The Interplay Between Knowledge Vulnerabilities and Trigger Parameters in the Occurrence of Knowledge Risks

Andrei Ștefan Neștian, Alexandra Luciana Guță and Silviu Mihail Tiță
Department of Management, Marketing and Business Administration, Faculty of Economics and Business Administration, Alexandru Ioan Cuza University of Iași, Romania

nestian@uaic.ro
luciana_guta@yahoo.com
silviutita@yahoo.com

Abstract: This study advances a new theoretical approach to understanding knowledge risk occurrence determined by the interplay between knowledge vulnerabilities and trigger parameters. While it is a continuation of a research project that investigated knowledge risk and the subsumed concept of "knowledge vulnerability", this framework fills a theoretical gap in the literature by putting forward an explanation for the occurrence of a knowledge risk from a process-based perspective conceptualised through knowledge vulnerabilities, events, triggers and impact. This study integrates theories of system accidents for developing a new theoretical framework. The Swiss Cheese Model of System Accidents (Larouzee and Le Coze, 2020) provides a foundation for a new process-based perspective on the occurrence of knowledge risks. Although knowledge vulnerabilities could be interpreted as weak points within knowledge systems, they do not, in themselves, generate adverse consequences. Instead, they represent the underlying conditions that give rise to the occurrence of knowledge risks, the manifestation of which subsequently causes a negative organisational impact. According to Bratianu and Bejinaru (2022), a vulnerability reflects a weakness in a system, in relation to external forces that could lead to different types of damages. Accordingly, follows a sequence that involves a vulnerability, an event or trigger, and a resulting negative impact on organizational knowledge or organizational outcome (e.g. quality level). We also examined the trigger parameters of the occurrence of a knowledge risk: intensity (magnitude), duration (persistence), dose (cumulative effect). This process-based approach to knowledge risks occurrence is illustrated using the knowledge risk types most commonly discussed in the literature. This paper contributes to better understanding on how knowledge risks may occur by adopting a process-based perspective that links knowledge vulnerabilities to knowledge risk occurrence.

Keywords: Knowledge vulnerabilities, Knowledge risks, Events, Trigger parameters, Process-based perspective

1. Introduction

In his seminal book on the fifth discipline – systems thinking, Senge (1990) identified five disciplines that describe learning organizations. Applying systems thinking in organizations requires organisational members to perceive the organization as a system. According to Senge (1990), systems thinking provides a framework for observing interrelationships rather than things, and for recognizing patterns of change instead of static representations at a single point in time.

In organizations where managers adopt systems thinking, appropriate *knowledge management systems (KMSs)* and *knowledge management routines* are expected to be established and continuously developed. When referring to KMSs, it is important to consider the interplay among people, processes and technology. The effectiveness of KMS consequently affects both organizational performance and business sustainability (Bratianu, Bejinaru and Ursache, 2024). KMSs are developed to facilitate organizational knowledge processes, including creation, store, retrieve, transfer and application (Alavi and Leidner, 2001, cited in Wang and Wang, 2016, p. 829). In this paper, we conceptualize KMSs as process integrators.

In this paper, we develop a process-based perspective for explaining knowledge risk occurrence. Although knowledge risks originate from knowledge vulnerabilities, the latter cannot produce negative consequences by themselves. Vulnerabilities can be described as "inherent characteristics of a system that create the potential for harm but are independent of the probabilistic *risk of the occurrence* ("event risk") of any particular hazard or extreme event" (Sarewitz, Pielke Jr. and Keykhah, 2003, p. 805). Adapting the concept of "vulnerability" to the field of knowledge management, according to Bratianu and Bejinaru (2022) knowledge vulnerabilities reflect weaknesses in a system that, in interaction with external forces, may lead to different types of damage, including human, financial, operational or physical damage. For the purposes of this study, the term "systems" refers to KMSs. Thus, this conceptual paper focuses on a sequence comprising a vulnerability, an event or trigger, and a resulting on either organizational knowledge, or an organizational outcome. In the latter case, examples include problems related to the quality achieved across different work processes or inconsistencies in the quality of the products or services provided by an organization. Consequently, the aim of this theoretical

research is to propose a new theoretical approach to knowledge risk occurrence determined by the interplay between knowledge vulnerabilities and trigger parameters.

