Vulnerabilities and Knowledge Risks in Knowledge Processes

Andrei Ștefan Neștian and Alexandra Luciana Guță
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

Abstract: This study aims to put forward measuring scales for two central concepts – vulnerabilities and knowledge risks – and identify the factors composing the two constructs. The research presented in this paper is part of a larger project investigating knowledge vulnerabilities and risks appearing in knowledge processes of organizations. In this sense, a new ontology developed by Brătianu et al. (2022) was used to design an instrument for measuring risks and vulnerabilities related to knowledge processes in organizations. Organizational knowledge dynamics perspective (Brătianu et al., 2022) was used to group knowledge risks typologies into the following clusters: knowledge creation, knowledge acquisition, knowledge loss, knowledge sharing, knowledge use, emotional knowledge dynamics, spiritual knowledge dynamics. Examples of knowledge risks belonging to such clusters may include a knowledge risk of non-creation and a knowledge risk of bad timing (for knowledge creation cluster), knowledge spillover or knowledge forgetting (for knowledge loss), as well as knowledge hiding and knowledge hoarding (for knowledge use). Our study fills a gap in the literature by suggesting a scale for measuring knowledge risks and grouping them by factor, and also a scale for measuring vulnerabilities and grouping them by type of vulnerabilty by means of principal components analysis. Current state of knowledge on vulnerabilities and knowledge risks comprises mainly theoretical approaches. Also, most studies do not discuss the concepts of knowledge risks and vulnerabilities together. The main novelty of our study lies in its quantitative approach to analysing knowledge-related vulnerabilities and risks. For this purpose, a questionnaire was applied to a sample of employees comprising both managers and non-managers from Romanian organizations. The factors resulted after having applied the principal components analysis have provided a clearer picture of the constructs of vulnerabilities and knowledge risks, leading to a deeper understanding of knowledge processes and their risks.

Keywords: Knowledge risks, Vulnerabilities, Knowledge processes, Knowledge dynamics

1. Introduction

The concept of knowledge risk has been the topic of several studies over the last three decades (Becerra, Lunnan and Huemer, 2008; Cooper, 2003; Massingham, 2010; Niwa,1989; Scott and Walsham, 2005; Zieba, Durst and Hinteregger, 2022). Its importance is given by the dificulties of pinpointing the invisible mecanisms determining the manifestation of such risks and the practical conditions favouring their occurrence. As knowledge risks are abstract concepts, several taxonomies have been coined over the years. This research is based on the study of Bratianu, Neștian and Guță (2022) that developed a taxonomy of knowledge risks based on the correspondence of knowledge risks with the knowledge processes in which they occur.

2. Literature Review

The theoretical approach is based on the assumption which has been derived from the general theory of risk, stating that each knowledge process containts actions, where knowledge represents the objects of specific processings, such actions taking place in contexts or modes favouring the apperance of knowledge risks that generate specific vulnerabilities in each knowledge process. The study sees knowledge vulnerabilities as the states of organisational knowledge systems that are perceived as triggering or facilitating the appearance of negative consequences in the organization's activity.

This study aims to suggest measuring scales for the concepts of vulnerabilities and knowledge risks and identify the factors of these two constructs. We present an instrument for measuring knowledge risks and vulnerabilities related to knowledge processes using a new ontology of Bratianu, Neștian and Guță (2022) towards knowledge risks based on organizational knowledge dynamics.

This new classification takes into account the dynamics of knowledge value for the firm, namely, how the value of an organization's knowledge may be affected by the presence of knowledge risks grouped by nature of knowledge processes. There is an implicit relation between knowledge processes and knowledge risks, while the nature of processes determines the nature of knowledge risk (Bratianu, Neștian and Guță, 2022).

In this study, the concept of knowledge risk is seen as a particular use of a generic concept of risk in knowledge processes, reflecting situations of negative consequences occurring due to decisions made regarding

knowledge processes under the influence of internal and external factors (Cameron and Raman, 2005; Massingham, 2010; Massingham, 2020; Society for Risk Analysis, 2018).

