

# Knowledge Processes Status and Knowledge Vulnerabilities in SMES. A Qualitative Approach

Andrei Ștefan NEȘTIAN<sup>1</sup>  
Alexandra Luciana GUȚĂ<sup>2</sup>  
Silviu Mihail TIȚĂ<sup>3</sup>

## **Abstract**

*Knowledge vulnerabilities have been analyzed within the literature predominantly at a theoretical level. This paper investigates the situation of Knowledge Management within small and medium sized enterprises (SMEs), in order to highlight different types of knowledge vulnerabilities that may occur in these organizations. The method is predominantly qualitative, the authors proposing a structured interview guide. Managers in SMEs were asked about the importance they attribute to different knowledge-related activities and their opinion on the state of the knowledge-related processes, in order to understand different types of knowledge vulnerabilities as perceived by the respondents. The results indicate that knowledge creation and knowledge sharing are among the processes that have a high to very high importance and also with few to very few vulnerabilities. There are also processes that seem more vulnerable, for example, knowledge use. Different strategies that managers use for limiting knowledge vulnerabilities emerged in this research. This study is a first attempt to propose a structured interview guide for assessing the knowledge processes status and knowledge vulnerabilities in SMEs.*

**Keywords:** *knowledge vulnerabilities, knowledge processes, knowledge risks, SMEs, qualitative research*

**JEL classification:** D80, D81, D83

**DOI:** 10.24818/RMCI.2026.3.535

## **1. Introduction**

This study presents a different approach in researching the presence of knowledge risks in organizations, using the taxonomy based on the organizational knowledge dynamics presented by the Bratianu et al. (2022) and proposing a predominantly qualitative method, through a structured interview guide.

The concept of knowledge risk is an important topic in the field of knowledge management and has been studied by a significant number of authors in

---

<sup>1</sup> Andrei Ștefan Neștian, Alexandru Ioan Cuza University of Iași, e-mail: nestian@uaic.ro

<sup>2</sup> Alexandra Luciana Guță, Alexandru Ioan Cuza University of Iași, e-mail: luciana\_guta@yahoo.com

<sup>3</sup> Silviu Mihail Tiță, Alexandru Ioan Cuza University of Iași, e-mail: silviutita@yahoo.com

the last almost forty years (Becerra et al., 2008; Bratianu et al., 2022; Cooper, 2003; Durst, 2019; Massingham, 2010; Niwa, 1989; Scott & Walsham, 2005; Zieba et al., 2022). The concept of 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). At the operational level, the losses created by the occurrence of a knowledge risk can be estimated based on the variation in the value produced at the level of different production processes or service delivery processes. At the strategic level, the losses can be estimated based on the overall value of: sales, the brand, the companies’ shares, or its competitive position.

Knowledge vulnerabilities are defined as reflecting “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” (Bratianu & Bejinaru, 2022, p. 2). Thus, knowledge vulnerabilities may also be considered “potential internal threats” (Bratianu et al., 2024, p. 71).

The current state of knowledge in the scientific literature analysing the concept of “knowledge vulnerability” is limited and focused on theoretical research. There are few exceptions, consisting of quantitative studies based on the proposal of measurement scales (Neșțian & Guță, 2023; Bratianu et al., 2025).

This paper is part of a larger project, which deals with knowledge vulnerabilities, as well as knowledge risks that may manifest themselves along knowledge processes. The aim of this paper is to analyse the situation of Knowledge Management within small and medium sized enterprises (SMEs), in order to highlight different types of knowledge vulnerabilities that may occur in this type of organization. Our study is exploratory (Saunders et al., 2007) and the method is predominantly qualitative. The paper contributes to the literature by including a first attempt to propose a structured interview guide for assessing the status of knowledge processes and knowledge vulnerabilities in SMEs.