2. Literature Review

This theoretical study focuses on the underlying mechanisms of the manifestation of knowledge risk. The fundamental concepts addressed in this paper, drawn from the field of knowledge management, are "knowledge risks" and "knowledge vulnerabilities". To these concepts, we add the notion of "trigger parameters". The conceptual mechanism developed and explained in this paper also incorporates the concepts of "event" and "impact".

Whereas a knowledge vulnerability represents a weakness within a knowledge system that may result in damage when exposed to external forces (adapted from Bratianu and Bejinaru, 2022), a knowledge risk reflects a situation with potential negative consequences generated by decisions concerning knowledge processes, influenced by external or internal factors (Cameron and Raman, 2005; Massingham, 2010; Massingham, 2020; Society for Risk Analysis, 2018). To gain deeper conceptual insights into risk manifestation, we analyzed models that explain the manifestation of risks in general. In addition to the classical models of probabilistic explanation, which conceptualize risk = probability x impact, we have discovered a second category, models built around the idea of occurrence of a triggering event of an accident. Two models contain useful explanatory elements for the manifestation of knowledge risks: the Swiss Cheese Model of System Accidents (Larouzee and Le Coze, 2020) and the bow-tie model (Delvosalle et al, 2006; Dianous and Fiévez, 2006). The Swiss Cheese Model of Systemic Accidents is a subcategory of systemic accident models. It uses the metaphor of holes in layers of defense to represent vulnerabilities, referred to as weaknesses in the model. The manifestation of risk is described as a situation in which an event passes through the cheese (representing the system) by traversing one of its holes, thus a triggering event encountering a vulnerability is needed (adapted from Larouzee and Le Coze, 2020; Reason, 2000).

To understand the latent nature of knowledge vulnerability, we can use Reason's (1993) perspective, used in the development of the Swiss Cheese Model. The author argues that identifying latent organizational failures is essential for the safety of complex systems. In his view "*Active failures* are unsafe acts committed by those at the "sharp end" of the system" (Reason, 1993, p. 224). They are the individuals who operate at the human-system interface, and "whose actions can, and sometimes do, have immediate adverse consequences" (Reason, 1993, p. 224). In contrast, he describes *latent failures* as "fallible decisions, taken at the higher echelons of the organization, whose damaging consequences may lie dormant for a long time, only becoming evident when they combine with local triggering factors (i.e., active failures, technical faults, atypical system states, etc.,) to breach the system's defenses" (Reason, 1993, p. 224).

According to the Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2013, p. 4), risk "is defined as the possibility that an event will occur and adversely affect the achievement of objectives" or as an event with a negative impact, "which can prevent value creation or erode existing value" (COSO, 2004b, p. 2). Events have the potential to hinder an organization's ability to achieve its operational goals. An event can also be interpreted as an incident or an occurrence from internal or external sources affecting the implementation of a strategy or the achievement of objectives (COSO, 2004a). The definition of an event proposed in the COSO (2004a) framework serves as a theoretical foundation for many risk management courses. The International Organization for Standardization (ISO) defines an event in its risk management vocabulary as the "occurrence or change of a particular set of circumstances" (ISO, 2022, Clause 3.3.11). Together with the perspectives discussed above, this definition provides a conceptual foundation that can be readily adapted and applied to the context of knowledge risks and knowledge vulnerabilities.

Within an event, the concept of "trigger" is associated with a limit dose. We argue that below the limit dose, no event occurs. So, a dose below the limit has no potential to damage the outcomes of knowledge processes. In contrast, an event occurs when there is an above-limit dose, meaning that the dose has the potential to damage the outcomes of knowledge processes. Accordingly, we consider the limit dose to be regarded as the trigger.