These concepts were used to develop seven clusters of knowledge risks grouped using a criterion of a relation between knowledge risk and knowledge process: (KC) – knowledge creation risks, (KA) – knowledge acquisition risks, (KL) – knowledge loss risks, (KS) – knowledge sharing risks, (KU) – knowledge use risks, (EKD) – emotional knowledge dynamics risks, and (SKD) – spiritual knowledge dynamics risks (Bratianu, Neștian and Guță, 2022). Several prominent papers in the field of knowledge risks were used to extract the risk typology, each presenting a slightly different knowledge risk typology (Bratianu et al, 2020; Durst and Henschel, 2020; Durst and Wilhelm, 2013; Durst and Zieba, 2017; Durst and Zieba, 2019; Durst and Zieba, 2020; Durst, 2019; Durst, Hintereger and Zieba, 2019; Zieba and Durst, 2018; Zieba, 2017). Also, we have analysed an array of perspectives to knowledge processes (Andreeva and Kianto, 2011; Andrews and Delahaye, 2000; Kraaijenbrink, 2012; Staab et al, 2001) as to suggest a list of knowledge processes to be used in the taxonomy.

The study questionnaire was constructed by utilising the above-mentioned taxonomy, alongside with scale development for knowledge risks and knowledge vulnerabilities.

As for the second concept of knowledge vulnerabilities, we reviewed the literature in the field on risk management. An accepted perspective is that vulnerability is a measure of likelihood for an asset to be attacked successfully by a given threat (Avci and Ozbulut, 2018) that may cause losses or damages. In case of knowledge vulnerabilities, the idea of an attack is not the most suitable perspective. Instead, we may see a threat as an event or context causing loss of knowledge to an organisation.

Vulnerabilities differ from risks as they possess three specific underliyng caracteristics related to the manifestation of knowledge risks. The first characteristic is the *deterministic capacity*, being the root of likelihood of knowledge risks manifestation (Bratianu, Neștian and Guță, 2022). A risk is a potential for loss and damage when a threat occurs. Knowledge vulnerabilities are the weak points of the knowledge system and the knowledge management routines that trigger or facilitate the apperarance of risks, exposing the organisation to threats. These weak points are the determinants of knowledge risks as they initiate the knowledge risks under the pressure of external forces (Bratianu and Bejinaru, 2022; Fuchs, Birkmann and Glade, 2012; Sarawitz, Pielke and Keyhah, 2003). The second caracteristic of vulnerabilities is the *capacity to respond* with a countering action (Marandola and Hogan, 2006). If the system has a vulnerability, the system's capacity to respond, when a risk is manifested, may be hindered. Third, vulnerabilities reduce system's *absorptive capacity*. When a risk is manifested, the presence of a vulnerability is related to a lower capacity of loss prevention or decrease, or recover to a normal state (Marandola and Hogan, 2006).

Starting from the conceptual framework and theoretical meaning of the concept of vulnerabilities, we developed a list of vulnerabilities related to each of the knowledge risks in the taxonomy put forward by Bratianu, Neștian and Guță (2022).

3. Methodology

3.1 Nature of the Study

The nature of our study is exploratory. Current state of knowledge on the concepts of knowledge vulnerabilities and knowledge risks is theoretical, comprising mostly taxonomies of knowledge risks, the literature on this topic being scarce. Our approach is deductive and our research strategy is survey-based, with the use of quantitative methods of analysis (Saunders, Lewis and Thornhill, 2007). The novelty of the study lies in a quantitative approach to the analysis of knowledge-related vulnerabilities and risks.

3.2 The Research Instrument

The instrument is a questionnaire comprising a filter question, a scale for measuring the types of knowledge risks, a scale for measuring the types of knowledge vulnerabilities, three questions at the end of the questionnaire regarding the following: position within the organization (management or execution), length of service within the organization (under one year, between one and five years, over 5 years), the organization's field of activity (open question).

Both scales for the latent variable "type of knowledge risk" and "type of knowledge vulnerability" range from one to five, 1 – total disagreement (the situation is not found in the organization); 2 – disagreement (rarely found in the organization); 3 – neither disagreement, nor agreement (found sometimes); 4 – agreement (frequently found); 5 – total agreement (the situation is curently found in the organization).

The scale for types of knowledge vulnerabilities and knowledge risks contains 21 and 19 items, respectively. Both scales were developed based on vulnerabilities and risks that may be associated with the following seven clusters of knowledge processes: knowledge creation, knowledge acquisition, knowledge loss, knowledge sharing, knowledge use, emotional knowledge dynamics and spiritual knowledge dynamics.