## **2. Literature review**

Knowledge management practice in SMEs is recognized as specific due to the size of the organizations. Knowledge management presents challenges due to the fact that “intangible assets accumulate in the organization through dynamic, unstructured, and often subtle processes that are not easily codified into formal training programs or captured in information systems” (Swap et al., 2001, p. 96). The focus on knowledge acquisition and learning, in order to reduce the uncertainties and risks of their initiatives (Sanchez & Ricart, 2010), especially at the strategic level, may be specific to SMEs, given that these organizations may usually not have very advanced mechanisms for capturing, maintaining and using knowledge. Thus, SMEs could use special knowledge management capabilities, allowing them to identify and transform both new and existing knowledge into

business opportunities that are of an innovative nature (Hock-Doepgen et al., 2021).

However, despite the particularities of SMEs, their knowledge processes are complete and similarly represented in SMEs, as they are in other organizations. We refer here to the main knowledge processes proposed in 2022 by Bratianu et al. (2022): knowledge creation, knowledge acquisition, knowledge sharing, knowledge use, knowledge loss, emotional knowledge processes and spiritual knowledge processes. However, the activities related to these knowledge processes are not strictly defined and precisely described in SMEs. They tend to be perceived by owners or managers rather as interests or general directions that they must take into account when deciding and implementing other activities.

This argument led us to a qualitative approach; to see to what extent the owners or managers of SMEs recognize the presence of these knowledge processes in their organizations, by asking them about the importance of the activities specific to these processes and also by asking them about their perception on the level of vulnerability of the organization in managing these processes. We considered that providing open answers to the interviews would give them the opportunity to make an honest self-assessment. Starting from this diagnosis, we analysed and highlighted the vulnerabilities expressed on these processes.

Knowledge processes contain actions, and within these actions, knowledge is the object of specific processing. These actions are carried out in ways or contexts that favour the occurrence of knowledge risks (Neșțian & Guță, 2023).

Based on the scientific literature, we consider the concept of knowledge risk as a particular case of the generic concept of risk, present in knowledge processes, reflecting those situations in which there could be negative consequences of decisions regarding knowledge processes under the influence of internal and external factors (Cameron & Raman, 2005; Massingham, 2010; Massingham, 2020; Society for Risk Analysis, 2018). Like other risks, knowledge risks can be calculated as the multiplication of probability and impact. The resulting loss is the considered impact. The most important assumption we use in defining knowledge risks is that there is a variation in the value of knowledge, with implications for the value created by the organization. Variations in the value of knowledge can arise due to the contributions of the variables of knowledge creation, knowledge acquisition, and knowledge loss within the boundaries of the organization (Bratianu et al., 2022). This perspective, of the variation of the value of knowledge, is also based on the idea that an organization is a knowledge entity with an interface with the external environment. The interface is like a permeable membrane, allowing knowledge flows into and out of the organization, since the knowledge management system is an open system. Another source of variations in the value of knowledge are changes in different contextual factors, which lead to a change in the distribution and relative value of organizational knowledge. The value of knowledge varies when there are transformations between the three basic knowledge fields: rational, emotional, and spiritual (Bratianu et al., 2022). Therefore, in this case we must consider the processes of knowledge sharing,

knowledge hiding, knowledge hoarding, and, more generally, any transformation of knowledge from one field to another.

The likelihood of a knowledge risk is related to the evolution of external or internal factors. Some of these factors may be completely outside the control of the company. However, some of the factors may be at least partially under the control or influence of the company. To understand these factors, we need to consider the concept of knowledge vulnerability.

In an organization, knowledge vulnerabilities are the roots of potential knowledge risks (Bratianu et al., 2022; Bratianu et al., 2024). One important aspect related to vulnerabilities is the capability to respond (Marandola & Hogan, 2006). However, the ability of a system to respond – when a risk occurs – can be hindered if the system has vulnerabilities. Vulnerabilities have another characteristic, which is that their presence reduces the absorptive capacity of a system. Thus, when risks occur, vulnerabilities imply a lower capacity to prevent or mitigate losses or to recover to a normal state (Marandola & Hogan, 2006).

