A Methodological Framework for the Assessment of Knowledge Risks

Samuel Foli

PhD in Business

Department of Business and Economics, School of Social Sciences

Reykjavík University

March 2025

Doctoral thesis committee

Professor Susanne Durst (Supervisor)
Department of Business Administration
Reykjavík University
Reykjavík, Iceland

Professor Ingi Rúnar Eðvarðsson
Faculty of Business Administration
University of Iceland
Reykjavík, Iceland

Professor Michele Borgia
Department of Management and Business Administration
University "G. D'Annunzio" of Chieti-Pescara
Pescara, Italy

Declaration:

This doctoral thesis is submitted to the Department of Business and Economics, School of Social Sciences, at Reykjavík University in partial fulfilment of the requirements for the degree of Doctor of Philosophy. The introductory part constitutes the formal thesis, encompassing a synthesis of the accompanying papers, which have been either published or submitted for peer review.

ISBN: 978-9935-539-64-9 (Print version)

ISBN: 978-9935-539-65-6 (Electronic version)

Abstract

Knowledge risk management (KRM) has emerged as an essential field dedicated to addressing the various risks associated with organisational knowledge. A significant aspect of KRM is the assessment of knowledge risks; however, this area remains relatively underexplored due to the absence of a comprehensive framework.

This PhD research aims to develop a comprehensive risk assessment framework for knowledge risks, incorporating Multi-Criteria Decision-Making (MCDM) models.

Article I identifies seven key knowledge risks in ICT-supported collaborative projects using Total Interpretive Structural Modelling (TISM) as one of the MCDM models. It highlights cybercrime and espionage as high-driving risks, establishing hierarchical interrelations among these risks and providing a structural model that facilitates systematic KRM.

Article II evaluates operational knowledge risks in SMEs using a grey- Decision-Making Trial and Evaluation Laboratory (DEMATEL) model. It identifies 11 critical risks, categorising them as causal (e.g., knowledge waste and gaps) and effect risks (e.g., relational risks and espionage). Outsourcing risks and improper knowledge application are identified as particularly significant. This categorisation aids SMEs in understanding and addressing their unique vulnerabilities effectively.

Article III focuses on knowledge leakage drivers in collaborative agreements using an integrated ISM-MICMAC model. It identifies nine key drivers, including incomplete contracts and horizontal competition, as critical risk factors. The study demonstrates how these drivers influence knowledge leakage and provides actionable insights for mitigating risks.

In the final complementary study, the research integrates TISM, DEMATEL, and Preference Ranking Organisation Method for Enrichment Evaluation (PROMETHEE) within its framework. The framework was tested using a case company to validate its practical use in assessing knowledge risks and in supporting informed decision-making.

Methodologically, this thesis contributes to the literature on KRM, particularly in the domain of knowledge risk assessment, by introducing a well-structured and promising framework.

- TISM is applied to capture the interdependencies among knowledge risks and knowledge risk factors.

- DEMATEL is used to weight extended criteria, providing a deeper understanding of their significance.
- PROMETHEE is applied to prioritise knowledge risk factors based on their level of importance.

The insights derived from this framework offer valuable guidance for managers, risk managers, CEOs, and business owners, enabling them to identify, analyse and evaluate, a wide range of knowledge risks effectively. This thesis not only fills a critical gap in the KRM, more specifically knowledge risk assessment literature but also provides a practical tool to enhance decision-making and organisational resilience.

Ágrip

Stjórnun áhættu tengdri þekkingu (e. Knowledge Risk Management, KRM) hefur þróast í að vera mikilvægt svið sem beinist að því að takast á við ýmsar áhættur sem tengjast skipulagsþekkingu. Mikilvægur þáttur KRM er mat á þekkingaráhættu, en þetta svið hefur verið tiltölulega lítið rannsakað vegna skorts á yfirgripsmiklu ramma.

Þessi doktorsrannsókn miðar að því að þróa heildstæða matsramma fyrir þekkingaráhættu með því að nýta fjölþátta ákvarðanatökulíkön (e. Multi-Criteria Decision-Making, MCDM).

- **Grein I** greinir sjö lykilþekkingaráhættur í samstarfsverkefnum sem styðjast við upplýsingatækni (ICT) með því að nota heildrænt túlkunarbyggingarlíkan (e. Total Interpretive Structural Modelling, TISM). Hún dregur fram netglæpi og njósnir sem drifkrafta og setur fram stigskipt tengsl milli áhættanna, ásamt því að bjóða upp á byggingarlíkan sem auðveldar kerfisbundið KRM.
- **Grein II** metur rekstrarþekkingaráhættur í litlum og meðalstórum fyrirtækjum (SME) með gráskalalíkani fyrir ákvarðanatöku og mat (e. Grey-DEMATEL). Hún greinir 11 mikilvægar áhættur og flokkar þær í orsakaáhættu (t.d. sóun og skort á þekkingu) og afleiðingaáhættu (t.d. tengslaáhættu og njósnir). Úthýsingaráhætta og rangt beiting þekkingar eru sérstaklega mikilvægir þættir sem hjálpa SME-fyrirtækjum að skilja og takast á við eigin veikleika.
- **Grein III** einbeitir sér að drifkröftum leka á þekkingu í samstarfssamningum með samþættu ISM-MICMAC líkani. Hún greinir níu lykildrifkrafta, þar á meðal ófullnægjandi samninga og lárétta samkeppni, sem mikilvæga áhættuþætti. Rannsóknin sýnir hvernig þessir drifkraftar hafa áhrif á leka þekkingar og veitir hagnýtar leiðbeiningar um áhættuminnkun.

Í lokarannsókninni samþættir rannsóknin TISM, DEMATEL og PROMETHEE innan ramma síns. Ramminn var prófaður með tilviksfyrirtæki til að sannreyna hagnýta notkun hans við mat á þekkingaráhættu og stuðning við upplýsta ákvarðanatöku.

Aðferðafræðilega leggur þessi ritgerð sitt af mörkum til fræðilegrar umfjöllunar um KRM, sérstaklega á sviði mats á þekkingaráhættu, með því að kynna vel uppbyggðan og efnilegan ramma:

- TISM er notað til að fanga innbyrðis tengsl milli þekkingaráhættu og áhættuþátta.

- DEMATEL er notað til að vega útvíkkaða mælikvarða og veita dýpri skilning á mikilvægi þeirra.
- PROMETHEE er notað til að forgangsraða áhættuþáttum eftir mikilvægi þeirra.

Þær innsýn sem fást úr þessum ramma veita stjórnendum, áhættustjórum, forstjórum og eigendum fyrirtækja dýrmætar leiðbeiningar til að bera kennsl á, greina og meta fjölbreytta þekkingaráhættu á áhrifaríkan hátt. Þessi ritgerð fyllir ekki aðeins mikilvægt skarð í fræðilegri umfjöllun um KRM, sérstaklega hvað varðar mat á þekkingaráhættu, heldur veitir einnig hagnýtt tæki til að bæta ákvarðanatöku og seiglu skipulagsheilda.

Acknowledgements

Foremost, I wish to extend my deepest gratitude to my esteemed advisor, Professor Susanne Durst. Her unwavering support has fostered my growth, learning, and advancement during the course of my doctoral journey. Her invaluable guidance, motivational words, receptive demeanour, and continuous accessibility have been unparalleled. Not only am I indebted to her for her scholarly mentorship and collaborative efforts, but also for the personal guidance and counsel that have significantly contributed to my development. I extend my heartfelt appreciation for recognising my potential and inspiring me to reach greater heights.

I extend my sincere thanks to my esteemed PhD committee members, namely Professor Ingi Rúnar Eðvarðsson and Professor Michele Borgia, for providing their support and endorsement.

A special acknowledgment is owed to my former academic institution, Tallinn University of Technology, as well as my fellow PhD colleagues within the department.

I am acutely aware of the profound significance of my family throughout this journey. In the absence of my biological parents, who are both regrettably no longer with us, I wish to dedicate this achievement to their memory: Mr. Francis Kofi Foli, who recently passed away this year, and my mother, Mrs. Salomey Yeboah, who departed a decade ago. To my siblings, Eunice Foli, Mercy Foli, and Charles Foli, and Vivian Foli, my heartfelt gratitude knows no bounds. Additionally, my heartfelt thanks go to my aunt, Clara Donkor, and her husband Amos Donkor, along with all my cousins. Finally, my heartfelt appreciation goes to my beloved wife, Mrs. Nadia Annor, and to our expected child, Gwynne-Caoimhe Foli-Annor.

May you all be blessed abundantly.

In loving memory of my late father and mother.

List of author's publications and conference presentations

Articles

Durst, S., **Foli, S.**, La Torre, M., & Borgia, M. (2025). AI-enabled enterprise risk management in cooperative banks - Successful paths to go. *Strategic Change* (Under Review).

Mallarge, J., Durst, S., **Foli, S.**, & Rothenberger, S. (2025). The education trilemma - Time for a reconsideration. *Critical Studies in Education* (Under Review).

Foli, S. (2025). Pathways to green product and service production: Evidence from Estonian SMEs. *Circular Economy and Sustainability* (Under Review).

Timiyo, A. J., & **Foli, S.** (2025). Knowledge leakage through social networks: a review of existing gaps, strategies for mitigating potential risk factors and future research direction. *VINE Journal of Information and Knowledge Management Systems*, *55*(2), 511-532.

Ahmadov, T., Durst, S., Nguyen, Q., **Foli, S.**, & Gerstlberger, W. (2025). Circular Economy Practices in Manufacturing SMEs: Exploration of Stakeholder Pressure, Managerial Perception, and the Mediating Role of Circular Economy Orientation. *Circular Economy*, *3*(1).

Ahmadov, T., **Foli, S.,** Durst, S., & Gerstlberger, W. (2024). The transition to a circular economy: different paths for international and non-international micro-manufacturing firms. *Discover Sustainability*, *5*(1), 178.

Durst, S., **Foli, S**., & Temel, S. (2024). The impact of ethical leadership on KM practices and performance. *Knowledge and Process Management*, *31*(4), 275-283.

Hammoda, B., & **Foli, S.** (2024). A Digital Competence Framework for Learners (DCFL): A Conceptual Framework for Digital Literacy. *Knowledge Management & E-Learning*, *16*(3), 477-500.

Zieba, M., Durst, S., **Foli, S.**, & Gonsiorowska, M. (2024). Hey student, are you sharing your knowledge? A cluster typology of knowledge sharing behaviours among students. *The International Journal of Management Education*, *22*(1), 100924.

Durst, S., **Foli, S.**, & Edvardsson, I. R. (2024). A systematic literature review on knowledge management in SMEs: current trends and future directions. *Management Review Quarterly*, *74*(1), 263-288.

Foli, S., Durst, S., & Domínguez, E. R. (2024). Evaluation of Operational Knowledge Risks in SMEs – Using a Grey-DEMATEL Technique. *Journal of Information and Knowledge Management*.

Durst, S., **Foli, S.**, La Torre, M., & Borgia, M. (2023). Knowledge risk management in banks-An area for improving organizational performance. *Heliyon*, *9*(11).

Durst, S., Edvardsson, I. R., & **Foli, S.** (2023). Knowledge management in SMEs: a follow-up literature review. *Journal of Knowledge Management*, 27(11), 25-58.

Durst, S., Davila, A., **Foli, S.**, Kraus, S., & Cheng, C. F. (2023). Antecedents of technological readiness in times of crises: A comparison between before and during COVID-19. *Technology in Society*, 102195.

Foli, S., Durst, S., & Temel, S. (2022). The link between supply chain risk management and innovation performance in SMEs in turbulent times. *Journal of Entrepreneurship in Emerging Economies*.

Foli, S., Durst, S., Davies, L., & Temel, S. (2022). Supply chain risk management in young and mature SMEs. *Journal of Risk and Financial Management*, *15*(8), 328.

Foli, S., & Durst, S. (2022). Analysing Drivers of Knowledge Leakage in Collaborative Agreements: A Magnetic Processing Case Firm. *Journal of Risk and Financial Management*, *15*(9), 389

Foli, S. (2022). Total interpretive structural modelling (TISM) and MICMAC approach in analysing knowledge risks in ICT-supported collaborative projects. *Vine Journal of Information and Knowledge Management Systems*.

Book chapters and technical paper

Durst, S., & **Foli, S.** (2025). Responsible and Inclusive Knowledge Management Made Concrete. In *Handbook of Inclusive Knowledge Management* (pp. 1-12). Auerbach Publications.

Foli, S. (2024). Unlocking Resource Efficiency: Pathways for Microenterprises in Estonia to Offer Green Products and Services. In *Small and Medium-Sized Enterprise (SME) Resilience - Strategies for Risk and Crisis Management*.

Foli, S. (2024). Discovering the Hidden String Connecting Knowledge Risks and the Digital Entrepreneurial Ecosystem. In *DIGITAL TRANSFORMATION FOR ENTREPRENEURSHIP* (pp. 51-70).

Ellyton, M., **Foli, S**., Hammoda, B., Mallarge, J., Durst, S., & Rothenberger, S. (2022). Inclusive Digital Education Access IDEA: Reference framework for inclusive digital education. *Inclusive Digital Education Access IDEA: Reference framework for inclusive digital education*.

Presentations at academic conferences and seminar

Knowledge hiding in team settings: team dimensions as contingency factors (Talshyn Tokyzhanova, **Samuel Foli** and Susanne Durst), Theory and Applications in the Knowledge Economy (TAKE) Conference "To Think the Unthinkable: The Critical Analysis of Intangibles" June 29-28, 2023, The Sopot University of Applied Science, Sopot, Poland.

The impact of ethical leadership on KM practices and performance (Susanne Durst, Serdal Temel, **Samuel Foli**), International Forum on Knowledge Asset Dynamics (IFKAD) "Managing Knowledge for Sustainability" June 7-9, 2023, The University of Basilicata, Matera, Italy.

Hey KIBS, are you managing your knowledge? Findings from a systematic literature review (**Samuel Foli**, Susanne Durst and Elena Dominguez Romero), Theory and Applications in the Knowledge Economy (TAKE) Conference "The Knowledge Economy and Society in the Post - Covid-19 Era" July 6 – 8, 2022, The Universidade Portucalense, Porto, Portugal

Knowledge hoarding vs. knowledge sharing personalities – towards a classification (Malgorzata Zieba, Susanne Durst, Martyna Gonsiorowska, **Samuel Foli**), 17th International Conference on Knowledge Management 2022 "Knowledge, Uncertainty and Risks: From individual to global scale" June 24-23, 2022, The Potsdam University of Applied Science, Potsdam, Germany

Evaluation of Operational Knowledge Risks in SMEs – using a Grey-Dematel Technique (**Samuel Foli**, Susanne Durst and Elena Dominguez Romero), 17th International Conference on Knowledge Management (ICKM) "Knowledge, Uncertainty and Risks: From individual to global scale" June 24-23, 2022, The Potsdam University of Applied Science, Potsdam, Germany

Enablers of Knowledge Management and Sustainable Business Performance of SMEs: A Synthesis and Review of the Literature (**Samuel Foli** and Jessica Adobi Timiyo), International Forum on Knowledge Asset Dynamics (IFKAD) "Knowledge Drivers for Resilience and Transformation" June 22-20, 2022, The Supsi University, Lugano, Switzerland.

List of studies

This doctoral thesis is based on the following original publications, which are referred to in the text by their Roman numerals (I-III):

I. **Foli, S.** (2022). Total interpretive structural modelling (TISM) and MICMAC approach in analysing knowledge risks in ICT-supported collaborative projects. *Vine Journal of Information and Knowledge Management Systems*, *52*(3), 394-410.

II. **Foli, S.,** Durst, S., & Romero, E. D. (2023). Evaluation of operational knowledge risks in SMEs–Using a Grey-DEMATEL technique. *Journal of Information & Knowledge Management*, *22*(06), 2350071.

III. **Foli, S.**, & Durst, S. (2022). Analysing drivers of knowledge leakage in collaborative agreements: A magnetic processing case firm. *Journal of Risk and Financial Management*, *15*(9), 389.

Declaration of contribution

My contributions to the papers in the thesis are explained in detail as follows:

Article I: I solely authored the paper.

Article II: I took on the role of lead author for the paper. My responsibilities included drafting the introduction and a section of the literature review. I was solely responsible for developing the methodology, conducting the analysis, leading the discussion, and formulating the conclusions. The co-authors contributed their insights to enrich the paper.

Article III: I took on the role of lead author for the paper. My responsibilities included drafting the introduction and a section of the literature review. I was solely responsible for developing the methodology, conducting the analysis, leading the discussion, and formulating the conclusions. The co-author contributed their insights to enrich the paper.

Table of contents

List of tables

List of figures

List of abbreviations

DEMATEL	Decision-Making Trial and Evaluation Laboratory
ISM	Interpretive Structural Modelling
KM	Knowledge Management
KRM	Knowledge Risk Management
KRA	Knowledge Risk Assessment
MCDM	Multiple-Criteria Decision-Making
PROMETHEE	Preference Ranking Organisation Method for Enrichment Evaluations
SLR	Systematic Literature Review
TISM	Total Interpretive Structural Modelling
WoS	Web of Science

1. Introduction

The significance of knowledge has been consistently emphasised, particularly in today's economy. This emphasis is supported not only by scientific research (e.g., Grant, 1996; Spender, 1996; Ho, 2009; Massingham and Massingham, 2014) but also by several reports[1][2] from reputable consultancy firms. It is widely acknowledged that knowledge holds intrinsic value as an asset (Grant, 1996), playing a pivotal role in enabling organisations to achieve positive results (Grant, 1996; Kogut and Zander, 1992), including heightened innovation (Migdadi, 2022), improved productivity and efficiency (Torabi and El-Den, 2017), enhanced agility (Pereira et al., 2019), continuous development (Waddell and Stewart, 2008), and a competitive edge (Rehman et al., 2022).

However, the traditional view of knowledge as entirely positive has evolved (Massingham, 2010; Brunold and Durst, 2012), with a growing realisation that (mismanaged) knowledge can present significant risks, recognised as knowledge risks (Durst and Zieba, 2019; Durst, 2013). These risks, often associated with intangibles or intellectual capital (Durst, 2013; Brunold and Durst, 2012), are primarily examined within the field of strategic management, the domain where this thesis is positioned, though some insights also emerge from information systems research (Jennex and Durcikova, 2013; Marabelli and Newell, 2012; Trkman and Desouza, 2012).

Knowledge risks are 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 organi[s]ation on any level" (Durst and Zieba, 2019, p. 2). Extant literature has suggested that these risks manifest in various forms, such as knowledge leakage (Ferenhof, 2016; Durst et al., 2015), knowledge loss (Durst and Wilhelm, 2011; Massingham, 2018), knowledge obsolescence (Tsang and Lee, 2018; Lee et al., 2021), unlearning and forgetting (Durst et al., 2020), and reputation damage (Durst and Zieba, 2019), all of which can pose significant threats to organisations.

[1] McKinsey Global Institute Report. (2012). Retrieved from https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-social-economy (Accessed on August 15, 2023)

[2] KPMG. Business Intelligence and Knowledge Management. Retrieved from https://kpmg.com/gr/en/home/services/advisory/management-consulting/it-advisory-services/business-intelligence-knowledge-management.html

Given the potential threats posed by knowledge risks, their management is an important step toward maintaining positive organisational outcomes.

1.1. Problem statement

As understanding of knowledge risks continues to deepen, the need for a dedicated framework to address these risks has become increasingly evident. A study by Durst (2021), for example, found that 24% of organisations involved in risk management incorporate knowledge risks as part of their risk management. This highlights the importance of knowledge risk management (KRM), defined by Durst et al. (2019) as a "systematic way of applying tools and techniques to identify, analy[s]e and respond to risks associated with the creation, application, and retention of organi[s]ational knowledge". While alternative definitions exist, this particular definition is widely recognised and frequently cited, offering a foundation for research and practice in this emerging field.

Despite its growing relevance, research on KRM remains limited, with significant gaps in both risk assessment frameworks and risk assessment tools. A risk assessment framework provides a structure for systematically, identifying, analysing and evaluating knowledge risks (ISO 31000). Conversely, risk assessment tools are practical models or techniques – such as decision trees or risk matrices – used within the framework to perform specific tasks like quantifying, or prioritising these risks (Cox, 2009). While frameworks guide the overall approach to risk assessment, tools execute the specific actions needed to implement that approach.

One of the key gaps is the lack of comprehensive risk assessment frameworks for knowledge risks. Most existing studies have focused on identifying and classifying knowledge risks through taxonomies, but few (e.g., Durst and Ferenhof, 2016; Massingham, 2010) have focused on developing frameworks to guide their systematic assessment. A related gap exists in the availability and suitability of risk assessment tools. Traditional tools, such as decision-tree approaches, often fall short when applied to the intangible and complex nature of knowledge risks. For instance, Massingham (2010) highlighted that such tools are prone to cognitive biases and subjectivity, which undermine their ability to clearly differentiate and prioritise risks.

While some contributions (e.g., Jennex and Durcikova, 2013; Padyab et al., 2015; Thalmann et al., 2014), from the information systems field have introduced tools/models/methodologies for

addressing risks associated with knowledge, these remain fragmented and narrowly focused. For example, Ilvonen et al. (2015) developed a model helps to identify knowledge security risks and provides a comprehensive approach to evaluating and balancing the costs and benefits of knowledge sharing and knowledge risk management. Many of these studies primarily emphasise IT systems, which do not inherently represent knowledge itself. Furthermore, they often rely solely on conventional criteria such as impact and frequency, which limits their ability to address the complex and interconnected nature of knowledge risks (Durst and Zieba, 2019).

The implications of these gaps are significant. Without comprehensive frameworks, organisations lack a clear structure for systematically understanding and assessing knowledge risks. This leaves them vulnerable to knowledge loss, leakage, and obsolescence, which can disrupt operations, erode competitiveness (Durst et al., 2019), and hinder long-term sustainability (El Khatib and Abbas, 2023, 2023). Meanwhile, the inadequacy of tools hampers decision-makers' ability to better assess and prioritise risks, leading to inefficiencies in resource allocation and an inability to implement targeted mitigation strategies.

1.2. Research aim, and questions

Against this backdrop, this PhD research aims to develop a comprehensive risk assessment framework for knowledge risks, integrating suitable risk assessment tools into its structure. To achieve this aim, the research is structured around three research questions, as follows:

RQ1. What are the components required to develop a comprehensive framework for the assessment of knowledge risks in organisations?

RQ2. How can improved risk assessment tools be integrated into the framework to address the complex nature of knowledge risks?

RQ3. How does the proposed knowledge risk assessment framework, when applied in an organisational setting, improve the identification, analysis, and evaluation of knowledge risks?

1.3. Connection between aim, research questions and studies

This thesis comprises three articles along with a complementary study. *Article I*, *Article II* and *Article II* address *RQ1*, while the complementary study (see Chapter 5) focuses on *RQ2* and *RQ3*.

The research questions are aligned with the research aim. *RQ1* explores the components necessary for developing the framework by applying and evaluating potential risk assessment tools independently. This evaluation identifies the strengths and weaknesses of the tools, ensuring their suitability for assessing knowledge risks. *RQ2* builds upon this foundation by integrating the selected tools into a unified framework, ensuring clear functionality and interoperability among its components. *RQ3* evaluates the framework's practical application, focusing on its effectiveness in real-world settings for identifying, analysing, and prioritising knowledge risks. Together, these research questions form a comprehensive approach to achieving the thesis's research aim.

Articles I, *II*, and *III* provide insights into *RQ1* by exploring various tools that can serve as components of the proposed framework. In *Article I*, Total Interpretive Structural Modelling (TISM) is applied to assess knowledge risks in ICT-collaborative projects, demonstrating its utility as an assessment tool. *Article II* uses Grey-DEMATEL to evaluate knowledge risks at the operational level in SMEs, highlighting its potential in understanding the relationships among risks. *Article III* applies Interpretive Structural Modelling (ISM) to identify and assess knowledge leakage risk factors in a magnetic case company, further contributing to the pool of assessment tools. These tools are examined for their potential integration into the framework, establishing their roles in addressing specific dimensions of knowledge risks.

The complementary study (**detailed in Chapter 5**) addresses *RQ2* and *RQ3* by integrating the models – TISM, DEMATEL, and PROMETHEE – into a unified framework. The integrated framework is then tested through a case study, assessing its practical applicability in a real-world organisational setting.

The connections between the aim of this thesis, the research questions, and the studies conducted is presented in **Figure 1**

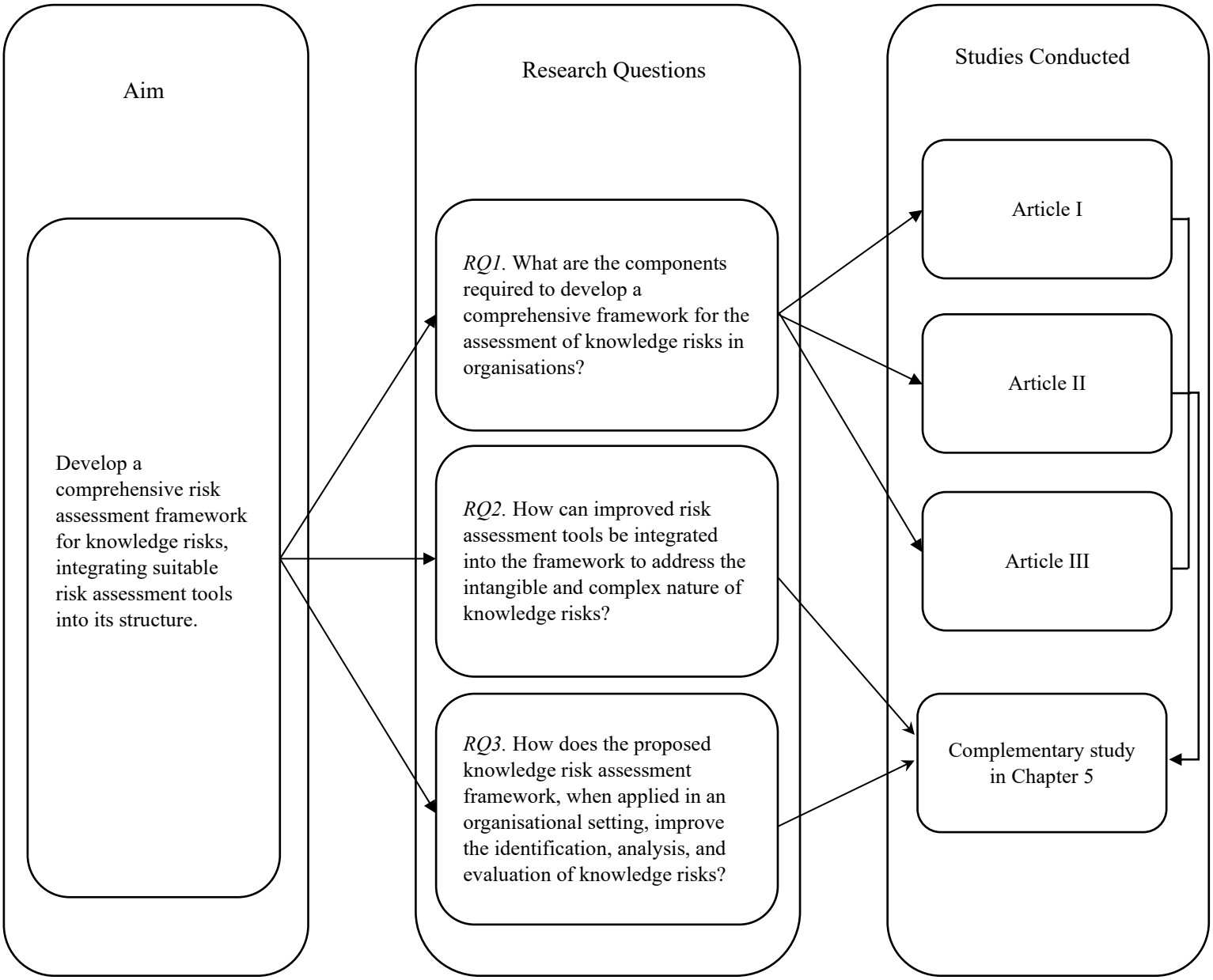


Figure 1 Connections between the aim of this thesis, the research questions, and the studies conducted

1.4. Contribution of the thesis

This thesis makes a **methodological contribution** to the field of knowledge risk management by developing a comprehensive risk assessment framework specifically designed to address knowledge risks. The framework integrates multiple risk assessment tools –TISM, DEMATEL, and PROMETHEE – each selected for their ability to address distinct aspects of knowledge risks, such as their interrelated nature and prioritisation challenges. DEMATEL facilitates the precise weighting of risk parameters, TISM identifies the driving and dependency power of risk factors, and PROMETHEE supports the ranking and prioritisation of risks based on multiple criteria. By unifying these tools into a cohesive structure, the framework offers a novel and systematic approach to identifying, analysing, and prioritising knowledge risks within an organisational setting.

In addition, the thesis contributes to the KRM literature by demonstrating the applicability of these tools through empirical studies. *Article I* applies TISM to assess knowledge risks in ICT-collaborative projects, *Article II* employs Grey-DEMATEL for operational-level risks in SMEs, and *Article III* uses ISM to evaluate knowledge leakage risks in a magnetic case company. These studies not only validate the individual tools but also highlight their potential as components of an integrated framework. Furthermore, this thesis contributes to the (knowledge) risk assessment tools literature by extending traditional risk assessment frameworks, which have predominantly focused on the probability of occurrence and severity of consequences. The proposed framework introduces additional dimensions – driving power and dependency power – by integrating variable weighting to these parameters. This framework allows for a more nuanced analysis of knowledge risk factors, capturing their interdependencies and enabling a deeper understanding of how these risk factors interact, influencing and being influenced by other risk factors.

The methodology developed in this thesis carries **practical contributions** as it provides a comprehensive flow chart for the application of the methodology, offering a useful tool for risk managers. The modelling approaches employed in this research hold practical value due to the inclusion of guidelines (in a form of steps), that could potentially be adapted and applied in various industry settings. The thesis also provides practitioners with a deeper understanding of the nature of knowledge risks and their threats or risk factors, including their drivers and dependencies. This information is valuable for practitioners in making informed decisions when dealing with these

risks. Managers within organisations should acknowledge that they can manage knowledge risks by anticipating their occurrence and implementing measures to mitigate their impact.

1.5. A guide to the remainder of this thesis

The doctoral thesis is organised as follows:

After the introduction **(Chapter 1)**, **Chapter 2** defines key concepts, presents the theoretical foundation of the PhD thesis, and details the systematic literature review (SLR) on knowledge risk management (KRM) research, which helps define the main focus of the PhD research. **Chapter 3** is dedicated to the research methodology, focusing on the research philosophy and research approaches employed in each of the articles (*Article I*, *Article II*, and *Article III*) as well as the complementary study. This chapter provides a detailed explanation of the chosen research methods, including the rationale behind their selection and their application in the respective studies. **Chapter 4** encompasses the three articles. **Chapter 5** presents the development and validation of the knowledge risk assessment framework (complementary study). Finally, **Chapter 6** presents the discussion and concludes with a summary of the contributions, limitations, and suggestions for future research.