The cluster „knowledge creation" contains the following risk typologies: knowledge risk of non-creation and knowledge risk of bad timing. The cluster „knowledge acquisition" comprises the knowledge risk of not acquiring the necessary knowledge at the required time and knowledge risk of wrong acquisition. „Knowledge loss" contains risks of knowledge loss with the retirement of people, risk of knowledge spillover and risk of knowledge forgetting. „Knowledge sharing" contains the risk of knowledge hiding and knowledge hoarding. The „knowledge use" cluster includes the risk of knowledge attrition when embedding it into products and services; the risk of knowledge waste. „Emotional knowledge dynamics" contains the emotional risk of organizational change and that of changing the managers. „Spiritual knowledge dynamics" comprises spiritual knowledge risk of changing the organzational values system and spiritual knowledge risks, when people work in different cultures in multinational companies (Bratianu, Neștian and Guță, 2022).

The filter question was applied as we were interested in analysing only private companies, and not public institutions or not-for-profit organizations. The survery was conducted online (between 20th and 26th of March 2023) using Google Forms. It helped us eliminate 13 out of 130 answers, which lead to a total of 117 valid questionnaires. To provide answers to all questions and items was mandatory for a questionnaire to be considered complete and then accepted to be sent.

3.3 The Sample

A link to the questionnaire was sent via different online channels (social media, software used in our teaching and research activities, etc.).

Out of a total of 420 people who received the questionnare, 130 respondents completed the questionnaire, 13 not working in private companies. There were 117 valid questionnaires and a valid rate of response of 27.8%.

We were interested in the perspectives of both managers and non-managers: 46.15% and 53.85% of the respondents, managers and non-managers, respectively.

Regarding the length of service in organisations (seniority), 35.04% of the respondents worked for over five years in the organization, 47.01% between one and five years, and only 17.95% under a year. Sample distribution by seniority of 117 respondents in companies strengthens the level of trust in the relevance of respondents' answers, considering that an employee with a longer length of service could know the company better.

As for organizations' field of activity, the sample comprising 117 respondents mentioned such areas as transportation, construction, retail, consultancy, online commerce, outsourcing, construction materials production, banking, drug promotion, automotive sector, real estate, metallurgy, legal sector, information technology, agriculture, medical equipment, marketing and services, finance consultancy, management consultancy, pharmaceutical industry, accounting, evaluation of movable and immovable properties, clinical research, commerce, audit and consultancy, hospitality industry, non-banking financial services – currency exchange, real estate and facilities, human resources, health, consultancy and training, public power supply and energy from renewable sources, sales and education.

3.4 Methods and Techniques Used for Data Analysis

For data processing and analysis, we used Microsoft Excel and Statistical Package for the Social Science (SPSS, version 20). Consistency (reliability) and factor analyses (principal components analysis - PCA) were conducted in SPSS. We have used reliability analysis for determining the internal consistency of the entire instrument (without the nominal scales), the scale for types of knowledge risks and knowledge vulnerabilities, respectively, the results obtained for the constructs' components "type of knowledge risks" and "type of knowledge vulnerability", respectively. PCA was used for extracting the components, also called factors, for each of the two latent variables: knowledge vulnerabilities and knowledge risks. The study also suggests the scales for both latent variables. Since similar quantitative studies have not been found in the literature on the topic, we applied exploratory factor analysis. There were no missing values as all items were mandatory for questionnaire completion and sending. Some items had to be reversed as they were positively or negatively formulated. Since we were measuring the vulnerabilities and risks, we chose to reverse the positively formulated items.

4. Results

4.1 Consistency Analysis

We tested the reliability of the entire questionnaire (only the ordinal scales, withouth nominal variables and open questions) and the reliability of the latent variables "type of knowledge vulnerability" and "type of knowledge risk".

The reliability analysis shows that the instrument and the scales for both latent variables have internal consistency, and therefore are reliable, since all Cronbach Alpha coefficients exceed the value of 0.7 (Hair et al, 2006). The values are shown in Table 1.