Researching the scientific literature in the field of knowledge management, we have not identified any empirical study that aims to assess the state of knowledge processes and knowledge vulnerabilities in companies. We identified only one study that presents a critical analysis of the scientific literature (Ursache, 2023) from which we can confirm that this is truly an emerging field: “So far, vulnerabilities have been analyzed in areas like disaster management, geography, climate change, economics, information security, and, more recently in cybersecurity founding various academic research, but the identification and analysis of knowledge vulnerabilities, in a more comprehensive way, have not yet been the topic of research in the knowledge domain” (Alexander, 2013; Chambers, 1989; Cutter, 1996; Dow, 1992; Gabor & Griffitch, 1980; Kasperson et al., 2001; Turner II et al., 2003, cited in Ursache, 2023, p. 531).

In this context, we can state that our paper is proposing the first empiric assessment of the status of knowledge processes and knowledge vulnerabilities in SMEs, based on a predominantly qualitative approach.

### **3. Methodology**

The research is exploratory (Saunders et al., 2007). Regarding the concept of “knowledge vulnerability”, the current state of knowledge is predominantly focused on theoretical research and rarely, with very few exceptions, have measurement scales been proposed (Neșțian & Guță, 2023; Bratianu et al., 2025). The method is predominantly qualitative.

The data has been collected through interviews. For this, a structured interview guide was developed, with 13 questions. The first question measures the importance given to eight types of activities regarding the knowledge that the organization must possess, that are evaluated on a scale from one to five, meaning: 1 – very low importance; 2 – low importance; 3 – normal/ medium importance; 4 – high importance; 5 – very high importance.

Towards the end of the interview guide there is a second question regarding the same types of activities, but focused on the respondents' perception of weaknesses or a low level of interest in their organization, which generate or could generate the manifestation of unfavourable situations. This question focuses on the perception of vulnerabilities. The scale is from one to five, meaning: 1 – the situation is very vulnerable; 2 – the situation is quite vulnerable; 3 – the situation is acceptable; 4 – the situation has few vulnerabilities; 5 – the situation has very few vulnerabilities.

The interview contains nine open-ended questions related to the knowledge activities considered in this research. All these knowledge activities are associated with the following knowledge processes: knowledge creation, knowledge acquisition, knowledge loss, knowledge sharing, knowledge use.

The interview ends with questions related to the size of the organization in which the respondent works (1-9 employees; 10-49 employees; 50-249 employees; 250 employees or more) and the number of employees that the respondent manages within the managed structure (company, department, branch, etc.): 0 employees ("I do not hold a managerial position"); 1-9 employees; 10-49 employees; 50-249 employees; 250 employees or more.

The main novelty of our study consists in carrying out an empirical study, through a structured interview, with an emphasis on a qualitative approach.

### 3.1 The respondents

The interviews focused on SMEs and were conducted online (between 2nd and 12th of February 2024) using Microsoft Teams. A number of 10 SMEs participated in the study, with one respondent (manager) from each of them. Details about the respondents and the companies' field of activity are presented in Table 1 below.

**Respondent profiles and companies' fields of activity**

**Table 1**

| ID  | Gender | Company field                       |
|-----|--------|-------------------------------------|
| I01 | M      | Interior Design                     |
| I02 | F      | Medical Equipment Manufacturing     |
| I03 | M      | Medical Services                    |
| I04 | M      | Consulting                          |
| I05 | F      | Equipment Services                  |
| I06 | M      | Fashion & Textile Manufacturing     |
| I07 | M      | Advertising & Marketing             |
| I08 | F      | Language Learning Services          |
| I09 | M      | Traditional Food & Catering         |
| I10 | M      | Consulting & Information Technology |

*Source:* Authors' analysis

With one exception, of one manager (ID I03, position as manager), all respondents are both managers and business owners of their companies.

Considering the size of the organizations, seven SMEs that participated in this study have between 10 and 49 employees, one has between 50 and 249 employees, and another one has between 1 and 9 employees.

Eight of the managers participating in the research manage between 10 and 49 employees, one manages between 50 and 249 employees, and another manages less than 10 employees.