For investigating these triggers, we take into consideration the following trigger parameters for knowledge risk occurrence: intensity (magnitude), duration (persistence), dose (cumulative effect). Hence, the concept of "event" is defined as being "a single action or outcome which characterizes a failure and potentially its subsequent propagation" (Cameron and Raman, 2005, p. 172). The occurrence of an event signifies that the knowledge system is exposed to an above-limit dose. Conversely, in the scenario of an absence of an event,

vulnerabilities can be considered to remain inactive or latent. In the perspective adopted in this study, dose represents the cumulative effect of intensity and duration. Accordingly, an above-limit dose is characterized by sufficient intensity and duration for an event to occur.

An interesting and complementary perspective is to view an event as a bifurcation point in a process. Event Tree Analysis, a methodology used for system security assessment, identifies events as generating a transition from the planned or normal operation of a process to an unplanned or abnormal mode of operation. Event Tree Analysis "begins by identifying the initial event and examines the event's development under different protective layers, creating a tree structure with paths illustrating the evolution from the initial event to potential consequences" (Zhu et al, 2025, p. 315).

In terms of risk management, before the occurrence of an event, the focus is on "threats", managers being primarily concerned with prevention. During and after the occurrence of an event, the focus shifts to "consequence management", where the manager's concentrate on mitigating and reducing the resulting consequences. In the *pre-event phase,* referred to as pre-crisis by Choraś et al (2016), it is important to implement a risk management process that enables the organization to anticipate risks and respond proactively (Choraś et al, 2016). In the *post-event phase*, referred to as post-crisis by Choraś et al (2016), it is important to maintain process functionality and identify the "lesson learned" from risk occurrence. These lessons provide feedback throughout the process for reducing the impact and the probability of similar risks occurring in the future (Choraś et al, 2016).

A related perspective, known as the "bow-tie" approach, is found in the works of de Dianous and Fiévez (2006) and Delvosalle et al (2006). Both studies describe an event as a bow-tie, in which, potential source of failure, referred to as "hazards", converge to the event from the left, while multiple potential consequences diverge from the event to the right. In line with this methodology, the bow-tie model is "centred on a critical event and composed of a fault tree on the left and of an event tree on the right" (de Dianous and Fiévez, 2006, p. 221). The bow-tie model also distinguishes the "top event", defined as the point where control over the process is lost, moment at which the situation can begin to deteriorate (Fiorentini and Marmo, 2018). Accordingly, risk management involves setting safety barriers on both sides of the event: to prevent the errors and block the expansion of negative consequences.

Based on the concepts analysed above, this study proposes a new process-based perspective on knowledge risk occurrence adapted from the theories in the field of system accidents, particularly the Swiss Cheese Model of System Accidents (Larouzee and Le Coze, 2020).

