
In this knowledge pill, KIBS SMES will learn about knowledge risks and how to develop a knowledge risk management strategy to manage these risks.

## Understanding knowledge risks

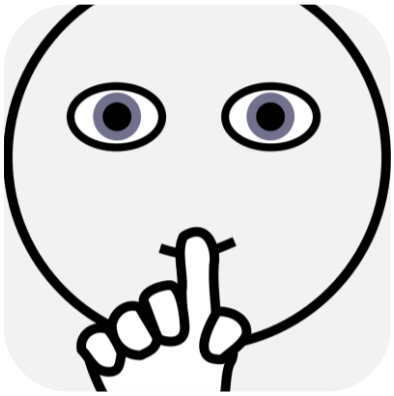
Knowledge risks can be defined as the "measure of the **probability** and **severity** of adverse effects of any activities engaging or related somehow to knowledge that can affect the functioning of an organization on any level" (Durst and Zieba, 2018, p. 2).

- SMEs in KIBS are particularly vulnerable to knowledge risks due to their **heavy** reliance on organizational knowledge to deliver services.
- While implementing a systematic KRM approach may be challenging, it is **beneficial**.
- These risks can be categorized into: **human**; **operational**; **technological**.

Co-funded by the Erasmus+ Programme of the European Union

Let's start by defining knowledge risks, which refer to the likelihood and severity of negative impacts on an organization resulting from knowledge-related activities (Durst and Zieba, 2018, p.2). Small and medium-sized enterprises (SMEs) in knowledge-intensive business services (KIBS) are particularly vulnerable to knowledge risks since they rely heavily on organizational knowledge to deliver services, and managing these risks systematically can be challenging due to limited resources. Despite the difficulties, implementing a systematic approach to knowledge risk management can be beneficial for SMEs in the short and long run. Knowledge risks can be categorized into three categories: human, operational, and technological.

## Human knowledge risks



Source: Image by OpenClipart-Vectors from Pixabay

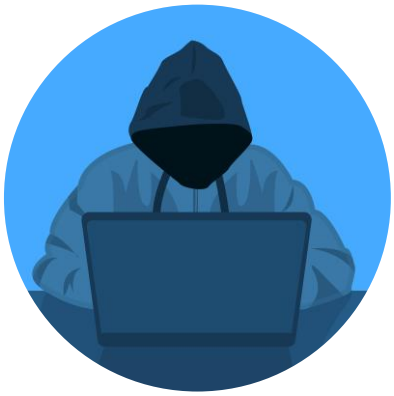
Human knowledge risks can be attributed to an **individual's personal**, **social**, **cultural**, and **psychological characteristics**. Some of these risks include:

- **Knowledge hiding** » involves **withholding** or **concealing** requested knowledge or information.
- **Knowledge hoarding** » involves **accumulating** knowledge or information that may not be shared.
- **Unlearning** » involves **giving up** outdated practices and can also be considered a knowledge risk.

Co-funded by the Erasmus+ Programme of the European Union

Human knowledge risks are associated with an individual's personal, social, cultural, and psychological characteristics. There are various types of risks under this category, such as knowledge hiding, which refers to the act of withholding or concealing requested knowledge or information. Knowledge hoarding is another risk, where individuals accumulate knowledge or information that they may not share with others. Finally, unlearning is a type of knowledge risk that involves giving up outdated practices.

## Technological knowledge risks



Source: Image by Shafin Al Asad Protic from Pixabay

Technological knowledge risks arise from **the use of technologies**, including information and communication technologies (ICT), but are not limited to those. These may occur as a result of situations such as:

- The use of **outdated** or **old technologies** can cause system failures, leading to data breaches, cyber attacks, and loss of sensitive information.
- Hackers taking advantage of vulnerabilities in the system, leading to the loss of intellectual property or financial information.

Co-funded by the Erasmus+ Programme of the European Union

Technological knowledge risks refer to risks that arise from the use of technology, including information and communication technologies (ICT). These risks may include situations such as using outdated or old technologies that can cause system failures, leading to data breaches, cyber attacks, and loss of sensitive information. Additionally, hackers may take advantage of vulnerabilities in the system, leading to the loss of intellectual property or financial information.

## Operational knowledge risks

Source: Image by Memed_Nurrohmad from Pixabay

Operational knowledge risks encompass all the risks that can arise from the **everyday** operations and functioning of organizations. This includes risks associated with making alliances or mergers, outsourcing, and applying wrong or obsolete knowledge in operations. For example, if an organisation:

- outsources a critical function to a third-party vendor that fails to deliver on expectations;
- uses outdated or incorrect knowledge in their operations.

Co-funded by the Erasmus+ Programme of the European Union

The operational category of knowledge risks includes all risks that can arise from the everyday operations of organizations. This encompasses risks associated with making alliances or mergers, outsourcing, and applying wrong or obsolete knowledge in operations. For example, if an organization outsources a critical function to a third-party vendor that fails to deliver on expectations, this can lead to a breakdown in operations and loss of customer trust. Additionally, if an organization uses outdated or incorrect knowledge in their operations, this can result in inefficiencies and suboptimal outcomes.

