

CORRELATIONS BETWEEN KNOWLEDGE RISKS AND KNOWLEDGE VULNERABILITIES ALONG KNOWLEDGE PROCESSES

Ștefan Andrei NEȘTIAN^a, Alexandra Luciana GUȚĂ^b, Silviu Mihail TIȚĂ^{c}*

^{a, b, c} Alexandru Ioan Cuza University of Iași, Romania

ABSTRACT

This research is a continuation of a study conducted in 2023 on the subject of knowledge vulnerabilities and risks in knowledge processes, within private companies. The initial study has been presented at an international conference and aimed to put forward measuring scales for the concepts of "knowledge vulnerabilities" and "knowledge risks", using a new ontology developed by Brătianu et al. (2022) in order to develop an instrument for measuring both knowledge risks and knowledge vulnerabilities. The present study aims to analyze the relationships that we found between the components of a latent variable that we named "types of knowledge vulnerabilities" and the components of another latent variable, namely "types of knowledge risks". This paper uses the components that were identified for types of knowledge vulnerabilities and for types of knowledge risks in the previous study, based on a sample of 117 valid questionnaires, the respondents being managers and employees (non-managers) from private companies from various fields of activity. The main findings of this study show that vulnerabilities related to knowledge loss and knowledge use present moderate positive and statistically significant correlations with all the knowledge risks components and that vulnerabilities related to emotional and spiritual knowledge dynamics presents a strong positive correlation with the risks with a similar name.

KEYWORDS: *correlation analysis, knowledge process, knowledge risk, knowledge vulnerability.*

DOI: 10.24818/IMC/2023/02.06

1. INTRODUCTION

The complexity of the knowledge management process, which includes activities and methods for creating, acquiring, storing, transferring and applying knowledge, generates a series of risks and vulnerabilities that need to be identified, analyzed, and addressed with the aim of avoiding or transforming them. Knowledge management can be seen as a set of processes enabling the construction of an organizational memory that integrates formal, informal, and semi-formal knowledge (Staab et al., 2001). The intensive use of information technologies in all processes can facilitate the increase in vulnerabilities and risks specific to knowledge management processes.

In the field of knowledge management, risks are abstract concepts. We refer in this case to different types of situations in which organizational knowledge can be affected in a negative way. Knowledge risk "describes a likelihood of any loss resulting from the identification, storage or protection of knowledge that may decrease the operational or strategic benefit of a company" (Durst (2019, p. 21).

* Corresponding author. E-mail address: silviutita@yahoo.com.

Knowledge risks – e.g. knowledge loss as a particular type of knowledge risk – are related to various managerial decisions regarding activities such as: human resource management (employee resignations, their retirement, providing essential information to poorly trained individuals or those lacking knowledge utilization and transfer skills); security or cyber-security; production or operations process management; reporting errors, etc. They are also related to vulnerabilities of the managerial system, which can include: reduced decision-making capacity; outdated or state-of-the-art technology that can transmit information to various web addresses through artificial intelligence programs; employee negligence driven by the low level of involvement and loyalty of new generations. In the current economic context, all these can lead to a series of changes in knowledge processes, of which, in our opinion, organizations must be aware and identify countermeasures. The aim of the study is to analyze the relationship between knowledge vulnerabilities components and knowledge risks components.

2. LITERATURE REVIEW

Knowledge is currently an important resource in the economic environment, and the management's ability to use it effectively and efficiently can lead to relevant outcomes.

Knowledge risk is defined, in different perspectives, as operational risk, caused by situations such as dependency on, transfer that was not intended, transfer that was intended but was not successful, or loss of knowledge assets (Bayer & Maier, 2006) or it can even reflect "a state of incomplete knowledge about an event or about the future" (Bratianu, 2018, p. 594). Knowledge risk requires a careful consideration of the nature of collaborative relationships, of the nature of risks or the contexts of the networks that organizations embark on, since networks usually imply knowledge risks that are associated with knowledge sharing (Trkman & Desouza, 2012) and also, at individual level, requires consideration of knowledge hiding, forgetting, unlearning, hoarding, missing or even inadequate competencies of employees (Durst & Zieba, 2019). A specific aspect about knowledge risks is that managers start caring about them in those cases when their appearance has negative consequences which imply losses that are significant for the organization (Bratianu et al., 2022).

