Measuring Knowledge Vulnerabilities in Knowledge Processes: A Scale Development

Constantin Bratianu[1], Andrei Ștefan Neștian[2], Alexandra Luciana Guță[2] and Silviu Mihail Tiță[2]

[1]UNESCO Department of Business Administration, Bucharest University of Economic Studies, Bucharest, Romania; Academy of Romanian Scientists, Romania

[2]Department of Management, Marketing and Business Administration, Faculty of Economics and Business Administration, Alexandru Ioan Cuza University of Iași, Romania

constantin.bratianu@gmail.com
nestian@uaic.ro
luciana_guta@yahoo.com
silviutita@yahoo.com

Abstract: The aim of this paper is to propose and test a new measuring scale for the concept of "knowledge vulnerabilities". With this research, we are continuing our work on a research project concerning knowledge risks and knowledge vulnerabilities that can manifest in organizations, alongside knowledge processes. In the context of a scarce literature concerning knowledge vulnerabilities, this research adds value by understanding and measuring knowledge vulnerabilities, as weak points of the knowledge system and of the knowledge management routines that could trigger or facilitate the appearance of risks, exposing the organization to threats. In this paper, we present an instrument for measuring knowledge vulnerabilities related to the knowledge processes within an organization, in the form of a questionnaire. This instrument is developed starting from a previously tested instrument, with 21 items, proposed by Neștian and Guță (2023). The new instrument contains 42 items, with newly developed items reflecting a deeper understanding of knowledge vulnerabilities. The taxonomy for knowledge vulnerabilities is based on a recent perspective of organizational knowledge dynamics (Bratianu, Neștian and Guță, 2022). In this research, seven knowledge processes are considered and vulnerabilities related to them are proposed: vulnerabilities related to knowledge creation, vulnerabilities related to knowledge acquisition, vulnerabilities related to knowledge loss, vulnerabilities related to knowledge sharing, vulnerabilities related to knowledge use, vulnerabilities related to emotional knowledge dynamics and vulnerabilities related to spiritual knowledge dynamics. The questionnaire has been applied in private companies, on both managers and non-managers. Principal components analysis was undertaken to highlight the components forming the construct of *vulnerabilities related to knowledge processes*. The factors resulting from applying the statistical method of principal components analysis on the data collected with this improved questionnaire are composed starting from a larger number of items and are better aligned with the theoretical perspective used, compared with the questionnaire developed in 2023 by Neștian and Guță. The items of the questionnaire loaded in the principal components can be used for relevant future studies on knowledge vulnerabilities. The resulting components offer a better picture regarding the conceptualization of the notion of vulnerabilities associated with knowledge processes.

Keywords: Knowledge vulnerabilities, Knowledge processes, Factor analysis, Measuring scale, Knowledge dynamics

1. Introduction

The wider context in which we are conducting this research is that of knowledge management systems as functional frameworks in any organization. Knowledge management systems "are composed of people, technology, and processes. The performance of any knowledge management system impacts on the organizational performance and its business sustainability" (Bratianu, Bejinaru and Ursache, 2024, p. 71). In these systems, specialized knowledge-related activities are carried out, in an organized, facilitated or spontaneous manner, ensuring that the organization, decision-makers, and all employees possess the appropriate knowledge to do their jobs. When we categorize these activities by their nature and purpose, we can distinguish several well-defined groups considered by theorists (Massingham, 2020; Nonaka and Takeuchi, 1995, 2019) as knowledge processes, such as knowledge acquisition, knowledge creation, knowledge sharing, or knowledge use. According to Harries (2012), the term *knowledge process* has two different meanings: "some refer to knowledge-intensive business operations that draw on a wide range of knowledge sources, require high expertise to complete, and present multiple choices between options that call for knowledge-based judgements; others refer to internal knowledge management functions that provide a service to such business processes" (Harries, 2012, p. 156). The first meaning is the narrowest, as it lacks the broader systemic vision that we can find in the second, which embraces the idea of organizational function, a typical part of a system. We consider knowledge processes to be those sets of activities carried out in organizations, in which transfers and transformations of knowledge are present, with the aim of ensuring adequate knowledge in all

organizational activities. Knowledge transfer occurs by sharing or disseminating knowledge from one individual or group to another. Knowledge transformations refer to activities where knowledge is modified, restructured, or reinterpreted in order to generate new insights, to adapt it to different contexts, or make it more useful for specific applications.