Our aim is to analyze the situation of Knowledge Management within SMEs, in order to highlight different types of knowledge vulnerabilities that may arise in this type of organizations. Thus, regarding the organizations in the sample, we are interested in their size and not their fields of activity. This led to a variety of fields in the sample.

### **3.2 Methods and techniques used for data analysis**

The interviews were conducted in Romanian, lasted approximately 30-40 minutes, and since we did not identify similar qualitative studies in the literature, the interview guide with the questions (and the scales, where applicable) is proposed by the authors. Microsoft Teams was used for the interviews and for automatic transcription. Handwritten notes were also taken during the interviews. Microsoft Excel and Atlas.ti 6.0 were used for data processing and analysis. The transcription results were corrected to improve the quality of the text, and during processing an ID was assigned for each subject (see Table 1). The responses were processed and organized using the qualitative data analysis software Atlas.ti 6.0, which allows us to annotate and code into themes different ideas related to knowledge vulnerabilities, discussed during the interviews.

## **4. Results**

The data in Table 2 reveal a profile that places a very high importance (equal to or above 4.50 out of a maximum of 5.00) on knowledge creation, knowledge sharing and knowledge acquisition from external sources. We also observe a high importance given to cultural knowledge sharing, knowledge use and knowledge loss prevention (between 4.00 and 4.20). The lowest importance is attributed to knowledge protection against unintentional disclosure (3.70) and knowledge acquisition from new employees (3.30).

The significance of the responses on the Likert scale starts from maximum vulnerability (very vulnerable = level 1) to minimal vulnerability (very few vulnerabilities = level 5). The results are presented in Table 2, which also highlights the gap between the importance given and the perceived lack of vulnerabilities, for all knowledge activities considered.

The highest perceived vulnerability is in terms of knowledge loss (3.00 out of 5.00), where the departure of experienced employees is considered a

vulnerability that is very difficult to reduce. Managers recognize the importance of stopping knowledge loss (importance 4.00 out of 5.00), but have difficulty preventing it. In this vulnerability we find the largest difference between the importance given and the perceived lack of vulnerabilities, thus revealing the greatest managerial concern.

**Comparative analysis between importance given and the perceived vulnerability  
(ranked in descending order of the lack of vulnerabilities)**

**Table 2**

| <b>Knowledge activities</b>                   | <b>Importance of knowledge activities</b> | <b>Perceived lack of vulnerability (reversed scale: 1 = maximum vulnerability; 5 = minimal vulnerability)</b> | <b>Gap between importance and perceived lack of vulnerability</b> |
|-----------------------------------------------|-------------------------------------------|---------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Knowledge Sharing                             | 4.70                                      | 4.30                                                                                                          | -0.40                                                             |
| Knowledge Acquisition (from external sources) | 4.50                                      | 4.10                                                                                                          | -0.40                                                             |
| Cultural Knowledge Sharing (to new employees) | 4.20                                      | 4.00                                                                                                          | -0.20                                                             |
| Knowledge Creation                            | 4.90                                      | 3.90                                                                                                          | -1.00                                                             |
| Knowledge Use                                 | 4.20                                      | 3.70                                                                                                          | -0.50                                                             |
| Knowledge Protection (against leakage)        | 3.70                                      | 3.45                                                                                                          | -0.25                                                             |
| Knowledge Acquisition (from new employees)    | 3.30                                      | 3.10                                                                                                          | -0.20                                                             |
| Knowledge Loss                                | 4.00                                      | 3.00                                                                                                          | -1.00                                                             |

*Source: Authors' own processings*

The second biggest vulnerability is related to knowledge acquisition from new employees (3.10 out of 5.00, on a scale of 1 to 5). Managers do not give much importance to this source of knowledge (importance 3.30 out of 5.00), but they recognize that this attitude does not put the company in the best position.

The third highest perceived vulnerability (3.45) refers to protecting company knowledge from unwanted disclosure, by limiting access, classifying information, and controlled dissemination of valuable knowledge, to avoid leaking manufacturing secrets or other knowledge to competitors, suppliers, or customers.