Table 1: Consistency Analysis of the Instrument and the Scales

Scale	Cronbach alpha coefficient
Entire instrument (both scaled: 40 items)	0.923
Scale for type of knowledge vulnerabilities (21 items)	0.883
Scale for type of knowledge risks (19 items)	0.856

4.2 Components Resulted for Knowledge Vulnerabilities and Knowledge Risks

The components resulted from principal component analysis for the latent variable "Types of knowledge vulnerabilities" are shown in Table 2 below. In the following table, K means "knowledge", C – "creation", A – "acquisition", L – "loss", S – "sharing" and U – "use". Also, EKD means "emotional knowledge dynamics" and SKD stands for "spiritual knowledge dynamics". The abbreviation "V" stands for the word "vulnerability". The number of each item (for example 2, from KA2_V) is its number in the cluster, as it was included into the theoretical cluster (knowledge acquisition, knowledge creation, etc.). For example, KA2_V is the second item included in the cluster of vulnerabilities related to knowledge acquisition.

Varimax rotation with Kaiser normalization was used. In Table 2, the items are displayed in descending order of their loadings, and only loadings higher than 0.5 are shown. According to Hair et al (2006), only loadings higher than 0.5 have practical relevance.

The solution contains 15 out of 21 items in the scale for knowledge vulnerabilities. Six items were eliminated due to such problems as individual measure of sample adequacy (MSA) lower than 0.5; very few significant correlations with other items; low communalities; loadings on two components (we guided after Hair et al, 2006). The total variance explained by four extracted components is 67.14%.

Table 2: Results for "Types of knowledge Vulnerabilities"

Rotated Component Matrix				
	Component			
	1	**2**	**3**	**4**
KA2_V: To obtain the necessary knowledge, we have ways that are aligned with organizational strategies.	0.818			
KA1_V: We have solutions through which, when necessary, we obtain the knowledge we need in time.	0.812			
KC2_V: We are connected in real time to the challenges / issues in the business environment.	0.658			
KC1_V: We have the capability to create new knowledge when it is needed.	0.649			
KU1_V: The organization has mechanisms through which it pursues access to new knowledge in the field.	0.619			
EKD2_V: Changing managers causes emotional problems for employees, affecting their performance.		0.876		
EKD1_V: Employees are put in situations where they feel strong negative emotions at work, affecting their performance.		0.822		
SKD1_V: The values shared by employees in the organization form a rigid system,		0.762		

Rotated Component Matrix				
	Component			
	1	2	3	4
which can be affected by the change of some of the managers or of the preferred ways of working.				
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.			0.738	
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.			0.684	
KA4_V: Decision-makers are not prepared for some situations that require decision-making.			0.620	
KU3_V: Some employees have skills useful to the organization, which are being neglected.			0.609	
KA3_V: Decision-makers are ignorant of the new knowledge that we need.			0.579	
KS1_V: The organization requires employees to share with colleagues the knowledge they use in their work.				0.856
KS2_V: Employees' current work includes activities that involve sharing knowledge with each other.				0.776
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.				

The value of Kaiser-Meyer-Ohlin (KMO) test is 0.835, which indicates that the solution obtained by applying principal components analysis is very good; Sig value of Chi-square (Bartlett's Test of Sphericity) is 0.00, which guarantees us a likelihood of 95% that there are statistically significant correlations between the variables (Pintilescu, 2007).

According to the items loaded on each component and taking into consideration the majority of the items included in each component (Hair et al, 2006), we suggest the following names for the four knowledge vulnerabilities components: component 1 – *vulnerabilities related to knowledge creation and knowledge acquisition* (Cronbach alpha 0.822), component 2 – *vulnerabilities related to emotional and spiritual knowledge dynamics* (0.845), component 3 – *vulnerabilities related to knowledge loss and knowledge use* (0.770) and component 4 – *vulnerabilities related to knowledge sharing* (0.759).

Table 3 includes the results obtained by applying PCA, with Varimax rotation with Kaiser normalization for types of knowledge risks. "R" stands for "risk". Items are displayed in descending order of their loadings; only loadings higher than 0.5 are shown. The solution contains nine out of 19 items in the scale for knowledge risks. We have eliminated 10 items due to such problems as very few significant correlations with other items and / or individual measures of sample adequacy (MSA) lower than 0.5; low communalities. Total variance explained by the three extracted components is 70.95%.