According to the Oxford Learner's Dictionaries (n.d.), "vulnerability" is "the fact of being weak and easily hurt physically or emotionally", while "risk" is "the possibility of something bad happening at some time in the future; a situation that could be dangerous or have a bad result". The connection between the two concepts is also evident in the case of knowledge management. A supplementary characteristic is the volatility of knowledge in an organization's memory, meaning that you cannot be sure about their existence or availability, despite the fact that they are possessed by individuals or are registered as intellectual property of a company. Volatility, a characteristic of memory that loses content due to the disappearance of tension, according to *Dicționar Explicativ al Limbii Române (DEX)*, generates a series of threats at the organizational level such as attrition, leakage, waste or loss of knowledge (Zieba et. al., 2022). Knowledge loss is a type of risk that is hard to avoid in the present economic environment, because of increasing retirement and also employee's turnover (Durst & Zieba, 2017).

Vulnerabilities usually indicate weaknesses in a knowledge management system (Ursache, 2023). This is why it is necessary to understand and diagnose situations of this kind and take strategic or tactical decisions aimed at eliminating the effects of vulnerable points in order to reduce future risks of knowledge loss, as a particularly relevant type of knowledge risk. "Vulnerabilities differ from risks as they possess three specific underlying characteristics related to the manifestation of knowledge risks" (Neșțian & Guță, 2023, p. 961): they are determinants of the risk, they diminish the response capacity and the absorptive capacity of the system. Brătianu and Bejenariu (2022, p. 1) mention that "vulnerabilities represent the roots of all possible risks, and they should be known

when systems are designed for diminishing the probable negative consequences of risks occurrences" (Brătianu & Bejenariu, 2022, p. 1).

Since the literature on the subject of knowledge risks is theoretical, and the literature on knowledge vulnerabilities is both theoretical and scarce, through the present study we intend to advance the fields of knowledge risks and knowledge vulnerabilities. This study is a step forward in covering this gap in the scientific literature. The study has a more practical approach and uses quantitative analysis for drawing interpretations and conclusions.

The larger research, from which this study is part of, is based on a taxonomy of knowledge risks proposed by Brătianu et al. (2022). This taxonomy is based on a correspondence made between knowledge risks with the knowledge processes along which they can occur. The proposed clusters by Brătianu et al. (2022) are: knowledge creation, knowledge acquisition, knowledge loss, knowledge sharing, knowledge use, emotional knowledge dynamics, and spiritual knowledge dynamics. The perspective from which this new taxonomy was proposed is from organizational knowledge dynamics. Referring to the dynamics of knowledge, it is necessary to consider the possibility that, when knowledge risks manifest, knowledge might reduce its value, according to Brătianu et al. (2022).

3. METHODOLOGY

3.1 The study

This study focuses on a correlation analysis between the components of "types of knowledge vulnerabilities" and the components of "types of knowledge risks", being part of a larger research. The literature on knowledge risks and knowledge vulnerabilities is theoretical. The study in which part of this paper's authors have proposed scales for measuring knowledge vulnerabilities and knowledge risks is, from our knowledge, the first paper that proposed a quantitative approach regarding knowledge vulnerabilities and risks.

Our research strategy is survey-based, the data being collected for the initial study, and our method of analysis is quantitative (Saunders et al., 2007).

3.2 The research instrument and the sample

The questionnaire, that was conceived for and used also in the initial study, contained: a filter question (we were only interested in private companies and not public institutions or not-for-profit organizations), a scale for measuring the types of knowledge vulnerabilities and another scale for the types of knowledge risks, and three questions regarding the position (management or execution) within the organization, length of service within the organization (under one year, between one and five years, over five years), the organization's field of activity (open question).

The scales for the latent variables "type of knowledge vulnerability" and "type of knowledge risk" have ranged from one to five, 1 meaning total disagreement (the situation is not found in the organization), 2 meaning disagreement (rarely found in the organization), 3 meaning neither disagreement, nor agreement (found sometimes), 4 meaning agreement (frequently found) and 5 meaning total agreement (the situation is currently found in the organization).