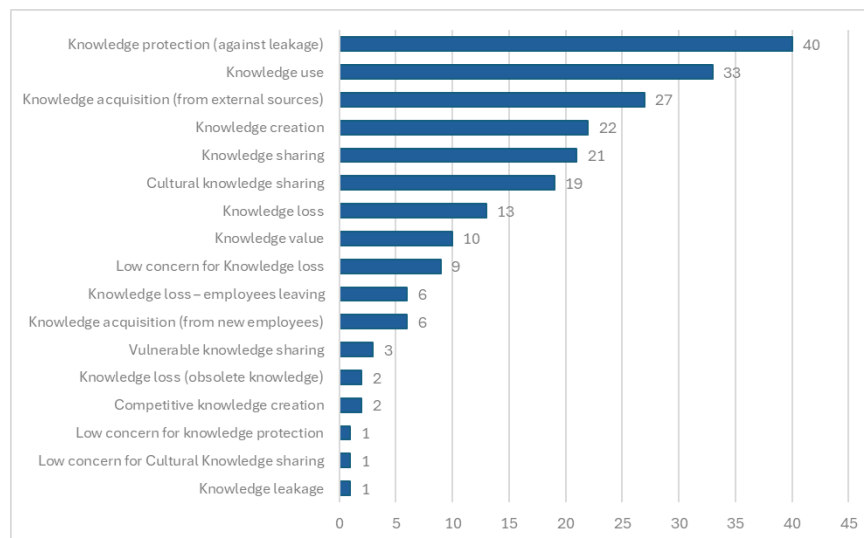
Managers did not attach much importance to these situations (3.70), despite the negative experiences. Managers adopted a rather passive attitude, considering that the natural way of collaborating with suppliers and customers makes it very difficult to protect all that valuable knowledge that can endanger the company's operations. However, two respondents reported the creation of new companies by former employees, taking important customers with them in the process.

On the fourth position as vulnerability, we can find knowledge use (3.70), with a gap of 0.50 points below the given importance. Managers have acknowledged that creating value by using the knowledge of their employees was far from the maximum potential of that possessed knowledge, creating a competitive disadvantage.

On the fifth position as vulnerability, knowledge creation, perceived at 3.90, reveals the biggest gap (1.00 point) from the given importance. With an average of 4.90, creating knowledge faster than competitors is recognized by the managers as the most important knowledge activity.

Knowledge sharing (4.30), knowledge acquisition from external sources (4.10) and cultural knowledge sharing to new employees (4.00) are considered the knowledge activities were the company experiences the least vulnerabilities. Also, these are considered knowledge related activities of high to very high importance (4.20-4.70) and have gaps below 0.50 points between the importance and the perceived lack of vulnerabilities.

The first part of the qualitative analysis, based on coding the answers in the transcript of the interviews, revealed the situation presented in Figure 1, with the frequencies of appearance of certain recurrent themes. It can be seen that the most frequent topic is related to knowledge protection (against leakage). Knowledge use, knowledge acquisition (from external sources), knowledge creation, knowledge sharing and cultural knowledge sharing follow, with frequencies between 19 and 33 appearances. Knowledge loss, a topic at which we could see that the lowest perceived lack of vulnerabilities registered in question 1 (3 points out of 5), appears here only 13 times. Considering the frequency and the perceived vulnerability, we may consider that managers are not necessarily aware of the dangers of knowledge loss.



**Figure 1: Frequency of appearance in interviews of references relevant for the main assigned codes**

*Source: Authors' own processings*

In the second part of the qualitative analysis, we analyse and comment on the open-ended responses provided by the managers.

Based on these answers, we assume that our SMEs attach great importance to the creation of new knowledge, which is necessary in the organization. A good part of the respondents is one step ahead of their competitors when it comes to producing new knowledge. For this to happen, it is necessary to know what the advantages of the organization are in relation to the competition, when discussing knowledge creation. Also, organizations must be permanently connected to the latest technologies, procedures or processes. This is an answer given by a respondent: “For a year now I have been trying to do this by identifying the needs of customers, because this is the only way I can differentiate myself in the market - when I understand exactly what their need is.”