2. Literature review

This chapter begins by defining several key concepts that may be understood differently in various contexts, providing clear definitions to ensure consistency throughout the thesis. It then explores the concept of knowledge risk management (KRM), reviews existing risk management (RM) frameworks for their relevance to knowledge-specific risks, and assesses their suitability in addressing challenges of managing knowledge as a critical asset. The theoretical foundation of the PhD thesis is presented to establish a basis for the research and its contribution to the field. Following this, a systematic literature review (SLR) is conducted. The SLR presents descriptive findings from the literature, including publication years, research methodologies used, and theoretical approaches. The main findings are presented, and gaps in the literature are identified and presented. Based on these identified gaps, the review informs an evaluation of multi-criteria decision-making (MCDM) models and makes a case for selected models as suitable tools for assessing knowledge risks.

2.1. Definition of key concepts

To better understand KRM, it is important to examine some key concepts that are central to this field of study. These include knowledge, risk, threat, knowledge risk, and KRM. These concepts are discussed below, drawing on insights from the research contributions of various scholars in KRM to provide a foundation for understanding KRM.

2.1.1. Knowledge

Knowledge is a key organisational asset, and many researchers have explored through several ideologies and perspectives, bringing unique understanding into how it creates and sustains organisational success. Walsh and Ungson (1991) view organisational knowledge as more than just information; it includes the skills, practices, and experiences that are ingrained in a company's culture and structure. Knowledge does not only include data but also assets such as insights and experiences essential for informed decision-making and skill-building for groups and individuals

as emphasised by Nonaka and Takeuchi (1995). Grant (1996) builds on this as he linked knowledge to the creation of innovation and value, emphasising its role in enhancing an organisation's core competencies. Spender (1996) contributes by highlighting knowledge as an adaptive element that evolves as it flows through the organisation. Davenport and Prusak (1998) take a practical approach in explaining knowledge as a key driver of efficiency and innovation, with the potential to transform the operational processes and bring about creativity within the organisation. Together with other perspectives, this highlights knowledge as both flexible and deeply embedded in the way an organisation function. It shapes decisions, encourages ongoing learning, and helps maintain a competitive edge.

In this thesis, knowledge is defined as contextual information held by a knowledge worker. It is personalised and includes facts, procedures, concepts, interpretations, ideas, observations, and judgements, which are then formalised into artefacts such as documentation, processes, and guidelines within organisations (Alavi and Leidner, 1999; Nonaka and Toyama, 2003). This definition aligns with the broader understanding of knowledge as both tacit and explicit (Polanyi, 1966). Tacit knowledge, deeply embedded in individual expertise and experience, is often difficult to articulate but essential for decision-making and innovation (Nonaka and Toyama, 2003). Explicit knowledge, on the other hand, can be codified and shared, enabling organisations to preserve and transfer valuable insights across teams and functions (Ibid). The process of formalising knowledge into artefacts ensures that it becomes accessible and actionable, supporting organisational learning and resilience. By defining knowledge as contextual and personalised, this thesis emphasises its dynamic and multifaceted nature. Knowledge is not merely static information but a living resource that evolves through interaction, application, and refinement. This definition is particularly relevant to the study of KRM, as it highlights the risks associated with knowledge as both an individual and organisational asset.

2.1.2. Risk

There are many different definitions of risk depending on the field, discipline, and professional association. The uncertainty surrounding the results of financial investments is considered risk in economics (Knight, 1921). The combination of the likelihood of a failure event and its effects is

referred to as risk in engineering[3]. Risk is the term used in environmental science to describe the possible negative impacts that environmental hazards may have on people or ecosystems (Kent and Allen, 2014). The possibility of loss or harm that is transferred through a policy agreement is referred to as risk in the insurance industry (ISO 31000, 2018). Expert organisations such as ISO define risk as the "effect of uncertainty on objectives," which includes both positive and negative deviations (ISO 31000, 2018). The perceived likelihood of a negative event, influenced by subjective judgement and cognitive biases, is a common definition of risk in psychology (Slovic, 1987). These differing definitions show how risk is complicated in relation to safety, planning, and decision-making in various contexts.

Some scholars including Coskun et al (2019) defined risk from the perspective of uncertainty as the level of uncertainty in achieving objectives, where unpredictable factors could impact performance and decision-making. By defining risk as exposure to possible loss that could adversely affect an organisation's assets, reputation, or financial position as a result of a combination of internal and external factors, the Committee of Sponsoring Organizations of the Treadway Commission (COSO)[4] expands on this definition. In support of this viewpoint, ISACA[5] defines risk as "the likelihood of an adverse event combined with the impact it would have on the organisation," highlighting the significance of evaluating the likelihood of adverse events as well as their potential impact on strategic goals. The idea is further developed in ISO 31000, which frames risk as a variable that, depending on how it is managed, can have both beneficial and detrimental effects on organisational goals. In organisational contexts, risk includes both opportunities and threats, as this definition emphasises. For the purpose of this thesis, risk is defined as the probability of an undesired or negative event occurring, along with the consequences or impacts that may result.

[3] IEC 62198 Revised IEC 62198:2001. Retrieved from https://webstore.iec.ch/en/publication/20350 (Accessed on December 31, 2024).
[4] COSO ERM 2017. Retrieved from https://commsrisk.com/new-cosoerm-framework-out-for-comment (Accessed on December 1, 2024).
[5] ISACA. Retrieved from https://www.isaca.org/-/media/files/isacadp/project/isaca/why-isaca/annual-report/annual-report-2023.pdf (Accessed on December 1, 2024).

2.1.3. Threat

Threat represents specific sources of potential harm that can exploit vulnerabilities within an organisation's systems, processes, or assets (Aven, 2011). Threats are more than just general risks; they are identifiable, tangible challenges that can directly undermine an organisation's security, integrity, and operational continuity (Boehm, 1991). Various scholars and frameworks have approached the concept of threat from different perspectives, enriching our understanding of how to effectively manage and mitigate these dangers.

Dubois et al. (2010) define threat as any circumstance or event with the potential to cause harm by exploiting vulnerabilities. This definition emphasises the importance of not only identifying potential threats but also understanding the vulnerabilities they might exploit. The National Institute of Standards and Technology (NIST) further elaborates on this by categorising threats into key areas such as environmental, operational, and technical threats. NIST's framework highlights the need for organisations to systematically address these threats through structured risk management practices, ensuring that each category is considered in its unique context.

Sommestad (2012), in the area of cybersecurity, emphasises the role of threat modelling, a process that involves identifying potential threats, understanding how they might exploit system vulnerabilities, and prioritising them based on their potential impact and likelihood. This approach has become essential in modern cybersecurity practices, where the complexity and interconnectivity of systems increase the potential for various types of threats (Ibid)

Threat and risk are related but different ideas, especially in management, security, and organisational contexts. Generally speaking, a threat is an occurrence or situation that has the potential to be harmful, whereas risk is the possibility and consequence of the threat occurring, frequently impacted by mitigating factors and vulnerabilities already in place (Aven, 2011). The two terms are similar in that they are linked to uncertainty and the possibility of negative consequences. A cyberattack, for example, is a threat, and the likelihood that it will happen as well as the extent of its effects make up the risk. They are essential to risk management decision-making processes since determining threats frequently forms the basis for evaluating risk (ISO 31000, 2018).

They vary, though, in their focus and scope. Threats are circumstances, whether internal or external, that have the capacity to be harmful but do not necessarily take probability or repercussions into account. On the other hand, risk is by definition a probabilistic evaluation of these results (Kaplan and Garrick, 1981). For instance, although an earthquake is a threat, risk assessment considers both the possibility of the event happening in a specific area and the resulting damages. Furthermore, risks cover more ground than threats, such as the general vulnerability of an IT infrastructure, while threats are more focused, such as a specific malware targeting systems. Knowing these differences helps organisations to conduct more accurate risk assessments, emphasising both threat identification and successful risk mitigation. In this thesis, threats will be regarded as risk factors – elements that influence the likelihood and impact of a risk occurring. These risk factors form the foundation for assessing risks and serve as a guide for developing and implementing mitigation measures.

2.1.4. Knowledge risk

The concept of knowledge risk (KR) has evolved significantly over time. In the study by Brunold and Durst (2012), these risks were initially referred to as intellectual capital (IC) risks, highlighting their broader scope within the domain of intangible assets. Early definitions were put forth to describe knowledge risks, however, these definitions did not appear to be comprehensive. This is not surprising given the novelty of the concept and the evolving understanding of it at the time. One such definition was proposed by Bayer and Maier (2006), who defined knowledge risk as an operational risk arising from reliance on, loss of, or unsuccessful or accidental knowledge transfer.

Another definition was presented by Perrott (2007), who characterised knowledge risk as the likelihood of any loss resulting from the identification, storage, or protection of knowledge, which could diminish the operational or strategic benefits of a company. While Perrott's definition acknowledged that knowledge risks can also impact strategic levels within an organisation, it did not fully recognise the severity of these risks at all organisational levels. In response to this limitation, Durst and Zieba (2019) proposed an alternative definition for knowledge risk. According to the authors (2019), knowledge risk can be defined as "a 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 organi[s]ation on any level" (p. 2). This definition is particularly relevant as it captures the likelihood and impact of negative effects across various organisational contexts while incorporating both operational and strategic dimensions. This thesis adopts Durst and Zieba's (2019) definition because it aligns with the objective of understanding and assessing knowledge risks comprehensively. Furthermore, it resonates with the thesis's perspective of viewing knowledge risks primarily as negative factors that threaten organisational functioning.

Organisational perspectives on knowledge risk highlight its role in safeguarding intellectual property, maintaining operational continuity, and sustaining competitive advantage. Massingham (2010) emphasises the operational risks of knowledge loss, particularly through employee turnover and inadequate knowledge transfer practices. Durst and Zieba (2017) highlight the strategic risks associated with mismanaging knowledge, which can undermine an organisation's ability to sustain competitive continuity. Bayer and Maier (2006) extend the discussion to inter-organisational risks, such as knowledge spillover in collaborative settings, while Teece (2000) stresses the importance of protecting proprietary knowledge to sustain innovation and market leadership. Despite their varied focuses, these perspectives collectively emphasise the need for careful management of knowledge as an intangible yet critical organisational asset.

Scholars have identified several specific types of knowledge risks, including knowledge loss (Durst and Wilhelm, 2012), knowledge leakage (Manhart and Thalmann, 2015), knowledge hoarding (Connelly et al., 2012), knowledge obsolescence (Massingham, 2014), ineffective knowledge transfer (Inkpen and Tsang, 2005), and restricted knowledge access (Disterer, 2001). Additional risks include cybersecurity threats (Von Solms and van Niekerk, 2013), knowledge misinterpretation (Crossan and Apaydin, 2010), dependence on external knowledge sources, and cultural resistance to knowledge sharing (McDermott and O'Dell, 2001). Acknowledging the potential negative consequences of these knowledge risks emphasises the importance of actively managing knowledge risk. This is where the concept of KRM comes into play.

2.2. Knowledge risk management (KRM)

Knowledge risk management (KRM) has been defined by several scholars, including Neef (2005), Massingham (2010), Coleman and Casselman (2016), Durst and Zieba (2017), and so forth, with different viewpoints regarding the protection of organisational knowledge. Starting from the earliest contributions, in Neef's (2005) view of KRM, it combines knowledge management and risk management strategies to control complexity and uncertainty. Neef highlights the necessity of an all-encompassing framework that reflects the interdisciplinary nature of KRM and manages knowledge risks similarly to other operational risks. Building on the foundation laid by Neef, Massingham (2010) views KRM as a crucial prerequisite for safeguarding an organisation's knowledge assets to maintain stability. Coleman and Casselman (2016) conceptualise KRM as an integral approach for optimising strategic decisions by managing the trade-offs between knowledge accumulation and risk. They propose that KRM involves aligning a firm's knowledge resources to mitigate risks while enhancing performance outcomes.

KRM is highlighted by Durst and Zieba (2017) as a component of a larger risk management strategy, identifying risks that can impair competitiveness such as knowledge leaks and expertise loss. Their perspective emphasises the dynamic relationship between organisational resilience and knowledge retention, demonstrating a proactive approach to managing KRM through preventative measures. Durst et al. (2019) further define KRM as "systematic way of applying tools and techniques to identify, analy[s]e and respond to risks associated with the creation, application, and retention of organi[s]ational knowledge" (p. 3). They outline a structured framework for implementing KRM, consisting of four key stages: (1) identification of risks, (2) quantification and/or evaluation of risks, (3) management and control of risks, and (4) continued reporting on the development of risks. This framework is illustrated in **Figure 2**.

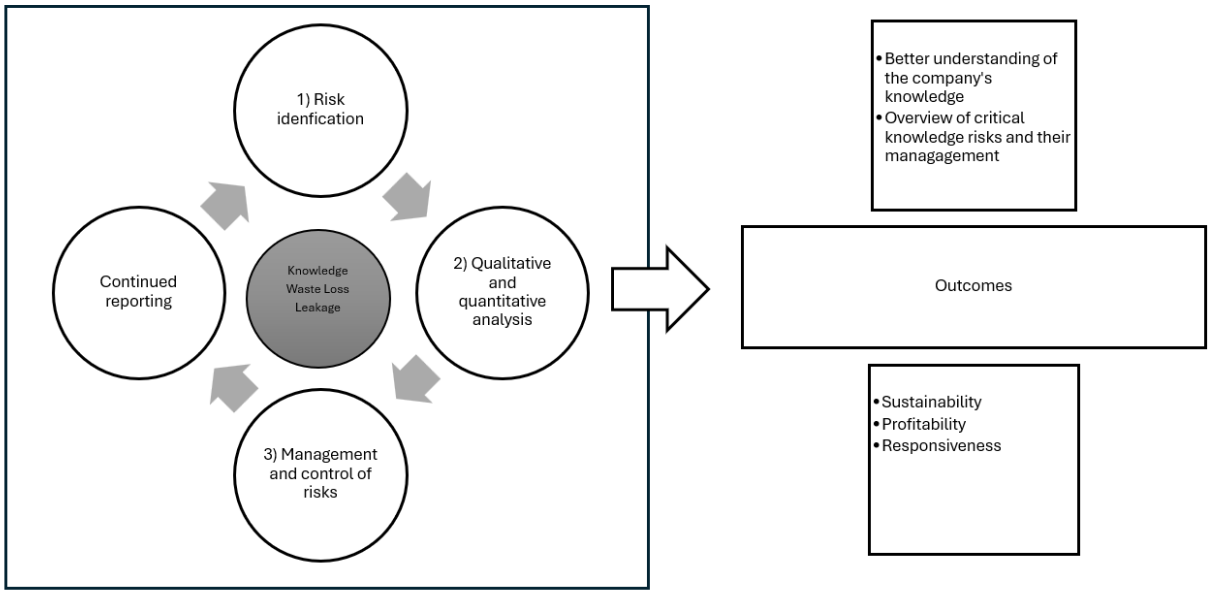


Figure 2 Framework for knowledge risk management in SMEs (Durst and Ferenhof, 2016, p. 202)

2.3. Risk management

A key component of attaining strategic goals and ensuring organisational resilience is risk management (Engemann and Henderson, 2014; Leflar and Siegel, 2013). According to Hillson (2016), it entails the systematic identification, evaluation, and mitigation of risks to reduce the possible effects they may have on operations, finances, compliance, and reputation. This process revolves around the development of frameworks – or standards, as these terms are often used interchangeably – that offer organised approaches to risk management, allowing organisations to incorporate risk management into governance and decision-making procedures (Aven, 2016).

Prominent frameworks, like the Risk Management Framework (RMF) from the National Institute of Standards and Technology (NIST) and ISO 31000 from the International Organisation for Standardisation, provide guidelines that are applicable in a variety of organisational contexts and industries (ISO:31000, 2018; Ross et al., 2010). According to Disterer (2013), these standards promote a proactive risk-aware culture by placing an emphasis on ongoing monitoring, stakeholder involvement, and the alignment of risk practices with organisational strategies. Adopting such frameworks can improve an organisation's ability to foresee, address, and recover from new

challenges (Power, 2004). This review will compare these frameworks along with others to evaluate their strengths and weaknesses in the context of assessing knowledge risks.

2.3.1. ISO 31000:2018 - risk management — Guidelines

ISO 31000:2018, "Risk Management – Guidelines," an international standard that provides a flexible and a high-level approach to risk management enables organisations in a variety of domains to address risk in accordance with their unique operational contexts and objectives. ISO 31000:2018 is useful for a variety of organisational types and industries because it offers a flexible framework for understanding, evaluating, and responding to risks. For example, ISO 31000 has been successfully applied in sectors such as healthcare, finance, manufacturing, and government services (Aven, 2011), demonstrating its use in both specialised and diverse industries. This standard emphasises the value of clear communication, leadership, and accountability in fostering a culture of risk awareness, which is essential for proactive risk management.

The ISO 31000:2018 framework follows the typical risk management process, as shown in **Figure 3**.

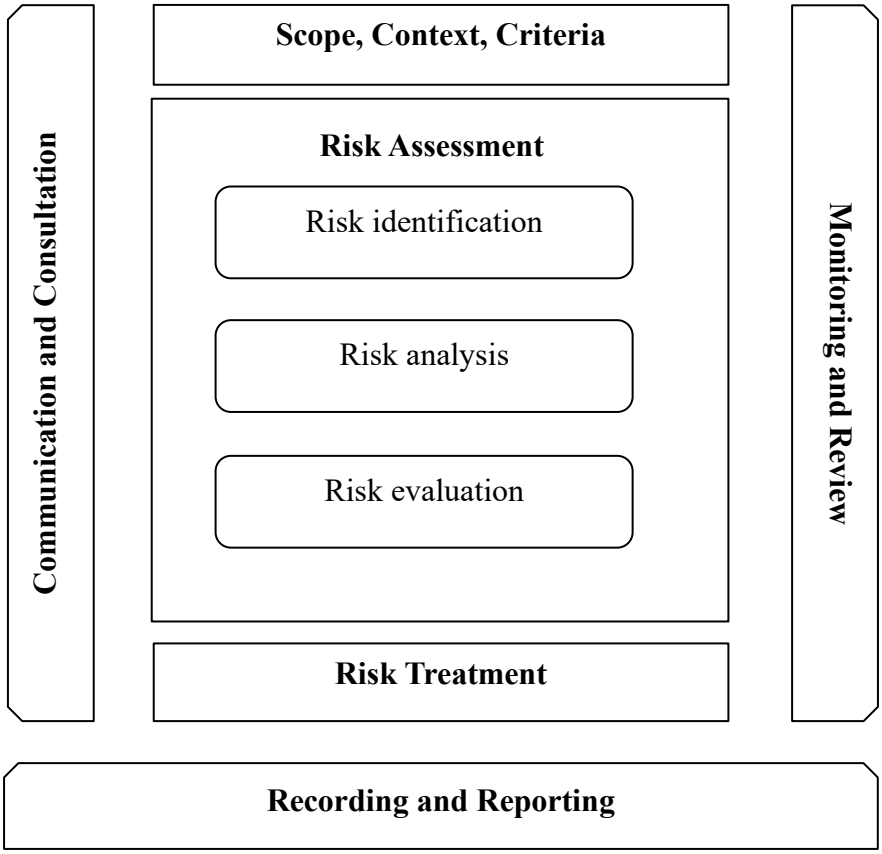


Figure 3 ISO 31000:2018

This framework aligns risk management practices with organisational governance and decision-making processes (ISO 31000, 2018), promoting a holistic risk management process. A notable strength of this framework is its integration into the organisation's broader strategies, ensuring risk management becomes an intrinsic component of decision-making and long-term planning (Ibid). This integration can help organisations anticipate and respond to potential risks, thereby enhancing resilience, particularly in volatile or rapidly changing environments.

Additionally, ISO 31000:2018's flexibility in risk treatment and controls allows organisations to customise their risk management practices (Hutchins, 2018). This adaptability is important as it enables organisations to adjust their risk management processes based on evolving risks or operational changes. Research (e.g., Sotamaa et al., 2024; Sodhi et al., 2012) indicates that organisations implementing ISO 31000:2018 benefit from improved agility, resilience, and decision quality, with studies showing enhanced risk-adjusted outcomes and stronger organisational resilience as a result of adherence to the standard.

2.3.2. The NIST risk management framework (RMF)

The risk management framework (RMF), developed by the National Institute of Standards and Technology (NIST), is a method for combining risk management and cybersecurity procedures in federal information systems (Ross and Johnson, 2010). The RMF, which was first presented in NIST Special Publication (SP) 800-37, integrates security measures and stresses ongoing monitoring at every stage of the system development life cycle (Ross, 2014). Security controls, implementing security controls, assessing security controls, authorising systems, and monitoring security controls are the six essential steps that make up this framework (See **Figure 4**). When combined, these actions give businesses a framework to handle cybersecurity threats in accordance with their individual risk tolerance levels, improving resilience and ensuring compliance with federal regulations (Ross and Johnson, 2010).

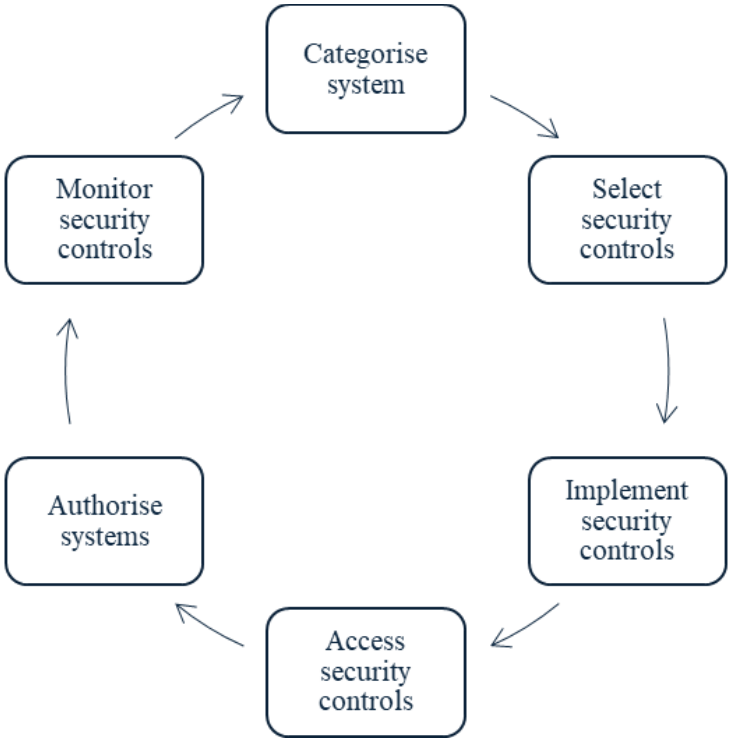


Figure 4 NIST Special Publication 800-37 Revision I (p. 8)[6]

[6] NIST Special Publication 800-37 Revision I. Retrieved from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-37r1.pdf (Accessed on December 13, 2024)

The RMF's versatility is one of its main advantages. It is appropriate for a wide range of entities due to its adaptability, which enables customisation to match different organisational needs and risk profiles. Research indicates that by incorporating risk management into core organisational procedures, the RMF promotes a proactive security culture. In addition, the RMF is in line with international security standards like ISO/IEC 27001, which makes it easier for it to be adopted globally (Disterer, 2013). Notwithstanding the fact that the RMF's methodical approach is beneficial for large businesses, small businesses with little funding may find it difficult to implement.

Focusing primarily on IT security, the RMF emphasises the importance of continuous risk assessment, a critical component in modern environments where cybersecurity risks are dynamic and constantly changing. The RMF process systematically protects organisational information systems by categorising them based on potential impact, selecting and implementing appropriate security controls, and assessing their effectiveness. It further ensures continuous protection through system authorisation and ongoing monitoring, adapting controls as needed to address evolving threats.

RMF provides a systematic approach to integrate security and privacy into organisational operations. This framework emphasises the importance of embedding security considerations at each stage of an organisation’s processes, creating a holistic approach to risk management that is both scalable and adaptable across industries and organisational types.

2.3.3. Other risk management frameworks

2.3.3.1. ISO 30401: Knowledge management systems standard

ISO 30401:2018, titled "Knowledge Management Systems – Requirements," provides a structured framework for organisations to effectively manage their knowledge resources. According to ISO 30401 (2018) “the organi[s]ation shall establish, implement, maintain and continually improve a knowledge management system, including the strategy, processes needed and their interactions, in accordance with the requirements of this international standard” (p. 6). It is applicable to organisations, regard less of its type or size, aiming to enhance their ability to create, capture, and

utilise knowledge for sustained value creation (ISO 30401, 2018). This standard aligns with the principles of strategic and systematic knowledge management (KM) to support improved decision-making, innovation, and efficiency (ISO 30401, 2018).

The ISO 30401 standard emphasises the integration of KM with an organisation's strategic goals. It outlines requirements for establishing, implementing, maintaining, and continually improving a KM system that facilitates knowledge sharing and retention across all levels of the organisation. ISO 30401 is not prescriptive but adaptable, enabling organisations to tailor its guidelines to their specific needs and contexts (ISO 30401, 2018).

According to ISO 30401 (2018), key elements of the framework include understanding the context of the organisation, ensuring leadership and commitment, defining KM-related policies, and providing appropriate support through resources and training. It encourages planning that identifies risks and opportunities, as well as implementing operational processes to foster knowledge-sharing practices. Regular performance evaluation and continual improvement are integral to sustaining the effectiveness of a KM system.

The implementation of ISO 30401 involves conducting a gap analysis to assess current KM practices against the standard's requirements. Securing top management commitment is critical for successful adoption, as is the establishment of a KM team responsible for overseeing the system's development and operation (Ibid). Organisations are encouraged to provide comprehensive training and adequate tools for employees to engage with KM processes effectively. The framework also highlights the importance of monitoring and evaluating KM initiatives to identify areas for enhancement and ensure alignment with organisational objectives (Ibid).

2.3.3.2. BSI standard 200-2

The BSI-Standard 200-2 ('IT-Grundschutz Methodology') provides a methodology for managing information security that can be tailored to the needs of organisations of all sizes. Its foundation is ISO 27001, which is based on BSI-Standard 200-1, "Management systems for information security (ISMS)". It contains instructions and guidelines for establishing a thorough foundation for risk analysis, confirming the current security level, and implementing a suitable level of information security. The three methodologies—"Standard Protection," "Basic Protection," and "Core

Protection"—included in BSI-Standard 200-2 are designed to help organisations attain and sustain a suitable degree of information security. The "Standard Protection" approach makes it possible to achieve a level of security for the business processes that are being considered that is suitable for safeguarding information related to the business and sufficient for meeting the requirements for regular protection. Although the "Basic Protection" approach offers a security level that is much lower than Standard Protection, it gives organisations a solid foundation on which to start implementing an information security management procedure. Lastly, when specific protection is needed for business processes and information, the "Core Protection" approach can be used.

2.3.3.3. Octave-S

The OCTAVE Method (Operationally Critical Threat, Asset, and Vulnerability Evaluation) (Alberts, et al., 1999) was developed at the Software Engineering Institute in 1999. It has been revised since then, and several iterations have been released. It uses a strategic, asset-based approach to evaluate information security risk, which can be implemented in big, hierarchical organisations. The OC-TAVE-S (Alberts, et al., 2005) is based on the OCTAVE approach and is a self-directed approach, meaning that people from an organisation assume responsibility for setting the organisation's security strategy. A small, interdisciplinary team of three to five people can lead Octave-S, which is designed to meet the limited resources and constraints typically found in small organisations (less than 100 people). The team gathers and analyses information to create a protection strategy and mitigation plans based on the specific operational security risks of the organisation. The team needs to be well-versed in the organisation's business and security procedures to carry out OCTAVE-S efficiently and independently.

Table 1 presents a concise summary of the strengths and weaknesses of the reviewed frameworks.

Table 1 Summary of the reviewed risk management frameworks

Framework	Strengths	Weaknesses
NIST RMF	- Comprehensive, integrates cybersecurity and risk management at every lifecycle stage.	- Resource-intensive, challenging for small organisations.

	- Highly adaptable, scalable for different organisational needs. - Aligns with international standards like ISO/IEC 27001 for global applicability. - Promotes a proactive security culture through continuous monitoring.	- IT-focused, less applicable to non-IT knowledge risks. - Complex, multi-step process may be time-consuming.
ISO 31000:2018	- Flexible, adaptable to diverse industries and contexts. - Embeds risk management into organisational governance and decision-making. - Focuses on stakeholder engagement, effective communication, and continuous improvement. - Enhances resilience and agility in volatile environments.	- High-level framework, less prescriptive for detailed implementation. - Requires strong leadership and accountability, which may vary in practice. - May lack specific technical controls compared to IT-centric frameworks.
ISO 30401	- Aligns knowledge management with organisational strategic goals. - Flexible and adaptable to various organisational contexts and industries. - Helps mitigate risks associated with knowledge loss, turnover, and duplication.	- Lacks explicit focus on knowledge risk assessment, leaving organisations without a structured way to identify and analyse these risks. - Does not provide quantitative tools for measuring and comparing the severity of risks, reducing decision-making precision. - Fails to emphasise interdependencies between knowledge risks, limiting its ability to address how one risk may trigger others.
BSI Standard 200-2	- Tailored methodologies ("Standard", "Basic", "Core Protection") for different security needs. - Provides a structured foundation for risk analysis and security implementation.	- May be overly complex for organisations without prior ISMS experience. - Focused heavily on information security, less applicable to other knowledge risk areas.
OCTAVE-S	- Suitable for small organisations with limited resources. - Strategic, asset-based approach tailored to specific operational risks. - Promotes self-directed implementation, reducing dependency on external consultants.	- Relies on internal expertise, which may be limited in small teams. - May not scale well for larger, more complex organisations. - Limited guidance for integrating with broader organisational governance frameworks.

The table highlights key strengths and weaknesses of widely recognised risk management frameworks, providing insights into their applicability for knowledge risk management (KRM).

The NIST RMF, for example, is comprehensive and integrates cybersecurity with risk management at every lifecycle stage, making it well-suited for IT-related risks. However, its resource-intensive nature and IT-centric focus may limit its use in addressing non-IT knowledge risks, such as knowledge loss or leakage. Similarly, ISO 31000:2018 provides a flexible, high-level approach adaptable to various industries, but its lack of prescriptive guidance for detailed implementation leaves gaps in addressing the nuances of knowledge risks, such as interdependencies that exist among these risks.

The ISO 30401 framework aligns knowledge management with strategic goals, making it relevant for managing knowledge-related challenges like loss or duplication. However, it lacks an explicit focus on assessing and quantifying knowledge risks, offering no structured approach to identify, measure, or prioritise these risks. This gap is particularly significant for organisations needing precise, actionable insights to mitigate the effects of these risks. Similarly, the BSI Standard 200-2 and OCTAVE-S frameworks, while providing tailored or simplified methodologies, tend to focus heavily on information security, leaving broader knowledge risks unaddressed.