## Knowledge risk management

Knowledge risk management (KRM) is a systematic way of applying tools and techniques to identify, analyze and respond to risks associated with the creation, application, and retention of organizational knowledge (Durst et al., 2016).

- A systematic approach to KRM can:
  - enhance agility and ability;
  - ensure long-term sustainability and success;
  - increase innovativeness;
  - drive growth and expansion.

Co-funded by the Erasmus+ Programme of the European Union

Now, knowledge risk management (KRM) refers to a systematic approach that involves the use of tools and techniques to identify, analyze, and respond to risks associated with the creation, application, and retention of organizational knowledge (Durst et al., 2016). Implementing a systematic approach to KRM can bring numerous benefits to an organization, including:
Enhancing agility and the ability to adapt to changing market conditions.
Ensuring long-term sustainability and success.
Increasing innovativeness by accessing current and relevant knowledge for generating new ideas and creating new products or services.
Driving growth and expansion by meeting the evolving needs of customers and markets.

## Step 1 - Formulation of KRM strategy


Source: Image by mohamed_hassan from Pixabay

The **initial** step towards effective KRM is to **formulate** a strategy. This includes

- identifying potential knowledge risks
- assessing their impact on the organization,
- developing a plan to manage or mitigate the identified risks
- ensuring alignment of the KRM strategy with the organization's overall strategy, goals, and objectives.

Requiring the involvement of a diverse group of stakeholders, including managers and employees.

Co-funded by the Erasmus+ Programme of the European Union

To effectively implement KRM, the first step is to develop a strategy that involves identifying potential knowledge risks, assessing their impact on the organization, and developing a plan to manage or mitigate them. This strategy should also align with the organization's overall strategy, goals, and objectives. It is crucial to involve a diverse group of stakeholders, including managers and employees, in the strategy formulation process.

## Step 2 - Identify existing KRM practices

This step is to identify existing KRM practices that address the organization's main challenges.

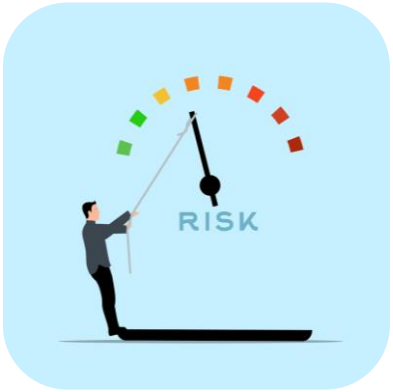
- Acknowledge that KRM concerns **all** aspects of the organization and goes beyond individual offices and departments.
- A broad range of offices and departments should be involved to increase the chance of **aligned actions**.
- A task force of selected employees should be established to **oversee** the process and involve all relevant stakeholders.

Source: Image by OpenClipart-Vectors from Pixabay

Co-funded by the Erasmus+ Programme of the European Union

Once the KRM strategy has been formulated, the next crucial step is to identify any existing KRM practices that are addressing the main challenges faced by the organization, such as the retirement of experienced employees or the need to adapt to new technologies. It is essential to acknowledge that KRM affects all aspects of the organization and extends beyond individual offices and departments. Therefore, involving a broad range of offices and departments in the process can increase the likelihood of aligned actions. A task force comprising selected employees should be established to oversee the KRM process and ensure the involvement of all relevant stakeholders.

## Step 3 - Assessment of existing KRM practices




Source: Image by mohamed_hassan from Pixabay

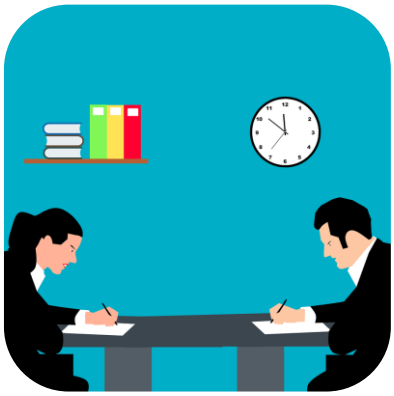
The third step involves assessing the **existing** KRM practices in relation to the KRM strategy formulated in step 1.

- This requires identifying current KRM practices, their purpose, and link to the overall KRM strategy.
- Both managers and the task force should be responsible for this assessment to ensure that all KRM practices are evaluated comprehensively.

Co-funded by the Erasmus+ Programme of the European Union

To advance with the KRM implementation process, the third step is to assess the current KRM practices in relation to the strategy formulated in the previous step. This entails identifying the purpose and link of each KRM practice to the overall KRM strategy. Managers and the task force should be involved in the assessment process to ensure that all KRM practices are evaluated comprehensively. By assessing the existing KRM practices, organizations can identify gaps and inconsistencies in managing knowledge risks, which ultimately leads to a more effective KRM strategy that aligns with the organization's goals and objectives.