Obtaining new knowledge from other organizations, through publications, training, consultancy, etc., is considered to be of high to very high importance. Managers in SMEs are concerned about obtaining new external knowledge, the situation regarding the acquisition of knowledge from other organizations being with few or even very few vulnerabilities. The SMEs in the sample are either members of international organizations, which helps them to find out about news in their field, or they buy articles, or they use open platforms.

Regarding attracting new knowledge through recruitment, the answers range from not relying on recruitment as a strategy to attract new knowledge into the organization, preferring outsourcing activities such as bringing in new clients, to finding people who have what the organization lacks or who are better than the organization. Responses regarding not recruiting at all – a potential vulnerability in terms of knowledge acquisition – were associated with the idea of providing knowledge only to new employees and even not thinking at all about recruiting as a way of acquiring knowledge. Facilitating knowledge acquisition by recruiting new employees was rated as having medium importance (3.30), and the perception is that the situation could be considered acceptable from a vulnerability point of view (3.10). This is an answer given by one respondent: “It’s very interesting because we constantly say that the good people in the industry are in the bigger companies, in the multinational companies. But we always look to recruit people who are better than our organization at that time.”

The situation in SMEs regarding the limitation of knowledge loss shows a variety of strategies through which managers try that. Some managers consider important the transfer of knowledge from employees leaving the company to someone else who will take over their duties. Other strategies are: offering incentives to employees or even keeping valuable employees, keeping written documents, sharing experiences, creating internal procedures and strict confidentiality agreements, regular transfer of knowledge from highly qualified employees to other employees.

Knowledge sharing among employees is perceived as an important aspect by SMEs managers. The sampled firms have several knowledge transfer strategies, such as mentoring, shadowing, senior collaboration with new employees, post-

factum analysis. This is a relevant answer given by one respondent: "...what trainings they sign up for or what conferences they have to attend, when they come back to the organization, at the next meeting, they have to give us a summary of the materials, of the things they saw, and all employees should know." Although managers presented several strategies for transferring knowledge from very experienced to less experienced employees – revealing a situation with few or very few vulnerabilities – when talking about facilitating knowledge transfer between employees, managers usually think first of new employees, in their first months at the company.

Some SME managers report that there has been no disclosure of manufacturing secrets or other valuable knowledge to their suppliers, customers or competitors. However, information leaks are frequently linked to employee behaviour. To protect against this vulnerability, strategies include layering information, classifying information or not storing certain types of documents on servers, and having procedures for document management. This latter strategy applies when working on projects that need to be uploaded to platforms. This is an answer given by a respondent: "We are a Monday-Friday kitchen, which gives our employees the weekend off. I could say the knowledge leakage happens in those weekend part-time jobs that we know our chefs do, especially during the events seasons."

Analyzing the attention paid to the application or maximum use of employees' knowledge or skills, in most cases managers in SMEs do not apply certain methods or strategies. What we found was that most managers make efforts to improve the knowledge/ skills of their employees, encourage employees to come up with ideas, innovations, try to help each other within the company, to be open. However, few managers mentioned investing in their employees through constant training, so there could be a vulnerability in terms of knowledge use, although this issue was rated as important. This is an answer given by a respondent: "...we keep the same people on projects. The same teams! We do not change them, or not very often."

In terms of assessing the protection of valuable knowledge and information with protected access, four main types of strategies were observed: very good protection of information on procurement and purchases (e.g. imposing confidentiality of negotiations on purchase prices); the need to protect electronic information (stored on servers or emails), as this has been a problem in the past; investing in employees, maintaining a good relationship with them, taking into account their development needs; loyalty and retention; classifying information and establishing the level of access or involvement of employees.

The last two types of strategy can be considered very useful, since valuable knowledge may leak when an employee leaves the organization.

The situation, from the point of view of protecting valuable knowledge and information with protected access, seems acceptable, according to the managers' rankings, but not necessarily with few vulnerabilities.