In summary, none of these frameworks comprehensively address the assessment of knowledge risks in a structured, quantifiable, and interconnected manner. This gap reinforces the need for a dedicated framework that integrates the strengths of existing frameworks while addressing their limitations.

2.4. Theoretical foundation

This section discusses the theoretical foundation underpinning this thesis.

2.4.1. Knowledge management perspective

This doctoral thesis is grounded in the field of Knowledge Management (KM), a discipline that focuses on the systematic processes through which knowledge is created, shared, retained, and utilised within organisations (Alavi, 2001). The KM perspective views knowledge as a critical organisational resource that drives value creation, supports innovation, and contributes to sustained competitive advantage (Grant, 1996). It places emphasis on the dynamic and iterative processes involved in managing knowledge effectively to address both opportunities and challenges within organisations (Easterby-Smith and Prieto, 2008).

In modern organisations, intangible resources such as skills, expertise, and organisational knowledge have become increasingly significant compared to tangible assets[7]. KM perspective posits that the success of organisations is contingent upon their ability to manage these knowledge resources strategically (Gold, 2001). It emphasises that the effective management of knowledge involves not only capturing and codifying explicit knowledge but also nurturing tacit knowledge embedded within individuals and teams (Nonaka et al., 1996). The interplay between tacit and explicit knowledge forms the basis for continuous learning and innovation within organisations (Smith, 2001), which is essential for sustaining competitive advantage (Mascitelli, 2000). The dynamic capabilities framework, often aligned with KM (Easterby-Smith and Prieto, 2008), further highlights the importance of developing organisational routines and processes that enable adaptation to changing environments through the effective use of knowledge resources (Teece et al., 1997).

Building on this understanding, it is important to consider not only the well-documented benefits that KM offers to organisations but also the potential risks, particularly those tied to knowledge itself. One significant concern is the phenomenon of "knowledge at risk," which highlights the vulnerabilities organisations face when dealing with outdated, siloed, or inaccessible knowledge (Durst and Wilhelm, 2013). This concept, introduced by Brunold and Durst (2012), shifts the focus

[7] McKinsey and Company. Retrieved from https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/getting-tangible-about-intangibles-the-future-of-growth-and-productivity (Accessed on December 30, 2024)

from the traditionally view of knowledge as solely a source of advantage to a more balanced perspective that recognises the dual nature of knowledge as both an asset and a potential liability.

The knowledge-at-risk perspective has garnered increasing attention in KM literature as it brings to light the strategic importance of managing knowledge-related risks proactively, thus emphasising the need for knowledge risk management (KRM). These risks can manifest in various forms, including knowledge loss due to employee turnover, reliance on outdated or inaccurate knowledge, and the failure to integrate knowledge effectively across organisational silos. Addressing these risks requires organisations to adopt a comprehensive KM approach that is combined with the organisation's risk management function (Zieba et al., 2022b; El Khatib and Ali, 2022).

This thesis adopts a KM perspective to better understand how organisations identify, analyse, and evaluate risks associated with their knowledge resources. It focuses on the need to investigate risks that may reduce the value of knowledge within organisations. Knowledge risks such as knowledge loss, leakage, and obsolescence can disrupt processes and negatively impact performance (Durst and Zieba, 2019; Sumbal et al., 2020; Daghfous et al., 2021). Addressing these risks requires a structured approach that integrates suitable tools and methods. Through KM perspective, this thesis establishes a foundation for understanding knowledge risks and provides a basis for developing a systematic approach to their assessment and management.

2.5. Systematic literature review approach

In this section, the outcomes of a systematic literature review (SLR) are presented to provide an overview of existing research on KRM, with the aim of identifying research gaps to inform the thesis aim. A SLR is a "systematic, explicit, and reproducible method for identifying, evaluating, and synthesi[s]ing the existing body of completed and recorded work produced by researchers, scholars, and practitioners" (Fink, 2013, p. 3). It follows a structured framework that allows for reproducibility and enhances the transparency of the research process. This includes various stages such as conceptualising research ideas, selecting relevant papers, conducting analysis, and interpreting the findings. To ensure adherence to the principles of systematic review, the author adopts the methodology by Jesson et al. (2011), which include mapping the field through a scoping review, conducting a comprehensive search, assessing quality, extracting and synthesising data, and writing up the review. This methodology has been widely used in management research (e.g., Jackson et al., 2020; Menghwar and Daood, 2021) and is particularly dominant in SLR studies on KM (e.g., Durst et al., 2023, 2024; Timiyo and Foli, 2023).

To initiate the review process, guided by the stated aim, the first step involved developing a research plan, which included determining the research questions of interest and specifying the keywords and a set of inclusion and exclusion criteria. In this particular case, the following questions were formulated:

- What are the trends in KRM research?

This question explores how KRM research has evolved, including trends in publications, research methods, and the theories used.

- What are the main themes in KRM?

This question seeks to identify the key topics explored in KRM research. This helps to clarify the primary areas of focus within the KRM field.

- What gaps exist in KRM research?

This question helps identify under-researched areas, guiding the thesis's direction.

The next step involved conducting a comprehensive search using specific search strings developed by the author. These search strings included terms such as "knowledge risk*" OR "knowledge-

based risk*" OR "intellectual capital risk*" OR "intangible risk*" OR "knowledge threat" OR "knowledge securit*" OR "knowledge vulnerabilit*" OR "knowledge loss" OR "knowledge protection" OR "organizational memory risk*" OR "organizational memory threat" OR "organizational memory securit*" OR "organizational memory vulnerabilit*" OR "organizational memory loss" OR " organizational memory protection" OR "intellectual property risk*" OR "intellectual property threat" OR "intellectual property vulnerabilit*" OR "intellectual property loss" OR "intellectual property protection" OR "knowledge risk management".

On June 18, 2024, the initial search conducted using the specified keywords on the Web of Science (WoS) database yielded 604 documents. A set of inclusion and exclusion criteria, detailed in **Table 2**, was developed and applied.

Table 2 Summary of inclusion and exclusion criteria

Inclusion criteria	**Exclusion criteria**
Time horizon: Not restricted	Not written in English
Types of documents: Article, Conference paper, Book chapter	Not peer-reviewed
Written in English	Papers without a significant focus KRM
Peer-reviewed	Review paper
Published in Business or Management journals	

These criteria were established based on the following rationale: First, since KRM is considered a relatively new field, the time period was not restricted to ensure a comprehensive coverage of the relevant literature, including both early contributions and recent advancements in the field. Second, to address concerns about the variability in the quality of conference papers and book chapters, only those from reputable sources were included. For example, conference papers from forums with established academic credibility and rigorous review processes, such as the Hawaii International Conference on System Sciences (HICSS), were deemed eligible. HICSS is widely recognised for its high-quality contributions to research in business, management, and technology, with a mostly dedicated track for papers related to knowledge risks/knowledge risk management. Similarly, book chapters were included only if published by reputable academic publishers such as Springer, which is known for its stringent editorial standards and focus on scholarly research. These selection criteria ensured that the included documents met recognised academic quality standards.

Additionally, review papers were excluded to focus solely on original research contributions. The aim of the review was to synthesise insights from empirical studies, theoretical frameworks, and original contributions to KRM. Including review papers could have led to duplication of findings, as reviews typically summarise existing literature rather than offering new empirical or theoretical insights.

The inclusion/exclusion process was further refined to align the selection of documents with the study's disciplinary focus on Business and Management. This step reduced the number of documents from 604 to 309, as many of the initial records were from unrelated fields such as engineering, health sciences, and computer science. Next, only documents written in English were included, reducing the count to 305. To ensure relevance, the selection was restricted to specific publication types – articles, conference papers, and book chapters – resulting in 297 documents.

The selected documents were downloaded into an Excel sheet for detailed screening. The first stage involved abstract screening, during which 236 papers were excluded for not meeting the inclusion criteria. Many of these papers used the terms "knowledge" and "risks" in close proximity (e.g., separated by a comma), but their content was unrelated to the study topic. Papers without a significant focus on KRM were excluded to maintain relevance. Specifically, only papers where KRM was a central topic of discussion, analysis, or investigation were included. For instance, papers that merely mentioned KRM in passing or as a minor aspect of a broader discussion were excluded. To determine whether a paper had a significant focus, its abstract, keywords, and main sections were carefully reviewed. If KRM was explicitly addressed as a key theme, framework, or research problem, the paper was included.

This abstract screening was followed by a full-text review, which resulted in the exclusion of an additional eight papers. These papers, despite containing the terms "knowledge" and "risks" in their abstracts, were found to lack a focus on knowledge risks or KRM. Ultimately, 53 papers met the inclusion and exclusion criteria.

To ensure no relevant articles were overlooked during the initial database search, a manual search was conducted using Google Scholar, following the approach recommended by Massaro et al. (2016). This approach involved scanning through the reference lists of key papers already identified in the review to find additional relevant studies. Furthermore, keyword searches were performed directly in Google Scholar to identify any articles that may not have been indexed in the Web of

Science database. The manual search process emphasised cross-referencing to capture any overlooked but significant contributions to the field. This additional effort identified five more papers, which were subsequently included, bringing the total number of papers for review to 58 (see **Table 19**).

The next stage of the systematic review process involved data extraction and synthesis, followed by the interpretation and writing of findings. This stage aimed to analyse and summarise the selected papers to provide a detailed overview of key insights. The overall SLR process, including the selection workflow, is summarised in **Figure 5**.

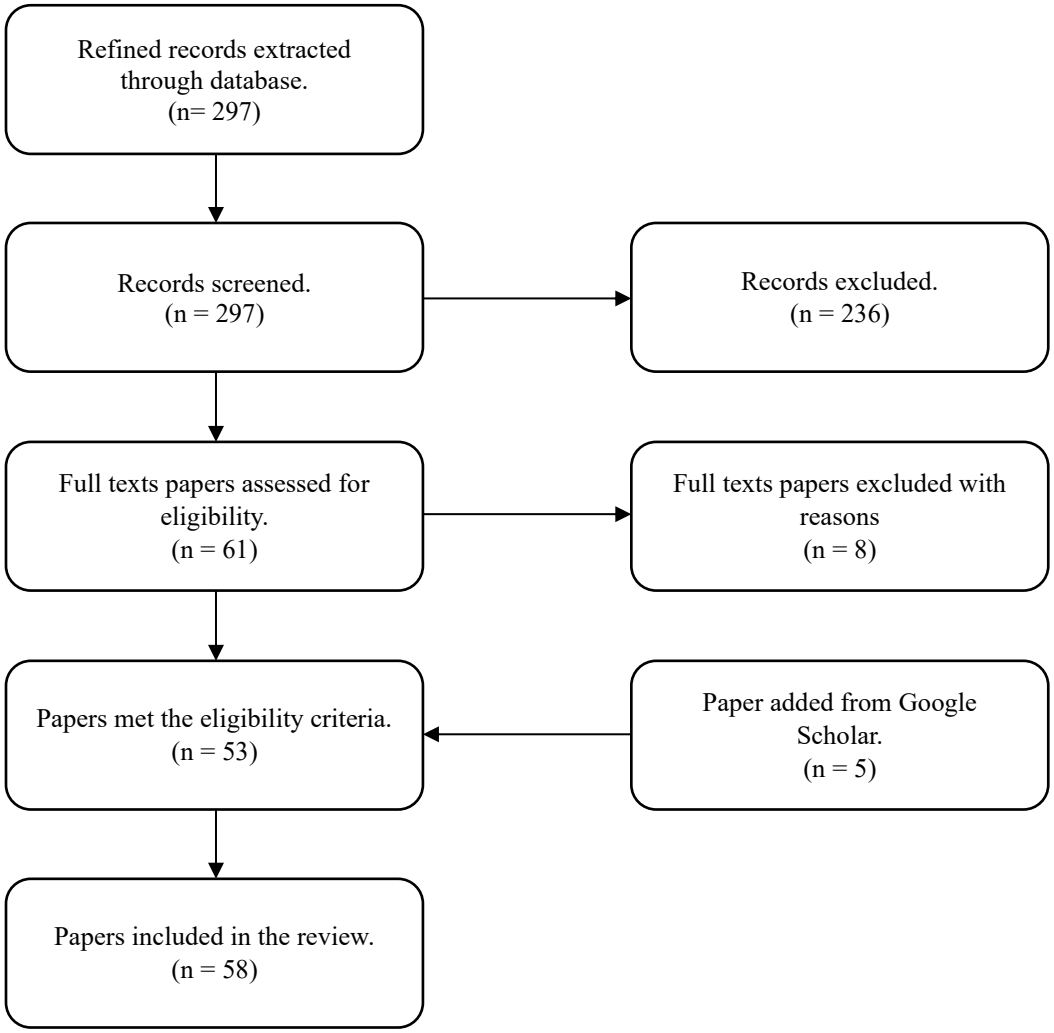


Figure 5 Flow chart of the selection process.

2.5.1. Descriptive findings

This section presents findings at the descriptive level for the papers included in the review. It begins with an analysis of publication activities throughout the years, followed by an examination of the publication outlets where research on KRM has been published and the research approaches/methods/techniques employed. The section concludes by shedding light on the theories or theoretical frameworks utilised in this field.

2.5.1.1. Year of publication

Figure 6 illustrates the publication trends related to KRM across various years. The data highlights a notable peak in 2022, with eight papers focusing on this topic. This trend reflects a growing interest and recognition of KRM as a significant area of research. The increasing trajectory of publications over time indicates heightened awareness of knowledge risks and their implications for organisational success.

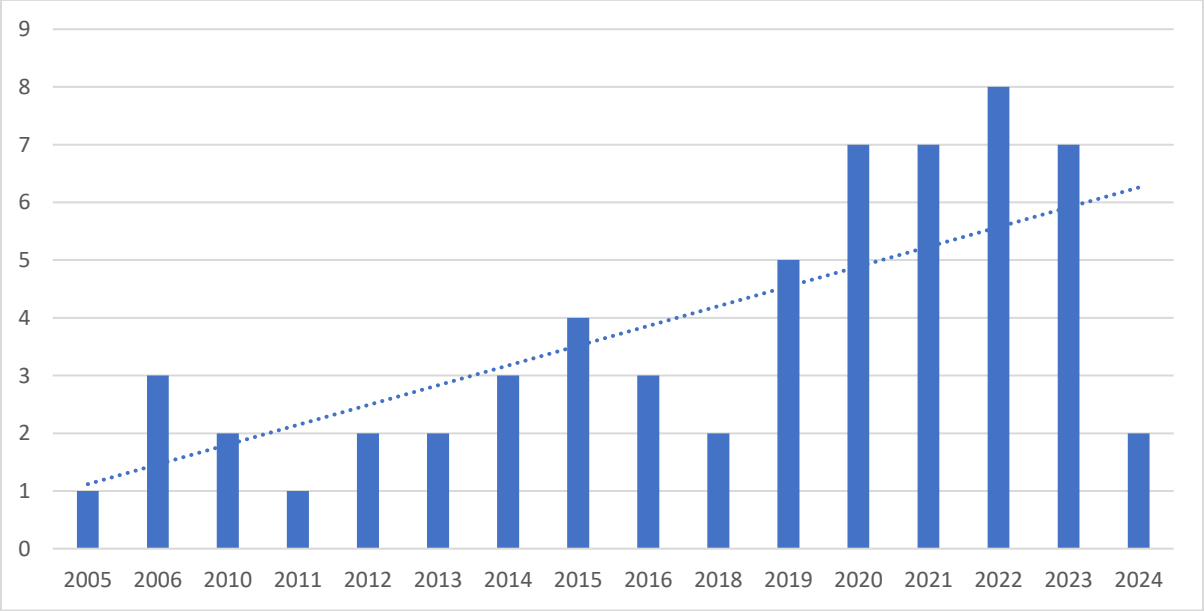


Figure 6 Number of published papers per year

2.5.1.2. Research approaches

The distribution of research approaches in studies on KRM is illustrated in **Figure 7**, categorising the methodologies into qualitative, quantitative, and conceptual approaches. The most prevalent approach is qualitative research, accounting for 54% of the total studies. This dominance reflects the exploratory nature of the field, as qualitative methods are well-suited for examining the context-specific and complex aspects of knowledge risks. Conceptual papers represent 21% of the research approaches, focusing primarily on defining and categorising knowledge risks. A significant portion of these conceptual studies centres on developing taxonomies of knowledge risks, which are foundational for organising and classifying the diverse types of risks organisations face. For instance, Durst and Zieba (2019) proposed a comprehensive taxonomy that organises knowledge risks into three categories: human, technological, and operational risks.

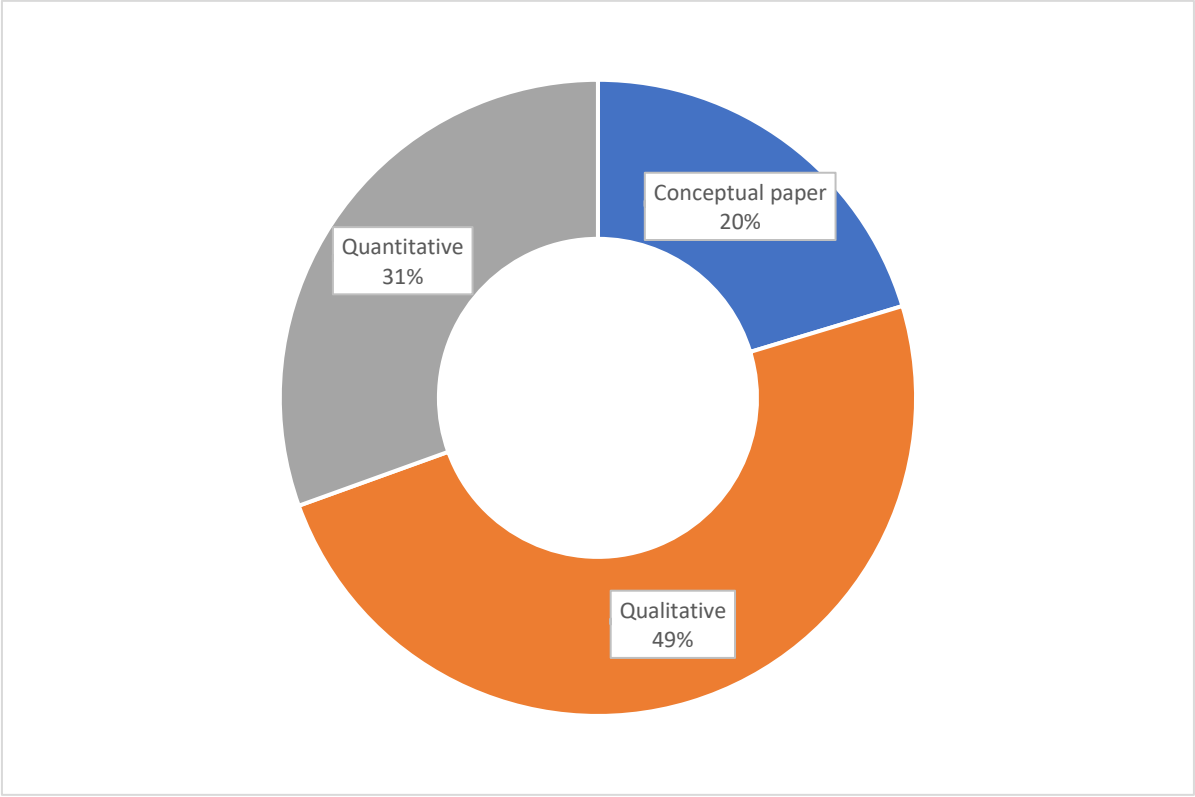


Figure 7 Research approaches used in the papers.

2.5.1.3. Theoretical perspectives

The use of theories/theoretical frameworks in the study of KRM has been limited, with only a few studies applying established theories. Among these, the knowledge-based view (KBV) is the most commonly used. For instance, El Khatib and Ali (2022) applied the KBV to examine the relationships between knowledge risks, organizational performance, and the sustainability of knowledge-intensive firms. Similarly, Zieba et al. (2022) used the KBV to explore how KRM influences organisational sustainability, with a focus on innovativeness and agility.

In some cases, KBV has been used alongside other frameworks. Trkman and Desouza (2012) combined the KBV with transaction cost economics to develop a framework for analysing knowledge risks in networks. Alternatively, Marabelli and Newell (2012) adopted a practice-oriented perspective to study the dynamics of knowledge transfer within and across networks.

2.5.2. Main findings

A structured approach was used to guide the analysis, with themes organised around the established sub-processes of risk management. These sub-processes – such as risk identification, risk assessment, and risk mitigation – provided a clear framework for categorising and synthesising the findings from the reviewed papers. Given KRM is fundamentally part of general risk management, using these sub-processes for synthesising the findings seems logical. The results are outlined below:

2.5.2.1. Identification of knowledge risks

The review covered sixteen papers that addressed different types of knowledge risks discussed in the literature. Elias and Wright (2006) reviewed the literature and surveyed knowledge-based organisations to identify general risks, such as inappropriate corporate information policies, employee turnover and lack of data transferability. Durst and Wilhelm (2012) studied how medium-sized firms address knowledge loss from employee departures or absences. They emphasise that effective succession planning in SMEs is crucial for transferring both tacit and explicit knowledge. Key risks include loss of tacit knowledge, knowledge gaps, and cultural challenges. Trkman and

Desouza (2012) addressed knowledge risks in organisational networks, particularly risks related to knowledge flow disruptions and IT vulnerabilities in information systems. Tantau and Paicu (2013) developed a comprehensive framework for identifying and categorising knowledge risks, including those related to knowledge creation, storage, sharing, application, and loss. Their work specifically examined how these risks influence the promotion of intrapreneurship within banking institutions.

Rehman and Kifor (2015) focused on the role of IT tools in managing knowledge risks within digital environments. They emphasised the importance of identifying risks specific to digital knowledge assets, such as cybersecurity vulnerabilities. North et al. (2019) focused on identifying risks specific to knowledge and information in supply chain interactions. Durst and Zieba (2019) provided a comprehensive understanding of knowledge risks in organisations. Their work entails an identification and categorisation of knowledge risks into human, technological and operation risks. Building upon the taxonomy by Durst and Zieba (2019), El Khatib et al. (2021) introduced a new category – strategic knowledge risks – which includes knowledge loss, knowledge leakage, and knowledge gaps.

Moreover, Zieba et al. (2021) conducted an exploratory study to investigate knowledge risks faced by organisations and examined whether the COVID-19 pandemic had influenced the prevalence of such risks. Bratianu and Bejinaru (2022) investigated vulnerabilities and risks within Knowledge Management Systems (KMS). Their qualitative analysis revealed operational risks stemming from inefficient management practices. Similarly, on another front, Hammoda and Durst (2022) and Temel and Durst (2021) delved into knowledge risks specifically within the domain of health and of radical technological innovations respectively. Zieba et al. (2022a) examined cyber risks as a critical component of technical knowledge risks in organisations. Their findings stressed the growing importance of cybersecurity in mitigating knowledge-related vulnerabilities. Fruhwirth et al. (2024) explored the types of knowledge risks and protection measures in data-driven business models. Their study highlighted risks associated with data misuse and inadequate data protection strategies. Finally, Thalmann et al. (2024) investigated informal knowledge-sharing practices in organisational networks, identifying vulnerabilities that can lead to data leaks and other knowledge risks.

2.5.2.2. Assessment of knowledge risks

The review covered nine papers discussing tools and methods utilised to assess knowledge risks in various organisational contexts. Lee et al. (2014) developed a metric that quantitatively measures the risk of knowledge drain associated with the departure of a member in communities of practice (CoP). Jennex and Durcikova (2020b) proposed a conceptual framework for risk management in knowledge systems, emphasising threat identification and assessment. Their framework outlines practical steps for systematically assessing risks to ensure robust knowledge management practices. In a related work, Jennex and Durcikova (2020a) created a risk and threat assessment framework tailored to sustainable knowledge systems, focusing on integrating sustainability principles into knowledge risk assessment.

Yarovenko et al. (2021) presented a quantitative approach to assess knowledge loss risks. Their study offers an innovative methodology to quantify risks, enabling organisations to identify critical vulnerabilities in knowledge assets. Similarly, Lee et al. (2021) provided a detailed assessment of knowledge risks, laying out theoretical and applied perspectives on knowledge risk evaluation.

Piri et al. (2021) proposed a dynamic model for computing risks associated with knowledge domains in organisational maps. Their work presents a novel method to dynamically adapt to evolving risks, enhancing organisational resilience. Ursache et al. (2023) developed a scoring system for knowledge vulnerabilities in the knowledge economy, providing a structured approach to evaluating risks in rapidly changing economic landscapes.

Thalmann et al. (2014) investigated methods for assessing and mitigating knowledge risks in collaborative environments, employing quantitative modelling and case studies. Their research combines assessment and mitigation strategies, offering practical insights for managing collaborative risks effectively. Similarly, Delak and Damij (2015) proposed frameworks for assessing knowledge risks in business processes. Their study utilised survey-based methods to identify risk factors and propose strategies for mitigating these risks.

2.5.2.3. Mitigation strategies

The review covered 20 papers discussing various mitigation strategies to address knowledge risks. Bayer and Maier (2006) proposed governance rules for inter-organisational knowledge transfer

risks, emphasising structured approaches to managing both intended and unintended knowledge transfer. Loomba (2006) developed a framework for managing knowledge risks, highlighting the importance of systematic identification and control mechanisms. Coleman and Casselman (2016) studied the interplay between knowledge sharing and protection strategies. They proposed methods for mitigating risks while maintaining competitive advantage. Durst et al. (2018) focused on SMEs, identifying key operational risks and proposing strategies for managing them effectively. Temel and Vanhaverbeke (2020) discussed knowledge risks in the context of open innovation management. Their work emphasised the importance of addressing risks during the implementation of innovation strategies.

Erickson and Rothberg (2010) examined the balance between knowledge sharing and protection within value-chain networks, providing actionable insights into managing risks while fostering collaboration. Gheorghe (2012) provided insights into managing organisational knowledge during change periods, emphasising strategies to safeguard knowledge assets. Von Solms and Van Niekerk (2013) explored cybersecurity strategies to protect knowledge assets, addressing risks arising from digital threats. Massingham (2014) focused on the role of organisational culture and knowledge flows in addressing risks, highlighting strategies to integrate KM tools effectively. Padyab et al. (2015) introduced a socio-technical framework for managing knowledge security risks, highlighting the interplay between technical and organisational factors. Manhart and Thalmann (2015) examined knowledge protection strategies in collaborative workspaces, identifying best practices for mitigating risks associated with sensitive knowledge sharing. Peltier (2016) provided a comprehensive overview of information security measures critical to knowledge protection. Sarigianni et al. (2016) proposes technical and organisational countermeasures, such as awareness training, social media policies, and access restrictions, to mitigate knowledge risks associated with social media use in financial institutions. Tsang and Lee (2018) explored the challenges of knowledge risks in open innovation, particularly for small and medium enterprises, and outlines strategies such as safeguarding intellectual property, fostering trust in collaborations, and developing robust knowledge-sharing frameworks to mitigate these risks.

Vlasov and Panikarova (2019) discussed knowledge risk management strategies in digital environments, focusing on preventing knowledge leakage. Shujahat et al. (2020) explored KRM within human resource management structures, emphasising tailored approaches for two-tier HRM

systems. Thalmann and Ilvonen (2020) investigated knowledge risk incidents through four cases, focusing on strategies for preventing and reacting to such risks. It highlighted the need for comprehensive mitigation measures, including learning from incidents to enhance knowledge protection practices.

Daghfous et al. (2021) incorporated the risk of knowledge loss into supply chain risk management frameworks, presenting strategies to address this issue. Zeiringer and Thalmann (2022) investigated mechanisms to balance knowledge sharing and protection, emphasizing safeguarding knowledge without stifling collaboration. Souto and Bruno-Faria (2022) analysed knowledge loss risk management strategies in a Brazilian public company, AMAZUL, providing detailed case-based insights into effective mitigation practices, while Zeiringer et al. (2024) examined data anonymisation as a strategy for managing knowledge risks in supply chains.

2.5.2.4. Knowledge risk management framework

While the analysis was primarily structured around the sub-processes of risk management, several studies also explored frameworks specific to KRM. Six papers focused on this topic.

Neef (2005) examined how progressive companies utilise KRM systems and techniques to manage risks related to ethical or reputation-damaging incidents. This conceptual study emphasised the interplay between knowledge and risk management systems. Massingham (2010) introduced a comprehensive framework for KRM, demonstrating how knowledge management tools can address organisational risks. Jafari et al. (2011) further elaborated on KRM in organisations, utilising quantitative modelling to provide practical case study insights. Müller and Mueller (2019) provided a comprehensive discussion on KRM processes, including identification, assessment, and mitigation strategies for managing knowledge loss in organisations. Their work focused on addressing knowledge loss driven by demographic shifts, employee turnover, and organisational restructuring. Gheorghioiu (2020) provided a conceptual overview of KRM, exploring its relevance and application in modern organisational settings. Zieba and Bongiovanni (2022) proposed an integrated framework for managing knowledge and security risks during crises such as COVID-19, expanding the discourse on KRM applicability in challenging contexts.

2.5.2.5. Relationship of knowledge risks and their management on organisational outcomes

A total of seven papers focused on examining the relationship between knowledge risks, their management, and organisational outcomes. Some studies addressed how knowledge risks negatively influence organisational performance, while others explored the relationship of KRM on organisational outcomes.

Durst et al. (2019) examined the relationship between KRM and organisational performance. Zieba et al. (2022) examined the effect of KRM on organisational sustainability, as well as the roles of innovativeness and agility in this relationship. Durst et al. (2023) investigated the application of KRM in banking, revealing its potential to enhance organisational performance. El Khatib and Ali (2022) explored knowledge risks and sustainability, particularly in relation to organisational performance. El Khatib and Abbas (2023) studied the intersection of knowledge risks, business sustainability, and organisational performance, focusing on knowledge-intensive firms in Lebanon. Zieba (2023) examined the relationship between emotions and knowledge risks, providing a conceptual analysis of how emotional factors influence risk perception and management. Bratianu et al. (2020) discussed the broader concept of knowledge risks within firms, emphasising their impact on organisational outcomes.

2.5.3. Gap(s) identified in the literature

The analysis of themes reveals that research in the field of KRM has seen considerable advancements over the years. These include the identification of a wide range of knowledge-related risks, the development of diverse strategies for mitigating these risks, and the development of various KRM frameworks tailored to different industries (e.g., Health: Hammoda and Durst, 2022) and organisational sizes (e.g., SMEs: Durst and Ferenhof, 2016). These contributions have enhanced the understanding of KRM.