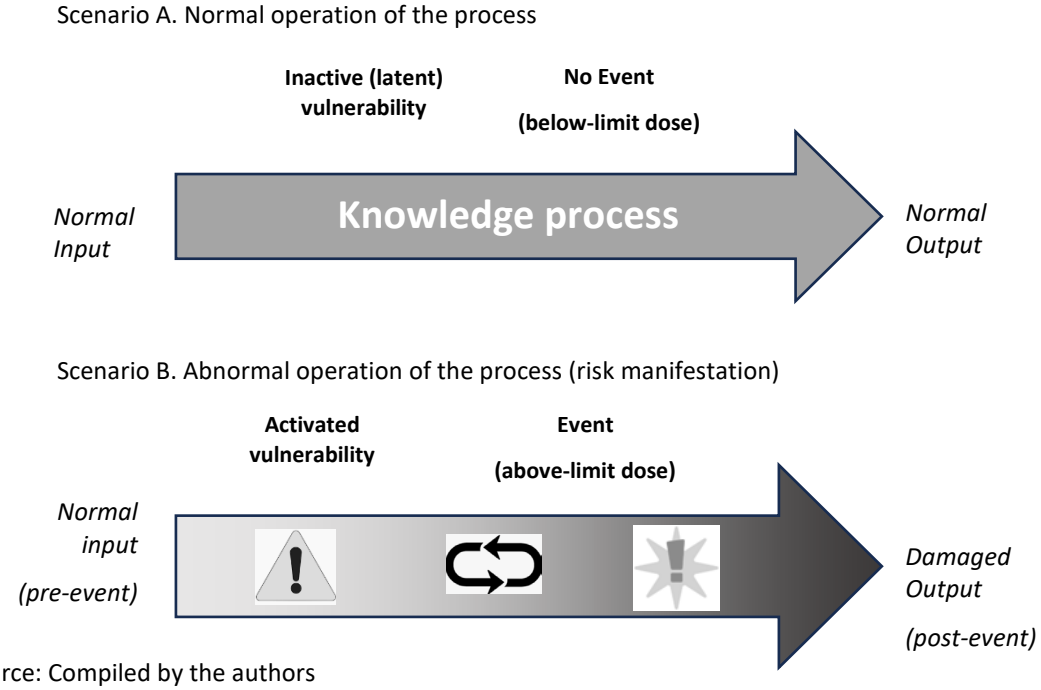
In a paper analysing the Swiss Cheese Model and its critiques, Larouzee and Le Coze (2020, p. 3), drawing on examples of disasters and the reports investigating them, argue that "human error, in itself, appeared to have limited value in making sense of the conditions that triggered disasters." Building on this perspective, we argue that, in situations with the potential of negative consequences, the robustness of a system may be more important than the occurrence of an individual employee's error.

The literature on knowledge risks either contains general classifications of knowledge risks or links them to knowledge processes. Durst and Zieba (2017) identify the following main types of knowledge risks: knowledge loss, knowledge attrition, knowledge leakage, knowledge spillover, knowledge waste, knowledge hiding and knowledge hoarding. In contrast, process-oriented approaches relate knowledge risks to the different knowledge processes in which they may occur. For example, Bratianu, Neștian and Guță (2022) proposed a taxonomy of knowledge risks based on the following knowledge processes: knowledge creation, knowledge acquisition, knowledge loss, knowledge sharing, knowledge use, emotional knowledge dynamics and spiritual knowledge dynamics. Their taxonomy is grounded in the concept of organizational knowledge dynamics, according to which the value of organisational knowledge may decrease as knowledge risks occur (Bratianu, Neștian and Guță, 2022).

3. The Proposed Model

Let us consider a stable system operating through a continuous process in which there is a vulnerability. The system's outputs remain within acceptable limits as long as no triggering events occur, that, through their interaction with the existing vulnerability, induce a transition of the system to an undesirable state. The change in the state of the system during such an event, resulting from the existence of a vulnerability, can be explained by a dose-response mechanism. Thus, exposing the system's vulnerability to a lower dose of the event-generated "stimulus" may allow the system to maintain its current state. Above a certain dose (quantity, value or intensity of that "stimulus", duration), the vulnerability may generate a different response, causing

the system to transition from its continuous (stable) state to a different state. This mechanism is illustrated in Figure 1.