A number of 117 valid questionnaires have been obtained and used also in the initial study, which aimed to put forward measuring scales for the concepts of knowledge risks and knowledge vulnerabilities. The questionnaire was sent on online channels such as social media and software used in our research and teaching activities. A total of 420 people received the link with the questionnaire, from which 130 people completed it. However, 13 people did not work in private companies, this leading to a number of 117 valid responses.

A percentage of 46.15% of the responders are managers and 53.85% are non-managers. In the matter of seniority (the length of service in the organization), a percentage of 47.01% of the

respondents have a length between one and five years and a percentage of 35.04% have a length of over five years in the organization. Only 17.95% of the respondents have less than one year.

3.3 Data analysis

The results are interpreted starting from a correlation analysis that we undertook. Taking into consideration that the majority of the variables' distributions do not meet the normality condition (Table 1), Spearman's correlation coefficient is the appropriate coefficient for interpreting the correlations between the variables. The variables taken into consideration are the components of "type of knowledge vulnerability" and the components of "type of knowledge risk".

Table 1. Testing the normality of distributions

	Shapiro-Wilk		
	Statistic	df	Sig.
Risk_C1	.983	117	.145
Risk_C2	.962	117	.002
Risk_C3	.938	117	.000
Vulnerab_C1	.904	117	.000
Vulnerab_C2	.960	117	.002
Vulnerab_C3	.979	117	.065
Vulnerab_C4	.821	117	.000

Source: Authors' own processing

For the analysis, Statistical Package for the Social Science (SPSS, version 20) was used. The components have been obtained in the initial study, after performing consistency (reliability) and factor analyses (principal components analysis - PCA) in SPSS version 20, after obtaining the results in Google Forms, downloaded and processed in Microsoft Excel.

4. RESULTS AND INTERPRETATION

The correlations between the knowledge vulnerabilities components and knowledge risks components are presented below (Table 2).

Table 2. Correlations between knowledge risks components and knowledge vulnerabilities components

			Vulnerab_ C1	Vulnerab_ C2	Vulnerab_ C3	Vulnerab_ C4
Spearman's rho	Risk_C1	Correlation Coefficient	.438**	.431**	.597**	.305**
		Sig. (2-tailed)	.000	.000	.000	.001
		N	117	117	117	117
	Risk_C2	Correlation Coefficient	.216*	.717**	.468**	.175
		Sig. (2-tailed)	.019	.000	.000	.060
		N	117	117	117	117
	Risk_C3	Correlation Coefficient	.346**	.421**	.479**	.135
		Sig. (2-tailed)	.000	.000	.000	.145
		N	117	117	117	117

Types of knowledge vulnerabilities:
 component 1 – vulnerabilities related to knowledge creation and knowledge acquisition
 component 2 – vulnerabilities related to emotional and spiritual knowledge dynamics
 component 3 – vulnerabilities related to knowledge loss and knowledge use
 component 4 – vulnerabilities related to knowledge sharing
 Types of knowledge risks:
 component 1 – risks related to knowledge creation and knowledge use
 component 2 – risks related to emotional and spiritual knowledge dynamics
 component 3 – risks related to knowledge acquisition

Source: Authors' own processing

In order to facilitate the understanding of the comments on these correlations, we are presenting below (Table 3) the items from the questionnaire that were included – after performing two separate principal components analyses – within each of the components resulted for knowledge vulnerabilities and knowledge risks.