However, a gap exists in the area of knowledge risk assessment. Despite its critical role in the overall risk management process – of which knowledge risk management is no exception – the systematic evaluation and prioritisation of knowledge risks have not received sufficient attention. This is particularly important because improved knowledge risk assessment forms the foundation for designing and implementing appropriate mitigation strategies. Without improved assessment,

subsequent steps in the KRM process, such as mitigation and monitoring, may lack the necessary foundation to address these risks.

These studies have proposed tools and frameworks for knowledge risk assessment; however, these efforts often fail to address the complexity and interrelatedness of knowledge risks. Massingham (2010) found that conventional decision tree approaches often fall short in this area due to cognitive biases. Through an empirical case study of the Australian Department of Defence, Massingham proposed a model that integrates knowledge management tools into the risk assessment process. This model aims to reduce subjectivity and cognitive biases, enabling managers to differentiate and prioritise risks. Thalmann et al. (2014) also addressed knowledge risk from a different angle. Their study introduces a framework for protecting organisational knowledge by translating organisational goals into specific controls. Their methodology, adapted from IT security management practices, enables organisations to evaluate and improve their knowledge protection measures, enhancing transparency and compliance with risk management standards. Ilvonen et al. (2015) introduced a model for managing knowledge security risks, framing knowledge risk management as a sensemaking process. Their model focuses on achieving a balance between knowledge sharing and security, supporting managers in evaluating risks while considering the associated costs and benefits.

Jennex and Durcikova (2020a, 2020b) proposed conceptual frameworks that emphasise threat identification and assessment in knowledge systems. These frameworks were further extended to incorporate sustainability principles in risk assessment. However, while these advancements have provided a foundation for knowledge risk assessment, they do not employ suitable decision-making tools capable of addressing the inherent complexity and interrelatedness nature of knowledge risks. Specifically, the frameworks lack mechanisms to systematically evaluate and prioritise risks when multiple interdependent and conflicting criteria are involved. Many of these studies rely on traditional methods/tools that fail to capture the interconnected nature of knowledge risks. The literature reflects a lack of decision-making tools, such as Multi-Criteria Decision-Making (MCDM) models, which could provide structured approaches to addressing the complexities of knowledge risks. Unlike traditional tools, MCDM models are designed to evaluate complex problems involving multiple, often conflicting criteria. These models are designed to account for interdependencies and interactions between various risk factors, enabling organisations to make

informed and balanced decisions. For instance, MCDM models can be used to prioritise knowledge risks by weighing factors such as the likelihood of occurrence, potential impact, and the resources required for mitigation. They allow for the inclusion of both qualitative and quantitative data, making them flexible and adaptable to various organisational contexts.

To address this gap, this PhD research will focus on developing a comprehensive risk assessment framework for knowledge risks. The framework will incorporate suitable decision-making tools, such as MCDM models, to provide a systematic and structured approach to knowledge risk assessment.

In the next section, MCDM models are reviewed and selected based on their potential to improve knowledge risk assessment and address the current limitations identified in the KRM literature.

2.5.4. Multiple criteria decision-making models (MCDM)

Multiple Criteria Decision-Making (MCDM) refers to a set of models or procedures used to evaluate and prioritise multiple, often conflicting criteria in decision-making processes (Belton and Stewart, 2012). These models assist decision-makers in systematically analysing various options to identify the most suitable choice. In the context of risk assessment, MCDM models can be particularly valuable as they enable the comprehensive evaluation of diverse risks, including those related to knowledge, such as knowledge obsolescence, intellectual property theft, and knowledge loss. There are many MCDM models which include: Analytic Hierarchy Process (AHP), Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS), Elimination and Choice Expressing Reality (ELECTRE), Multi-Attribute Utility Theory (MAUT), Simple Additive Weighting (SAW), Decision-Making Trial and Evaluation Laboratory (DEMATEL), Total Interpretive Structural Modelling (TISM), and Preference Ranking Organisation Method for Enrichment Evaluation (PROMETHEE) etc. The following sections provide a review of these models.

2.5.4.1. Analytic hierarchy process (AHP)

Saaty (1980) developed the Analytic Hierarchy Process (AHP), a structured decision-making model, to handle complex problems with several criteria. AHP simplifies complex decision

problems by breaking them down into manageable components. This hierarchical decomposition enhances focus on specific criteria and sub-criteria during the decision-making process, allowing for a comprehensive analysis of each element's relative importance (Ibid). Additionally, AHP's use of pairwise comparisons enables detailed assessments that accommodate both qualitative and quantitative criteria, providing a better understanding of the decision factors involved (Chen et al., 2013; Aladayleh and Aladaileh, 2024). The model also incorporates a consistency check mechanism to assess the logical soundness of judgements, reducing the likelihood of errors and ensuring the reliability of the decision-making process (Saaty, 2016). Numerous industries, including risk assessment, healthcare, and supply chain management, use the AHP extensively (Ishizaka et al., 2011).

However, AHP's reliance on human judgement in pairwise comparisons introduces subjectivity, which can lead to biases, especially when decision-makers have differing opinions (Munier et al., 2021). Furthermore, AHP has been criticised for the phenomenon of rank reversal, where the introduction or removal of alternatives can change the ranking of existing options, potentially leading to inconsistent decision outcomes (Maleki and Zahir, 2013). The traditional 1-9 scale used in AHP for comparisons may not capture the true intensity of preferences in certain situations, potentially oversimplifying complex judgements (Maleki and Zahir, 2013). Moreover, as the number of criteria and alternatives increases, the number of required comparisons grows exponentially, making the process cumbersome and time-consuming.

2.5.4.2. Technique for order of preference by similarity to ideal solution (TOPSIS)

Hwang and Yoon (1981) developed TOPSIS, which assesses options according to how far they deviate from the ideal solution. TOPSIS operates on the principle that the optimal alternative should have the shortest geometric distance from the positive ideal solution (PIS) and the farthest from the negative ideal solution (NIS) (Kuo, 2017). This model involves calculating the Euclidean distance of each alternative from these ideal and anti-ideal solutions, thereby facilitating a ranking based on their relative closeness to the ideal (Papathanasiou, 2018). TOPSIS has found extensive application across various domains, including logistics (Bottani and Rizzi, 2006), environmental risk assessments (Jozi and Majd, 2014), and project management (Jabbarzadeh, 2018; Behzadian et al., 2012), among others.

One of the strengths of TOPSIS is its straightforwardness and ease of implementation. The method's reliance on geometric distance calculations renders it computationally efficient, making it suitable for real-time decision-making scenarios (Goyal and Kaushal, 2017; Alojaiman, 2023). Furthermore, TOPSIS is also capable of handling both quantitative and qualitative criteria, providing a flexible framework for diverse decision-making contexts (Rahim et al., 2021). Its ability to offer a clear ranking of alternatives based on their proximity to the ideal solution aids decision-makers in selecting the most appropriate option among a set of alternatives.

However, despite its advantages, TOPSIS is not without limitations (Madi et al., 2026). A significant critique is its assumption that criteria are equally weighted, which may not accurately reflect the complexities of real-world decision-making scenarios where criteria often have varying degrees of importance (Ibid). This equal weighting can lead to oversimplified analyses and potentially suboptimal decisions. Additionally, TOPSIS can be sensitive to the relative scaling of criteria, where differing units or scales can disproportionately influence the outcome if not properly normalised (Ibid). Moreover, the model does not inherently account for the potential interdependencies among criteria, which can be a critical factor in complex decision-making environments.

2.5.4.3. Elimination and choice expressing reality (ELECTRE)

The ELECTRE (ELimination and Choice Expressing REality) family of outranking methods, introduced by Bernard Roy in the mid-1960s, has been instrumental in addressing complex decision-making scenarios involving multiple, often conflicting criteria. These models facilitate pairwise comparisons among alternatives to establish dominance relations, thereby aiding in the selection, ranking, or sorting of options. ELECTRE's versatility has led to its application across various domains (Figueira et al., 2013), including urban development, water resource management, and energy planning.

A significant advantage of ELECTRE lies in its capacity to handle both qualitative and quantitative criteria, allowing for a comprehensive evaluation of alternatives (Nafisur Rahman, 2024). This is particularly beneficial in real-world situations where decision parameters are not solely numerical. Additionally, ELECTRE methods do not require the compensation of poor performance in one

criterion by excellent performance in another, aligning well with decision contexts where trade-offs are not permissible (Baseer et al., 2023). This non-compensatory nature ensures that alternatives are assessed more holistically, reflecting realistic decision-making processes.

However, the complexity of ELECTRE methods presents certain challenges (Figueira et al., 2010). The procedures involved, including the construction of concordance and discordance matrices, can be intricate and computationally intensive, especially as the number of criteria and alternatives increases (Ibid). Moreover, the reliance on user-defined thresholds, such as indifference, preference, and veto thresholds, introduces a degree of subjectivity into the analysis (Ibid). These thresholds significantly influence the outcome, and their arbitrary selection can lead to inconsistent or biased results. Therefore, careful consideration and justification of these parameters are essential to maintain the model's robustness.

2.5.4.4. Multi-attribute utility theory (MAUT)

Multi-Attribute Utility Theory (MAUT) is a decision-making framework that evaluates alternatives based on multiple criteria by quantifying the utility – or overall satisfaction – derived from each option (Keeney, 1993). MAUT is particularly effective in scenarios necessitating trade-offs among competing criteria, such as resource allocation and policy formulation (Gerst, 2011). MAUT facilitates a structured approach to complex decision-making processes, by constructing utility functions that reflect decision-makers' preferences (Nikou and Klotz, 2014; Kailiponi, 2010).

A significant advantage of MAUT is its ability to tailor utility functions to the specific preferences of decision-makers (Collins et al., 2006). This customisation ensures that the evaluation process aligns with individual or organisational value systems, thereby enhancing the relevance and acceptance of the outcomes. Moreover, MAUT's systematic approach aids in elucidating the inherent trade-offs between different attributes, providing a transparent rationale for selecting one alternative over another (Ibid). This is valuable in policymaking and resource distribution, where decisions often involve balancing conflicting objectives.

However, the implementation of MAUT is not without challenges. One of the primary difficulties lies in the accurate assessment of utility values for each criterion (Dodgson et al., 2009). This process can be intricate and data-intensive, requiring precise quantification of subjective

preferences, which may not always be straightforward (Ibid). Additionally, the construction of utility functions demands a thorough understanding of the decision context and the stakeholders' value structures, necessitating significant time and expertise (Ibid). The complexity of MAUT models can also lead to computational challenges, especially when dealing with a large number of attributes and alternatives.

2.5.4.5. Simple additive weighting (SAW)

Simple Additive Weighting (SAW), also known as the weighted sum model, is among the most straightforward techniques in MCDM. Its fundamental premise involves assigning weights to various criteria, scoring each alternative against these criteria, and computing a weighted sum to determine the most favourable option (Kabassi, 2009). This model's simplicity and ease of implementation have led to its widespread application across diverse fields.

The appeal of SAW largely stems from its intuitive approach, which allows decision-makers to straightforwardly aggregate multiple criteria into a single evaluative score (Hosseinzadeh Lotfi et al., 2023). This facilitates clear communication of the decision-making process and outcomes to stakeholders, enhancing its practical utility. However, despite these advantages, SAW is not without its criticisms and limitations.

A significant critique of SAW is its inherent assumption of linearity and compensability among criteria (Triantaphyllou and Triantaphyllou, 2000). The model presumes that a poor performance in one criterion can be offset by a superior performance in another, implying a direct trade-off capability between criteria (Ibid). This assumption may not hold in real-world scenarios where certain criteria are non-compensatory or exhibit complex interdependencies. For instance, in supplier selection, a supplier's failure to meet a critical quality threshold cannot simply be compensated by lower costs, as quality may be a non-negotiable criterion.

Moreover, SAW's reliance on precise weight assignments introduces subjectivity into the decision-making process (Taherdoost, 2023). Determining accurate weights for each criterion can be challenging, particularly in situations involving multiple stakeholders with differing priorities. This subjectivity can lead to biases, potentially skewing the decision outcome. Additionally, SAW is

sensitive to the scaling of criteria; without proper normalisation, criteria measured on different scales can disproportionately influence the aggregated scores, leading to erroneous conclusions.

2.5.4.6. Decision-making trial and evaluation laboratory (DEMATEL)

The Decision-Making Trial and Evaluation Laboratory (DEMATEL) method, introduced by Fontela and Gabus in 1974, is a prominent tool in MCDM that facilitates the analysis and visualisation of complex causal relationships among factors within a system. DEMATEL enables decision-makers to map out interdependencies, distinguishing between cause-and-effect elements, thereby providing a structured approach to problem-solving in intricate scenarios by employing matrices and directed graphs (Thakkar and Thakkar, 2021).

One of the primary strengths of DEMATEL lies in its capacity to handle both qualitative and quantitative data, making it adaptable across various domains (Ahmad et al., 2024). Its application spans fields (Si et al., 2018) such as supply chain (risk) management, environmental planning, healthcare, finance, and engineering, where understanding the interplay between multiple factors is essential for effective decision-making. For instance, in supply chain management studies (e.g., Das et al., 2022; Singh et al., 2024), DEMATEL has been utilised to identify key drivers affecting performance, enabling managers to prioritise interventions that enhance efficiency and resilience. In the context of knowledge risk assessment, DEMATEL's ability to explain causal relationships is particularly beneficial. Knowledge risks, such as data leakage, human error, and knowledge decay, often exhibit complex interdependencies that can complicate mitigation efforts. By applying DEMATEL, organisations can construct a visual representation of these risks, categorising them into cause-and-effect groups. This categorisation aids in identifying pivotal risks that, if addressed, could alleviate multiple related issues, thereby optimising resource allocation and strategic planning.

Despite its advantages, DEMATEL is not without limitations. The method relies heavily on expert judgment to evaluate the relationships among factors, which can introduce subjectivity and potential bias into the analysis (Li and Xiao, 2024). Additionally, as the complexity of the system increases, the number of factors and interrelations can become overwhelming, making the analysis cumbersome and time-consuming. To address these challenges, researchers have proposed

integrating DEMATEL with other models. For example, combining DEMATEL with the Analytic Network Process (ANP) can enhance decision-making by accounting for both interdependencies and the relative importance of factors. Furthermore, the application of fuzzy logic to DEMATEL allows for the incorporation of uncertainty and vagueness in expert assessments, improving the method's reliability in complex decision-making scenarios.

2.5.4.7. Total interpretive structural modelling (TISM)

Total Interpretive Structural Modelling (TISM) is an advanced MCDM model that extends the traditional Interpretive Structural Modelling (ISM) by incorporating interpretative logic into the analysis of complex systems (Menon and Suresh, 2020; Sushil, 2012). This improvement allows for better insight into the relationships among various elements within a system (Ibid), making TISM particularly valuable in fields requiring comprehensive analysis of interdependencies, such as organisational research, manufacturing, and service sectors.

TISM has developed through its use in various fields, helping researchers answer key questions about what happens, how it happens, and why (Sushil and Dinesh, 2022). TISM helps build theoretical models by identifying variables, explaining their relationships, and showing the reasons behind them (Sushil, 2012). This structured approach is essential for understanding complex issues and creating frameworks to guide decisions.

One of the significant advantages of TISM is its ability to transform unclear, poorly articulated mental models into visible and well-defined representations (Sushil, 2012). This transformation is achieved through a systematic process that involves the identification of elements, establishment of contextual relationships, development of a reachability matrix, and construction of a hierarchical model. The resulting digraph not only depicts the relationships among elements but also provides interpretative insights, offering a comprehensive understanding of the system under study.

Siddiqui (2024) demonstrates the practical utility of TISM in analysing barriers to deploying circular supply chains. By employing TISM, researchers were able to identify and structure the complex interrelationships among various barriers, providing a clear roadmap for organisations aiming to implement sustainable practices. This emphasises TISM's capacity to handle multifaceted

issues, offering a structured approach to dissecting and addressing challenges in dynamic environments.

Despite its strengths, TISM is not without limitations. The model relies heavily on expert judgement, which can introduce subjectivity into the analysis (Manjunatheshwara and Vinodh, 2018). Additionally, the complexity of the modelling process may pose challenges, particularly when dealing with large systems with numerous elements and relationships. To mitigate these challenges, it is essential to ensure a diverse and knowledgeable panel of experts and to employ systematic procedures for data collection and analysis. Furthermore, integrating TISM with other models, such as MICMAC analysis, can enhance the robustness of the findings by providing additional layers of validation.

2.5.4.8. Preference ranking organisation method for enrichment evaluation (PROMETHEE)

The Preference Ranking Organisation Method for Enrichment Evaluation (PROMETHEE), developed by Brans et al. in 1982, is a robust multi-criteria decision-making (MCDM) technique that has gained prominence for its ability to rank alternatives by considering both qualitative and quantitative factors. This flexibility makes it particularly well-suited for KRM, where diverse and sometimes intangible risks need to be assessed and prioritised. PROMETHEE facilitates pairwise comparisons among alternatives, allowing decision-makers to allocate weights to various criteria based on their significance and alignment with organisational priorities (Macharis et al., 2015).

A significant strength of PROMETHEE lies in its capacity for customisation. By assigning weights to individual risk factors, the model aligns the ranking process with the organisation's strategic objectives. For example, in a research-intensive organisation, knowledge retention risks might take precedence over operational risks (Albadvi et al., 2007), such as outdated systems, due to the critical role that knowledge assets play in driving innovation. This adaptability ensures that the evaluation framework is tailored to the specific context and goals of the organisation, enhancing its relevance and utility.

Another advantage of PROMETHEE is its ability to incorporate trade-offs between criteria. The visual representation tools associated with PROMETHEE, such as the GAIA plane, allow decision-

makers to visualise the relative positioning of alternatives and understand the trade-offs between competing priorities (Macharis et al., 2004). This ensures rational and informed decision-making, enabling organisations to justify their risk mitigation strategies comprehensively.

PROMETHEE has been applied across various domains to address complex decision-making challenges. For instance, it has been used in project management to rank risks associated with different project alternatives, aiding in resource allocation and planning. In the context of environmental management, PROMETHEE has helped prioritise ecological conservation strategies by balancing economic, social, and environmental criteria. These applications underscore its versatility and effectiveness in dealing with multi-faceted decision problems.

2.5.4.9. Selected MCDM models

Having evaluated the strengths and weaknesses of various MCDM models, the integration of DEMATEL, TISM, and PROMETHEE presents a comprehensive framework for tackling complex decision-making scenarios. Each of these models contributes distinctively, and their combined application may enhance the improvement in the assessment of knowledge risks.

DEMATEL could be particularly useful in mapping intricate causal relationships among knowledge risk factors. By distinguishing between cause-and-effect elements, it may enable the identification of pivotal risks with cascading impacts on other areas. This capability could provide valuable insights for prioritising interventions to mitigate systemic vulnerabilities. For example, Zekhnini et al. (2024) applied DEMATEL to assess risks associated with Supply Chain 5.0 digitalisation. Their study analysed the interdependencies and causal relationships between critical risks in digital supply chains, highlighting the importance of proactive management strategies to address emerging challenges and ensure the sustainability of supply chain operations. Similarly, this model could help in knowledge risk assessment by identifying key risks and their cascading effects, enabling organizations to better understand the interdependencies between these risks.

TISM could complement DEMATEL by establishing a hierarchical structure for the identified risks. It may help explain interdependencies and stratify risks into different levels, such as strategic versus operational, providing a structured approach for addressing them systematically. This

hierarchical modelling might be particularly valuable in analysing complex systems where understanding the layered nature of risks is critical for effective decision-making.

PROMETHEE has the potential to add another dimension by facilitating the ranking and prioritisation of risks based on organisational objectives and criteria. Its ability to handle both qualitative and quantitative data could allow for a nuanced assessment aligned with specific strategic goals. Prioritisation is essential for effective resource allocation and targeted risk mitigation. For example, Torbacki (2021) successfully used a hybrid MCDM model combining DEMATEL-based ANP (DANP) and PROMETHEE II to evaluate cybersecurity in Industry 4.0.

3. Research methodology

This chapter elaborates on the methodology employed in the thesis. It starts by introducing the research design, research philosophy, research approach, research strategy, methodological choice, time horizon and research techniques. The chapter concludes with a brief discussion of the ethical considerations that guided the research.

3.1. Research design

A research design serves as a framework for guiding the implementation of the research process (Bell et al., 2022). It provides a systematic plan and procedure that encompasses decisions ranging from broad assumptions to specific methods of data collection and analysis, all aimed at achieving the research objectives (Creswell and Creswell, 2017). Essentially, the research design can be considered as a blueprint that outlines a series of choices made to effectively address the research questions at hand. To illustrate these crucial decisions in the research design, Saunders et al. (2019) introduced the concept of the research onion, which serves as a visual representation of the different layers of decision-making. Each layer within the research onion model provides increasing levels of detail compared to the outer layers. The research onion begins with the layer pertaining to research philosophy, followed by research approaches, research strategies, choices, time horizons, and finally, research techniques and procedures. **Figure 8** highlights the specific choices made in this particular doctoral thesis and their justifications are given in the subsequent sub-sections.

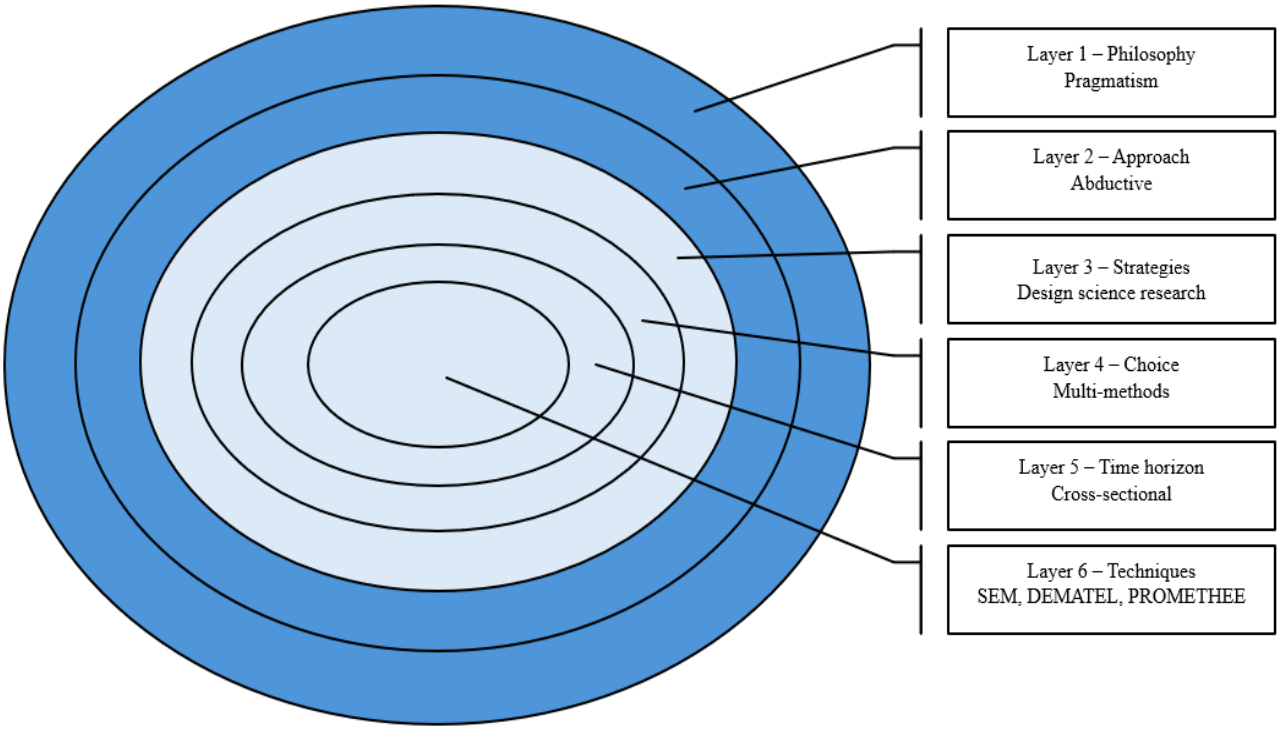


Figure 8 Research onion

Source: Adapted from Saunders et al. (2019)

3.2. Research philosophy

Research philosophy plays a role in establishing the reliability and credibility of the research process (Biedenbach and Müller, 2011). This is because a researcher's alignment with a specific philosophical stance—such as positivism, interpretivism, realism, or pragmatism—shapes the approach to inquiry and influences methodological choices (Henn et al., 2005). **Table 3** presents a brief comparison of these research philosophies. However, given my alignment with pragmatism, this section emphasises the pragmatist philosophy and illustrates how it informed and guided this research.

Table 3 Comparison between research philosophies

Research philosophy	**Ontology: the researcher's view of the nature of reality or being**	**Epistemology: the researcher's view regarding what constitutes acceptable knowledge**	**Data collection techniques: most often used**
Positivism	Reality exists independently of social actors and is objective.	Knowledge is derived from observable and measurable phenomena. Emphasis is on causality, generalisations, and simplification of phenomena.	Structured methods, large-scale sampling, and quantitative techniques; occasionally, qualitative methods.
Realism	Reality is objective and exists regardless of perception (realist), though social conditioning shapes its interpretation (critical realist).	Observable phenomena provide credible data, facts. Insufficient data means inaccuracies in sensations (direct realism). Alternatively, phenomena create sensations which are open to misinterpretation (critical realism). Focus on explaining within a context or contexts	Method choice is driven by context; can be quantitative or qualitative.
Interpretivism	Reality is socially constructed, subjective, and varies across individuals.	Subjective meanings and social phenomena. Focus upon the details of situation, a reality behind these details, subjective meanings motivating actions	Qualitative methods, small sample sizes, and in-depth exploration.
Pragmatism	External, multiple, view chosen to best enable answering of research question	Either or both observable phenomena and subjective meanings can provide acceptable knowledge dependent upon the research question. Focus on practical applied research, integrating different perspectives to help interpret the data	Mixed or multiple method designs, quantitative and qualitative

(Source: Adapted from Saunders et al. 2009)

As a researcher, I identify with pragmatism because my philosophical orientation stems from a focus on practical outcomes and a flexible approach to addressing research problems. Pragmatism, as a research philosophy, prioritises the use of methods and tools that are most effective for achieving the research objectives, rather than adhering strictly to a single methodological paradigm (Andersen and Mitchell, 2023). This orientation aligns closely with my research on knowledge risk assessment, where the complexity and multifaceted nature of the phenomenon required a combination of methods tailored to the specific demands of each research question.

This pragmatic perspective influenced my work on *Research Question 1*, where I sought to identify suitable models to address the limitations of existing frameworks and contribute to the development of an improved knowledge risk assessment framework. Recognising that no single method could fully address this complexity, I adopted a pluralistic approach. For instance, I used expert discussions and a structured matrix-style questionnaire to collect qualitative data, which was converted into a quantitative model using TISM, as detailed in *Article I*. This approach allowed me to explore how qualitative insights could inform a structured, objective model. Similarly, in *Article III* (Foli and Durst, 2022), I extended this exploration by conducting a literature review to identify key risk factors for knowledge leakage. The findings were refined through collaborative validation with case company participants, including employees and the CEO, and were subsequently modelled using ISM. In another study (Foli et al., 2023), I employed grey-DEMATEL to examine knowledge risks from a different methodological angle, further demonstrating the pragmatic principle of adapting methods to the needs of the research question. This methodological pluralism exemplifies how pragmatism enabled me to integrate subjective expert insights with rigorous modelling techniques, ensuring a thorough investigation of knowledge risks.

For *Research Question 2*, my pragmatist stance was evident in the development of a unified framework that integrated three distinct models — TISM, DEMATEL, and PROMETHEE. Each model was chosen for its specific strengths, and their integration was guided by the principle of utilising the most effective tools for achieving the research goal. By addressing the limitations of individual methods and leveraging their complementary strengths, I was able to construct a more comprehensive framework. This process reflects the core tenet of pragmatism: practical problem-solving through methodological adaptability.

In addressing *Research Question 3*, I applied pragmatism by combining subjective and empirical approaches to evaluate the proposed framework. Through brainstorming sessions and discussions with participants, I collected qualitative insights and empirical data to assess the framework's practicability. This approach aligns with the epistemological stance of pragmatism, which values both observable phenomena and subjective interpretations, depending on the needs of the research. By adapting my methods to the specific requirements of this research question, I ensured that my findings were grounded in both practical applicability and theoretical validity.

3.3. Research approach

Research approaches are categorised into three types: deductive, inductive, and abductive (Saunders et al., 2009). Deductive research begins with existing theories and tests their applicability or validity through empirical observations, often focusing on hypothesis testing to confirm or refine theoretical constructs. In contrast, inductive research builds theories or frameworks by observing patterns in empirical data and generalising these findings (Yin, 2009). Abductive research, however, combines elements of both, iteratively moving between theory and data to develop plausible explanations for observed phenomena. This doctoral thesis adopts an abductive approach, recognising its potential to bridge gaps between theoretical models and practical applications.

An abductive approach was particularly suited to this research for several reasons. First, the study begins by drawing on existing models, such as TISM, DEMATEL, and PROMETHEE, to address the complexities of knowledge risk assessment. These models provide a theoretical foundation for the research. However, as the study progresses, empirical observations from expert input informed modifications and refinements to the framework, reflecting the iterative nature of abductive reasoning. For example, in addressing *Research Question 1*, the research evaluates existing models to identify their strengths and limitations, using empirical insights to adapt these models for integration into a unified framework.

This abductive stance also shapes the responses to *Research Questions 2* and *3*. In developing and testing the unified framework, the research iteratively applies models to an organisational context, analysing empirical feedback to refine the framework. This process aligns with the abductive principle of oscillating between theory and practice, ensuring that the resulting framework is both theoretically sound and practically relevant.

3.4. Research strategy

According to Saunders et al. (2009), research strategies include surveys, case studies, grounded theory, ethnography, action research, experiments, and archival research. The choice of a research strategy can be determined by the research questions, the existing body of knowledge, available time and resources, and the researcher's philosophical stance.

Given these considerations, this research aligns with Design Science Research (DSR) as its strategy, aligning with the pragmatist philosophical stance underpinning this study. Design Science Research (DSR) is defined as "research that invents a new purposeful artefact to address a generalised type of problem and evaluates its utility for solving problems of that type" (Venable and Baskerville, 2012, p. 142). The iterative design, development, and evaluation of frameworks central to DSR (Peffers et al., 2007) align with the pragmatist ethos of achieving practical, actionable solutions while contributing to theoretical advancements.

While Järvinen (2007) argues that action research (AR) shares similar characteristics with DSR and may even be considered a part of it, other scholars, such as Iivari and Venable (2009), assert that AR and DSR are decisively distinct. Specifically, AR focuses on solving immediate, context-specific problems through a participatory approach, whereas DSR aims to create frameworks that address broader problem domains. This distinction underlines the suitability of DSR for this study, as the goal is to develop a framework that not only addresses the complexities of knowledge risk assessment but also offers generalisable insights for broader application.