These processes can be more or less effective, more or less faulty, more of less secured. We build this research around the concept of knowledge vulnerabilities, the weak points in these processes that could trigger or facilitate the appearance of knowledge risks.

2. Literature Review

The taxonomy of knowledge processes we are going to use in this research is that proposed in 2022 by Bratianu, Neștian and Guță (2022): knowledge creation, knowledge acquisition, knowledge sharing, knowledge use, knowledge loss, emotional knowledge processes, and spiritual knowledge processes. This taxonomy is based on the theory of knowledge fields and knowledge dynamics (Bratianu and Bejinaru, 2019, 2020).

The particularities of knowledge processes derive from the nature of knowledge, which, as Bratianu (2022) states, is an intangible resource that should be understood as a nonlinear field composed of rational knowledge, emotional knowledge, and spiritual knowledge. The nonlinearity raises questions about the value of knowledge and the value created by these knowledge processes. This is due to the fact that the value of an organization's knowledge may be more or less volatile and needs to be looked at from the perspective of its dynamics, and also put in the context of the knowledge processes that may be affected by a loss in the value of knowledge, due to the manifestation of different types of knowledge risks (Bratianu, Neştian, and Guţă, 2022).

The concept of *knowledge risk* is derived from the generic concept of risk, when applied to knowledge processes, having probability and impact as main characteristics. Knowledge risks reflect potential situations in which there could be some negative consequences of decisions regarding knowledge processes under the influence of internal and external factors (Cameron and Raman, 2005; Massingham, 2010; Massingham, 2020; Society for Risk Analysis, 2018). According to Perrott (2007, as cited in Durst, 2019, p. 21), 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". Due to the nature of their occurrence, knowledge risks are clearly linked to the specific knowledge processes in any organization (Cameron and Raman, 2005; Durst and Zieba, 2020; Massingham, 2020; Nakash and Bouhnik, 2022; Waring and Glendon, 1998). Understanding, identifying and evaluating knowledge risks can help firms in mitigating possible damages as a result of activating one of these risks.

Our study is focused on *knowledge vulnerabilities*, a concept deeply related to the concept of *knowledge risks* appearing in knowledge systems and knowledge management routines. Vulnerabilities are considered weak points of the knowledge system and of the knowledge management routines that may generate or initiate the knowledge risks under the pressure of some external forces (Bratianu and Bejinaru, 2022; Fuchs, Birkmann and Glade, 2012, Sapountzaki, 2012, Sarawitz, Pielke and Keykhah, 2003, as cited in Bratianu and Bejinaru, 2022). Bratianu and Bejinaru (2022, p. 688) are considering that "vulnerabilities reflect some system's weaknesses with respect to some external forces that may produce physical, financial, operational, or human damages. Vulnerabilities show why different systems have different reactions to the changes produced in the external environment". Knowledge vulnerabilities can lead to possible adverse consequences for the firm and its performance. Knowledge vulnerabilities are potential roots of knowledge risks, and due to their hidden forces, they are generally ignored by managers. For instance, in a knowledge-intensive organization, let's imagine that there is a large segment of employees who should retire almost simultaneously. When they retire, they will take with them all their experience and competencies, which help the firm to achieve a competitive advantage. Therefore, they will produce a huge knowledge loss that is a significant risk in losing that competitive advantage (DeLong, 2004). The knowledge vulnerability consists in the existence of that large segment of retiring employees, and the knowledge risk will be a huge knowledge loss for the firm. If managers are aware of that vulnerability, then they should find solutions for programming a gradual retirement, together with measures of transferring most of the experience from the retiring people to those who remain within the firm. That means intergenerational knowledge sharing programs. In any firm, one knowledge vulnerability can generate several possible knowledge risks. Also, a knowledge risk can have several potential knowledge vulnerabilities. For instance, the risk of knowledge loss can be generated by the vulnerability discussed above, but also by the dissatisfaction of some experts who might decide to leave the firm for other opportunities to work. If managers are aware of the knowledge vulnerabilities in their firms, they can identify them and take measures to reduce or eliminate them. In this way, there will be a decrease of knowledge risks

probabilities in that firm, and a significant reduction in the possible negative consequences for the firms' business.