Where considered necessary, depending on the field of activity, SMEs have methods to accommodate the new employee to the organizational culture. Employees learn about „cultural” knowledge through trainings, shadowing, help from more experienced colleagues. Some managers consider this to be a topic that does not influence their activity. Overall, the situation seems to present few vulnerabilities.

## 5. Conclusion

The SMEs that participated in this study also have a wide range of strategies for knowledge sharing, such as: mentoring, shadowing, seniors' collaboration with new employees, post-factum analysis. Therefore, knowledge sharing is among the knowledge activities in which these SMEs face the fewest vulnerabilities.

Although the results indicate that knowledge creation and knowledge sharing are among the processes which are of high to very high importance and also with few to very few vulnerabilities, in the case of knowledge creation the gap between importance and perceived vulnerability is the biggest (1 point).

A perceived vulnerability (only 3 points out of 5) to knowledge loss was revealed, although managers applied some strategies to limit different forms of knowledge loss. Among the strategies that emerged we can mention the transfer of knowledge from an employee leaving the organization to someone else, keeping written documents or sharing experiences.

Managers are very interested in protecting knowledge (against leakage), given the fear of losing knowledge due to the inadequate use of certain technologies (cloud, platforms, email, social networks, etc.) and less concerned about an employee leaving with unique expertise. Some of them believe that sharing knowledge is always wise: if more information is transferred without fear of filters, even to competitors and customers, the company will grow.

The scientific literature has focused more on knowledge risks than on vulnerabilities, while also focusing on theoretical studies or bibliometric analyses (e.g., Bratianu and Bejinaru, 2022).

Thus, this study's research instrument is useful for helping managers to become aware of the importance given to knowledge activities that the organization must possess and the weaknesses or low levels of interest in their organization, which can lead to the manifestation of unfavourable situations, the results providing useful information for decision-making processes.

In conclusion, through this paper, we aimed to analyze Knowledge Management situations in SMEs, in order to highlight different types of knowledge vulnerabilities that may arise in this type of organization. To this end, we approached the research in a predominantly qualitative way and solicited the opinions of managers and business owners on the importance of knowledge activities and the perception of vulnerabilities related to them.

This study has some limitations and also opens some possibilities for future research. First, we must start by stating that this study represents a first

attempt to propose a structured interview guide for assessing the state of knowledge processes and knowledge vulnerabilities in SMEs, by measuring and obtaining details about knowledge activities, their importance and perceived vulnerabilities. The approach, based on collecting qualitative data from a small number of SMEs, does not allow any generalization of the results.

The results can also be challenged from a theoretical perspective: the small size of an SME leads to a limited stock of knowledge and its presence in few replicas, either in documents or in people's minds. Thus, in SMEs, some knowledge is more likely to be unique, therefore the impact of the presence or loss of some knowledge may be greater. The departure of the most valuable employee with the greatest expertise from a company with 10 employees has a greater impact on the evolution of that business, compared to the departure of the best employee from a company with 300 employees.

Therefore, the results show that we can improve this methodology to help managers and business owners of SMEs to become aware of the topics related to knowledge-based activities and the associated vulnerabilities. Future research can focus on larger companies and can be approached using quantitative methods that can be developed based on the current findings.