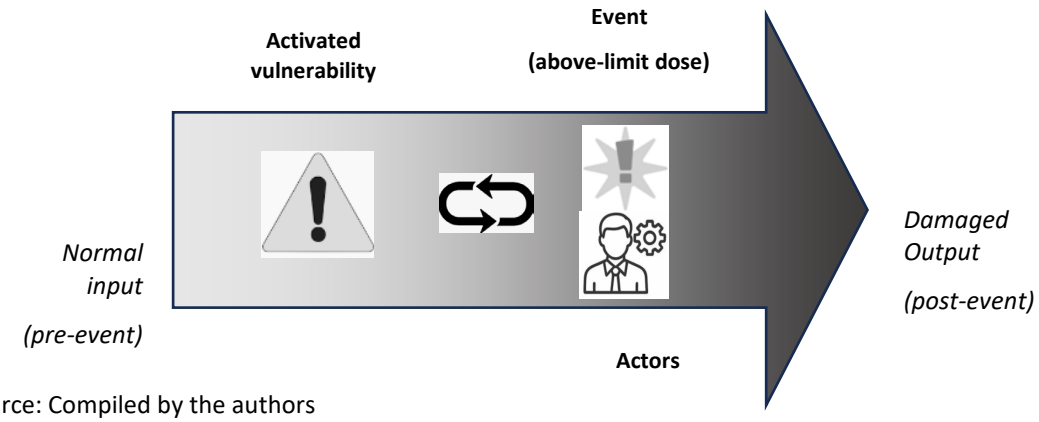
Source: Compiled by the authors

Figure 1: Normal operation and risk manifestation scenarios

Therefore, we can conceptualize a response function describing the effect of the intensity of the stimulus generated by the event on the vulnerability, in which the output of the function represents the consequences for the state of the system or of its output or outcome. The response functions of a vulnerability to a stimulus within an event may be different: they may be stepped ladder (discontinuous), continuous, binary (Yes/ No), and so on.

For example, not every departure of an older employee leads to a loss of knowledge for the organization. If a mediocre employee leaves, there is a higher probability that all their knowledge has already been incorporated into the procedures, rules and actions in the processes in which they have intervened. However, if the value of their knowledge is high (e.g. they are an exceptional employee or a leader in their professional field), and a consistent part of it is tacit, the loss of their unique knowledge may be irremediable. From our perspective, potential damage is associated with both the loss of tacit knowledge and to the lack of capability to develop the tacit knowledge available throughout the organization. As highlighted by Nonaka and Takeuchi (2019, p. 4) "dependence on explicit knowledge prevents companies from coping with change". In this case, the dose is represented by the "value" of the knowledge that the company loses when the event, namely "the retirement of employee X", occurs. The vulnerability, in this case, is represented by the employee's uniqueness and the value of their knowledge. Because of inadequate knowledge management, the organization failed to implement measures to ensure that this tacit knowledge was articulated and included into procedures, lessons learned by others, and so on. The higher the value of an employee's tacit knowledge, the higher the "dose". The lower its diffusion, the greater the vulnerability. The concentration of knowledge in a small number of individuals represents a vulnerability, while a departure of one of these individuals constitutes the triggering event. This example is related to a lack of *knowledge sharing* and may also be associated with *knowledge hoarding* or *knowledge hiding*. It also represents a form of *knowledge loss*, with a negative impact on knowledge use within the organization.

The following diagram presents the proposed model of risk occurrence, based on the interaction between vulnerabilities and events with a dose-response mechanism.



Source: Compiled by the authors

Figure 2: The AVEALD (Activated Vulnerability by an Event with an Above-Limit Dose) Model for Knowledge Risk Manifestation

A knowledge risk materialises when, within a knowledge process characterized by a latent knowledge vulnerability, an event occurs involving the intervention of actors, thereby exposing the vulnerability to an above-limit dose. The vulnerability and the parameters of the triggering event together generate a different state of the process, characterised by a damaged output, as shown in Figure 2.

Reason (2000) proposed two approaches to human error: the person approach and the system approach. While the person approach focuses on individuals' errors – an approach that involves blaming humans for lack of attention or forgetfulness – the system approach focuses on the conditions under which employees work, seeking to build defences that prevent the occurrence of errors or mitigate their effects. Our focus on vulnerabilities, interpreted as weak points within KMSs, and their interplay with trigger parameters in the occurrence of knowledge risks is aligned with Reason's (2000) system approach.

The Swiss Cheese Model presents the barriers within a system as slices of cheese and the system's weaknesses as holes in the cheese (Larouzee and Le Coze, 2020). However, as Larouzee and Le Coze (2020) point out, the diagram illustrating the Swiss cheese model proposed by Reason (2000) did not distinguish between active and latent errors (named by Reason, 2000, as active failures and latent conditions), although this differentiation was made in the paper. Latent conditions refer to "micro view of human error, which sees accidents (human error) and safety (human performance) as two sides of the same coin" (Larouzee and Le Coze, 2020, p. 4). From the Swiss cheese model, we adopt to the concept of latent errors or conditions. These latent conditions include the notion of "safety", which contrasts with the presence of vulnerability in a system.