3.5. Research choice

In alignment with my pragmatic stance and design science research as the research strategy, this study employs a multi-methods approach to address the research questions. A multi-methods approach integrates both qualitative and quantitative methodologies, providing the flexibility needed to explore complex phenomena such as KRM and enabling a comprehensive understanding of the research problem. This choice is particularly justified in the context of KRM, where addressing diverse and multi-faceted research questions often requires combining exploratory and confirmatory techniques.

The integration of qualitative and quantitative methods aligns with the iterative nature of DSR, where frameworks are designed, developed, and evaluated through multiple stages of research. For example, qualitative methods such as expert interviews and structured discussions were employed to gather in-depth insights and context-specific knowledge during the initial stages of framework development. These methods were instrumental in identifying key factors and components relevant to knowledge risk assessment, particularly in addressing Research Question 1. Quantitative methods, on the other hand, were utilised to model and validate these insights using tools such as TISM, DEMATEL, and PROMETHEE. This allowed for the systematic prioritisation and analysis of knowledge risks, addressing the practical and theoretical demands of *Research Questions 2* and *3*.

The choice of a multi-methods approach is also justified by its ability to balance the strengths of qualitative and quantitative methods. Qualitative methods provide the depth and flexibility required to explore emergent patterns, understand participants perspectives, and refine framework design. Quantitative methods offer the rigor and precision necessary for testing hypotheses, validating models, and generalising findings where appropriate. By combining these approaches, the study ensures both the richness of exploratory insights and the robustness of empirical validation.

Furthermore, adopting a multi-methods approach reflects the core principles of pragmatism, which emphasises methodological flexibility and the use of tools best suited to the research problem. Pragmatism rejects rigid adherence to a single methodology, instead advocating for a problem-centred approach that prioritises practical outcomes and actionable solutions. This approach was essential for bridging the gap between theory and practice in KRM.

3.6. Time horizon

The time horizon for this research was cross-sectional, as data collection occurred at specific points in time rather than over consistent intervals. This approach involved capturing data snapshots rather than tracking changes or trends over a prolonged period. For instance, in the complementary study, while participants were approached multiple times during data collection, the purpose was not to uncover temporal trends or repeatedly measure the same variables but rather to gather specific, contextually relevant insights. A similar cross-sectional approach was employed in *Articles I*, *II*,

and *III*, where data collection was designed to address particular aspects of the research questions within defined timeframes.

3.7. Research techniques

This section elaborates on the research techniques used to collect and analyse data, focusing on how these approaches were employed to address the research questions outlined in this study.

3.7.1. Structured questionnaires and discussion sessions

To address *Research Question 1*, which focuses on identifying the components required to develop a comprehensive framework for assessing knowledge risks, data collection utilised a combination of structured questionnaires and discussion sessions. These methods were specifically designed to collect data, establish contextual relationships among knowledge risks, and validate these relationships through iterative engagement with participants.

3.7.1.1. Structured questionnaires

Structured questionnaires were employed in the form of a matrix-style instrument (refer to *Article I*, *II*, and *III*). This approach allowed participants to evaluate the relationships among various knowledge risk factors systematically. The matrix format required respondents to indicate the presence and strength of relationships between pairs of risks, which is an important step in establishing contextual interdependencies. For example, in Article I, participants assessed how knowledge risks, particularly in ICT collaborative projects, such as cybercrime, outdated technologies, influenced digitisation risk, and so on. The data collected through these questionnaires provided the foundation for applying models like TISM, which relies on relational data to map hierarchical relationships among these risks.

The structured nature of the questionnaire ensured consistency across responses, enabling the collection of reliable and comparable data. The matrix format also facilitated the identification of nuanced relationships that may not emerge through open-ended questioning or unstructured methods. This approach is particularly well-suited to the complexity of knowledge risks, where

interdependencies among risk factors are critical to understanding their propagation and impact within an organisation.

3.7.1.2. Discussion sessions

Discussion sessions complemented the structured questionnaires by engaging participants in a more interactive and iterative process. These sessions included professionals and academics with expertise in KRM, as well as key stakeholders from the case company. The primary objectives of the discussion sessions were:

1. To validate the contextual relationships identified through the structured questionnaires.
2. To refine the understanding of specific knowledge risks and their interdependencies.
3. To incorporate organisational insights that may not be apparent through the literature or standalone questionnaires.

For instance, in *Article III*, discussion sessions helped to contextualise risks such as incomplete contracts and weak bring-your-own-device (BYOD) policies. Participants provided insights into how these knowledge risks manifested within the case company's operational environment, adding practical relevance to the theoretical relationships derived from the literature and questionnaires.

3.7.2. Data analysis

Given the nature of this research, the data analysis process is inherently tied to the modelling techniques employed for developing the framework. As the analysis forms an integral part of the application of these models, it will be discussed in alignment with the specific models used in this thesis. The following section presents a detailed explanation of these models and their role in the analytical process.

3.7.2.1. Total interpretive structural model (TISM)

Article I employs the Total Interpretive Structural Model (TISM) to evaluate knowledge risks and achieve an understanding of the interrelationships and multi-dimensional properties among these risks. TISM is a refined version of the widely recognised Interpretive Structural Modelling (ISM) technique. While ISM is traditionally used to analyse and visualise relationships and hierarchies among variables in a system (Sushil, 2012), TISM extends this capability by detailing the reasoning and interpretations behind these relationships. This added interpretive layer enhances the model's transparency, robustness, and applicability in complex tasks (Obi et al., 2020) such as assessment of knowledge risks.

TISM was selected for this research due to its unique strengths in analysing complex interdependencies among knowledge risks, a task that requires a systematic and nuanced approach. Knowledge risks often involve multiple layers of influence and interconnection, making traditional linear methods insufficient. TISM enables the development of a hierarchical model that identifies foundational risks – those with high driving power – and their influence on dependent risks. This structural analysis ensures that interventions can be directed at root causes, providing a cascading effect that mitigates multiple vulnerabilities simultaneously. By incorporating participants judgement into the modelling process, TISM bridges theoretical concepts with practical insights, making it an ideal method for addressing the research objectives.

The analytical process of TISM integrates elements of both deductive and inductive reasoning, making it a hybrid approach. Initially, the process draws on existing theories and prior research to identify relationships among variables (refer to Article I). This deductive phase ensures that the model is grounded in established principles, such as those derived from literature on knowledge risks. As the model evolves, participant input is introduced to refine and validate these relationships, adding an inductive dimension. This iterative refinement allows the model to adapt based on specific observations and feedback from participants, ensuring that it remains relevant to the organisational context. In this way, TISM leverages the strengths of both reasoning approaches, combining structured theoretical insights with empirical adaptability.

A critical aspect of TISM is the reliance on expert input, which plays a role in data collection and model refinement. Participants, selected for their specialised knowledge and experience in knowledge risk management, were engaged to provide judgements on the relationships between

variables. These judgements were collected through structured questionnaires and discussion sessions, designed to capture nuanced insights into how different knowledge risks interact. The input of participants was particularly important for validating and refining the relationships identified in the initial stages of the modelling process. Their feedback ensured that the model was both theoretically sound and practically applicable, improving its accuracy and validity.

The integration of participant insights not only validated the proposed relationships but also enhanced the model's contextual relevance. By incorporating organisational perspectives, TISM was able to address specific challenges faced by the case company, such as informal knowledge sharing and weak monitoring practices. This adaptability underscores the model's utility in aligning theoretical frameworks with real-world complexities, making it a valuable tool for knowledge risk assessment.

The outcome of applying TISM in this research was a hierarchical model that provided a detailed understanding of how knowledge risks are interconnected. This model served as a foundation for subsequent analytical techniques, enabling a comprehensive approach to knowledge risk management. By systematically combining deductive and inductive reasoning with expert validation, TISM proved to be a robust and flexible analytical tool, well-suited to the complexities of this study. The process of data analysis was seamlessly embedded in the modelling stages, ensuring that the findings were both reliable and actionable. Through its application, TISM contributed significantly to addressing the research questions, providing insights that are not only theoretically robust but also practically relevant to the field of knowledge risk management.

Table 4 Profile of experts

Sr No.	Expert	Position	Work experience (years)	Relevance of the participant to the current study
1	A	KM head	8	Involved in several collaborative projects both international and local level; small and large firms, with the use of ICT tools
2	B	Research scholar	2	Research focuses on knowledge risks, and also involved in projects with partners from different

				countries where means of communication and knowledge exchange were executed through various digital tools
3	C	KM specialist	6	Have managed company's knowledge-based and have also acted the role of a project manager in several projects

Source: Article I

3.7.2.2. Grey-DEMATEL

Similarly, *Article II* employed a MCDM approach. However, it utilises the grey-DEMATEL analysis to model knowledge risks specifically at the operational level of SMEs. The grey-DEMATEL analysis combines the principles of grey theory and the DEMATEL technique. The grey theory is known for its effectiveness in handling judgemental ambiguities (Baafi et al., 2021), while the DEMATEL technique is a valuable tool for establishing causal relationships among complex variables using matrices and graphs (Shao et al., 2016). The classic DEMATEL, however, may not adequately address problems associated with incomplete information, uncertainty, and subjective evaluation. Consequently, a grey-DEMATEL analysis has been developed as a combined methodology that enhances judgemental decisions through cause-effect diagrams (Rajesh and Ravi, 2017). This analytical tool proves particularly useful in resolving complex issues (Govindan et al., 2016), such as dealing with knowledge risks, which are typically dynamic (BrĂTianu, 2018).

Similar to TISM, the grey-DEMATEL analysis does not strictly fall under the category of either deductive or inductive reasoning. Instead, it belongs to the multivariate analysis methods used for decision-making and exploring relationships between variables. The grey-DEMATEL analysis operates through a distinct methodology that combines subjective and objective assessments to analyse complex relationships. Like in Article I, the utilisation of this analytical tool relies heavily on expert input. In the case (referred to *Article II*), the authors' insights and knowledge are integrated into the modelling process, emphasising their crucial role in the analysis.

3.7.2.3. PROMETHEE

The PROMETHEE approach, introduced by Brans et al. (1982), is a well-established outranking technique commonly used for managing MCDM problems. In contrast to other MCDM methods like TISM and DEMATEL, PROMETHEE incorporates several salient features that contribute to its effectiveness. First, it takes into account the importance of criteria, providing a means to showcase the relationship levels between criteria (Brans et al., 1986). This allows decision-makers to gain a comprehensive understanding of the relative significance of each criterion in the decision-making process. Second, PROMETHEE facilitates consensus-building among decision-makers with different perspectives, enabling them to reach agreement on the available alternatives (Brans et al., 1986). Lastly, the method is characterised by a clear logic and a simple computation process, enhancing its usability and practicality (Brans et al., 1986). In this study, the PROMETHEE approach is integrated with the previously applied MCDM modelling approaches, namely TISM and DEMATEL, to develop a novel methodology known as TISM-DEMATEL-PROMETHEE. This integrated methodology aims to evaluate knowledge risks comprehensively and effectively.

This model was applied in a complementary study to assess knowledge leakage risk factors within a case company. Data was gathered from participants through brainstorming and discussion sessions (refer to **Chapter 5**). The table below provides detailed information about the participants.

Table 5 Profile of participants

Position	**Work experience**
Director of Advisory	15+ years in consultancy or advisory roles, leadership in strategic planning.
Head of Advisory	10-15 years in advisory services, proven ability to lead cross-functional teams.
Senior Advisor	7-10 years in advisory roles, expertise in specialised sectors (e.g., finance, tech).
Senior Advisor	7-10 years in advisory roles, excellent problem-solving and stakeholder management.
Senior Advisor	7-10 years in advisory roles, strong track record in driving client outcomes.

Junior Economist	2-4 years in economic research or analysis, advanced skills in econometrics.
Junior Economist	1 year in economic research, experience in data modelling and forecasting.
Intern	Currently pursuing a relevant degree.

3.8. Ethical considerations

This doctoral research followed strict ethical standards at every stage, including for the individual articles that make up the thesis. Key ethical principles such as informed consent, confidentiality, privacy, and avoiding harm were observed to ensure the research was conducted responsibly. Although the study did not involve highly sensitive topics, these measures ensured its ethical integrity.

One important step was obtaining informed consent from all participants. Before taking part, participants were clearly informed about the study's purpose, the voluntary nature of their involvement, and their right to withdraw at any time without giving a reason or facing any consequences.

Confidentiality and privacy were also a priority. Participants' identities and the organisations they represented were kept anonymous. Data from questionnaires and discussion sessions were anonymised using measures like pseudonyms to protect sensitive information during analysis and reporting. All collected data were securely stored in an electronic database, accessible only to the researcher.

4. Studies of the Thesis

This part of the thesis includes the three articles of the thesis. The next section is dedicated to *Article I*, following *Article II*. Section 4.3 is then dedicated to *Article III*.

4.1. Study 1 - Total interpretive structural modelling (TISM) and MICMAC approach in analysing knowledge risks in ICT-supported collaborative project

Samuel Foli

Abstract

Purpose – As emphasised by the theory of knowledge-based view, knowledge constitutes the basic element for a firm's competitive advantage. Consequently, a firm's knowledge at risk could have an adverse effect on its performance. In this regard, this paper aims to investigate potential knowledge risks present in an (ICT)-supported collaborative project and establishes inter- and multi-relationships among these risks.

Design/methodology/approach – In this paper, an integrated approach using the total interpretive structural modelling (TISM) technique and MICMAC analysis is implemented to determine the hierarchical inter- relationships among knowledge risks and classify them according to their driving and dependence power.

Findings – The result reveals seven knowledge risks. The analysis establishes cybercrime and espionage as high drivers of knowledge risks in an ICT-supported collaborative project. Further, a comprehensive model is developed showing the hierarchical structure and multi- and inter-relationships among the analysed risks.

Practical implications – From a practical viewpoint, the proposed model in this study will be of great importance to practitioners because it highlights the most prominent knowledge risks in an ICT-supported collaborative project. Additionally, it will provide a clue for effective knowledge risk management in a systematic approach.

Originality/value – To the best of the author's knowledge, this is one of the first studies to use both the TISM technique and MICMAC analysis to identify and classify knowledge risks in an ICT-supported collaborative project.

Keywords Knowledge risk, Total interpretive structural modelling (TISM), MICMAC analysis, Technique, ICT-supported collaborative project

Paper type Conceptual paper

1. Introduction

The pandemic has amplified the essence for firms to collaborate even with their competitors. Firms from the USA, China and Germany, for example, collaborated by sharing knowledge to develop a vaccine against COVID-19 (New York Times, 2020). From both a theoretical and practical perspective, there are numerous reasons why firms collaborate. According to a Harvard Business Review published magazine:

[.. .] successful companies view each alliance as a window on their partners' broad capabilities [.. .] use the alliance to build skills in areas outside the formal agreement and systematically diffuse new knowledge throughout their organizations (Hamel et al., 1989, para. 7).

When firms collaborate, knowledge is being created, which is important for firms to gain new competitive advantages. Exchanges across organisational boundaries, however, can also result in losses of competitive knowledge or the disclosure of business insights to other companies or to competitors (North et al., 2020). Additionally, with increasing digitalisation of firms, digital technologies are increasingly used to enhance project collaboration; therefore, knowledge is more at risk within such an environment (Zeiringer and Thalmann, 2021; Durst and Ferenhof, 2014).

This paper aims to investigate potential knowledge risks in an information and communication technology (ICT)-supported collaborative project using total interpretive structural modelling (TISM) technique, as well as to determine the driving force and the dependence power of each risk, using Matriced' Impacts Croise's Multiplication Applique' e a UN Classement (MICMAC) analysis. Based on the aim of this paper, the following objectives are proposed:

- to identify and rank potential knowledge risks in ICT-supported collaborative project;
- to establish a mutual relationship, relative importance and interdependence of each risk with the help of the TISM technique; and
- to analyse the driving and dependence power of the knowledge risks by using MICMAC analysis.

Prior research has paid little attention to knowledge risks (Durst and Zieba, 2020; Durst, 2019). The existing literature has focused on the mitigation strategies for knowledge risks (Ferenhof, 2020; Durst et al., 2018; Durst and Ferenhof, 2016; Trkman and Desouza, 2012; Durst et al., 2020) and much less on analysis of the mutual relationships between knowledge risks. Studies (Delak and Damij, 2015) aimed at identifying and analysing potential knowledge risks do not provide a clear understanding of the relationship between them. Few of these studies that have identified and analysed knowledge risks have mainly relied on taxonomy to establish linkages of them (Durst and Zieba, 2017, 2019; Maniasi et al., 2006). But, taxonomy is not able to explain the interpretation of structural links, and it is not completely transparent. To overcome the limitations of taxonomy and fill the literature gap, the TISM technique has been applied to establish the relationships among risks and find out which of them are having strong dependence power (knowledge risks that mainly

depend on other knowledge risks) and driving power (knowledge risks that initiate other knowledge risks). The TISM technique is said to be robust in establishing complex interrelationships among variables in theory (Verma et al., 2018; Warfield, 1974). Conceptualisation and model building are made possible using this technique to transform an abstract or unstructured mental model into a well-articulated model. By incorporating the opinions of experts into the TISM technique, the author was also able to focus solely on the relevant risks in practice that are likely to be present in an ICT-supported collaborative project.

Next is a review of the literature and presentation of the theoretical background; Section 3 introduces the methodology of the study; Section 4 demonstrates the development of the model and presents the results; and conclusion covers the implications, limitations and future directions of the paper.

2. Literature review

2.1 ICT-supported collaborative project

A collaborative project involves two or more firms with different inputs working together, aiming to achieve a more successful result than if they had completed it individually (Bellini et al., 2019). However, in the case of an ICT-supported collaborative project, the internet plays an evitable role in the success of the project. The following are the main features of an ICT-supported collaborative project:

- improve communication among the partners;
- each partner contributes something distinctive;
- each partner is usually kept motivated and happy;
- use of project collaboration tools such as a spreadsheet; and
- collegiality among partners is present.

Hence, this study adopts the above features to describe a typical ICT-supported collaborative project.

2.2 Knowledge risk

Having studied the current body of knowledge on risk, it appears there are several definitions used and, to some extent, being proposed by scholars. In the context of this study, the present paper hinges on the definition given by Haimes (2009), describing risk as “a measure of the probability and severity of adverse effects” (p. 1648).

On the other hand, knowledge risk can be defined as the possibility of any loss related to the identifying, storing or protecting of knowledge that may decrease an organisation's operational or strategic ability to achieve its goals (Perrott, 2007). Literature suggests (Durst and Zieba, 2019) three broad categories of knowledge risks: human, technological and operational. Nevertheless, the study discusses some specific risks under these broad categories as described in the following sections.

2.3 Cybercrime

Cybercrime is recognised as a man-made risk (Soomro and Hussain, 2019) orchestrated by internet fraudsters to carry out illegal activities within the cyber community, leading to undesirable effects on organisations (Paoli et al., 2018). The illegal activities include the spread of viruses, malware and unethical hacking. In the occurrence of cybercrime, knowledge intended to stay within the confines of an organisation is illegally appropriated by an outsider (e.g. hacker, fraudster), which in effect leads to knowledge loss. Past studies (Durst and Zieba, 2019, 2020) have emphasised the direct linkage cybercrime has with knowledge loss.

2.4 Digitalisation

As businesses begin to gravitate towards digital solutions, the need for digital security should also be of equal concern to them because digitalisation as a model exposes businesses to greater risk. The term digitalisation refers to the use of digital technologies and their integration into business products and services (Björkdahl, 2020). Considering the complexity of business operations and processes that have been in existence over the past decades, the concept of digitalisation was meant to restore balance in the business sphere; however, it rather appears digitalisation has its own repercussions in which knowledge loss is one of them (Lan, 2007). Extant studies (Durst and Zieba, 2020; Jansen, 2016) acknowledge that businesses implementation of digitalisation could pose a risk to trigger knowledge loss.

2.5 Social network sites

A social network site (SNS) is a virtual community where users can create individual public profiles, interact with real-life friends and meet other people based on shared interests (Kim and Shen, 2020). SNS is usually connected with Web-based services to effectively function. These Web-based services allow individuals to connect with others through software, application or cloud technology that provides standardised Web protocols to interoperate, communicate and exchange data messaging (Wolf et al., 2018).

The common types of SNS widely used by billions of people globally are Facebook, WhatsApp, Twitter and LinkedIn. Because of the wide range of users on these platforms, organisations are strategically adopting SNS to reach their potential customers and engage with partners. However, SNS also has the potential to leak important business secrets to the outside world (Annansingh, 2020). Also, studies by Sarigianni et al. (2015) and Temel and Durst (2021) have empirically demonstrated the association between employee SNS usage and knowledge risks.

2.6 Outsourcing

A myriad of studies (Hoecht and Trott, 2006; Mahmoodzadeh et al., 2009) have confirmed that outsourcing, typically operational outsourcing, exposes organisations to knowledge risk. During the course of outsourcing, the focal organisation is more expected to share knowledge with the outsourcee (supporting firm) to ensure that services being solicited are rendered appropriately. As a result, valuable secrets within the focal organisation get leaked unknowingly to the outsourcee (Durst and Ferenhof, 2014), which can have a detrimental impact on the focal organisation's competitiveness.

Durst and Zieba (2019) identified outsourcing as a knowledge risk because it involves transferring part of the business function to an external party of which the organisation (focal) has limited supervision and control over their activities. In this case, less is known by the focal organisation as to whether the knowledge transmitted to the external party is used purposely for the required task only, and more importantly, the knowledge is securely protected and void of exposure to any third party. Empirical evidence shows that outsourcing, in any form or shape (e.g. strategic alliance), poses knowledge risks (Inkpen et al., 2019; Ferenhof et al., 2016).

2.7 Espionage

There is no unified definition in the literature as far as espionage is concerned. As a matter of fact, espionage definition varies from one context to the other; hence, by virtue of this study, espionage is defined as the act of spying into a company's private vault to appropriate its intellectual property without its consent (Fischer et al., 2019). In recent times, espionage has been tied to cybercrime, popularly known as cyber espionage, as its fertile ground to operationalise is on the internet (Wangen, 2015). According to Durst and Zieba (2019), competition among businesses is what breeds espionage activities and in turn, present knowledge at risk.

2.8 Communication

In a simple term, communication is a process of exchange of ideas, information and knowledge between two persons or in a group. In the business context, communication involves negotiation,

socialisation and exchange of knowledge between employees within and outside the business (Gibson, 2002). In the process of communication, there is a tendency of revealing material knowledge to the outsider unknowingly, which in effect could result in knowledge loss. Hence, communication has been recognised as a tool (risk) to instigate knowledge loss (Christina et al., 2016)

2.9 Outmoded technologies

One of the key facilitators of knowledge loss is the use of outmoded technologies (Wong et al., 2021). Most often technologies are updated when experts identify flaws in the technology architecture, which could likely expose businesses to risks. Therefore, businesses are expected to ensure constant updates of their existing technologies, however, even if there is a need for a major overhaul they ought to do so to prevent undesirable risks. A study by Durst and Zieba (2019) indicates that outmoded technology and knowledge risk are inseparable.

3. Method

Over the past years, researchers have used a plethora of techniques, emerging from both non-statistical and statistical assumptions, to establish relationships among items of variables and constructs. In this study, the author implemented the TISM technique to investigate knowledge risks and also to better understand the inter- and multi-relationship properties that exist among these risks. Figure 1 illustrates concrete steps underlying the TISM technique application in this study. The MICMAC analysis was then used as a complementary tool for categorisation of the risks under investigation.

TISM technique is a modified version of the known interpretive structural modelling (ISM). With the ISM technique, variables are identified and processed through simple structural modelling to establish connectivity within a given system (Obi et al., 2020; Sushil, 2012). In the case of the TISM technique, variables are identified in a similar fashion; however, it involves an interactive learning process where logical insights are derived from a given complex system for theory building (Menon and Suresh, 2020). Hence, Obi et al. (2020, p. 369) described the TISM technique as:

[...] a qualitative modeling technique that builds upon the strengths of interpretive structural modeling (ISM) technique by providing in the model the logical explanation of how the factors link with each other and allowing for an explicit explanation of the links (direct and transitive) in the model.

While, the application of MICMAC analysis reveals the indirect relationships among variables (Dhir and Sushil, 2017).

Unlike the other qualitative analysis techniques, e.g. thematic, that investigate patterns in data to establish relationships among themes, the TISM technique applies the structural self- and pair-wise interaction matrix to connect variables (Obi et al., 2020) based on their relations and further align them in hierarchical order according to their driving and dependence power (Kedia and Sushil, 2013). The application of the TISM technique is not alien to the social science discipline, especially in the area of knowledge management (Dhir and Dhir, 2020; Lim et al., 2017; Singh et al., 2003; Singh and Kant, 2007, 2008).

4. Model development and results

Drawing on the extant literature using a systematic review process, several potential knowledge risks were discovered. However, through discussion and brainstorming with industry and academia experts (Appendix), seven knowledge risks were deemed likely to be present in an ICT-supported collaborative project (Table 1).

To develop the model of knowledge risk, the risks identified were analysed to establish connection and disconnection through critical thinking and reflection with support from the

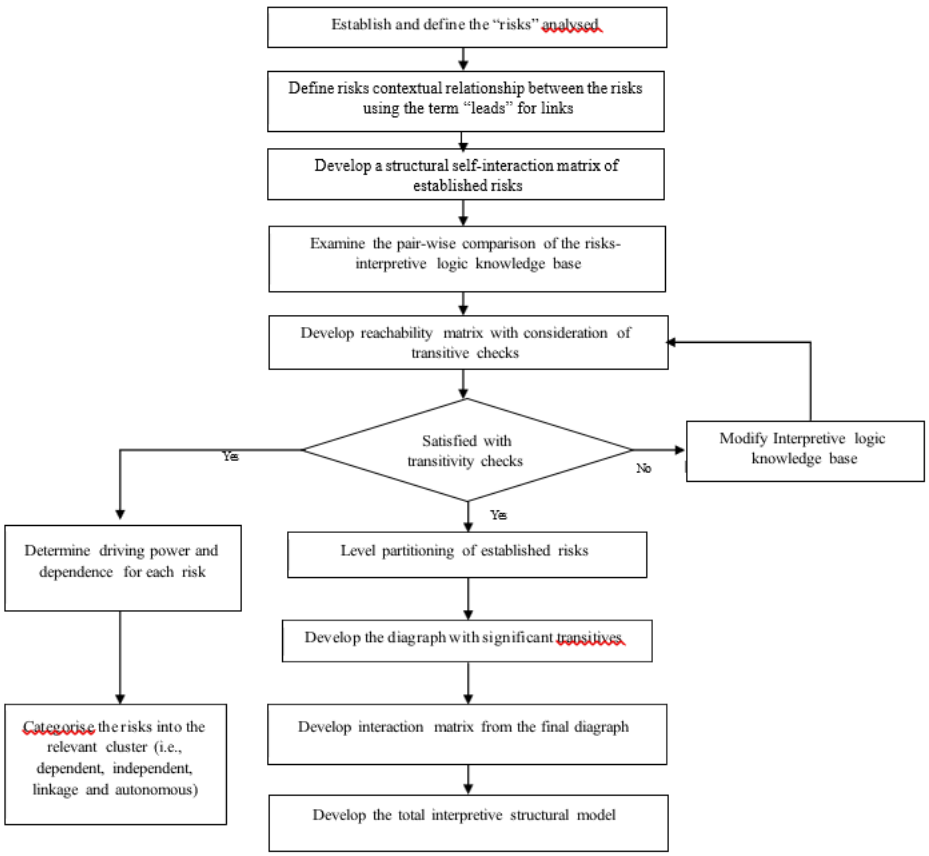


Figure 1. TISM technique

Source: Adapted from Obi et al. (2020)

experts. Using the phrase “will A1 leads to A2” or the reverse statement “will A2 leads to A1”, the contextual relationships were formulated. To meet the TISM technique criteria, the relationship interpretation was carried out through a thorough evaluation of the knowledge risks identified by checking the effects each one of them would have on the other, as illustrated by Table 2. This process is regarded as the distinguishing factor between ISM and TISM techniques (Dhir and Dhir, 2020). Moreover, Table 2 depicts the variable codes assigned to the risk variables for the study.

As a result of the analysis of the expert views, an interpretive logic matrix was developed, which was converted into binary values to develop an initial reachability matrix, and a transitivity check was performed to generate the final reachability matrix (Table 3). The table explains the nature of the relationships that exist among the risks. From the result, it is observed that there is a more direct type of relationship among the risks than that of the indirect relationships, which are being represented by the transitivity relationships (“1*”). As there are many relationships in the system, it demonstrates that risks associated with knowledge are closely related and complex in nature (Durst and Zieba, 2019). The dependence and driving forces were also computed for each of the risks.

Table 1. Knowledge risks in an ICT-supported collaborative project

S. no.	Risks	Operational definition	Literature support
1	Cybercrime	Risk of exposure to critical knowledge within a cyberspace as a result of cyberattacks	Durst *et al.* (2019), Durst and Zieba (2019, 2020), Jennex and Durcikova (2020), Renaud *et al.* (2019), Tan *et al.* (2016) and Temel and Durst (2021)
2	Digitalisation	Risk of exposure to critical knowledge as projects are exclusively delivered within a digitalised platform	Christina *et al.* (2016), Durst *et al.* (2019), Durst and Zieba (2019, 2020) and Temel and Durst (2021)
3	SNS	A form of risk that is caused through the disclosure of critical knowledge in an informal way mostly facilitated by the use of SNSs	Christina *et al.* (2016), Durst *et al.* (2019), Durst and Zieba (2019, 2020), Eugene Jennex (2014), Massingham (2008) and Temel and Durst (2021)
4	Outsourcing	Risk of exposure to knowledge as a result of outsourcing work packages of the project to a third-party such as creation of website	Bahli and Rivard (2003), Durst and Ferenhof (2014), Durst *et al.* (2019), Durst and Zieba (2019, 2020), Inkpen *et al.* (2019), Jiang *et al.* (2013), Ritala *et al.* (2015), Tan *et al.* (2016), Temel and Durst (2021) and Zhang *et al.* (2018)
5	Espionage	A risk resulting from a form of commercial intelligence gathering, usually, but not exclusively, on the part of industry competitors, which could indirectly or directly affect partners in a collaborative project	Chan (2003), Durst and Zieba (2019, 2020), Jennex and Durcikova (2020), Temel and Durst (2021) and Whitman and Mattford (2019)
6	Communication	Risk of exposure to critical knowledge due to ease and frequency of communication	Christina *et al.* (2016), Durst and Zieba (2019, 2020), Jiang *et al.* (2013) and Temel and Durst (2021)
7	Outmoded technologies	Risk associated with the use of obsolete technologies such as out-of-date or expired software	Durst and Zieba (2019, 2020) and Tan *et al.* (2016)

Source: Compiled by the author

Table 2. Identifying relationships between risks and interpretations

Risk code	Risk	Contextual relationship Will Risk A1 leads Risk A2 . . . A7?	Interpretation How do you think Risk A1 leads Risk A2 . . . A7?
A1	Cybercrime		
A2	Digitalisation		
A3	SNSs		
A4	Outsourcing		
A5	Espionage		
A6	Communication		
A7	Outmoded technologies		

Source: Compiled by author

The partition of risk level, as shown in Table 4, was generated from the final reachability matrix. According to the result, two dependent iterations were executed till all the risks were fully partitioned according to their respective levels. Two sets of levels were discovered: Level 1 consists of A1 and A5, and Level 2 comprises A2, A3, A4, A6 and A7.