Regarding some problems with corellations and with MSA values, we looked for explanations in the literature. According to Lorenzo-Seva and Ferrando (2021), MSA can highlight two types of problematic items: *noisy* items – items that behave almost randomly, and *redundant* items – the items sharing specific content with the other ones. Based on the exploratory factor analysis, we consider risks related to knowledge sharing to be related to other items in the scale for knowledge risks, and therefore reflecting other types of risks.

Table 3: Results for "Types of Knowledge Risks"

Rotated Component Matrix			
	Component		
	1	2	3
KU1_R: Some knowledge used in my organization is outdated / obsolete as new inventions have appeared.	0.842		
KU2_R: Some knowledge used in my organization is corrupt as we had waited too long	0.839		

Rotated Component Matrix			
	Component		
	1	2	3
before it was used.			
KC2_R: Employees' ideas are sometimes expressed too late compared to the time when they could have been used.	0.636		
KA1_R: We do not sometimes obtain new knowledge in the needed time-frame.	0.615		
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.		0.863	
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.		0.827	
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.		0.797	
KA3_R: We sometimes acquire knowledge that is not useful for the needs of our organization.			0.893
KA2_R: We sometimes acquire knowledge „unsuitable" to the needs of our organization.			0.878
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.			

The value of KMO test is 0.728, which indicates that the solution obtained by applying principal components analysis is good. Sig value of Chi-square (Bartlett's Test of Sphericity) is 0.00, which guarantees with a likelihood of 95% that there are statistically significant correlations between the variables (Pintilescu, 2007).

We propose the following names for the three components obtained for knowledge risks, in line with the items loaded on each component and taking into consideration the majority of the items included in each component (Hair et al, 2006): component 1 – *risks related to knowledge creation and knowledge use* (Cronbach alpha 0.775), component 2 – *risks related to emotional and spiritual knowledge dynamics* (0.809) and component 3 – *risks related to knowledge acquisition* (0.846).

Figures 1 and 2 below present the components obtained for knowledge vulnerabilities and knowledge risks.

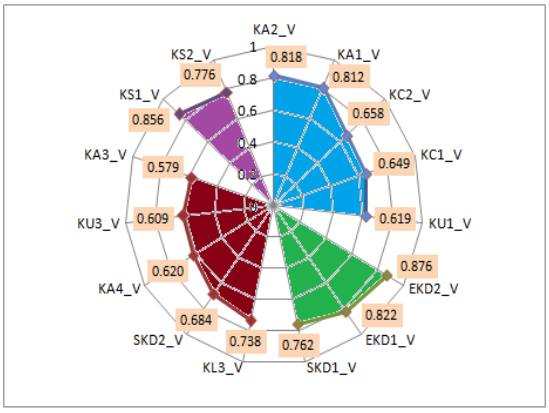

Figure 1: Components for Knowledge Vulnerabilities

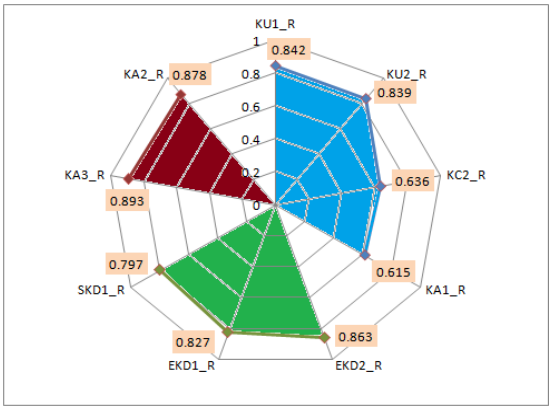

Figure 2: Components for Knowledge Risk

5. Conclusion

This study aimed to suggest measuring scales for knowledge vulnerabilities and knowledge risks and identify the factors composing the two constructs. Thus, a first conclusion is that we can see different associations, both for vulnerabilities and risks, in the grouping of different knowledge processes. For the vulnerabilities scale, knowledge creation grouped together with knowledge acquisition, knowledge loss with knowledge use, emotional and spiritual knowledge dynamics, knowledge sharing resulted by itself in a component. For risks, knowledge creation grouped with knowledge use, emotional and spiritual knowledge dynamics also grouped

together, knowledge acquisition resulted by itself in a component. There are some major differences between the components for each of the two constructs. These differences concerning knowledge-related processes comprise knowledge creation vulnerabilities combining in a single factor with knowledge acquisition vulnerabilities, and knowledge creation risks combining in a single factor with knowledge use risks; knowledge use vulnerabilities combining in a single factor with knowledge loss vulnerabilities, while knowledge use risks combining in the same factor with knowledge creation risks. Knowledge sharing as a knowledge process appears only in the factorial solution for vulnerabilities, being though eliminated from the solution for knowledge risks. Table 4 is a visual representation that compares the results by types of knowledge vulnerabilities and knowledge risks.