Considering the above explanations regarding knowledge risk manifestation, we further present several examples linking the concepts of vulnerability, trigger, dose, manifested risk and impact within organizations. In these examples, we take into consideration two concepts: intensity (magnitude) and duration (persistence). The dose is the cumulative effect of these two dimensions. In risk management, the discussion of magnitude has a long history. Johnson (1998) proposes a scale for measuring risk intensity based on the Richter Earthquake Measurement Scale. Moody's Analytics (2022) refers to persistence in a report examining this concept in the context of environmental, social and governance risk management culture. Persistence is considered a characteristic of such a culture and refers to the introduction, maintenance, and updating of risk mitigation measures. These ideas can be adapted to the field of knowledge risks.

An example of a sequence starting from vulnerabilities, passing through events, considering a certain dosage and leading to negative impact focuses on the risk of *knowledge loss* and considers its impact on *knowledge use*. Let us consider a situation in which an organization's knowledge is concentrated in a small number of employees. Let us add to this context a lack of succession planning within the organization. These are the two vulnerabilities considered in this example. In this case, the triggers could consist of employees leaving the organization or retiring, or the employees leaving a community of practice. The dose is determined by the level of expertise of those employees. If an employee is an expert possessing unique knowledge, especially in the form of tacit knowledge, the impact could be the dissolution of the core knowledge network. The greater the magnitude (intensity) and the persistence (duration) of the triggers, the greater the negative consequences for an organization in terms of the loss of core knowledge. Thus, this example focuses knowledge loss risks while also illustrating their negative implications for the organization's use of knowledge.

Another relevant example can be described based on the presence of other vulnerabilities related to *knowledge loss*, with potential negative impact on the way the organization *creates* and/ or *uses knowledge*. Such vulnerabilities include the improper classification of the knowledge that should be classified and lack of, or insufficient mechanisms for protecting databases and more complex information systems used for knowledge storing. The triggers would consist of situations in which certain knowledge is needed but is difficult to access, or situations in which knowledge that should not be accessible can nevertheless be accessed. The dose is determined by the sensitivity of that knowledge, referring both to situations in which needed knowledge is difficult or impossible to access, and to situations in which knowledge can be accessed although it should not be accessible. In the first case, the potential impact on the organization (the damaged outcome) consists of difficulties in the process of *knowledge use* (e.g. working with incomplete knowledge) or in the process of *knowledge creation* (e.g. poor data collection and/ or analysis). In the second case, the potential impact for organizations (the damaged output) consists of difficulties generated by the *spillover* of sensitive knowledge to a competing entity, for example by facilitating pre-emptive market promotions launched by a competitor. This example refers to risks related to knowledge loss and knowledge spillover while also highlighting their implications for knowledge creation and knowledge use.

Our next example is related to *knowledge waste*. According to Durst and Zieba (2017, p. 55), knowledge waste "means not making use of the available and potentially useful knowledge in the organisation". In this case, the vulnerability within a KMS consists of an improper mechanism for transferring knowledge either from the individual to the team level, from the team to the organizational level, or both. Another vulnerability arises when certain knowledge is available at organizational level, but managers either lack the experience to make use of that knowledge or do not possess the tacit knowledge and intuition needed to recognise the opportunity to use it. In this case, the trigger consists of situations in which organizations need to generate new ideas in order to remain competitive but, for various reasons, fail to do so. The dose is determined by the utility of the knowledge that remains unused. The impact may consist of a decrease in an organization's competitiveness.