After application of the TISM technique, the MICMAC analysis was also performed to categorise the risks into various clusters of common properties. The MICMAC analysis grouped the risks into two main clusters, namely, linkage and dependent clusters. This was operationalised using the driving and dependence power derived from the final reachability matrix, as shown in Figure 2. The risks located in the dependent cluster are A1 and A5, whereas the risks within the linkage cluster are A2, A3, A4, A6 and A7.

5. Discussion

The objective of this study is to investigate potential knowledge risks and, more importantly, to understand the relationships among these risks. The result of the study reveals seven potential knowledge risks, namely, cybercrime, digitalisation, SNS, outsourcing, espionage, communication and outmoded technologies. The key findings of the study are the TISM model (Figure 3) showing the hierarchical structure and multi- and inter-relationships among the identified risks

Table 3. Final reachability matrix

Risk	A1	A2	A3	A4	A5	A6	A7	Driving power
A1	1	0	0	0	1	0	0	2
A2	1	1	1	1*	1	1	1	7
A3	1	1	1	1	1	1	1	7
A4	1	1	1	1	1	1	1*	7
A5	1	0	0	0	1	0	0	2
A6	1	1*	1	1	1	1	1*	7
A7	1	1*	1*	1	1	1	1	7
Dependence	7	5	5	5	7	5	5	39

Note: 1* denotes transitivity relationship

Table 4. Partition of risk level

Risk	Reachability	Antecedent	Intersection	Level
Iteration 1				
A1	1,5	1,2,3,4,5,6,7	1,5	1
A2	1,2,3,4,5,6,7	2,3,4,6,7	2,3,4,6,7	
A3	1,2,3,4,5,6,7	2,3,4,6,7	2,3,4,6,7	
A4	1,2,3,4,5,6,7	2,3,4,6,7	2,3,4,6,7	
A5	1,5	1,2,3,4,5,6,7	1,5	1
A6	1,2,3,4,5,6,7	2,3,4,6,7	2,3,4,6,7	
A7	1,2,3,4,5,6,7	2,3,4,6,7	2,3,4,6,7	
Iteration 2				
A2	2,3,4,6,7	2,3,4,6,7	2,3,4,6,7	2
A3	2,3,4,6,7	2,3,4,6,7	2,3,4,6,7	2
A4	2,3,4,6,7	2,3,4,6,7	2,3,4,6,7	2
A6	2,3,4,6,7	2,3,4,6,7	2,3,4,6,7	2
A7	2,3,4,6,7	2,3,4,6,7	2,3,4,6,7	2

Source: Compiled by author

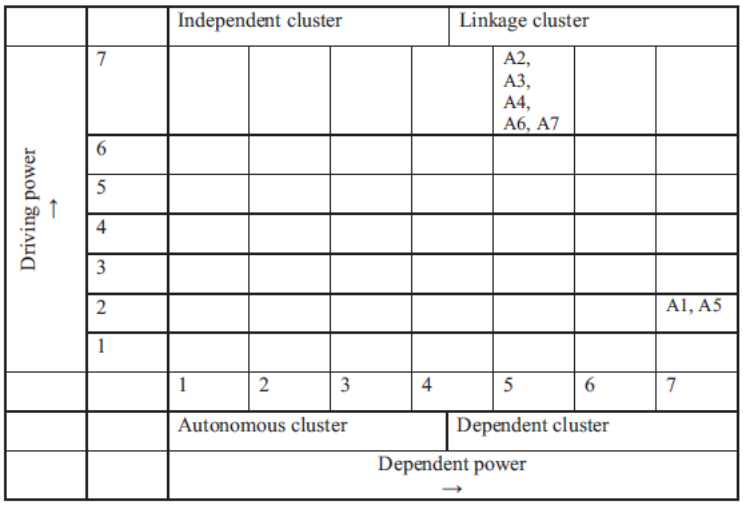


Figure 2. MICMAC analysis

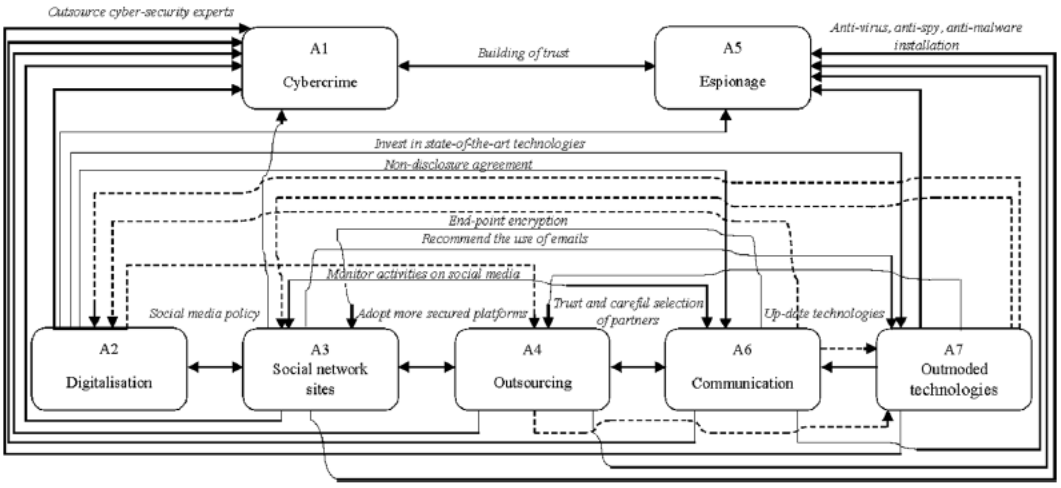


Figure 3. Total interpretive structural model of knowledge risks (hierarchical model)

and classification of risks using MICMAC analysis. In the model, cybercrime and espionage are positioned at the top level. This implies that cybercrime and espionage are dependent on other risks, which means that any action of other risks will somewhat affect these risks. In the same vein, it also implies that the occurrence of other risks, to some extent, triggers the occurrence of cybercrime and espionage.

The result suggests that digitalisation, SNSs, outsourcing, communication and outmoded technology strongly influence cybercrime and espionage in an ICT-supported collaborative project. The results of this study align with the Zeiringer and Thalmann (2021) study, which evaluated knowledge risks in a data-centric environment. Research by Durst and Zieba (2019) who also examined knowledge risks and discovered using a concept map that risks related to old technologies, espionage and digitalisation, among others, can be linked to cybercrime. Also, comparing the findings of previous studies (Chan, 2003; Whitman and Mattford, 2019), it appears that espionage usually takes place within a networked system. Due to this, for espionage to pose a threat to knowledge, the availability of digitalised platforms is necessary. Further, outmoded technologies pose a threat to knowledge because the security needed to guarantee protection is not adequate. Thus, it is easier for a third party to compromise the system, thereby putting the knowledge of the partners at risk.

According to the MICMAC analysis, cybercrime and espionage are categorised under dependent cluster; thus, aside from their high dependency, they possess low driving power. This implies that other risks such as digitalisation, SNS, outsourcing, communication, outmoded technologies have a high effect on cybercrime and espionage, while these same risks (cybercrime and espionage) have very little influence on other risks. Also, it is worth noting that cybercrime and espionage share the same level of risk (linked by a double arrow in the model), which is directly related to previous studies (Freet and Agrawal, 2017; Gragido and Pirc, 2011; Wangen, 2015).

The second level of the model is occupied by risks from digitalisation, SNS, outsourcing, communication and outmoded technologies. These risks are categorised under a linkage cluster depicting high driving power and low dependent power, as validated by the MICMAC analysis. High driving power implies that these risks have a greater influence on other risks, i.e. cybercrime and espionage, as illustrated in the model. According to the result, digitalisation has a strong relationship with SNSs, while SNSs and communication both pose the same risks. In part, this can be explained by the shift away from traditional email and telephone communication to social networks. Outsourcing often requires communication – the models demonstrate that the risks of outsourcing and communication are the same, but the situation exacerbates when tools used for communicating are outdated and have weak security features.

A closer look at the connecting lines (Figure 3) provided additional insight into the strength of the relationships among the risks identified. While lines without dashes signify stronger links and line with dashes indicate weaker links between risks, it is observed that outmoded technologies has a stronger link to communication, however, there is a weak link connecting communication to outmoded technologies. The risk effect of outmoded technologies is stronger on communication while the inverse is weak. It is interesting to note that all knowledge risks categorised under linkage demonstrate direct effects on both cybercrime and espionage. No effect is observed, whether direct or indirect, from risks under the dependent cluster on the linkage cluster. Following the above discussion, it is clear that knowledge risks have both inter- and multi-relationships. As such, knowledge risk management (KRM) should be considered systematically and holistically, rather than in isolation (Durst and Zieba, 2019), which in turn, maximise organisational performance (Durst et al., 2019)

Having mathematically modelled knowledge risks using TISM and MICMAC analysis, the author suggested concrete countermeasures to deal with these risks (Figure 3). According to Durst and Ferenhof (2014), firms need to take the time to carefully select their partners and build trust before participating in any form of partnership. As emphasised, collaborated projects, which mostly over-rely on the use of digital platforms, pose a danger to partners' critical knowledge because such an environment facilitates the easy exchange of knowledge. In terms of cybercrime, handling such risks is quite technical, so Durst and Zieba (2020) recommend firms to hire or outsource cyber-analysts who are expert in their field to build strong cyber-architectures and firewall systems to prevent them from being compromised. Although outsourcing comes along with risk; however, this risk is inactive when there is trust building over time. Tse et al. (2014) argue that using more secure platforms and updated technologies for communication are the effective ways to mitigate knowledge risks. Furthermore, the authors emphasise that a ban on the use of SNSs at work as a safety precaution is an effective strategy to curb knowledge risks. In cases where partners are required to engage through the use of SNSs, the implementation of encryption (Sarigianni et al.,

2015) could help prevent possible cyber-attacks. Typically, in any ICT-supported collaborative project, the collaborative tools used are often agreed upon by the partners before the project begins. Therefore, to avoid unnecessary exposure to other risks, it is recommended that partners use and stick to these tools as much as possible. Another important mechanism recognised by Serna et al. (2017) that could control knowledge risk is non-disclosure agreements and patents. In a non-disclosure agreement, all partners are legally bound not to act inappropriately on information or knowledge exchange as a way to take advantage on the other partner.

6. Implications

Besides fulfilling the objectives of this study – identifying potential knowledge risks; evaluating and analysing multi- and inter-relationships among the risks; constructing a hierarchical structure for the risks based on their driving and dependence power – the results have enormous implications to theory. The present paper extends the literature of knowledge risk through the application of TISM technique and MICMAC analysis. TISM technique and MICMAC analysis are widely used in multiple fields for conceptualisation purposes and to answer fundamental questions of theory building, such as "what", "how" and "why", outlined by Whetten (1989). In this paper, the "what" question has been answered through identification of knowledge risks based on literature and experts' opinions, while the "how" and "why" questions have been addressed by demonstrating the strength and power of these risks through interpretive analysis.

Practitioners in this field could also use this model as a reference point in their development of risk management strategies. The seven risks identified with key characteristics will serve as an awareness guide for industry players to better understand the nature of certain kinds of risks organisations are exposed to, to give more priority to these risks while constructing a risk management framework. The study results show that cybercrime and espionage are the most significant risks, so strategies to mitigate knowledge risks should be implemented with a highest priority on reducing these risks rather than attempting to manage all risks. The MICMAC diagram, which shows the driving and dependence power, offers valuable insights about the threat and interdependency of these knowledge risks for managements who are keenly interested in ensuring knowledge is protected. Lastly, the concrete countermeasures proposed in this study will assist managers with novel strategies into handling knowledge risks.

7. Conclusion

In this paper, the author reviewed knowledge risks based on the literature and recommendations from experts to enhance the understanding of knowledge risks. The study has advanced research in the area of knowledge risk through theory building by implementing the TISM technique and

MICMAC analysis. It examined the inter- and multi-relationship between knowledge risks in an ICT-supported collaborative project through thorough discussions and deliberation among experts from both academia and industry. Taking into account the context, the present study contributes to collaboration literature by identifying specific knowledge risks based on their relevance and level of dependency within an ICT- supported collaborative project. To the best knowledge of the author, this study is the first of its kind to investigate knowledge risks in an ICT-supported collaborative project environment.

Although the paper makes several useful contributions both theoretically and to practice, it has some shortcomings. As it has always been, the major limitation of every conceptual paper is its inadequate ability to confirm and validate proposed findings/models due to inadequate or lack of empirical data. This paper is no exception to this rule. For that reason, the author proposes to future researchers to consider testing the model through a wide range of data using a survey. To strengthen the theoretical validation, other statistical techniques such as structural equation modelling may be used, with the moderating effects of the size of the collaboration partners. Turning to longitudinal case study approach will also be of great importance to especially practitioners to better understand knowledge risks because risk, generally, is dynamic and changes over a time period (Williams and Durst, 2019). The knowledge risks identified in this study may not be exhaustive. Future research could investigate other forms of knowledge risks and their types, which would expand on what has been established in this study.

References

Annansingh, F. (2020), “Bring your own device to work: how serious is the risk?”, Journal of Business Strategy, Vol. 42 No. 6, pp. 392-398, doi: 10.1108/JBS-04-2020-0069.

Bahli, B. and Rivard, S. (2003), “The information technology outsourcing risk: a transaction cost and agency theory-based perspective”, Journal of Information Technology, Vol. 18 No. 3, pp. 211-221.

Bellini, E., Piroli, G. and Pennacchio, L. (2019), “Collaborative know-how and trust in university–industry collaborations: empirical evidence from ICT firms”, The Journal of Technology Transfer, Vol. 44 No. 6, pp. 1939-1963, doi: 10.1007/s10961-018-9655-7.

Björkdahl, J. (2020), “Strategies for digitalization in manufacturing firms”, California Management Review, Vol. 62 No. 4, pp. 17-36.

Chan, M. (2003), “Corporate espionage and workplace trust/distrust”, Journal of Business Ethics, Vol. 42 No. 1, pp. 45-58.

Christina, S., Stefan, T. and Markus, M. (2016), “Protecting knowledge in the financial sector: an analysis of knowledge risks arising from social media”, presented at the 2016 49th HI International Conference on System Sciences (HICSS), IEEE, Koloa, HI, USA, pp. 4031-4040.

D, S.K. and Vinodh, S. (2020), "TISM for analysis of barriers affecting the adoption of lean concepts to electronics component manufacture", International Journal of Lean Six Sigma, Vol. 11 No. 6, pp. 1127-1159, doi: 10.1108/IJLSS-09-2018-0100.

Delak, B. and Damij, N. (2015), "Knowledge risk assessments", Presented at the 2015 European Conference on Knowledge Management, Academic Conferences International Limited, p. 997.

Dhir, S. and Dhir, S. (2020), "Modeling of strategic thinking enablers: a modified total interpretive structural modeling (TISM) and MICMAC approach", International Journal of System Assurance Engineering and Management, Vol. 11 No. 1, pp. 175-188.

Dhir, S. and Sushil, (2017), "Flexibility in modification and termination of cross-border joint ventures", Global Journal of Flexible Systems Management, Vol. 18 No. 2, pp. 139-151.

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

Durst, S. and Ferenhof, H.A. (2014), "Knowledge leakages and ways to reduce them in small and medium-sized enterprises (SMEs)", Information, Vol. 5 No. 3, pp. 440-450, available at: www.mdpi.com/2078-2489/5/3/440

Durst, S. and Ferenhof, H.A. (2016), "Knowledge risk management in turbulent times", in North, K. and Varvakis, G. (Eds), Competitive Strategies for Small and Medium Enterprises, Springer International Publishing, Cham, pp. 195-209.

Durst, S. and Zieba, M. (2017), "Knowledge risks – towards a taxonomy", International Journal of Business Environment, Vol. 9 No. 1, pp. 51-63, doi: 10.1504/ijbe.2017.084705.

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

Durst, S. and Zieba, M. (2020), "Knowledge risks inherent in business sustainability", Journal of Cleaner Production, Vol. 251, p. 119670.

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

Durst, S., Lindvall, B. and Bruns, G. (2020), "Knowledge risk management in the public sector: insights into a Swedish municipality", Journal of Knowledge Management, Vol. 24 No. 4, pp. 717-735, doi: 10.1108/JKM-12-2017-0558.

Durst, S., Zieba, M. and Ferenhof, H.A. (2018), "Knowledge risk management in organizations", IFKAD 2018-13th International Forum on Knowledge Asset Dynamics, 4-6 July, Delft.

Eugene Jennex, M. (2014), "A proposed method for assessing knowledge loss risk with departing personnel", VINE, Vol. 44 No. 2, pp. 185-209.

Ferenhof, H.A. (2020), “Toyota kata approach – a way to mitigate knowledge risks in start-ups”, in Durst, S. and Henschel, T. (Eds), Knowledge Risk Management from Theory to Praxis, Springer, Cham, pp. 33-47.

Ferenhof, H.A., Durst, S. and Selig, P.M. (2016), “Knowledge waste and knowledge loss? What is it all about?”, Navus - Revista de Gestão e Tecnologia, Vol. 5 No. 4, pp. 38-57.

Fischer, R.J., Halibozek, E.P. and Walters, D.C. (2019), “Selected security threats of the 21st century”, Introduction to Security, Elsevier, Butterworth-Heinemann, Oxford, pp. 487-505.

Freet, D. and Agrawal, R. (2017), “Cyber espionage”, in Schintler, L.A. and McNeely, C.L. (Eds),

Encyclopedia of Big Data, Springer International Publishing, Cham, pp. 1-5.

Gibson, R. (2002), Intercultural Business Communication: An Introduction to the Theory and Practice of Intercultural Business Communication for Teachers, Language Trainers, and Business People, OUP, Oxford.

Gragido, W. and Pirc, J. (2011), “1 - Cybercrime and espionage and the new security 101”, in Gragido, W. and Pirc, J. (Eds), Cybercrime and Espionage, Syngress, Boston, pp. 1-20.

Haimes, Y.Y. (2009), “On the complex definition of risk: a systems-based approach”, Risk Analysis, Vol. 29 No. 12, pp. 1647-1654.

Hamel, G., Doz, Y.L. and Prahanland, C.K. (1989), “Collaborating with your competitor and win”,

Harvard Business Review, January-February, pp. 133-139.

Hoecht, A. and Trott, P. (2006), “Outsourcing, information leakage and the risk of losing technology- based competencies”, European Business Review, Vol. 18 No. 5, pp. 395-412.

Inkpen, A., Minbaeva, D. and Tsang, E.W.K. (2019), “Unintentional, unavoidable, and beneficial knowledge leakage from the multinational enterprise”, Journal of International Business Studies, Vol. 50 No. 2, pp. 250-260.

Jansen, C. (2016), “Developing and operating industrial security services to mitigate risks of digitalization”, IFAC-PapersOnLine, Vol. 49 No. 29, pp. 133-137.

Jennex, M. and Durcikova, A. (2020), “Creating sustainable knowledge systems: towards a risk and threat assessment framework”, Journal of Strategic Innovation and Sustainability, Vol. 15 No. 4, pp. 138-152, doi: 10.33423/jsis.v15i4.2965.

Jiang, X., Li, M., Gao, S., Bao, Y. and Jiang, F. (2013), “Managing knowledge leakage in strategic alliances: the effects of trust and formal contracts”, Industrial Marketing Management, Vol. 42 No. 6, pp. 983-991.

Kedia, P.K. and Sushil, (2013), "Total interpretive structural modelling of strategic technology management in automobile industry", presented at the 2013 Proceedings of PICMET '13: Technology Management in the IT-Driven Services (PICMET), pp. 62-71.

Kim, C. and Shen, C. (2020), "Connecting activities on social network sites and life satisfaction: a comparison of older and younger users", Computers in Human Behavior, Vol. 105, p. 106222.

Kumar, H., Singh, M.K. and Gupta, M.P. (2019), "A policy framework for city eligibility analysis: TISM and fuzzy MICMAC-weighted approach to select a city for smart city transformation in India", Land Use Policy, Vol. 82, pp. 375-390, doi: 10.1016/j.landusepol.2018.12.025.

Lan, P. (2007), "Tapping tacit knowledge on a digital platform", International Journal of Learning and Intellectual Capital, Vol. 4 No. 3, p. 315.

Lim, M.K., Tseng, M.-L., Tan, K.H. and Bui, T.D. (2017), "Knowledge management in sustainable supply chain management: improving performance through an interpretive structural modelling approach", Journal of Cleaner Production, Vol. 162, pp. 806-816.

Mahmoodzadeh, E., Jalalinia, S. and Nekui Yazdi, F. (2009), "A business process outsourcing framework based on business process management and knowledge management", Business Process Management Journal, Vol. 15 No. 6, pp. 845-864.

Maniasi, S., Britos, P. and García-Martínez, R. (2006), "A taxonomy-based model for identifying risks", Paper presented at the JIISIC.

Massingham, P. (2008), "Measuring the impact of knowledge loss: more than ripples on a pond?",

Management Learning, Vol. 39 No. 5, pp. 541-560.

Menon, S. and Suresh, M. (2020), "Total interpretive structural modelling: evolution and applications", in Raj, J.S., Bashar, A. and Ramson, S.R.J. (Eds), Innovative Data Communication Technologies and Application, Springer International Publishing, Cham, Vol. 46, pp. 257-265.

New York Times (2020), "Search for coronavirus vaccine becomes a global competition", available at: www.nytimes.com/2020/03/19/us/politics/coronavirus-vaccine-competition.html (accessed 29 March 2020).

North, K., De Carvalho, A.B., Braccini, A.M., Durst, S., Carvalho, J.Á., Gräslund, K. and Thalmann, S. (2020), "Knowledge risks in supply chain interactions of SMEs: an exploratory study", 2019 Knowledge Management in Digital Work Environments, State-of-the-Art and Outlook, WM 2019, 18 March 2019 through 20 March 2019, Gesellschaft für Informatik, Potsdam, Germany, pp. 161-171.

Obi, L., Hampton, P. and Awuzie, B. (2020), "Total interpretive structural modelling of graduate employability skills for the built environment sector", Education Sciences, Vol. 10 No. 12, p. 369, doi: 10.3390/educsci10120369.

Paoli, L., Visschers, J. and Verstraete, C. (2018), “The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium”, Crime, Law and Social Change, Vol. 70 No. 4, pp. 397-420.

Perrott, B.E. (2007), “A strategic risk approach to knowledge management”, Business Horizons, Vol. 50 No. 6, pp. 523-533.

Renaud, K., Von Solms, B. and Von Solms, R. (2019), “How does intellectual capital align with cyber security?”, Journal of Intellectual Capital, Vol. 20 No. 5, pp. 621-641.

Ritala, P., Olander, H., Michailova, S. and Husted, K. (2015), “Knowledge sharing, knowledge leaking and relative innovation performance: an empirical study”, Technovation, Vol. 35, pp. 22-31.

Sarigianni, C., Thalmann, S. and Manhart, M. (2015), “Knowledge risks of social media in the financial industry”, International Journal of Knowledge Management, Vol. 11 No. 4, pp. 19-34.

Serna, C.A., Bosua, R., Maynard, S. and Ahmad, A. (2017), “Addressing knowledge leakage risk caused by the use of mobile devices in Australian organizations”, PACIS 2017 Proceedings, available at: https://aisel.aisnet.org/pacis2017/224

Singh, M.D. and Kant, R. (2007), “Knowledge management barriers: an interpretive structural modeling approach”, presented at the 2007 IEEE International Conference on Industrial Engineering and Engineering Management, pp. 2091-2095.

Singh, M.D. and Kant, R. (2008), “Knowledge management barriers: an interpretive structural modeling approach”, International Journal of Management Science and Engineering Management, Vol. 3 No. 2, pp. 141-150.

Singh, Shankar, R., Narain, R. and Agarwal, A. (2003), “An interpretive structural modeling of knowledge management in engineering industries”, Journal of Advances in Management Research, Vol. 1 No. 1, pp. 28-40.

Soomro, T.R. and Hussain, M. (2019), “Social media-related cybercrimes and techniques for their prevention”, Applied Computer Systems, Vol. 24 No. 1, pp. 9-17.

Sushil, (2012), “Interpreting the interpretive structural model”, Global Journal of Flexible Systems Management, Vol. 13 No. 2, pp. 87-106.

Tan, K.H., Wong, W.P. and Chung, L. (2016), “Information and knowledge leakage in supply chain”, Information Systems Frontiers, Vol. 18 No. 3, pp. 621-638.

Temel, S. and Durst, S. (2021), “Knowledge risk prevention strategies for handling new technological innovations in small businesses”, VINE Journal of Information and Knowledge Management Systems, Vol. 51 No. 4, pp. 655-673.

Trkman, P. and Desouza, K.C. (2012), “Knowledge risks in organizational networks: an exploratory framework”, The Journal of Strategic Information Systems, Vol. 21 No. 1, pp. 1-17, doi: 10.1016/j.jsis.2011.11.001.

Tse, D.W.K., To, D.H., Chen, X., Huang, Z., Qin, Z. and Bharwaney, S. (2014), “An Investigation of how businesses are highly influenced by social media security”, in Wang, L.S.L., June, J.J., Lee, C.H., Okuhara, K. and Yang, H.C. (Eds), Multidisciplinary Social Networks Research, MISNC 2014, Communications in Computer and Information Science, Springer, Berlin, Heidelberg, Vol. 473, pp. 311-324, doi: 10.1007/978-3-662-45071-0_25.

Verma, A., Seth, N. and Singhal, N. (2018), “Application of interpretive structural modelling to establish interrelationships among the enablers of supply chain competitiveness”, Materials Today: Proceedings, Vol. 5 No. 2, pp. 4818-4823.

Wangen, G. (2015), “The role of malware in reported cyber espionage: a review of the impact and mechanism”, Information, Vol. 6 No. 2, pp. 183-211, doi: 10.3390/info6020183.

Warfield, J.N. (1974), “Developing interconnection matrices in structural modeling”, IEEE Transactions on Systems, Man, and Cybernetics, Vol. SMC-4 No. 1, pp. 81-87.

Whetten, D.A. (1989), “What constitutes a theoretical contribution?”, The Academy of Management Review, Vol. 14 No. 4, pp. 490-495.

Whitman, M.E. and Mattford, H.J. (2019), Management of Information Security, 6th ed., Cengage Learning, Boston, MA.

Williams, C. and Durst, S. (2019), “Exploring the transition phase in offshore outsourcing: decision making amidst knowledge at risk”, Journal of Business Research, Vol. 103, pp. 460-471, doi: 10.1016/j.jbusres.2018.01.013.

Wolf, M., Sims, J. and Yang, H. (2018), “Social media? What social media?”, UK Academy for Information Systems Conference Proceedings 2018, available at: https://aisel.aisnet.org/ukais2018/3

Wong, W.-P., Tan, K.H., Govindan, K., Li, D. and Kumar, A. (2021), “A conceptual framework for information-leakage-resilience”, Annals of Operations Research, Vol. ahead-of-print No. ahead-of-print, pp. 1-21, doi: 10.1007/s10479-021-04219-5.

Zeiringer, J.P. and Thalmann, S. (2021), “Knowledge sharing and protection in data-centric collaborations: an exploratory study”, Knowledge Management Research and Practice, Vol. ahead-of-print No. ahead-of-print, pp. 1-13, doi: 10.1080/14778238.2021.1978886.

Zhang, Y., Liu, S., Tan, J., Jiang, G. and Zhu, Q. (2018), “Effects of risks on the performance of business process outsourcing projects: the moderating roles of knowledge management capabilities”, International Journal of Project Management, Vol. 36 No. 4, pp. 627-639.

Appendix

Drawing inspirations from a study by D. and Vinodh's (2020) regarding the minimum number of experts' opinions for the TISM, this study conveniently solicited opinions from three experts; two from the industry and one from academia. Using two out of three as a benchmark (Kumar, 2019), seven knowledge risks passed this stage. The results were based on the experts' past experience regarding project collaboration using ICT tools (Table A1).

Table A1. Experts' opinion on knowledge risks

Rank	Prominent risks identified in the literature	Experts' opinion
1	Cybercrime	3 out of 3
2	Digitalisation	3 out of 3
3	SNS	3 out of 3
4	Outsourcing	3 out of 3
5	Espionage	3 out of 3
6	Outmoded technologies	2 out of 3
7	Communication	2 out of 3
8	Unlearning	1 out of 3
9	Hoarding	1 out of 3
10	Relational	1 out of 3
11	Forgetting	1 out of 3
12	Hiding	1 out of 3

Table A2. Profile of experts

Sr no.	Expert	Position	Work experience (years)	Relevance of the participant to the current study
1	A	KM head	8	Involved in several collaborative projects both international and local level; small and large firms, with the use of ICT tools
2	B	Research scholar	2	Research focuses on knowledge risks, and also involved in projects with partners from different countries where means of communication and knowledge exchange were executed through various digital tools
3	C	KM specialist	6	Have managed company's knowledge-based and have also acted the role of a project manager in several projects

4.2. Study 2 - Evaluation of Operational Knowledge Risks in SMEs — Using a Grey-Dematel Technique

Samuel Foli

Susanne Durst

Elena Dominguez Romero

Abstract.

The increasing recognition of the negative impact of knowledge risks on the operations of small and medium-sized enterprises (SMEs) has led to a need for effective methods to evaluate and manage these risks. SMEs often adopt a reactive approach to risk management, which may not be sufficient to address the complex and evolving nature of knowledge risks. This study aims to use the grey-DEMATEL technique to evaluate operational knowledge risks in SMEs, with a focus on identifying the most critical risks and their potential causes and effects. The results revealed 11 operational knowledge risks, and found that outsourcing risks are the most critical among them. Communication risks and improper knowledge application were also found to be significant. Additionally, these risks were successfully categorised into effect risks (including relational risk, espionage, knowledge waste, and continuity risk) and causal risks (including knowledge waste, risks related to knowledge gaps, and the risk of using obsolete or unreliable knowledge). These categories provide a framework for understanding the potential causes and effects of operational knowledge risks and may be useful for designing risk management strategies. To the best of the authors' knowledge, this is one of the first studies to use the grey-DEMATEL technique to evaluate operational knowledge risks in SMEs.

Keywords: Grey-DEMATEL technique; operational knowledge risk; knowledge risk management; KRM; small and medium-sized enterprises; SMEs.