Table 4: Comparative Results for "Types of Knowledge Vulnerabilities" and "Types of Knowledge Risks"

Comp. 1	KA2_V
	KA1_V
	KC2_V
	KC1_V
	KU1_V
Comp. 2	EKD2_V
	EKD1_V
	SKD1_V
Comp. 3	KL3_V
	SKD2_V
	KA4_V
	KU3_V
	KA3_V
Comp. 4	KS1_V
	KS2_V

Comp. 1	KU1_R
	KU2_R
	KC2_R
	KA1_R
Comp. 2	EKD2_R
	EKD1_R
	SKD1_R
Comp. 3	KA3_R
	KA2_R

Note: We used different shades of gray to mark different knowledge processes

A potential explanation for the combining of knowledge *loss* and knowledge *use vulnerabilities* in the same factor, and knowledge *creation* with knowledge *use risks*, lies in the fact that when companies have vulnerabilities leading to loss of knowledge, it could also involve vulnerabilities related to knowledge use. Further, this complex vulnerability may correlate with risks related to knowledge use, which may also lead to knowledge creation risks, since it is harder to create new knowledge when organizations have problems related to knowledge use.

Another interesting result is related to the process of knowledge sharing. Regarding vulnerabilities, PCA led us to a factor referred to as vulnerabilities related to knowledge sharing. However, for the factorial solution for risks related to knowledge processes, we decided that it was correct to eliminate the items measuring knowledge sharing, thus the solution for this type of risks does not contain a factor for knowledge sharing. A possible explanation may be the fact that vulnerabilities related to knowledge sharing do not transpose in risks related to the process of knowledge sharing but in risks related to other knowledge processes. However, an alternative explanation may be related to the small size of the sample, which is a limitation of the present study.

Another potential explanation that needs to be cautiously treated (due to sample size and the exploratory nature of the study) is the fact that we may need to rethink some of the items, and reformulate or conceptually reframe them into other clusters than the initial ones (considering the current empirical results).

Althouth it needs further improvement and testing, the proposed scale is a first step in performing a quantitative assessment of risks and vulnerabilities related to knowledge processes in organizations. We believe that the components resulted by applying principal components analysis offer a clearer picture on the constructs of vulnerabilities and knowledge risks, leading to a deeper understanding of knowledge processes and their associated risks.

The results of this study need to be cautiously treated due to the small size of the sample (117 valid responses) and the applied convenience sampling technique. Therefore, future research can include sample extension and a systematic sampling; scale refinement and further testing – exploratory and confirmatory; longitudinal studies for companies interested in knowledge risks and vulnerabilities.

After refinement, the scale will be useful for organizations intending to assess their knowledge vulnerabilities and risks. Correlations between the components of knowledge risks and knowledge vulnerabilities, as well as the calculation of means for each component could offer valuable information for taking managerial decisions.

References

Andreeva, T. and Kianto, A. (2011) "Knowledge processes, knowledge-intensity and innovation: a moderated mediation analysis", *Journal of Knowledge Management,* Vol, 15, No. 6, pp 1016-1034.

Andrews, K.M. and Delahaye, B.L. (2000) "Influences on knowledge processes in organizational learning: The psychosocial filter", *Journal of Management studies*, Vol 37, No. 6, pp 797-810.

Avci, O. and Ozbulut, O. (2018) "Threat and vulnerability risk assessment for existing subway stations: A simplified approach", *Case Studies on Transport Policy*, Vol 6, No. 4, pp 663-673.

Becerra, M., Lunnan, R. and Huemer, L. (2008) "Trustworthiness, risk, and the transfer of tacit and explicit knowledge between alliance partners", *Journal of Management Studies,* Vol 45, No. 4, pp 691-713.

