Safety and Health at Work, Vol. 5, Issue 2,* 53–59, available at: https://doi.org/10.1016/j.shaw.2014.03.002.

Jones, L.A. (2020). Reputation Risk and Potential Profitability: Best Practices to Predict and Mitigate Risk through Amalgamated Factors. *Capitol Technology University ProQuest Dissertations Publishing*, Order No. 28152966, available at: https://www.proquest.com/dissertations-theses/reputation-risk-potential-profitability-best/docview/2466047018/se-2.

Landoll, D.J. (2021). The security risk assessment handbook: A complete guide for performing security risk assessments. *CRC Press*.

Li, Z., Wei, J., Marinova, D.V., & Tian, J. (2020). Benefits or costs? The effects of diversification with cross-industry knowledge on corporate value under crisis situation. *Journal of Knowledge Management, Vol. 25, Issue 1*, 175–226, available at: https://doi.org/10.1108/jkm-11-2019-0659.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. *Energy Reports, Vol. 7*, 8176–8186, available at: https://doi.org/10.1016/j.egyr.2021.08.126.

Lipa, M. (2020). Risk-knowledge infinity cycle. *Pharmaceutical Regulatory Science Team*, available at: https://prst.ie/rkicycle.

Lipa, M., Kane, P., & Green, A. (2022). Advancing competency in managing risk and knowledge: Steps toward operationalisation of the risk-knowledge infinity cycle (RKI cycle) – Part 1: Improving effectiveness of risk-based decision making (RBDM). *Technological University Dublin*, available at: https://doi.org/10.21427/JV8W-0272.

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

Oladejo, B. (2019). A knowledge management system for intellectual property management in legal firms. *African Journal of Computing & ICT Reference Format, Vol. 12, Issue 4*, 1–12.

Rhem, A.J. (2015). *Why do knowledge management (KM) programs and projects fail? Knowledge Management Institute*, available at: https://www.kminstitute.org/blog/why-do-knowledge-management-km-programs-and-projects-fail.

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). *Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk?*. Available at: https://doi.org/10.7249/wr1208.

Rumanti, A.A., Wiratmadja, I.I., Sunaryo, I., Ajidarma, P., & Ari Samadhi, T.M. (2019). Firm innovation capability through knowledge sharing at Indonesian small and medium industries: Impact of tacit and explicit knowledge perspective. *IEEE 6th International Conference on Industrial Engineering and Applications (ICIEA),* Tokyo, Japan, available at: https://doi.org/10.1109/iea.2019.8714947.

Sickler, J. (2021). *What is reputational risk? Defining and managing reputation risk*. Available at: https://www.reputationmanagement.com/blog/reputational-risk.

Su, H. (2014). Business ethics and the development of intellectual capital. *Journal of Business Ethics, Vol. 119, Issue 1*, 87–98, available at: https://doi.org/10.1007/s10551-013-1623-4.

Talet, A., & Talet, M.Z. (2018). The role of knowledge management with risk management for information technology projects risk assessment. *International Journal of Environment and Sustainability, Vol. 6, Issue 2*, 1–18.

Torabi, S.A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science, Vol. 89*, 201–218, available at: https://doi.org/10.1016/j.ssci.2016.06.015.

Yarovenko, H., Bilan, Y., Lyeonov, S., & Mentel, G. (2021). Methodology for assessing the risk associated with information and knowledge loss management. *Journal of Business Economics and Management, Vol. 22, Issue 2*, 369–387, available at: https://doi.org/10.3846/jbem.2021.13925.