4. Discussion

The proposed model, AVEALD (Activated Vulnerability by an Event with an Above-Limit Dose), postulates that the manifestation of a knowledge risk within a process is related both to the existence of one or more vulnerabilities and to the occurrence of an event capable of activating them. This approach incorporates the idea of the latent existence of knowledge vulnerabilities, created and overlooked by managers and other actors involved in the process. Therefore, knowledge managers need to assess these latent vulnerabilities in order to understand and mitigate knowledge risks. The proposed model also includes the idea that a manifestation of a knowledge risk requires a triggering event of a certain intensity, a certain duration, or "dose". This requires knowledge managers to estimate the limit dose of potential events capable of activating latent vulnerabilities. Understanding this non-linear conceptual model is important for predicting scenarios in which the organization may encounter difficulties in one or more knowledge processes. Accordingly, the operational focus for knowledge managers should shift from the general objective of mitigating knowledge risks to a process-oriented perspective centred on identifying and assessing vulnerabilities, together with evaluating the limit dose of events that may activate them.

5. Conclusion

The aim of this study was to propose a new theoretical approach to knowledge risk occurrence caused by the interplay between knowledge vulnerabilities and trigger parameters. To develop this approach, we considered the most frequently addressed types of knowledge risks in the knowledge management literature.

The novelty of our approach lies in adopting a sequential perspective involving vulnerabilities, events or triggers, and the possible negative impacts on either organizational knowledge or an organizational outcome or output. We considered the following trigger parameters related to the occurrence of a knowledge-related risk: intensity (magnitude), duration (persistence) and dose (cumulative effect). Through this approach, we introduce a new perspective, that complements the classical probabilistic perspective on knowledge risk manifestation and is congruent with it.

Also, understanding this non-linear conceptual model is useful for predicting scenarios in which organizations may face difficulties related to knowledge processes. To better understand and mitigate knowledge risks, managers, and particularly knowledge managers, need to assess the latent vulnerabilities, as well as the limit dose of potential events capable of activating them. Additionally, in the case of small and medium sized

enterprises (SMEs), managers should also pay attention to the possibility that knowledge risks may be even greater, as the small size of these organizations may result in more limited knowledge stocks or flows than in larger organizations.

The limitation of this research lies in its theoretical nature. Further research aimed at developing measurement instruments would be appropriate and would require the creation of methodologies to overcome the difficulties in operationalizing the concepts referred to in this study.

Ethics Declaration: Ethical clearance was not required for the research.

AI Declaration: AI tools have not been used for the creation of the paper.

References

Bratianu, C. and Bejinaru, R. (2022) Exploring vulnerabilities and risks related to knowledge management systems. In Schiuma, G. and Bassi, A. (eds.) Proceedings of the 17th International Forum for Knowledge Asset Dynamics, pp 687-700.

Bratianu, C., Bejinaru, R. and Ursache, V.M. (2024) "The Impact of Knowledge Vulnerabilities on Knowledge Risks", Review of International Comparative Management, Vol 25, No. 1, pp 70-79. doi: 10.24818/RMCI.2024.1.70.

Bratianu, C., Neștian, A.Ș. and Guță, A.L. (2022) "Knowledge risks taxonomy based on the organizational knowledge dynamics", Ekonomicko-manazerske spektrum, Vol 16, No. 2, pp 61-71. doi: 10.26552/ems.2022.2.61-71.

Cameron, I.T. and Raman, R. (2005) Process Systems Risk Management, 1st Edition, Elsevier, Amsterdam.

Choraś, M., Kozik, R., Flizikowski, A., Hołubowicz, W. and Renk, R. (2016) Cyber Threats Impacting Critical Infrastructures. In Setola, R., Rosato, V., Kyriakides, E. and Rome, E. (eds.) Managing the Complexity of Critical Infrastructures: A Modelling and Simulation Approach. Studies in Systems, Decision and Control, Vol 90, pp 139-161, Springer, Cham. doi: 10.1007/978-3-319-51043-9_7.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004a) "Enterprise Risk Management – Integrated Framework. Application Techniques", [online], https://www.macs.hw.ac.uk/~andrewc/erm2/reading/ERM%20-%20COSO%20Application%20Techniques.pdf.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004b) "Enterprise Risk Management – Integrated Framework. Executive Summary", [online], https://ms.hmb.gov.tr/uploads/sites/2/2019/09/COSOERM.pdf.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013) "Internal Control – Integrated framework. Executive Summary", [online], https://www.sechistorical.org/collection/papers/2010/2013_0501_COSOInternal.pdf.

de Dianous, V., and Fiévez, C. (2006) "ARAMIS project: A more explicit demonstration of risk control through the use of bow–tie diagrams and the evaluation of safety barrier performance", Journal of Hazardous Materials, Vol 130, pp 220–233. doi: 10.1016/j.jhazmat.2005.07.010.