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 (IFKAD),* pp 687-700.

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.

Bratianu, C., Neștian, A.Ș., Tiță, S.M., Vodă, A.I., and Guță, A.L. (2020) "The impact of knowledge risk on sustainability of firms", *Amfiteatru Economic*, Vol 22, No. 55, pp 639-652.

Cameron, I. and Raman, R. (2005) *Process systems risk management. 1st edn.* Elsevier.

Cooper, L. P. (2003) "A research agenda to reduce risk in new product development through knowledge management: a practitioner perspective", *Journal of Engineering and Technology Management,* Vol 20, No. 1-2, pp. 117-140.

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

Durst, S. and Zieba, M. (2019) "Mapping knowledge risks: towards a better understanding of knowledge management", *Knowledge Management Research & Practice,* Vol 17, No. 1, pp. 1-13.

Durst, S. (2019) "How far have we come with the study of knowledge risk?", *VINE Journal of Information and and Knowledge Management Systems,* Vol 49, No. 1, pp 21-34.

Durst, S. and Wilhelm, S. (2013) "Do you know your knowledge at risk?", *Measuring Business Excellence*, Vol 17, No. 3, pp 28-39.

Durst, S. and Henschel, T. (2020) *Knowledge risk management. From theory to praxis*, Springer Nature, Cham.

Durst, S., and Zieba, M. (2020) "Knowledge risks inherent in business sustainability", *Journal of Cleaner Production,* Vol 251, pp 1-10.

Durst, S., Hintereger, C. and Zieba, M. (2019) "The linkage between knowledge risk management and organizational performance", *Journal of Business Research*, Vol 105, pp 1-10.

Fuchs, S., Birkmann, J. and Glade, T. (2012) "Vulnerability assessment in natural hazards and risk analysis: current approaches and future challenge", *Natural Hazards*, Vol 64, pp 1969-1975.

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.

Kraaijenbrink, J. (2012) "Integrating knowledge and knowledge processes: A critical incident study of product development projects", *Journal of product innovation management*, Vol 29, No. 6, pp. 1082-1096.

Lorenzo-Seva, U., and Ferrando, P. J. (2021) "MSA: The Forgotten Index for Identifying Inappropriate Items Before Computing Exploratory Item Factor Analysis", *Methodology,* Vol 17, No. 4, pp. 296–306.

Marandola, E. and Hogan, D.J. (2006) "Vulnerabilities and risks in population and environment studies", *Population and Environment*, Vol 28, pp 83-112.

Massingham, P. (2010) "Knowledge risk management: a framework", *Journal of Knowledge Management,* Vol 14, No. 3, pp 464.

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

Niwa, K. (1989) *Knowledge-based risk management in engineering: a case study in human-computer cooperative systems. 1st edn,* John Wiley & Sons, Inc.

Pintilescu, C. (2007) *Analiză statistică multivariată*, Alexandru Ioan Cuza" University Publisher, Iași.
Sarawitz, D., Pielke, 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.
Saunders, M., Lewis, P. and Thornhill, A. (2007) *Research Methods for Business Students, Fourth Edition*, Prentice Hall, Harlow.
Scott, S.V. and Walsham, G. (2005) "Reconceptualizing and managing reputation risk in the knowledge economy: Toward reputable action",*Organization Science,* Vol 16, No. 3, pp 308-322.
Society for Risk Analysis (2018) "Society for risk analysis glossary", https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf
Staab, S., Studer, R., Schnurr, H.P., and Sure, Y. (2001) "Knowledge processes and ontologies", *IEEE Intelligent systems*, Vol 16, No. 1, pp 26-34.
Zieba, M. (2017) "Knowledge safety – insights from the SME Sector", *Journal of Management and Business Administration. Central Europe,* Vol 25, No. 3, pp 78-96.
Zieba, M. and Durst, S. (2018) *Knowledge risks in the sharing economy.* In: Vătămănescu, E.M. and Pînzaru, F. (eds.). *Knowledge management in the sharing economy*, pp. 253-270, Springer International Publishing.
Zieba, M., Durst, S. and Hinteregger, C. (2022) "The impact of knowledge risk management on sustainability", *Journal of Knowledge Management*, Vol 26, No. 11, pp 234-258.