In this research, seven knowledge processes are considered and vulnerabilities related to them are proposed: vulnerabilities related to knowledge creation, vulnerabilities related to knowledge acquisition, vulnerabilities related to knowledge loss, vulnerabilities related to knowledge sharing, vulnerabilities related to knowledge use, vulnerabilities related to emotional knowledge dynamics and vulnerabilities related to spiritual knowledge dynamics.

3. Methodology

3.1 Nature of the Study

The study is exploratory, the present research being part of a larger research project. Regarding the concept of "knowledge vulnerabilities", the literature is quite scarce. It is mostly theoretical and not much has been published on the subject of measuring knowledge vulnerabilities, nor on linking the concept with knowledge processes. Neștian and Guță (2023), in an exploratory and quantitative study, have proposed two scales, one for measuring knowledge vulnerabilities and another one for measuring knowledge risks. Both scales from the above-mentioned study have been developed based on a new taxonomy of knowledge risks, proposed by Bratianu, Neștian and Guță (2022). This new classification has been proposed in the literature by considering organizational knowledge dynamics and proposes knowledge risks typologies along seven clusters regarding knowledge processes: knowledge creation, knowledge acquisition, knowledge loss, knowledge sharing, knowledge use, emotional knowledge dynamics and spiritual knowledge dynamics. Neștian and Guță (2023) have considered these seven clusters both for knowledge risks and for knowledge vulnerabilities. This research is based on the above-mentioned studies and it is focused on developing a measurement scale for the construct of "knowledge vulnerabilities". We are using a deductive approach, quantitative methods of analysis and the research strategy is survey-based (Saunders, Lewis and Thornhill, 2007).

3.2 The Research Instrument

The research instrument that we are proposing and testing is a questionnaire, that contains the following:

- A filter question – applied so that only respondents from private companies would answer the whole questionnaire, since we were interested only in this type of organization and not also on public institutions or not-for-profit organizations; also, respondents not working at the time of completing the questionnaire could not complete the whole questionnaire.
- A measurement scale for the construct "types of knowledge vulnerabilities".
- One question concerning the position of the respondent in its organization – management or execution position.
- One question concerning the length of service of the respondent within the organization: under one year; between one and five years; over five years.
- One open question about the organization's field of activity.

The scale for each of the latent variables "type of knowledge vulnerability" ranges from one to five. One means total disagreement (the situation is not found in the organization); 2 – disagreement (the situation is rather not found in the organization); 3 – neither disagreement, nor agreement (the situation is sometimes found in the organization); 4 – agreement (the situation is found to a large extent in the organization); 5 – total agreement (the situation is characteristic to the organization). The scale contains a total number of 42 items, with six items for each of the seven types of knowledge vulnerabilities related to knowledge processes. This newly proposed instrument is developed based on a previous tested instrument, developed by Neștian and Guță (2023), which contains 21 items. Our instrument contains 42 items and includes newly developed items that reflect a deeper understanding of the concept of "knowledge vulnerabilities".

The survey has been conducted online, as part of a larger survey. Google Forms was used and data has been collected between 19th and 31st of December 2024. A number of 198 answers were obtained and the filter question helped us eliminate 28 answers, thus remaining with a total of 170 respondents working in commercial societies at the moment they completed the questionnaire. In order for an answer to be considered complete and afterwards to be sent, providing answers to all questions and items was set as mandatory in the Google form. The questionnaire was sent though different channels, such as software that we use in our teaching and research activities and social media.