1. Introduction

In recent years, disruptions to operations have become a major concern for many organisations, particularly smaller ones (Allianz Global Corporate and Specialty, 2022). The gravity of this issue has prompted organisations to galvanise their operations strategy with risk evaluation frameworks in order to be prepared for any possible contingencies. More specifically, evaluation of knowledge risks can be useful in this context, as many of these risks can disrupt day-to-day business operations if not addressed in a timely manner. In previous studies (e.g. Durst and Zięba, 2019; Temel and Durst, 2020), these risks have been classified as operational knowledge risks.

Organisations of all sizes and types recognise the potential negative impact knowledge risks can have on their day-to-day operations, however, small- and medium-sized enterprises (SMEs), due to the limited resources available to them (Durst and Ferenhof, 2014), are particularly disadvantaged in taking pragmatic measures to address them. A further concern is the interrelationships between these risks (Foli, 2022) that can lead to a complex and time-consuming evaluation process, which typically requires the involvement of a specialised team. For SMEs, this may not be a viable option.

Research indicates that our understanding of knowledge risks is in its infancy since this research field is still relatively new (Durst et al., 2020; Massingham, 2008). Moreover, while operational knowledge risks have received less research attention, literature on their evaluation/assessment is limited. The majority of previous studies (e.g. Durst and Zięba, 2019, 2020; Tsang and Lee, 2018) has been conceptual in nature, and have primarily focused on the identification of knowledge risks and recommending measures for mitigating them. Apart from the admission that research on knowledge risks is underdeveloped, there is less emphasis placed on SMEs (Temel and Durst, 2020). In this regard, there is a knowledge gap in the field regarding the evaluation of operational knowledge risks in SMEs. Yet, the evaluation of operational knowledge risks in SMEs is important owing to the fact that operations constitute a unique subunit within SMEs and constitute a major function for the creation of value. Additionally, in the event of a disruption, operations are the first to be affected.

Against this background, the aim of the paper is to enrich the knowledge risks research by comprehensively evaluating potential knowledge risks that SMEs face in their operations. More specifically, this study builds on Temel and Durst's (2020) research using the grey-DEMATEL technique to estimate the prominence values of operational knowledge risks and the degree of interaction between them.

Although there are few studies that examine the interrelationships between knowledge risks based on taxonomies (e.g. Durst and Zięba, 2019; Hammoda and Durst, 2022; Temel and Durst, 2020) or multi-criteria decision-making models such as interpretive structural modelling (ISM) (Foli, 2022; Foli and Durst, 2022) and analytic hierarchy process (AHP) (Tsang et al., 2016). For example, Foli

(2022) establishes the inter- and multi-relationship among potential knowledge risks within an ICT-supported collaborative project. Even though the ISM identifies structural relationships among risks, it does not indicate the prominence of those relationships (Sufiyan et al., 2019). By using DEMATEL, we can determine the position of each operational knowledge risk and its influence over one another, and therefore determine which risk is most influential (Bakir et al., 2018; Biswas and Gupta, 2019; Vishvakarma et al., 2022). However, it has some limitations regarding the subjectivity and impreciseness of experts' inputs (Zavadskas et al., 2008). By integrating the grey theory with DEMATEL, these limitations can be eliminated (Haleem et al., 2019).

The paper is structured as follows. The following section provides an over- view of the knowledge risks SMEs are exposed to at the operational level. This is followed by the method used for this study with a clear step-by-step application of the grey-DEMATEL technique. The results are then presented and discussed. The paper concludes with a conclusion and future research directions.

2. Theoretical Framework

2.1. Knowledge risks

There is great variation in how risk is perceived according to culture, context, and discipline (Zheng, 2017). Risks can be viewed from a wider and narrower perspective. Risks from a wider perspective describe uncertain future events; they can be positive and negative (Brustbauer, 2016). The ISO 31000:2018 standard defines risk as "the effect of uncertainty on objectives" (ISO, 2018). According to this definition, risks are not limited to harmful events, but the focus is more on the impact of risks on the organisations' objectives (Leitch, 2010). Risks from a narrower perspective are mainly seen as financial loss due to uncertainty. Risk and uncertainty are closely connected as the former does not exist without the latter (Hetland, 2003).

As the acceptance of risks forms part of every business activity (Heinze and Henschel, 2021) discussions around risks are closely connected to organisational decision-making. With regard to the types of risks to be addressed, organisations should focus on both financial and non-financial risks (Durst, 2013). In the past, the focus has primarily been on financial risks, recent research however reveals an increasing interest in the study of risks related to knowledge, intangibles, and intellectual capital (e.g. Brunold and Durst, 2012; Durst, 2013; Durst and Zięba, 2019; Harvey and Lusch, 1999). In considering both risks related to tangibles and intangibles, such as knowledge risks, it is expected to have a more balanced and holistic picture of firms' operations and their risk-bearing capacity (Stam, 2009). Even though the study of knowledge risks is still in its infancy, there are already a few studies (e.g. Durst et al., 2020; Massingham, 2010; Zieba et al., 2022) that have empirically demonstrated the connection between knowledge risks and different forms of performance. Trkman and Desouza (2012) defined knowledge risk "as a likelihood of any loss from an event connected with the identification, storage or protection of knowledge that may decrease the operational or strategic benefit of any party involved in the network" (p. 5). And according to

Durst and Zięba (2019), knowledge risks can be classified into three major categories: human, technological, and operational. The knowledge risk taxonomy proposed by these authors suggests that there are not only many operational knowledge risks but that these risks are also significantly influenced (amplified or triggered) by the risks of the other two dimensions.

In a later study, Durst and Zięba (2020) tried to establish the link between knowledge risks and business sustainability by taking advantage of the taxonomy proposed in their 2019 paper. Operational knowledge risks accounted for a significant share of the possible risks faced by organisations in the quest for sustainability, for example, knowledge waste, knowledge gaps, communication risks, and risk of knowledge acquisition are among those that have the potential to affect all three pillars of organisational sustainability.

2.2. Knowledge risks in small- and medium-sized enterprises (SMEs)

As crucial as SMEs are to global economic development (Surya et al., 2021), there is no universal definition of what SMEs are (Thu, 2020). In the literature, SMEs are typically specified in terms of quantitative or qualitative definitions. The quan- titative definition of SMEs determines their classification as micro-, small-, and medium-sized based on indicators such as the number of employees, turnover per annum, and balance sheet per annum (Belghitar et al., 2021; Durst et al., 2022).

There are weaknesses to this quantitative definition; as some scholars (e.g. Bouchard and Basso, 2011; Thu, 2020) have criticised the indicator of the number of employees as misleading because a firm's growth does not necessarily correspond to the hiring of employees. Furthermore, there is a wide variation in the threshold across contexts. According to the European Commission (2008), SMEs cannot have more than 249 employees, whereas in the United States, the threshold is 500 (the United States International Trade Commission, 2010). These and many other reasons have led to a qualitative approach being considered in the definition of SMEs. In the qualitative definition, SMEs are considered to be businesses with independent owners and are often operated by those owners (Buculescu, 2013). Additionally, scholars (e.g. Foli et al., 2022; Haselip et al., 2014; Storey, 2016) tend to use the disadvantages of SMEs as a way to define them, such as their resource constraints and inability to attract and retain talent.

It is evident from the various definitions and characteristics of SMEs that the liability of smallness, which refers to limitedness resources and capabilities, is what distinguishes SMEs generally. The liability of smallness of SMEs leaves them more vulnerable than large companies to knowledge risks, which limits their ability to take a proactive or dedicated approach to reduce these risks (Eggers, 2020). Research has revealed that SMEs are generally less concerned about knowledge risks, and most do not have a single strategy to deal with them. In contrast to larger organisations, which possess the necessary resources to address knowledge risks holistically, SMEs can benefit from operational knowledge risk management, which is more risk-averse and focuses on protecting

day-to-day operations. In addition to this, the structure and nature of SMEs, in general, make them even more susceptible to operational knowledge risks, emphasising their importance in this context.

Among all other studies (e.g. Durst and Zieba, 2019, 2020) on knowledge risks that have dealt with the classification of knowledge risks into operational, techno- logical, and human dimensions, Temel and Durst's (2020) work appears to be the first to focus exclusively on small businesses; though some overlaps are evident.

Hence, this paper draws on the operational knowledge risks presented in Temel and Durst's (2020) paper. Table 1 provides a summary of these risks.

3. Method

In this research, a grey-based DEMATEL technique is used to assess operational knowledge risks. The grey-based DEMATEL technique encompasses the grey theory

Table 1. An overview of the operational knowledge risks.

Risk code	Knowledge risk	Meaning
K01	Knowledge waste	Loss of strength from reinventing the wheel when not using the available knowledge (Durst and Ferenhof, 2016; Zieba, 2020).
K02	Risks related to knowledge gaps	Situations in which a lack of knowledge prevents the organization from performing its most vital functions (Durst *et al.*, 2017).
K03	Relational risks	Arising from opportunistic behaviour by partners (Coras and Tantau, 2013; Delerue, 2005).
K04	Outsourcing risks	Caused by the fact that organisations tend to rely too heavily on their outsourced firms, which slows internal knowledge management (Coras and Tantau, 2013; Durst and Ferenhof, 2014; North *et al.*, 2020; Tan *et al.*, 2016).
K05	Risk of using obsolete/ unreliable knowledge	Risks of using stale knowledge which might negatively influence the organisation's new way of doing things (North *et al.*, 2020; Zięba and Durst, 2018).
K06	Risk of improper knowledge application	Risks because of misunderstanding which lead to undesired organisational agenda (Temel and Durst, 2020; Zięba and Durst, 2018).
K07	Espionage	Risks resulting from unlawfully spying and retrieving organizational critical knowledge (North *et al.*, 2020; Zięba *et al.*, 2021).
K08	Continuity risks	Risks because of a firm's inability to maintain its core capabilities over time (Temel and Durst, 2020).
K09	Communication risks	Risks of nuances within communication channels between two parties (Coras and Tantau, 2013; Durst and Leyer, 2014; Zięba *et al.*, 2021).
K10	Knowledge acquisition risks	Risks associated with an organisation's ability to acquire new knowledge (Temel and Durst, 2020; Zięba *et al.*, 2021).
K11	Knowledge transfer risks	Risks that emanate from the inability of employees to effectively transfer knowledge among colleagues (Al-Jabri and Al-Busaidi, 2018; Durst and Zięba, 2017).

and decision-making trial and evaluation laboratory (DEMATEL) technique. The grey theory is effective in dealing with ambiguities in judgments (Fu et al., 2001). Whereas the DEMATEL is an essential tool to establish causal relationships among complex variables using matrices and graphs (Shao et al., 2016). Hence, a grey-based DEMATEL technique is a combined methodology that enhances judgmental decisions using cause-effect diagraphs (Rajesh and Ravi, 2017). As Lee et al. (2021) suggest that most risk evaluation is governed by judgmental opinion and choice, so it is appropriate to use a grey-based DEMATEL technique in this study. In addition, this technique helps resolve complex issues (Govindan et al., 2016; Khan et al., 2020; Seker et al., 2017) such as dealing with knowledge risks, which are typically dynamic (Bratianu, 2018). Previous research has demonstrated that the grey-based DEMATEL technique is typically applied using input and opinions from a small group of experts on the topic. In this study, inputs and opinions were solicited solely from the authors, who have extensive experience in knowledge risks, particularly among SMEs.

Concrete steps using the Grey-DEMATEL technique

- Step 1: Develop a grey direct-relation matrix

To develop the grey direct-relation matrix, an initial direct relationship matrix is formulated using the evaluation of risk $r = \{\text{ri} \mid i = 1, 2,\ldots,n\}$ by k through pairwise comparisons using the linguistic scale. Table 2 shows the five-point linguistic scale and its associated grey numbers. This initial direct relationship matrix is converted into a grey initial direct relationship matrix by transforming the linguistic terms into the corresponding grey numbers. Hence, the k number of the grey direct relationship matrix Z is obtained. The element of the grey direct-relation matrix is represented as $\otimes Zij$ (i.e. risk i influence j).

- Step 2: Formulate the normalised grey direct-relation matrix

The overall grey relation matrix is transformed into the normalised grey direct- relation matrix (see Table 3) N using the following equations:

$$\otimes s = \left[\underline{s}, \underline{s}\right] = \frac{1}{\max\limits_{0 \le i \le n} = \sum_{j=0}^{n} \otimes Z_{ij}} \quad i, j = 1, 2, 3, \ldots, n, \tag{1}$$

Table 2. Grey linguistic scale.

Linguistic terms	Grey numbers
No influence (No)	[0, 0]

Low influence (L)	[0, 0.25]
Medium influence (M)	[0.25, 0.5]
High influence (H)	[0.5, 0.75]
Very high influence (VH)	[0.75, 1]

Source: Adapted from Liu *et al.* (2020).

Table 3. Normalised grey direct-relation matrix of risk (K).

Risks	K01	K02	K03	K04	K05	K06	K07	K08	K09	K10	K11
K01	[0, 0]	[0, 0.03]	[0, 0]	[0.09, 0.09]	[0.13, 0.12]	[0, 0.03]	[0.13, 0.12]	[0.09, 0.09]	[0, 0]	[0, 0]	[0.09, 0.09]
K02	[0.13, 0.12]	[0, 0]	[0, 0]	[0.13, 0.12]	[0, 0.03]	[0.13, 0.12]	[0.04, 0.06]	[0.13, 0.12]	[0, 0]	[0.13, 0.12]	[0, 0]
K03	[0, 0]	[0, 0]	[0, 0]	[0.09, 0.09]	[0, 0]	[0.09, 0.09]	[0.13, 0.12]	[0, 0]	[0, 0]	[0, 0.03]	[0.04, 0.06]
K04	[0, 0.03]	[0, 0]	[0.13, 0.12]	[0, 0]	[0, 0.03]	[0.04, 0.06]	[0.13, 0.12]	[0.13, 0.12]	[0.09, 0.09]	[0.09, 0.09]	[0.13, 0.12]
K05	[0.13, 0.12]	[0.09, 0.09]	[0, 0]	[0, 0]	[0, 0]	[0.13, 0.12]	[0, 0]	[0.09, 0.09]	[0.04, 0.06]	[0, 0.03]	[0, 0]
K06	[0.13, 0.12]	[0, 0]	[0, 0.03]	[0, 0]	[0.09, 0.09]	[0, 0]	[0.04, 0.06]	[0.09, 0.09]	[0, 0]	[0.09, 0.09]	[0, 0]
K07	[0, 0]	[0, 0.03]	[0, 0.03]	[0, 0]	[0, 0]	[0, 0]	[0, 0]	[0.13, 0.12]	[0, 0]	[0, 0]	[0.09, 0.09]
K08	[0, 0]	[0, 0]	[0, 0]	[0.13, 0.12]	[0, 0]	[0, 0]	[0, 0]	[0, 0]	[0, 0]	[0, 0]	[0, 0]
K09	[0.13, 0.12]	[0, 0.03]	[0.13, 0.12]	[0.09, 0.09]	[0.13, 0.12]	[0.13, 0.12]	[0.13, 0.12]	[0, 0.03]	[0, 0]	[0.13, 0.12]	[0.13, 0.12]
K10	[0, 0]	[0.09, 0.09]	[0, 0]	[0, 0]	[0.04, 0.06]	[0.09, 0.09]	[0, 0]	[0.04, 0.06]	[0, 0]	[0, 0]	[0, 0]
K11	[0, 0]	[0.04, 0.06]	[0.09, 0.09]	[0.13, 0.12]	[0, 0.03]	[0.04, 0.06]	[0, 0]	[0.04, 0.06]	[0, 0]	[0, 0]	[0, 0]

Source: Compiled by authors.

Table 4. Total relation matrix of the risks (K).

Risks	K01	K02	K03	K04	K05	K06	K07	K08	K09	K10	K11
K01	[0.028, 0.043]	[0.019, 0.062]	[0.031, 0.04]	[0.134, 0.146]	[0.141, 0.149]	[0.039, 0.084]	[0.16, 0.16]	[0.163, 0.18]	[0.018, 0.022]	[0.02, 0.037]	[0.124, 0.132]
K02	[0.164, 0.165]	[0.021, 0.035]	[0.031, 0.038]	[0.187, 0.179]	[0.046, 0.087]	[0.169, 0.176]	[0.104, 0.122]	[0.218, 0.218]	[0.018, 0.022]	[0.166, 0.164]	[0.051, 0.053]
K03	[0.017, 0.025]	[0.006, 0.019]	[0.022, 0.033]	[0.109, 0.119]	[0.013, 0.026]	[0.103, 0.12]	[0.156, 0.153]	[0.058, 0.066]	[0.01, 0.012]	[0.021, 0.058]	[0.075, 0.095]
K04	[0.032, 0.077]	[0.021, 0.042]	[0.169, 0.17]	[0.079, 0.085]	[0.03, 0.082]	[0.099, 0.134]	[0.185, 0.185]	[0.21, 0.219]	[0.095, 0.104]	[0.118, 0.136]	[0.179, 0.178]
K05	[0.177, 0.173]	[0.096, 0.114]	[0.017, 0.027]	[0.058, 0.063]	[0.046, 0.056]	[0.164, 0.171]	[0.051, 0.058]	[0.154, 0.167]	[0.051, 0.07]	[0.038, 0.076]	[0.035, 0.039]
K06	[0.153, 0.148]	[0.02, 0.031]	[0.008, 0.044]	[0.039, 0.044]	[0.115, 0.124]	[0.031, 0.043]	[0.073, 0.095]	[0.138, 0.151]	[0.008, 0.012]	[0.097, 0.109]	[0.026, 0.032]
K07	[0.002, 0.01]	[0.005, 0.039]	[0.013, 0.046]	[0.034, 0.041]	[0.002, 0.01]	[0.008, 0.021]	[0.007, 0.016]	[0.15, 0.15]	[0.003, 0.004]	[0.005, 0.013]	[0.093, 0.102]
K08	[0.004, 0.009]	[0.003, 0.005]	[0.022, 0.021]	[0.141, 0.132]	[0.004, 0.01]	[0.013, 0.016]	[0.024, 0.022]	[0.027, 0.026]	[0.012, 0.013]	[0.015, 0.016]	[0.023, 0.022]
K09	[0.19, 0.191]	[0.039, 0.089]	[0.173, 0.178]	[0.17, 0.183]	[0.184, 0.193]	[0.208, 0.22]	[0.214, 0.21]	[0.139, 0.179]	[0.023, 0.028]	[0.171, 0.183]	[0.198, 0.194]
K10	[0.035, 0.04]	[0.095, 0.104]	[0.005, 0.01]	[0.028, 0.032]	[0.06, 0.084]	[0.112, 0.122]	[0.019, 0.025]	[0.082, 0.106]	[0.005, 0.008]	[0.025, 0.03]	[0.009, 0.011]
K11	[0.02, 0.037]	[0.049, 0.075]	[0.115, 0.123]	[0.178, 0.174]	[0.013, 0.058]	[0.076, 0.108]	[0.048, 0.054]	[0.182, 0.184]	[0.016, 0.019]	[0.031, 0.043]	[0.036, 0.039]

Source: Compiled by authors.

$$N = \otimes\ s * Z, \tag{2}$$

$$\otimes n_{ij}\left[\underline{s} * \otimes z_{ij}, \underline{s} * \otimes z_{ij}\right]. \tag{3}$$

- Step 3: Compute the total relation matrix

The total relation matrix T (see Table 4) is determined by using following equation:

$$T = N\,(I - N)^{-1}, \tag{4}$$

where I is the identity matrix.

Step 4: Compute the causal parameters

The causal parameter is determined using the following equations:

$$\otimes R_i = \sum_{j=1}^{n} t_{ij}\theta_i, \tag{5}$$

$$\otimes C_j = \sum_{i=1}^{n} t_{ij}\theta_j. \tag{6}$$

$\otimes R_i$ represents the direct and indirect influence of the risks i over the other risks, and $\otimes C_j$ represents the influence received by risk j by the other risk.

- Step 5: Calculate the prominence (P_i) and net effect (E_i)

The prominence (P_i) and net effect (E_i) of the risks are determined using the following equations:

$$\otimes P_i = \otimes R_i + \otimes C_i, \quad i = j, \tag{7}$$

$$\otimes E_i = \otimes R_i - \otimes C_i, \quad i = j. \tag{8}$$

The causal relationship diagraph is developed using the net effect value (shown in Table 5). A positive value of $\otimes E_i$ shows the net effect (cause) of the risk on the system and a negative value represents the net effect on the risks caused by the system.

4. Findings and Discussion

Based on the grey-DEMATEL analysis, the degree of prominence is determined for each risk, and each risk is classified into a "cause" and "effect" category.

On the basis of the calculated net cause/effect values (see Table 5 and Fig. 1), the causal (operational knowledge) risks can be categorised as follows: outsourcing risks (K04) > communication risks (K09) > knowledge waste (K01) > risk of using obsolete/unreliable knowledge (K05) > risks related to knowledge gaps (K02). Among these causal risks, outsourcing risks (K04) are the most influential in the causal category, thus suggesting that outsourcing risks are the most important causal (operational knowledge) risks. As emphasised in several studies

Table 5. Prominence and net effect of the risks.

Risks	R_i	C_i	$R_i + C_i$	$R_i - C_i$	Cause/Effect
K01	[0.877, 1.055]	[0.822, 0.918]	[1.699, 1.973]	[0.054, 0.137]	Cause
K02	[1.174, 1.26]	[0.373, 0.617]	[1.547, 1.877]	[0.802, 0.643]	Cause
K03	[0.59, 0.725]	[0.607, 0.729]	[1.197, 1.454]	[–0.016, –0.003]	Effect
K04	[1.216, 1.41]	[1.157, 1.197]	[2.373, 2.608]	[0.059, 0.213]	Cause
K05	[0.886, 1.014]	[0.652, 0.879]	[1.538, 1.894]	[0.234, 0.135]	Cause
K06	[0.707, 0.833]	[1.021, 1.216]	[1.728, 2.049]	[–0.314, –0.383]	Effect
K07	[0.322, 0.451]	[1.04, 1.1]	[1.362, 1.551]	[–0.719, –0.649]	Effect
K08	[0.289, 0.292]	[1.52, 1.646]	[1.809, 1.938]	[–1.231, –1.354]	Effect
K09	[1.708, 1.85]	[0.259, 0.314]	[1.968, 2.164]	[1.449, 1.536]	Cause
K10	[0.476, 0.572]	[0.707, 0.866]	[1.182, 1.438]	[–0.231, –0.293]	Effect
K11	[0.764, 0.915]	[0.851, 0.896]	[1.616, 1.81]	[–0.087, 0.019]	Effect

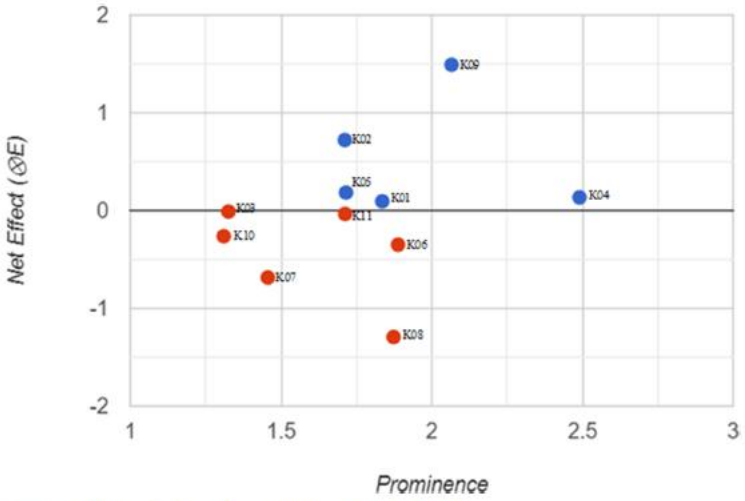
Source: Compiled from authors.

(e.g. Coras and Tantau, 2013; Durst and Ferenhof, 2014; North et al., 2020), outsourcing activities often expose valuable knowledge to external parties, particularly competitors. Occasionally, independent contractors may work for clients who are competing and attempting to increase their market share. As a result of an innovation developed by a contractor specifically for the focal firm being transferred to a competitor, the incumbent firm may suffer a loss of competitiveness (Tan et al., 2016).

Communication risks (K09) are regarded as the second most influential casual risk, despite receiving less scientific attention than other knowledge risks. Specifically, within the context of the study, the significance of this risk can be attributed to the fact that SMEs as organisations are typically flat in nature, which means that activities are primarily conducted at the operational level, requiring effective and effective communication between employees and external stakeholders. Therefore, any interference with the communication process between a recipient and a sender carries the risk of the intended message being lost, misunderstood, or never delivered; and is most often associated with explicit forms of knowledge (Durst and Leyer, 2014).

Knowledge waste (K01) is the third significant operational knowledge risk within the causal risk category. It has been strongly associated with the danger of reinvention (Durst and Ferenhof, 2016), which occurs when organisations seek knowledge that may already exist, perhaps in another form, but needs to be transformed or converted in order to become useful. This situation is particularly prevalent among SMEs when they have to go through several processes in order to complete a project; a series of processes that could have been shortened if precedents had been followed, particularly in cases of similar projects which have previously been completed. Generally, this type of risk is associated with organisations that fail to maintain records of their knowledge (Durst and Ferenhof, 2016).

Similar to the calculation of net cause/effect values (see Table 5 and Fig. 1), the effect risk can also be categorised as follows: risk of improper knowledge application



Source: Designed by authors (*Note*: • Effect • Cause).

Fig. 1. The DEMATEL prominence-causal relationship diagram.

(K06) > continuity risk (K08) > knowledge transfer risks (K11) > espionage (K07) > relational risk (K03) > knowledge acquisition risks (K10). Theoretically, these eight risks are influenced by the causal risks, which ultimately increase the knowledge risk of SMEs. In the effect risk category, improper knowledge application (K06) is the most significant. While this form of risk is concerned with the misuse of knowledge (Temel and Durst, 2020), it may arise from a variety of sources, including the misinterpretation of knowledge (Coras and Tantau, 2013), a lack of skills and abilities (Durst et al., 2017), and ineffective management of resources (Zięba and Durst, 2018). Considering this, we argue that causal risks such as knowledge gaps, communication risks, and even the use of obsolete or unreliable knowledge are likely to contribute to this effect (operational knowledge) risk, especially when an organisation recognises a potential innovation opportunity, but does not have the required skills or capabilities to execute it.

Figure 1 illustrates the degree of prominence of each operational knowledge risk, which provides an indication of which risks should be addressed in order of priority. An operational knowledge risk with a high prominence value is one that has a significant impact on other risks, or is affected by other risks, and must therefore be addressed in the short term. Based on the findings, the 11 operational knowledge risks have been ranked according to their prominence: outsourcing risks (K04) > communication risks (K09) > risk of improper knowledge application (K06) > continuity risk (K08) > knowledge waste (K01) > risk of using obsolete/unreliable knowledge (K05) > knowledge transfer risks (K11) > risks related to knowledge gaps (K02) > espionage (K07) > relational risk (K03) > knowledge acquisition risks (K10).

According to the findings, outsourcing appears to pose the greatest risk. To reduce outsourcing risks, SMEs are expected to reduce their scope of cooperation (Durst and Ferenhof, 2014) which can be accomplished through the use of a rigorous contract between the focal firm and the

contractor that restricts the number of activities and interactions between the two parties. As some outsourcing may require the focal firm to expand its scope to other departments, which further increases knowledge risks since more knowledge will be shared and more people will be involved in the process, it can be challenging to draft a contract that covers all possible occurrences, rights, and obligations. Besides that, it is even more challenging for the focal firm to keep track of what (knowledge) leaves the organisation. Nevertheless, if reducing the scope of their cooperation proves to be a strategic disadvantage, careful communication (Durst and Ferenhof, 2014) can be practised in order to prevent knowledge from leaking out.

5. Conclusion

In this paper, the grey-DEMATEL is applied to evaluate knowledge risks at the operational level of SMEs, and the following conclusions are drawn. (1) The causal category of operational knowledge risks in SMEs include outsourcing risks, communication risks, knowledge waste, the risk of using obsolete/unreliable knowledge, and risks related to knowledge gaps. (2) Also included in the effect category of operational knowledge risks for SMEs are risk of improper knowledge application, continuity risk, knowledge transfer risks, espionage, relational risk, and knowledge acquisition risks. (3) The critical operational knowledge risks in SMEs are as follows: outsourcing risks, communication risks, risk of improper knowledge application, continuity risk, knowledge waste, risk of using obsolete/unreliable knowledge, knowledge transfer risks, risks related to knowledge gaps, espionage, relational risk, and knowledge acquisition risks.

Findings from the study have implications for both theory and practice. From a theoretical perspective, the paper contributes to the underdeveloped body of knowledge about knowledge risks and KRM. More specifically, it introduces a new technique for knowledge risk evaluation known as grey-DEMATEL; a rigorous analytical technique for analysing risks (Seker et al., 2017).

In addition, the study may be of interest to practitioners (e.g. directors, owners, and managers) as it can help them evaluate knowledge risks at the operational level in a more holistic manner and provide them with information regarding the priori- ties in terms of the specific risks to address at a certain point in time. Since SMEs have limited resources, a priority scale will help them address the most relevant risks. In this study, the grey-based DEMATEL technique is clearly and systematically applied, offering practitioners a means of easily implementing it in their own organisations. Practitioners can benefit from this technique since it will prevent them from committing judgmental errors when conducting risk assessments. As indicated by Yazdani et al. (2020), such a technique is expected “to increase the quality of final decision and to reduce human judgmental errors” (p. 970).

All studies have limitations, and this one is no exception. Since the operational knowledge risks identified in this study may not be exhaustive, future research could use the Delphi-interview approach with more emphasis on KM experts to identify risks that might have been overlooked in

this study. Additionally, future research should incorporate inputs from these KM experts during the risk assignment process for a more robust assignment of the identified risks according to the grey-linguistic scale.

References

Al-Jabri, H and KA Al-Busaidi (2018). Inter-organizational knowledge transfer in Omani SMEs: Influencing factors. VINE Journal of Information and Knowledge Management Systems, 48(3), 333–351.

Allianz Global Corporate and Specialty (2022). Allianz risk barometer results appendix 2022. Available at https://www.agcs.allianz.com/content/dam/onemarketing/agcs/ agcs/reports/Allianz-Risk-Barometer-2022-Appendix.pdf. Accessed on 25 August 2022.

Bakir, S, S Khan, K Ahsan and S Rahman (2018). Exploring the critical determinants of environmentally oriented public procurement using the DEMATEL method. Journal of Environmental Management, 225, 325–335.

Belghitar, Y, E Clark, V Dropsy and S Mefteh-Wali (2021). The effect of exchange rate fluctuations on the performance of small and medium sized enterprises: Implications for Brexit. The Quarterly Review of Economics and Finance, 80, 399–410.

Biswas, B and R Gupta (2019). Analysis of barriers to implement blockchain in industry and

service sectors. Computers and Industrial Engineering, 136, 225–241.