Delvosalle, C., Fievez, C., Pipart, A. and Debray, B. (2006) "ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries", Journal of Hazardous Materials, Vol 130, pp 210–219. doi: 10.1016/j.jhazmat.2005.07.005.

Durst, S. and Zieba, M. (2017) "Knowledge risks – towards a taxonomy", International Journal of Business Environment, Vol 9, No. 1, pp 51-63.

Fiorentini, L. and Marmo, L. (2018) "Sound Barriers Management in Process Safety: Bow-tie Approach According to the First Official AIChE-CCPS Guidelines", Chemical Engineering Transactions, Vol 67, pp 253-258. doi: 10.3303/CET1867043.

International Organization for Standardization (ISO) (2022) "ISO 31073:2022(en) Risk management –Vocabulary", [online], https://www.iso.org/obp/ui/#iso:std:iso:31073:ed-1:v1:en:term:3.3.11.

Johnson, R. (1998) "Risk Management by Risk Magnitudes", [online], https://www.unwin-co.com/files/RiskMgtByRiskMags,1998.pdf.

Larouzee, J. and Le Coze, J.-C. (2020) "Good and bad reasons: The Swiss cheese model and its critics", Safety science, Vol 126, 104660. doi: 10.1016/j.ssci.2020.104660.

Massingham, P. (2010) "Knowledge risk management: a framework", Journal of Knowledge Management, Vol 14, No. 3, pp 464-485. doi: 10.1108/13673271011050166.

Massingham, P. (2020) Knowledge management: Theory in practice, SAGE Publications Ltd, London.

Moody's Analytics (2022) "Measuring Persistence in ESG Risk Management Culture", [online], https://www.moodys.com/web/en/us/insights/resources/Measuring_Persistence_in_ESG_June2022.pdf.

Nonaka, I. and Takeuchi, H. (2019) The Wise Company: How Companies Create Continuous Innovation, Oxford University Press, New York.

Reason, J. (1993) The Identification of Latent Organizational Failures in Complex Systems. In Wise, J. A., Hopkin, V. D. and Stager, P. (eds.) Verification and Validation of Complex Systems: Human Factors Issues. NATO ASI Series, Vol 110, pp 223–237, Springer, Berlin, Heidelberg. doi: 10.1007/978-3-662-02933-6_13.

Reason, J. (2000) "Human error: models and management", BMJ, Vol 320, pp 768-770. doi: 10.1136/bmj.320.7237.768.

Sarewitz, D., Pielke Jr., R. and Keykhah, M. (2003) "Vulnerability and Risk: Some Thoughts from a Political and Policy Perspective", Risk Analysis, Vol 23, No. 4, pp 805-810. doi: 10.1111/1539-6924.00357.

Senge, P. M. (1990) The Fifth Discipline: The Art and Practice of the Learning organization, Doubleday, New York.

Society for Risk Analysis (2018) "Society for Risk Analysis Glossary", [online], https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf.

Wang, Y.-M. and Wang, Y.-C. (2016) "Determinants of firms' knowledge management system implementation: An empirical study", Computers in Human Behavior, Vol 64, pp 829-842. doi: 10.1016/j.chb.2016.07.055.

Zhu, T., Meng, C., Han, X., Wang, Y., Dang, J., Chen, H., Qi, M. and Zhao, D. (2025) "A risk assessment framework for water electrolysis systems: Mapping System Theoretic Process Analysis (STPA) and Event Tree Analysis (ETA) into Fuzzy Bayesian Networks (FBN)", Process Safety and Environmental Protection, Vol 194, pp 306-323. doi: 10.1016/j.psep.2024.11.117.