3.3 The Sample

Out of the total of 170 respondents working in private companies, 57.1% are managers and 42.9% are non-managers. Concerning the length of service in the organization (seniority), the greatest percentage of respondents, 46.5%, worked for over five years in the organization, 42.4% worked between one and five years, and 11.2% worked for under a year in the organization, at the time of completing the questionnaire. The distribution of respondents by seniority is an argument concerning the trustworthiness of the respondents' answers, since employees with greater seniority in a company ought to know and understand the company better, from a knowledge management point of view. Since we were interested in developing a measuring scale to be used regardless of a company's field of activity, we did not limit our sample to certain fields of activity. Thus, among the fields mentioned by the respondents, we can find: accounting/ auditing/ financial/ tax consulting, agriculture, alcoholic beverages production, architecture and urban planning design, automobiles sales, automotive industry, aviation, banking/ financial services, business services outsourcing, business to business certified translations, business/ management consulting, call centre (debt collection), chemical industry, commerce, construction, custom printing, e-commerce, education/ training, fast moving consumer goods, fintech, foreign exchange/ investments, gear wheel production/ specific processes for aircraft, global payments, heavy trade in metallurgical products, hospitality, human resources, information and communication technology, insurance, marketing/ market research, mass media, medical field, non-banking financial sector, pharmaceutical field, private security, production of solutions for energy efficiency, real estate development, shoe cleaning services, sports betting, trade of professional measuring and testing equipment for telecommunications, transportation/ logistics, wellness, zootechnics.

3.4 Methods and Techniques Used for Data Analysis

Microsoft Excel and Statistical Package for the Social Science (SPSS, version 20) was used for data processing and analysis. Consistency analysis and Principal components analysis (PCA) have been conducted in SPSS. Consistency analysis was undertaken both for the entire instrument (without the nominal scales and the open question) and for the results obtained for the construct's components "type of knowledge vulnerability", for determining the internal consistency. PCA was undertaken for extracting the components of the latent variable "knowledge vulnerabilities". Although the instrument proposed in this study has been developed based on a previous tested instrument, developed by Neștian and Guță (2023), our instrument contains a double number of items, having newly developed ones, which reflect a better and deeper understanding of the construct of "knowledge vulnerabilities". Considering that all items in the questionnaire were mandatory in the online form, we have no missing values. The scale developed for measuring knowledge vulnerabilities has both positively and negatively formulated items, thus, part of the items had to be reversed. We decided to reverse the positively formulated items, given the nature of the concept under study. In total, 34 out of 42 items have been reversed, before proceeding to consistency analysis and PCA.

4. Results

4.1 Consistency Analysis

We tested the internal consistency for the scale "type of knowledge vulnerability", which means that we tested the whole instrument, but without the nominal scales and the open question. The Cronbach alpha coefficient obtained for the scale for types of knowledge vulnerabilities, with a total of 42 items, is equal to 0.946. The scale is reliable, the coefficient exceeding the threshold of 0.7 (Hair et al, 2006).

4.2 Components Resulted for Knowledge Vulnerabilities

The results obtained though PCA are shown in Table 1 below. Items are displayed in descending order of the loadings. Only loadings greater than 0.55 are shown.

Table 1: Results for "Types of knowledge vulnerabilities"

Rotated Component Matrix							
	Component						
	1	2	3	4	5	6	7
KS2: Employees' current work includes activities that involve sharing knowledge with each other.	0.791						
KS3: We have a system that incentivizes employees to share their knowledge with other colleagues, without losing any privileges.	0.743						