Table 3. Items in the components of knowledge vulnerabilities and knowledge risks

Types of knowledge vulnerabilities	
C1	KA2_V: To obtain the necessary knowledge, we have ways that are aligned with organizational strategies.
	KA1_V: We have solutions through which, when necessary, we obtain the knowledge we need in time.
	KC2_V: We are connected in real time to the challenges / issues in the business environment.
	KC1_V: We have the capability to create new knowledge when it is needed.
	KU1_V: The organization has mechanisms through which it pursues access to new knowledge in the field.
C2	EKD2_V: Changing managers causes emotional problems for employees, affecting their performance.
	EKD1_V: Employees are put in situations where they feel strong negative emotions at work, affecting their performance.
	SKD1_V: The values shared by employees in the organization form a rigid system, which can be affected by the change of some of the managers or of the preferred ways of working.
C3	KL3_V: Sporadic use of some ways of working makes it difficult to remember the details that lead to the most efficient way of accomplishing tasks.
	SKD2_V: In the organization, there is a chance of occurrence of problems related to a different interpretation of some of the communicated information due to different cultural origin of those involved.
	KA4_V: Decision-makers are not prepared for some situations that require decision-making.
	KU3_V: Some employees have skills useful to the organization, which are being neglected.
	KA3_V: Decision-makers are ignorant of the new knowledge that we need.
C4	KS1_V: The organization requires employees to share with colleagues the knowledge they use in their work.
	KS2_V: Employees' current work includes activities that involve sharing knowledge with each other.
Types of knowledge risks	
C1	KU1_R: Some knowledge used in my organization is outdated / obsolete as new inventions have appeared.
	KU2_R: Some knowledge used in my organization is corrupt as we had waited too long before it was used.

	KC2_R: Employees' ideas are sometimes expressed too late compared to the time when they could have been used.
	KA1_R: We do not sometimes obtain new knowledge in the needed time-frame.
C2	EKD2_R: Changing managers led to negative employee emotions, causing further deterioration of the way employees use or make their knowledge available to the organization.
	EKD1_R: When employees experience strong negative emotions at work, it causes further deterioration of the way they use or make their knowledge available to the organization.
	SKD1_R: Making changes in the organization's system of values had negative consequences on the way employees used or made their knowledge available to the organization.
C3	KA3_R: We sometimes acquire knowledge that is not useful for the needs of our organization.
	KA2_R: We sometimes acquire knowledge „unsuitable” to the needs of our organization.

Source: Authors' own processing, based on the initial study

From the total number of 12 correlations between the four components for types of knowledge vulnerabilities and the three components for types of knowledge risks, two correlations are not statistically significant and 10 are statistically significant (with Sig.<0.01 or Sig.<0.05).

From the 10 correlations that are statistically significant, only one correlation is positive and strong; six correlations are positive and moderate and three correlations are positive and weak. We are interested in the strong and respectively the moderate correlations between the components of knowledge vulnerabilities and the components of knowledge risks.

There is a strong positive correlation (Spearman coefficient correlation equal to 0.717) between risks related to emotional and spiritual knowledge dynamics and vulnerabilities related to emotional and spiritual knowledge dynamics. Given the items included in each of these two components (Table 3), this result is very plausible, and shows that this type of vulnerability can lead to the manifestation of this type of knowledge risk (although we did not test causality). Also, this component of knowledge risks is moderately and positively correlated (0.468) with vulnerabilities related to knowledge loss and knowledge use.

Between risks related to knowledge creation and knowledge use and the first three components for knowledge vulnerabilities there are moderate positive correlations: with vulnerabilities related to knowledge creation and knowledge acquisition the coefficient is 0.438, with vulnerabilities related to emotional and spiritual knowledge dynamics the coefficient is 0.431 and with vulnerabilities related to knowledge loss and knowledge use the coefficient is 0.597. These results show that each of the first three components for knowledge vulnerabilities have a moderate contribution to the manifestation of risks related to knowledge creation and knowledge use. Thus, except vulnerabilities related to knowledge sharing, vulnerabilities that are related to creation and acquisition of knowledge, knowledge loss and use and also emotional and spiritual knowledge dynamics are moderated and positively related to risks concerning the processes of creation and use of knowledge.

Risks related to knowledge acquisition present two moderate positive correlations, with vulnerabilities related to emotional and spiritual knowledge dynamics (0.421) and with vulnerabilities related to knowledge loss and knowledge use (0.479).

5. CONCLUSIONS

The correlation analysis indicates that managers should be most aware of vulnerabilities related to emotional and spiritual knowledge dynamics, since this component has one strong positive correlation and two moderate positive correlations with the components of knowledge risks, all three correlations being statistically significant. Therefore, changing managers, negative emotions or values affected by changes (of managers or of the preferred ways of working) are aspects that organizations should pay attention to, since these situations may be vulnerabilities leading to the manifestation of knowledge risks.