## References

1. Becerra, M., Lunnan, R. & Huemer, L., 2008. Trustworthiness, risk, and the transfer of tacit and explicit knowledge between alliance partners. *Journal of Management Studies*, 45(4), pp. 691-713. <https://doi.org/10.1111/j.1467-6486.2008.00766.x>
2. 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 (IFKAD), 20-22 June 2022, Lugano*, pp. 687-700.
3. Bratianu, C., Bejinaru, R. & 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
4. Bratianu, C., Neșțian, A.Ș. & Guță, A.L., 2022. Knowledge risks taxonomy based on the organizational knowledge dynamics. *Ekonomicko-manazerske spektrum*, 16(2), pp. 61-71. [dx.doi.org/10.26552/ems.2022.2.61-71](https://doi.org/10.26552/ems.2022.2.61-71)
5. Bratianu, C., Neșțian, A.Ș., Guță, A.L. & Tiță, S.M., 2025. Measuring Knowledge Vulnerabilities in Knowledge Processes: A Scale Development. In: Kianto, A. & Toth, I. eds. *Proceedings of the 26<sup>th</sup> European Conference on Knowledge Management (ECKM), 04-05 September 2025, Lahti*. Reading: Academic Conferences International Limited, pp. 140-147. [Accessed 30 September 2025]. Available from: <https://doi.org/10.34190/eckm.26.1.3773>
6. Cameron, I. & Raman, R., 2005. *Process systems risk management. First Edition*. Amsterdam: Elsevier
7. 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*, 20(1-2), pp. 117-140. [https://doi.org/10.1016/S0923-4748\(03\)00007-9](https://doi.org/10.1016/S0923-4748(03)00007-9)

8. Durst, S., 2019. How far have we come with the study of knowledge risk?. *VINE Journal of Information and and Knowledge Management Systems*, 49(1), pp. 21-34. <https://doi.org/10.1108/VJKMS-10-2018-0087>
9. Hock-Doepgen, M., Clauss, T., Kraus, S. & Cheng, C.F., 2021. Knowledge management capabilities and organizational risk-taking for business model innovation in SMEs. *Journal of business research*, 130, pp. 683-697. <https://doi.org/10.1016/j.jbusres.2019.12.001>
10. Marandola, E. & Hogan, D.J., 2006. *Vulnerabilities and risks in population and environment studies*. Population and Environment, 28, pp.83-112.
11. Massingham, P., 2010. Knowledge risk management: a framework. *Journal of Knowledge Management*, 14(3), pp. 464-485. <https://doi.org/10.1108/13673271011050166>
12. Massingham, P., 2020. *Knowledge management. Theory in practice*, London: SAGE
13. Neșțian, A.Ș. & Guță, A.L., 2023. Vulnerabilities and Knowledge Risks in Knowledge Processes. In: Matos, F. & Rosa, Á. eds. *Proceedings of th 24<sup>th</sup> European Conference on Knowledge Management (ECKM), 07-08 September 2023, Lisbon*. Reading: Academic Conferences International Limited, pp. 960-968. [Accessed 30 March 2024]. Available from: <https://doi.org/10.34190/eckm.24.1.1416>
14. Niwa, K., 1989. *Knowledge-based risk management in engineering: a case study in human-computer cooperative systems. First Edition*, New York: John Wiley & Sons, Inc.
15. Sanchez, P. & Ricart, J.E., 2010. Business model innovation and sources of value creation in low-income markets. *European Management Review*, 7, pp. 138-154. <https://doi.org/10.1057/emr.2010.16>
16. Saunders, M., Lewis, P. & Thornhill, A., 2007. *Research Methods for Business Students. Fourth Edition*, Harlow: Prentice Hall
17. Scott, S.V. & Walsham, G., 2005. *Reconceptualizing and managing reputation risk in the knowledge economy: Toward reputable action*. Organization Science, 16(3), pp. 308-322.
18. Society for Risk Analysis. 2018. *Society for risk analysis glossary* [Online] (Updated August 2018) Available at: <https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf> [Accesed 30 March 2024].
19. Swap, W., Leonard, D., Shields, M. & Abrams, L., 2001. Using Mentoring and Storytelling to Transfer Knowledge in the Workplace. *Journal of management information systems*, 18(1), pp. 95-114. <https://doi.org/10.1080/07421222.2001.11045668>
20. Ursache, V. M. (2023). Knowledge Vulnerabilities: Definitions and Interpretations “Ovidius” University Annals, *Economic Sciences Series*, 23(1), pp. 529-536.
21. Zieba, M., Durst, S. & Hinteregger, C., 2022. The impact of knowledge risk management on sustainability. *Journal of Knowledge Management*, 26(11), pp. 234-258. <https://doi.org/10.1108/JKM-09-2021-0691>