Rotated Component Matrix							
	Component						
	1	2	3	4	5	6	7
KS1: The organization incentivizes employees to share with colleagues the knowledge they use in their work.	0.713						
KS4: The employees use various face-to-face or on online platforms solutions to freely dialogue with colleagues on topics or projects in which they are involved.	0.702						
KS6: The firm encourages employees and managers to attend professional conferences and workshops from within the country and from abroad and then share the novelties which they found there.	0.627						
KC4: We have developed an efficient system for stimulating creative thinking and collecting employees' proposals for creating new processes, products and services.		0.794					
KC5: We have developed strategies to stimulate knowledge creation in line with current and future market requirements, by rewarding the most valuable ideas.		0.734					
KC2: We are connected in real time to the challenges / issues in the business environment.		0.640					
KC6: We have an open system for innovation, through which we analyse what customers want and stimulate them to contribute with ideas to the creation of new products and services.		0.608					
KC3: We have a group / department that specifically deals with the innovation process in the firm.		0.597					
EKD1: Employees are put in situations where they feel strong negative emotions at work, affecting their performance.			0.878				
EKD2: The way in which changing managers from their position is usually carried out generates emotional problems for employees, affecting their performance.			0.843				
EKD5: The leadership style of the managers generates a predominantly negative emotional climate.			0.817				
SKD2: The firm's set of values and principles highlights the importance of creating products and services for the society that meet quality requirements and lead to an increasing respect towards the firm.				0.754			
SKD5: The firm's top management has vision, defining strategies for the firm's development and achievement of competitive advantages.				0.681			
SKD4: The firm's managerial philosophy is based on creating an atmosphere of collaboration internally, and partnerships with other firms and governmental institutions externally.				0.626			
SKD6: In relations with partners or collaborators from abroad, we are aware of the importance of knowing their cultural values and respecting them.				0.552			
KL3: We have a system for incentivizing older employees to share their experience and knowledge with younger colleagues.					0.709		
KU3: We created a knowledge map in the firm, so that to be able to know who knows what and what experience they have, so that in new projects we don't constantly start from scratch.					0.665		
KA3: The firm has developed a strategy to attract and hire people with experience and the skills needed for the new business areas.					0.620		
KL5: The firm makes efforts, so that in its relations with suppliers, customers and other business partners, to preserve its manufacturing secrets or other types of valuable knowledge.						0.802	
KL4: The firm makes efforts to protect its new products and services by obtaining patents or other forms of intellectual property in accordance with applicable law.						0.761	
KU6: Before introducing them, we test the new procedures, technologies or processes, to reduce risks and errors.							0.740

Rotated Component Matrix							
	Component						
	1	2	3	4	5	6	7
KU5: We are aware that some information and knowledge become outdated when we introduce new procedures, technologies or processes in the production of products and services.							0.720
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.							

In the table, "K" is the abbreviation for "knowledge", "A" stands for "acquisition", "C" for "creation", "L" for "loss", "S" for "sharing" and "U" for "use". EKD means "emotional knowledge dynamics" and SKD means "spiritual knowledge dynamics". The number allocated to each item, for example 2 in the case of the item KS2, is the number of the item within the knowledge process theoretical cluster: item number 2 for knowledge sharing.

The solution obtained contains a number of 24 items out of the total of 42 items. A number of 18 items have been eliminated through principal components analysis because of issues such as the following: very few significant correlations with other items; low communalities; similar levels of loadings on two different components; lack of loadings over 0.5 on a component or individual measure of sample adequacy (MSA) below 0.5. In our decisions, we guided after Hair et al (2006). Since our sample is consists of 170 valid answers, which is above the threshold of a sample size of 150 answers in order for a factor loading of 0.45 to be statistically significant (Hair et al, 2006), we could have kept all the items with loadings of 0.45 or above. However, striving for practical significance, we decided to keep only items with loadings above 0.5. It is considered that only loadings equal to at least 0.5 have practical relevance (Hair et al, 2006). There is one exception – we had an item with a loading just above 0.5, but we decided to eliminate it from the solution, because it did not frame well, at a conceptual level, within the component. Removing this item led to a higher level of the total variance explained by the seven extracted components, equal to 70.16%.

The value of Kaiser-Meyer-Ohlin (KMO) test is 0.886. The obtained value indicates a very good solution obtained through principal components analysis. The Sig value of Chi-square (Bartlett's Test of Sphericity) is 0.00. This guarantees, with a likelihood of 95%, that there are statistically significant correlations between the variables (Pintilescu, 2007).

We propose the following labels for the components, considering the items loaded on each of them:

- component 1: vulnerabilities related to knowledge sharing (with a Cronbach alpha equal to 0.874)
- component 2: vulnerabilities related to knowledge creation (Cronbach alpha 0.821)
- component 3: vulnerabilities related to emotional knowledge dynamics (0.846)
- component 4: vulnerabilities related to spiritual knowledge dynamics (0.788)
- component 5: vulnerabilities related to knowledge from experience (0.718)
- component 6: vulnerabilities related to knowledge loss (0.735)
- component 7: vulnerabilities related to knowledge use (0.600).