## Step 4 – Improve an existing - or develop a (new) KRM practices



Source: Image by mohamed_hassan from Pixabay

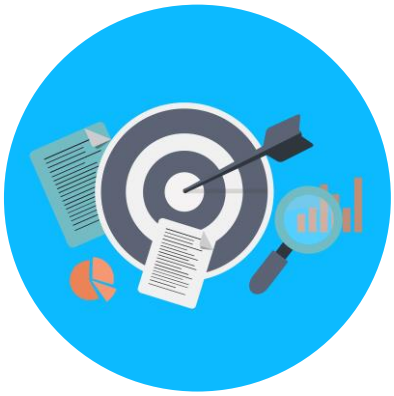
When developing and improving KRM practices

- ❑ Question existing routines and structures that may no longer be effective against knowledge challenges.
- ❑ Create a well-structured KRM practices that align with each other and include risk management processes should be developed.
- ❑ The focus should be on addressing the most critical knowledge risks and aligning with the planned KRM strategy and practices.
- ❑ Both managers and the established task force are responsible.

Co-funded by the Erasmus+ Programme of the European Union

The next step is to improve the existing KRM practices and develop new ones. This involves questioning the effectiveness of existing practices and structures in dealing with knowledge risks and focusing on developing well-structured KRM practices that are aligned with each other. The development process should include risk management processes such as identification, analysis, management, and reporting. The focus should be on the most critical knowledge risks and aligning the improved approaches with the planned KRM strategy and practices. Managers and the task force established are responsible for this step.

## Step 5 - Implementation of KRM strategy



Implementation of the KRM strategy

- Obtain commitment from key stakeholders for successful execution of the KRM strategy.
- Allocate adequate time for implementation process and provide KRM training to all members.
- Effective internal communication is essential to ensure understanding of the KRM strategy and practices.

Managers have **primary** responsibility for implementation and should appoint a **task force** for operative level implementation.

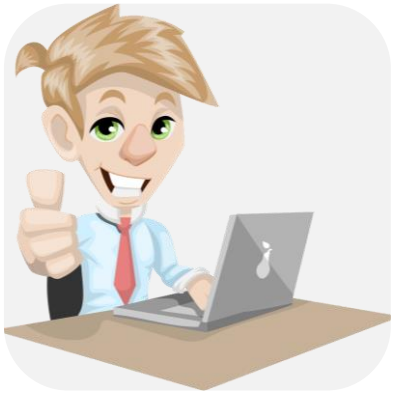
Source: Image by Megan Rexazin from Pixabay

Co-funded by the Erasmus+ Programme of the European Union

The fifth step involves the actual implementation of the strategy and practices developed in the previous steps. It is crucial to have the commitment of key stakeholders in the SME to ensure the successful execution of the KRM strategy. Adequate time should be allocated for the implementation process, and all members of the organization should receive appropriate KRM training. Effective internal communication is also vital to ensure that everyone understands the KRM strategy, practices, and the reasons behind them.

Managers have the primary responsibility for implementing the KRM strategy and practices, and they should appoint a task force to oversee the operative level implementation. Advisors and coaches can provide additional support to the task force.

## Step 6 - Continued assessment



Source: Image by GraphicMama-team from Pixabay

Continuous assessment is the final step of implementing KRM.

- ensuring KRM strategy is aligned with organizational goals and objectives;
- addressing any inconsistencies or gaps immediately;
- monitoring the effectiveness of KRM strategy;
- adjusting KRM strategy.

Regular review and updating of KRM strategy can help identify new risks and achieve long-term success.

Co-funded by the Erasmus+ Programme of the European Union

In the final step, it is essential to continuously assess whether the execution of the KRM strategy is aligned with organizational goals and objectives. Any inconsistencies or gaps should be immediately addressed. This step involves monitoring and evaluating the effectiveness of the KRM strategy and practices and adjusting them as necessary. Ongoing assessment helps to identify new knowledge risks and ensures that the organization is well-prepared to mitigate them. Regular review and updating of the KRM strategy can help KIBS SMEs achieve long-term success in a rapidly changing knowledge-driven economy.

## Sources and find out more!


Durst, S., Hinteregger, C., & Zieba, M. (2019). The linkage between knowledge risk management and organizational performance. *Journal of Business Research*, *105*, 1-10. https://doi.org/10.1016/j.jbusres.2019.08.002

Durst, S., Lindvall, B., & Bruns, G. (2020). Knowledge risk management in the public sector: insights into a Swedish municipality. *Journal of Knowledge Management*, *24*(4), 717-735.

Durst, S., & Zieba, M. (2019). Mapping knowledge risks: towards a better understanding of knowledge management. *Knowledge Management Research & Practice*, *17*(1), 1-13. https://doi.org/10.1080/14778238.2018.1538603

Zieba, M., Durst, S., & Hinteregger, C. (2022). The impact of knowledge risk management on sustainability. *Journal of Knowledge Management*, *26*(11), 234-258. https://doi.org/10.1108/JKM-09-2021-0691



Co-funded by the Erasmus+ Programme of the European Union

KNOWMAN

More about the project:
knowmanproject.eu

This project has been funded with support from the European Union. This document and all its content reflect the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.