The second type of knowledge vulnerabilities that managers need to pay attention are vulnerabilities related to knowledge loss and knowledge use. This type of knowledge vulnerability presents moderate positive and statistically significant correlations with all the knowledge risks components. Thus, these two knowledge processes – knowledge loss and knowledge use – which in the initial study have resulted in a single component, need to be handled with care, and maybe even develop knowledge systems that are less and less vulnerable over time, in order to diminish the risks that can occur.

The limitations of this study come from the convenience sampling technique and the small size of the sample, namely 117 valid responses, thus future research can include sample extension.

REFERENCES

- Bayer, F., Maier, R. (2006). Knowledge risks in inter-organizational knowledge transfer. *Proceedings of I-KNOW '06 Graz, Austria*, 200-208.
- Bratianu, C. (2018). A Holistic Approach to Knowledge Risk. *Management Dynamics in the Knowledge Economy*, 6(4), 593-607. DOI 10.25019/MDKE/6.4.06
- Bratianu, C., Bejinaru, R. (2022). Exploring vulnerabilities and risks related to knowledge management systems. In: Schiuma, G., Bassi, A. (Eds.). *Proceedings of the 17th International Forum for Knowledge Asset Dynamics* (pp. 687-700), SUPSI University, 20-22 June 2022, Lugano, Switzerland.
- Bratianu, C., Neșțian, A.Ș., Guță, A.L. (2022). Knowledge risks taxonomy based on the organizational knowledge dynamics. *Ekonomicko-manazerske spektrum*, 16(2), 61-71. [dx.doi.org/10.26552/ems.2022.2.61-71](https://doi.org/10.26552/ems.2022.2.61-71)
- Dicționar Explicativ al Limbii Române – DEX (n.d.). In DexOnline. Retrieved June 30, 2023, from <https://dexonline.ro/>
- Durst, S. (2019). How far have we come with the study of knowledge risk? *VINE Journal of Information and Knowledge Management Systems*, 49(1), 21-34. <https://doi.org/10.1108/VJIKMS-10-2018-0087>
- Durst, S., Zieba, M. (2017). Knowledge risks – towards a taxonomy. *International Journal of Business Environment*, 9(1). 51-63. <https://doi.org/10.1504/IJBE.2017.084705>
- Durst, S., Zieba, M. (2019). Mapping knowledge risks: towards a better understanding of knowledge management. *Knowledge Management Research & Practice*, 17(1), 1-13. DOI: 10.1080/14778238.2018.1538603
- Neșțian, Ș.A., Guță, A.L. (2023). Vulnerabilities and knowledge risks in knowledge processes. *Proceedings of the 24th European Conference on Knowledge Management*, 960-968.

- Oxford Learner's Dictionaries (n.d.). In Oxford Learner's Dictionaries. Retrieved June 30, 2023, from <https://www.oxfordlearnersdictionaries.com>
- Saunders, M., Lewis, P., Thornhill, A. (2007). *Research Methods for Business Students*. 4th edition. Prentice Hall.
- Staab, S., Schnurr, H.P., Studer, R., Sure, Y. (2001). Knowledge Processes and Ontologies, *IEEE Intelligent Systems*, 16(1), 26-34. DOI: 10.1109/5254.912382
- Trkman, P., Desouza, K. (2012). Knowledge risks in organizational networks: An exploratory framework, *The Journal of Strategic Information Systems*, 21(1), 1–17. <https://doi.org/10.1016/j.jsis.2011.11.001>
- Ursache, V.M. (2023). Knowledge Vulnerabilities: Definitions and Interpretations, "*Ovidius*" *University Annals, Economic Sciences Series*, XXIII(1), 529-536.
- Zieba, M., Durst, S., Hinteregger, C. (2022). The impact of knowledge risk management on sustainability. *Journal of Knowledge Management*, 26(11), 234-258. <https://doi.org/10.1108/JKM-09-2021-0691>