Regarding the Cronbach alpha values obtained for the components resulted after applying principal components analysis, although it is recommended that the coefficients' value exceed 0.7, values equal to or above 0.6 are accepted in exploratory research, according to Hair et al (2006).

5. Discussion

Considering the aim of the paper, which is to propose and test a new measuring scale for the concept of "knowledge vulnerabities", a discussion is needed concerning labeling the obtained components. Thus, regarding the factor labels, a closer look in Table 1 at component 5 – vulnerabilities related to knowledge from experience, shows us a problematic component from the point of view of its conceptual content. One of the seven components that we obtained through factor analysis should have been vulnerabilities related to knowledge acquisition.

Considering the three items included in component 5, from a conceptual perspective we see that one item (KL3) is for vulnerabilities related to knowledge loss when older employees share their experience, another one for vulnerabilities related to creation of knowledge maps about experiences (KU3) and only the last one is for vulnerabilities related to knowledge acquisition through hiring people with experience (KA3). Thus, we

decided that labelling component 5 as vulnerabilities related to knowledge from experience is a more appropriate label compared with vulnerabilities related to knowledge acquisition.

However, at a closer look, the result can be explained. The conceptual focus of the three items is the following: KL3 – incentivizing knowledge sharing to limit losses, KU3 – structuring knowledge, KA3 – knowledge acquisition through new employees. Thus, for example, the item that we considered to measure vulnerabilities related to knowledge loss (KL3), can be considered to reflect knowledge acquisition, not per se, but as a form of acquisition through or from the experiences – and also the knowledge – that older employees have. The emphasis is on the existence, within the organization, of a system for incentivizing this type of behaviour. Also, the item that we considered to measure vulnerabilities related to knowledge use (KU3), can be considered to reflect knowledge acquisition in an indirect way, through the experience of other colleagues in the firm. Considering that, by creating a knowledge map, other employees may acquire new knowledge, item KU3 can be conceptually linked with knowledge acquisition.

Then, if we were to compare the results obtained in this research with those obtained by Neștian and Guță (2023), first of all, we can notice what we obtained a number of seven components. Six of the resulted components could be labelled exactly according to the conceptual perspective, even if some of the items had to be deleted when applying principal components analysis. Knowledge creation has resulted in a component by itself, compared to Neștian and Guță's (2023) research, but, considering knowledge acquisition, we did not obtain a component for this type of vulnerability. Instead, we named the component as vulnerabilities related to knowledge from experience. Concluding, this is a major difference between the mentioned study and the results obtained in the present study.

Considering the other five components that we have obtained by applying principal components analysis, the comparison with Neștian and Guță's (2023) study looks as follows: emotional knowledge dynamics and spiritual knowledge dynamics, which were combined in a single component, have differentiated themselves in two different components. Also, knowledge loss and knowledge use have resulted in two different components, as compared to having them together in one component in Neștian and Guță's (2023) research. Vulnerabilities related to knowledge sharing is a component by itself in our study as well as in Neștian and Guță's (2023) study.

6. Conclusion

The purpose of this research is to propose and test a measurement scale for knowledge vulnerabilities, an emergent concept in knowledge management that is strongly related to knowledge risks. However, there is a scarcity in the literature concerning knowledge vulnerabilities although their understanding and measurement can reduce or even eliminate the knowledge risks associated with knowledge intensive organizations.

The results that we obtained were possible through widening the number of items, aligning them better with the theoretical perspective used and through a larger sample. We have obtained a solution with seven factors and 24 items, compared to four factors and 15 items in Neștian and Guță's (2023) study. Six of the seven factors are, from a conceptual point of view, aligned with categories of knowledge processes stated as theoretical foundation, allowing us to name them accordingly, and thus confirming the conceptual clarity of the research instrument.

The proposed instrument and the results obtained have practical implications for managers, for example in decision-making processes which are strongly influenced by knowledge dynamics (Bratianu, Paiuc and Bejinaru, 2024; Hill, 2008; Kahneman, 2011).

Also, the items in our questionnaire loaded in the principal components obtained can be used in future relevant studies. In terms of the entire questionnaire, all the 42 items may be subject to confirmatory factor analysis, for testing the validity for a construct's theoretical structure or the factorial structure of a measurement instrument (Byrne, 2010).

Concerning the conceptualization of vulnerabilities associated with knowledge processes, the components that we have obtained through principal components analysis offer a better picture.

The limitations of our study are related to the fact that we did not use systematic sampling, nor did we take, so far, a confirmatory approach, which is needed for validation purposes. Future research can include an extension of the sample and consider a confirmatory approach.

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. (2022) *Knowledge strategies*, Cambridge University Press, Cambridge.

Bratianu, C. and Bejinaru, R. (2019) "The Theory of Knowledge Fields: A Thermodynamics Approach", *Systems*, 7(2), pp 1-12. doi: 10.3390/systems7020020.

Bratianu, C. and Bejinaru, R. (2020) "Knowledge dynamics: A thermodynamics approach", *Kybernetes*, 49(1), pp 6-21. doi: 10.1108/K-02-2019-0122.

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*, 25(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*, 16(2), pp 61-71. doi:10.26552/ems.2022.2.61-71.

Bratianu, C., Paiuc, D. and Bejinaru, R. (2024) *The Impact of knowledge dynamics on multicultural leadership and the mediating role of cultural intelligence.* In Obermayer, N. and Bencsik. A. (eds.) *Proceedings of the 25th European Conference on Knowledge Management (ECKM 2024),* pp 103-108. doi:10.34190/eckm.25.1.2465.

Byrne, B.M. (2010) *Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming, 2nd Edition,* Routledge, New York.

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

DeLong, D.W. (2004) *Lost knowledge: Confronting the threat of an aging workforce,* Oxford University Press, Oxford.

Durst, S. (2019) "How far have we come with the study of knowledge risk?", *VINE Journal of Information and Knowledge Management Systems,* 49(1), pp 21-34. doi:10.1108/VJIKMS-10-2018-0087.

Durst, S. and Zieba, M. (2020) "Knowledge risks inherent in business sustainability", *Journal of Cleaner Production*, 251, 119670, pp 1-10. doi: 10.1016/j.jclepro.2019.119670.

Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E. and Tatham, R.L. (2006) *Multivariate data analysis, 6th Edition*, Pearson Prentice Hall, New Jersey.

Harries, S. (2012) *Records Management and Knowledge Mobilisation: A Handbook for Regulation, Innovation and Transformation,* Chandos Publishing, Oxford.

Hill, D. (2008) *Emotionomics: Leveraging emotions for business success*, Revised Edition, Kogan Page, London.

Kahneman, D. (2011) *Thinking, fast and slow*, Farrar, Straus and Giroux, New York.

Massingham, P. (2010) "Knowledge risk management: a framework", *Journal of Knowledge Management*, 14(3), pp 464-485. doi:10.1108/13673271011050166.

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

Nakash, M. and Bouhnik, D. (2022) "Risks in the absence of optimal knowledge management in knowledge-intensive organizations", *VINE Journal of Information and Knowledge Management Systems*, 52(1), pp 87-101. doi: 10.1108/VJIKMS-05-2020-0081.

Neștian, A.Ș. and Guță, A.L. (2023) *Vulnerabilities and knowledge risks in knowledge processes*. In Matos, M. and Rosa, Á. (eds.) *Proceedings of the 24th European Conference on Knowledge Management (ECKM 2023)*, pp 960-968. doi:10.34190/eckm.24.1.1416.

Nonaka, I. and Takeuchi, H. (1995) *The knowledge-creating company: How Japanese companies create the dynamics of innovation*, Oxford University Press, Oxford.

Nonaka, I. and Takeuchi, H. (2019) *The wise company: How companies create continuous innovation*, Oxford University Press, Oxford.

Pintilescu, C. (2007) *Analiză statistică multivariată*, Editura Universității "Alexandru Ioan Cuza" din Iași, Iași.

Saunders, M., Lewis, P. and Thornhill, A. (2007) *Research methods for business students, 4th Edition*, Prentice Hall, Harlow.

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

Waring, A.E. and Glendon, A.I. (1998) *Managing Risk: Critical issues for survival and success into the 21st century,* Thomson Learning, London.