Bouchard, V and O Basso (2011). Exploring the links between entrepreneurial orientation and intrapreneurship in SMEs. Journal of Small Business and Enterprise Development, 18(2), 219–231.

Bratianu, C (2018). A holistic approach to knowledge risk. Management Dynamics in the Knowledge Economy, 6(4), 593–607.

Brunold, J and S Durst (2012). Intellectual capital risks and job rotation. Journal of Intellectual Capital, 13(2), 178–195.

Brustbauer, J (2016). Enterprise risk management in SMEs: Towards a structural model. International Small Business Journal, 34(1), 70–85.

Buculescu, MM (2013). Harmonization process in defining small and medium-sized enter- prises. Arguments for a quantitative definition versus a qualitative one. Theoretical and Applied Economics, 9(586), 103–114.

Coras, EL and AD Tantau (2013). A risk mitigation model in SME's open innovation projects. Management and Marketing, 8(2), 303.

Delerue, H (2005). Relational risk perception and alliance management in French biotechnology SMEs. European Business Review, 17(6), 531–546.

Durst, S (2013). An exploratory study of intangibles risk disclosure in annual reports of banking companies from the UK, US, Germany and Italy — Some descriptive insights.

Financial Reporting, (1), 81–120. Available at http://digital.casalini.it/10.3280/ FR2013-001005.

Durst, S, G Bruns and IR Edvardsson (2017). Retaining knowledge in smaller building and construction firms. International Journal of Knowledge and Systems Science, 8(3), 1–12.

Durst, S and H Ferenhof (2014). Knowledge leakages and ways to reduce them in small and medium-sized enterprises (SMEs). Information, 5(3), 440–450.

Durst, S and HA Ferenhof (2016). Knowledge risk management in turbulent times. In Competitive strategies for Small and Medium Enterprises, pp. 195–209. Cham: Springer. Durst, S, S Foli and IR Edvardsson (2022). A systematic literature review on knowledge management in SMEs: Current trends and future directions. Management Review Quarterly, 1–26.

Durst, S and M Leyer (2014). How can SMEs assess the risk of organisational knowledge? In Proceedings of the LWA 2014 Workshops: KDML, IR, FGWM, Aachen, Germany, pp. 299–309. Available at https://ceur-ws.org/Vol-1226/paper46.pdf.

Durst, S and M Zięba (2017). Knowledge risks-towards a taxonomy. International Journal of Business Environment, 9(1), 51–63.

Durst, S and M Zięba (2019). Mapping knowledge risks: Towards a better understanding of knowledge management. Knowledge Management Research and Practice, 17(1), 1–13. Durst, S and M Zięba (2020). Knowledge risks inherent in business sustainability. Journal of Cleaner Production, 251, 119670.

Eggers, F (2020). Masters of disasters? Challenges and opportunities for SMEs in times of crisis. Journal of Business Research, 116, 199–208. European Commission (2008). Putting small businesses first. Available at http://ec.europa.eu/enterprise/entrepreneurship/docs/sme_pack_en_2008_full.pdf. Accessed on 25 August 2022.

Foli, S (2022). Total interpretive structural modelling (TISM) and MICMAC approach in analysing knowledge risks in ICT-supported collaborative project. VINE Journal of Information and Knowledge Management Systems, 53(3), 394–410.

Foli, S and S Durst (2022). Analysing drivers of knowledge leakage in collaborative agreements: A magnetic processing case firm. Journal of Risk and Financial Management, 15(9), 389, Available at https://www.mdpi.com/1911-8074/15/9/389.

Foli, S, S Durst and S Temel (2022). The link between supply chain risk management and innovation performance in SMEs in turbulent times. Journal of Entrepreneurship in Emerging Economies,. doi: 10.1108/JEEE-03-2022-0084.

Fu, C, J Zheng, J Zhao and W Xu (2001). Application of grey relational analysis for corrosion failure of oil tubes. Corrosion Science, 43(5), 881–889.

Govindan, K, R Khodaverdi and A Vafadarnikjoo (2016). A grey DEMATEL approach to develop third-party logistics provider selection criteria. Industrial Management and Data Systems, 116(4), 690–722.

Haleem, A, S Khan and MI Khan (2019). Traceability implementation in food supply chain: A grey-DEMATEL approach. Information Processing in Agriculture, 6(3), 335–348.

Hammoda, B and S Durst (2022). A taxonomy of knowledge risks for healthcare organizations. VINE Journal of Information and Knowledge Management Systems, 52(3), 354–371.

Harvey, MG and RF Lusch (1999). Balancing the intellectual capital books: Intangible liabilities. European Management Journal, 17(1), 85–92.

Haselip, J, D Desgain and G Mackenzie (2014). Financing energy SMEs in Ghana and

Senegal: Outcomes, barriers and prospects. Energy Policy, 65, 369–376.

Heinze, I and T Henschel (2021). Risk(ing) sophistication: Towards a structural equation model for risk management in small and medium-sized enterprises. International Journal of Entrepreneurship and Small Business, 44(4), 386–412.

Hetland, PW (2003). Chapter eight uncertainty management. In Appraisal, Risk and Uncertainty, NJ Smith (ed.), Construction Management Series, pp. 59–88. London: Thomas Telford.

Khan, S, A Haleem and MI Khan (2020). Enablers to implement circular initiatives in the supply chain: A grey DEMATEL method. Global Business Review, doi: 10.1177/0972150920929484.

Lee, RW, JY Yip and VW Shek (2021). Knowledge Risk and Its Mitigation: Practices and Cases. Emerald Group Publishing.

Leitch, M (2010). ISO 31000: 2009 — the new international standard on risk management. Risk Analysis, 30(6), 887–892.

Massingham, P (2010). Knowledge risk management: A framework. Journal of Knowledge Management, 14(3), 464–485.

North, K, AB De Carvalho, AM Braccini, S Durst, JÁ Carvalho, K Gräslund and S Thalmann (2020). 4.1 Knowledge risks in supply chain interactions of SMEs: An exploratory study. In 2019 Knowledge Management in Digital Work Environments, State-of-the-Art and Outlook, WM 2019, Potsdam, Germany, 18 March 2019–20 March 2019, pp. 161–171. Gesellschaft für Informatik.

Rajesh, R and V Ravi (2017). Analyzing drivers of risks in electronic supply chains: A grey–DEMATEL approach. The International Journal of Advanced Manufacturing Technology, 92(1), 1127–1145.

Seker, S, F Recal and H Basligil (2017). A combined DEMATEL and grey system theory approach for analyzing occupational risks: A case study in Turkish shipbuilding industry. Human and Ecological Risk Assessment: An International Journal, 23(6), 1340–1372.

Shao, J, M Taisch and M Ortega-Mier (2016). A grey-DEcision-MAking Trial and Evaluation

Laboratory (DEMATEL) analysis on the barriers between environmentally friendly products and consumers: Practitioners' viewpoints on the European automobile industry. Journal of Cleaner Production, 112, 3185–3194.

Stam, CD (2009). Intellectual liabilities: Lessons from the decline and fall of the Roman

Empire. The Journal of Information and Knowledge Management Systems, 39(1), 92–104.

Storey, DJ (2016). Understanding the Small Business Sector. Routledge.

Sufiyan, M, A Haleem, S Khan and MI Khan (2019). Evaluating food supply chain performance using hybrid fuzzy MCDM technique. Sustainable Production and Consumption, 20, 40–57.

Surya, B, F Menne, H Sabhan, S Suriani, H Abubakar and M Idris (2021). Economic growth, increasing productivity of SMEs, and open innovation. Journal of Open Innovation: Technology, Market, and Complexity, 7(1), 20.

Tan, KH, WP Wong and L Chung (2016). Information and knowledge leakage in supply chain. Information Systems Frontiers, 18(3), 621–638.

Temel, S and S Durst (2020). Knowledge risk prevention strategies for handling new technological innovations in small businesses. VINE Journal of Information and Knowledge Management Systems, 51(4), 655–673.

Thu, DA (2020). The competitiveness of small and medium enterprises in the tourism sec- tor: The role of leadership competencies. Journal of Economics and Development, 23(3), 299–316.

Trkman, P and KC Desouza (2012). Knowledge risks in organizational networks: An exploratory framework. The Journal of Strategic Information Systems, 21(1), 1–17.

Tsang, HWC and RW Lee (2018). Mitigation of knowledge risks in open innovation. In In Open Innovation and Knowledge Management in Small and Medium Enterprises, S Durst, S Temel and HA Ferenhof (eds.), pp. 183–203. Available at https://doi. org/10.1142/9789813233591_0010.

Tsang, HWC, WB Lee and E Tsui (2016). AHP-driven knowledge leakage risk assessment model: A construct-apply-control cycle approach. International Journal of Knowledge and Systems Science, 7(3), 1–18.

United States International Trade Commission (2010). Small and mediumsized enterprises: Overview of participation in U.S. exports. Available at https://www.usitc.gov/publications/332/pub4125.pdf. Accessed on 25 August 2022.

Vishvakarma, NK, RK Singh and RRK Sharma (2022). Cluster and DEMATEL analysis of key RFID implementation factors across different organizational strategies. Global Business Review, 23(1), 176–191.

Yazdani, M, AE Torkayesh and P Chatterjee (2020). An integrated decision-making model for supplier evaluation in public healthcare system: The case study of a Spanish hospital. Journal of Enterprise Information Management, 33(5), 965–989.

Zavadskas, EK, A Kaklauskas, Z Turskis and J Tamošaitiene (2008). Selection of the effective dwelling house walls by applying attributes values determined at intervals. Journal of Civil Engineering and Management, 14(2), 85–93.

Zheng, L (2017). Does online perceived risk depend on culture? Individualistic versus collectivistic culture. Journal of Decision Systems, 26(3), 256–274.

Zieba, M (2020). Knowledge risk management in companies offering knowledge-intensive business services. In Knowledge Risk Management, pp. 13–31. Cham: Springer.

Zieba, M and S Durst (2018). Knowledge risks in the sharing economy. In Knowledge Management in the Sharing Economy, pp. 253–270. Cham: Springer.

Zieba, M, S Durst, M Gonsiorowska and Z Zralov (2021). Knowledge risks in organiza- tions — Insights from companies. In European Conference on Knowledge Management, Academic Conferences International Limited, Coventry, UK, pp. 864–873.

Zieba, M, S Durst and C Hinteregger (2022). The impact of knowledge risk management on sustainability. Journal of Knowledge Management, 26(11), 234–258.

4.3. Study 3 - Analysing Drivers of Knowledge Leakage in Collaborative Agreements: A Magnetic Processing Case Firm

Samuel Foli

Susanne Durst

Abstract: Due to the embeddedness of organisations in networks, collaborations, and business relationships, knowledge leakage has become a common concern. In this regard, this paper aims to investigate drivers of knowledge leakage in collaborative agreements using an integrated ISM-MICMAC model. Based on insights from employees including the CEO of a magnetic processing firm, we validate the proposed model. The findings of our study reveal nine key drivers that influence knowledge leakage in collaborative agreements. In terms of level of influence, incomplete contract is the most influential driver, followed by sub-contracting activities. Last, the nine drivers are classified into two main clusters: independency cluster—weak dependence power with high driving power—and linkage cluster—strong dependence and driving power.

Keywords: knowledge leakage; interpretive structural model (ISM); MICMAC analysis; collaborative agreements; driver; case study; small firm

1. Introduction

The uncertain business landscape, where continuous updating of knowledge is essen- tial for securing a sustained competitive advantage (Durst 2020; Yang et al. 2021), under- scores the importance of collaboration among organisations even more. By establishing a collaborative agreement—which is essentially an agreement between organisations to work together to achieve a mutually beneficial objective—organisations can align their resources to create new knowledge and remain competitive (Papadas et al. 2019; Pateman et al. 2016; Zhou et al. 2022). Collaboration among organisation is indisputable as a crucial ingredient to successfully realising projects (Bond-Barnard et al. 2018), particularly when each partner possesses complementary resources that are rare and unique (Belderbos et al. 2015). It has been shown that when organisations collaborate, projects can be accomplished more effectively and efficiently because they are able to overcome individual limitations in ability and resources that would otherwise impede the execution or completion of projects.

Despite the fact that collaborations have many advantages, there is also a dark side. A possible dark side to collaboration arises from the exchange of information or knowledge, the very basis of collaboration (Garousi Mokhtarzadeh et al. 2021; Scaliza et al. 2022). It is this bidirectional flow of knowledge that can cause valuable organisational knowledge to seep out with the wrong persons. This phenomenon is often referred to as “knowledge leakage”. As defined by Frishammar et al. (2015), knowledge leakage is the disclosure of valuable knowledge that is supposed to remain within the boundaries of an organisation. In the context of collaboration, knowledge leakage can also result from firms misappropriating valuable knowledge of a focal firm in an inter-organisational framework. Typically, this happens when partners develop opportunistic behaviour in pursuit of self-interest and are less willing to cooperate (Jiang et al. 2013).

Although it is evident from the literature on collaborations that knowledge sharing and knowledge creation have received considerably more attention (e.g., Goi et al. 2022; Ho and Ganesan 2013; Kleber et al. 2019), research on knowledge leakage, in general, is relatively growing (Durst et al. 2015). Previous studies (e.g., Ahlfänger et al. 2022; Fawad Sharif et al. 2022; Jiang et al. 2016; Oxley and Sampson 2004; Raza-Ullah 2021) on knowledge leakage in collaboration (be it, e.g., strategic alliances or coopetition) have largely focused on governance control mechanisms, such as formal and informal contracts (i.e., social contract based on trust). These mechanisms have been used primarily for controlling and minimising knowledge leakage in different forms of collaboration. As an example, Fawad Sharif et al. (2022) analyse how distrust, partner learning intent, and human resource management influence knowledge leakage in collaborative projects. In a strategic alliance, Jiang et al. (2016) examine the links between partners’ trustworthiness and knowledge leakage. Besides the fact that knowledge leakage is not a fully understood phenomenon yet, previous research has provided limited insights into the factors that may cause knowledge leakage in collaborative settings (Li and Kang 2019). Consequently, there is little evidence of identifying and modelling the interactions between the drivers of knowledge leakage, particularly in collaborative settings. This gap in the literature is worth addressing for important reasons. First

and foremost, to have a better understanding of this fragmented research field (Durst et al. 2015). A second consideration is that, since it appears that knowledge leakage is intrinsically a complex phenomenon (Durst et al. 2015; Wu et al. 2021), a deeper understanding of knowledge leakage within the context of collaborative agreements, as a complex social system, can also be developed. In specific terms, addressing this gap is imperative, as it would provide a clearer picture of this complexity issue that is often only hinted at (Wang et al. 2021; Wayne Gould 2012; Wu et al. 2021) which in turn is important for the further development of knowledge leakage as an important element of both (knowledge) risk management and knowledge management in general (Zieba et al. 2022).

Therefore, this study proposes an integrated interpretive structural modelling (ISM)— Cross-Impact Matrix Multiplication Applied to Classification (MICMAC) model to investigate drivers of knowledge leakage in collaborative agreements and establish their interrelationships. Specifically, the research objectives are as follows:

- To identify key drivers of knowledge leakage in collaborative agreements;
- To establish hierarchical relationships among the drivers;
- To classify the drivers based on their driving and dependency power; and
- To validate the model using a magnetic processing firm as a case study.

The following justifies the selection of a magnetic processing firm as the subject of the case study. The firm is a small and privately-owned enterprise that specialises in magnetic processing, using high-tech to develop non-assembled and highly customised products for its clients. The industry is competitive, as acknowledged by an employee from the case firm, it also forms part of a global supply chain network, positioning the firm in a more complex environment. This poses a greater threat regarding knowledge leakage (Durst and Ferenhof 2014; Durst et al. 2015; Oxley and Wada 2009). Additionally, due to its small size, the firm faces the problem of liability of smallness, making it heavily dependent on its partners, suppliers and clients, which increases the possibility of knowledge leakage thus making the selected firm an appropriate study subject.

The first research objective is achieved by conducting a thorough literature review, based on peer-reviewed scientific papers, and further validated by the opinions of employees from the case firm. The second research objective is achieved by using the ISM technique, which is widely used to establish interrelationships between complex variables (Ali et al. 2022; Singh et al. 2019). The third objective of the research is addressed using MICMAC analysis. MICMAC has been deemed an effective analysis tool for classifying variables into distinct clusters with unique characteristics (Jung et al. 2021). Finally, the fourth objective is reached through the continued involvement of the employees including the CEO of the case firm.

To this end, this research contributes in several ways to advance the study of knowledge leakage by focusing on the interrelationships between key drivers of knowledge leakage in collaborative

agreements. First, a comprehensive overview and description of drivers that have been reported in the literature are provided. Furthermore, this study in- corporates the employees'—from the case firm—inputs to build an integrated model using the ISM technique and MICMAC analysis, a first in knowledge leakage studies. Finally, this work supports practitioners in developing a better understanding of the complex nature of knowledge leakage in collaborative settings.

The remainder of this paper is structured as follows: Section 2 presents a literature review. Section 3 provides an overview of the research methodology. The Section 4 presents the model development and validation while Section 5 discusses the final model and its implications. Finally, Section 6 concludes with some limitations and suggested future research directions.

2. Literature Review

2.1. Knowledge Leakage in Collaborative Agreements

According to several studies (e.g., Durst and Ferenhof 2014; Guo et al. 2021; Zhao and Liang 2011), collaborative agreements can expose organisations to the dan- ger of knowledge leakage. In collaborative agreements that are based on co-opetition, where collaboration and competition are intertwined (Hoffmann et al. 2018), the likelihood of knowledge leakage becomes even more evident. Theoretically, collaborative agreements are designed to bring organisations together to accomplish a shared objective by learning from one another and more efficient use of resources (Bakker et al. 2008), however, this may not necessarily be the case in practice, since partners may have incongruent private interests, resulting in opportunistic behaviour such as misappropriation of knowledge (Jiang et al. 2013). Although the exchange of knowledge between firms is necessary, the more core knowledge is shared, the greater the likelihood of losing the firm's competitive advantage (Frishammar et al. 2015; Galati et al. 2019). In this regard, it is necessary to find and maintain a balance.

Kaiser et al. (2021) expressed a similar viewpoint regarding the optimal level of knowledge sharing and knowledge protection practices as a means of minimising knowledge leakage. Using a semiconductor industry context, they designed a grey-box model to protect knowledge from leakage in data-centric collaborations. Kunttu and Neuvo (2019) found that mutual trust building, based on a personal level relationship, is one of the key processes that enable partners to balance learning and protection while simultaneously lowering informational barriers in collaborations. In an R&D collaborative project, Hurmelinna-Laukkanen (2011) examined 242 Finnish companies in order to better understand the issue of maintaining an optimal balance between knowledge sharing and knowledge protection primarily to curb knowledge leakage. Their results revealed that the efficient application of knowledge protection while engaging in knowledge sharing practices among varying partners facilitates innovation performance. This confirms the existing notion of an appropriate balance between knowledge sharing and knowledge protection. To illuminate the dilemma of knowledge protection and knowledge sharing in collaborative business partnerships,

Wei et al. (2018) drew upon transaction cost and psychological contract theories. The authors were primarily interested in determining how knowledge protection affects partnership quality and project outcomes. Results showed that knowledge protection adversely impacted partnership quality and project performance. Likewise, this demonstrates the importance of having a balanced approach to knowledge sharing to maximise project performance and knowledge protection to minimise knowledge leakage. The determination of the right equilibrium justifies the complexity associated with

knowledge leakage in collaborative arrangements.

2.2. Key Drivers of Knowledge Leakage in Collaborative Agreements

Having reviewed the literature, we identified several drivers of knowledge leakage in collaborative agreements. Opportunistic behaviour has been identified as one driver that may trigger knowledge leakage in collaborations among firms (Estrada et al. 2016; Fawad Sharif et al. 2020b). As early as 1975, Williamson (1975) defined opportunistic be- haviour as "self-interest seeking with guile" (p. 9). In collaborative agreements, opportunistic behaviour is accompanied by a breach of trust as a partner attempts to misappropriate proprietary knowledge (Estrada et al. 2016; Jiang et al. 2013).

Distrust is regarded as one of the most critical drivers of knowledge leakage in collaborative agreements (Raza-Ullah 2021); which is defined as the expectation that a partner will act detrimentally to the focal firm (Govier 1994). According to Fawad Sharif et al. (2022), the lack of trust is responsible for knowledge leakage since the presence of distrust leads partner firms to focus on personal goals instead of the project's overall objectives. This, in turn, can result in them developing opportunistic intentions and misappropriating valuable knowledge from the focal firm. One way to restrain opportunistic actions is through the implementation of a formal contract between collaborating firms which is in line with the transaction cost theory. In contrast, "without formal contracts, partner firms have stronger incentives to acquire each other's knowledge beyond the scope of the cooperative agreement" (Jiang et al. 2013, p. 985). Thus, the lack of formal contracts may allow opportunistic behaviour to spread between partner firms, resulting in knowledge leakage.

An era in which inter-firm collaborations are increasingly driven by digital transformation (Appio et al. 2021), inadequate technological competence of employees (Altukruni et al. 2021), weak Bring-Your-Own-Device (BYOD) policies (Serna et al. 2017), and substandard security measures (Altukruni et al. 2021; Durst and Zieba 2019) pose a risk of sensitive knowledge being exposed or compromised. This exposed knowledge may even end up with external parties who are not part of the collaborative agreement and eventually result in reputational damage (Ahmad et al. 2014) and loss of competitiveness for the affected firm (Durst et al. 2015; Ritala et al. 2015).

Moreover, research (e.g., Nishat Faisal et al. 2007; Norman 2002; Oxley and Wada 2009) has strongly linked knowledge leakage to subcontracting activities such as outsourcing, which are typically referred to as vertical relationships (Tidd and Izumimoto 2002). Ac- cording to some

scholars (e.g., Belderbos et al. 2004; Huo et al. 2022), vertical relationships orchestrate knowledge leakage less since they are mostly non-competitive. However, this may not always be the case since downstream partners may wish to take advantage of the upstream firm's dependence (Fang et al. 2016).

Individual incentives may also trigger knowledge leakage in collaborative agreements, but research on this aspect has been scarce (Tan et al. 2016). In this case, an employee is incentivised to provide confidential information about his/her firm to out- siders through fraudulent means, resulting in inappropriate knowledge disclosure. In this regard, dissatisfied or disloyal employees—viewed as a concrete form of knowledge leakage (Durst and Ferenhof 2014)—may be a target for engaging in such activities. In addition, collaboration between competing firms may lead to knowledge leakage (Lee 2002; Zhao et al. 2002). It is the tension between value creation and value appropriation that often causes partners to act opportunistically, which increases the likelihood of knowledge leakage (Raza-Ullah and Eriksson 2017). The situation is even more precarious in that competing firms often possess specialised knowledge that gives them an edge over their competitors, so when knowledge leaks occur, there can be significant adverse effects on the firm in question.

Below (Table 1) is a summary of the identified drivers of knowledge leakage in collaborative agreements pending opinions from employees of the case firm for validation.

Table 1. Literature support to the identified drivers.

Codes	Drivers	Descriptions	References
D01	Distrust	Neither of the partners involved in collaborative agreements can be relied upon by the other.	Qiu and Haugland (2019), Jiang et al. (2016), Yang et al. (2019), Taylor (2005), Guo et al. (2020), Deniaud et al. (2016), Fawad Sharif et al. (2020b, 2022), and Vafaei-Zadeh et al. (2020)
D02	Incomplete contracts	Weak or no legal contract in place to protect the core knowledge of partners involved in the collaboration.	Jiang et al. (2013), Yang et al. (2019), Taylor (2005), Guo et al. (2020), Ahlfänger et al. (2022), Deniaud et al. (2016), and Fawad Sharif et al. (2020b)
D03	Substandard security measures	Lack or inadequate security guidelines to oversee knowledge exchange between partners in collaborative arrangements.	Hislop et al. (2018), Durst and Zieba (2019), Frishammar et al. (2015), and Altukruni et al. (2021)
D04	Weak BYOD policies	A lack of strict rules underpinning bring your own device (BYOD) policies could expose the focal and partner firms' core knowledge to cyberattacks (third party).	Serna et al. (2017), Shabtai et al. (2012), and Altukruni et al. (2021)
D05	Insufficient technological competence	Emerging technologies used in collaborative arrangements put a firm's core knowledge at risk of leakage due to a lack of tech know-how.	Ahmad et al. (2014), Hislop et al. (2018), Jiang et al. (2013), Christina et al. (2016), Altukruni et al. (2021), and Zeiringer and Thalmann (2022)
D06	Perceived opportunism	Partners attempt to gain an advantage by misappropriating the core knowledge of the focal firm.	Estrada et al. (2016), Norman (2002), Oxley and Wada (2009), and Fawad Sharif et al. (2020a, 2022)
D07	Expected incentives	The act of exposing core knowledge to a partner or external party for an incentive by a player in collaborative arrangements.	Tan et al. (2016)
D08	Existence of horizontal competition	Cooperation encourages partners to take advantage of exposed core knowledge.	Lee (2002), and Zhao et al. (2002)
D09	Sub-contracting activities	Cooperation agreements between firms often result in subcontracting activities rather than collaborations, which often result in unknowingly transferred core knowledge.	Tan et al. (2016), Foli (2022), Nishat Faisal et al. (2007), Dye and Sridhar (2003), and Zhang et al. (2011)

3. Research Methodology

The research methodology, which integrated the ISM technique and MICMAC to analyse key drivers of knowledge leakage in collaborative agreements, used for this study is illustrated in Figure 1. In this integrated model, the ISM technique is used to establish a contextual relationship among the drivers and leads to the development of a structural model of the drivers, while the MICMAC analysis is used to categorise the drivers into clusters based on their influencing power.

Several multi-criteria decision-making (MCDM) techniques are available in the literature, which are considered effective at addressing complex issues, such as DEMATEL, Graph theory, AHP, and ANP (dos Santos Gonçalves and Campos 2022). In DEMATEL, for example, cause-effect relationships between variables are revealed. Graph theory can be used to establish interactions among variables; however, the graph edges pose a reliability concern (Wagner and Neshat 2010). In terms of drawing a hierarchy of variables, AHP is an effective tool (Jakhar and Barua 2014). The

ANP can also provide dependencies between variables, but it is considered complicated and not widely accepted (Zhao et al. 2021).

None of the MCDM techniques is effective in establishing contextual relationships between variables by assessing their influencing power, as ISM-MICMAC does (Bux et al. 2020).

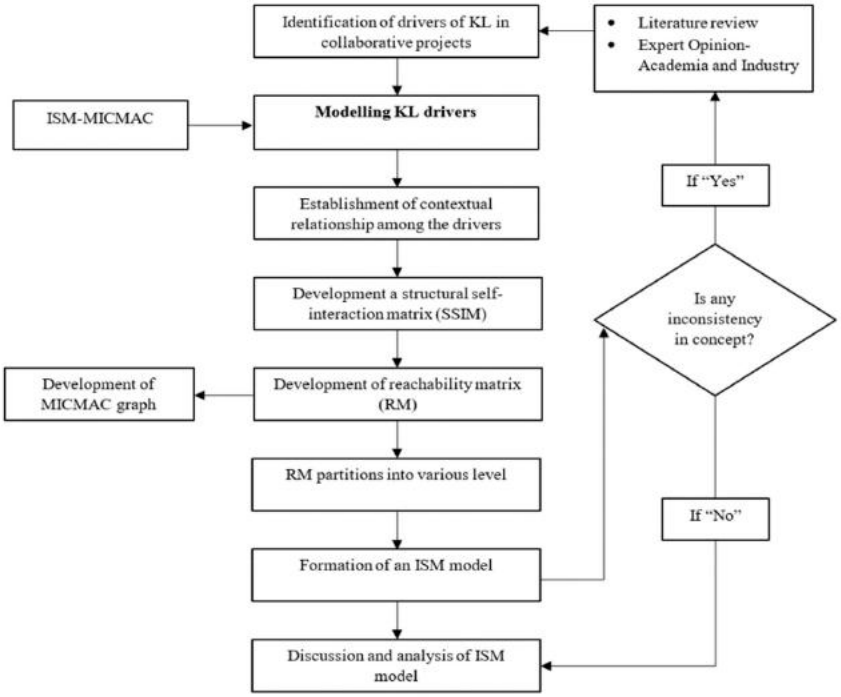


Figure 1. Steps in the research methodology.

Researchers have utilised the ISM-MICMAC integrated approach in a wide variety of areas, such as promoting sustainability through corporate social responsibility (Bux et al. 2020), managing risks in the agri-food supply chain (Ramos et al. 2021), addressing barriers to Industry 4.0 (Goel et al. 2022) and reducing supply chain risks in wind power projects (Troche-Escobar et al. 2018).

As a starting point, the key drivers of knowledge leakage in collaborative agreements identified through the literature review were listed in an Excel spreadsheet along with brief descriptions, which were then sent via email in advance to the case firm. Having access to this firm was made possible through an employee of the firm who participated in a summer school in connection with a research project. This employee mainly serves as the firm's communication officer with additional responsibilities such as risk management and ESG strategy implementation and is the direct point of contact with the firm's collaborators, i.e., suppliers, partners, and B-to-B customers; whose role is suitable for the present study.

In the validation process, two discussion sessions were conducted following Haleem et al.'s (2016) work. During the first discussion session, the communication officer, the CEO, and two members of the operations team participated. This discussion aimed to validate the identified drivers derived

from the literature, which is the immediate step prior to the modelling phase. Additionally, this met the minimum eligibility criteria for the use of this technique (see Haleem et al. 2016; Mathiyazhagan et al. 2013; Ravi and Shankar 2005). While in the second session, discussions were held in order to reach a consensus concerning the contextual relationships among the validated drivers; a phase technically included in the modelling process.

The next sections discuss the modelling phase of the validated drivers.

3.1. Interpretive Structural Modelling (ISM) Technique

Managing knowledge leakage in collaborative arrangements is a demanding task, particularly since it involves drivers that are complex in nature. Due to this reason, a powerful tool is necessary to assist in understanding and managing this complexity. ISM meets this requirement. Warfield (1973) developed the ISM to examine complex issues by analysing unorganised factors and converting them into a well-structured model. The interpretive nature of this technique derives from its ability to utilise experts in its application. By applying this technique, it is possible to establish interrelationships among the identified drivers of knowledge leakage in collaborative agreements and construct a structured model based on the knowledge and experience of the case firm's employees.

Following the first step which identified and validated the key drivers, the ISM technique was applied as follows:

- Contextual relationship between the identified key drivers is developed to determine which pairs of drivers should be checked;
- Structural self-interaction matrix (SSIM) is developed for the drivers that show pair- wise relationships among them;
- Reachability matrix (RM) is derived from the SSIM by replacing each cell entry with 1 and 0, as well as checking the matrix for transitivity. Assuming transitivity of contextual relations is a fundamental tenet of ISM. The rule states that if variable A is related to variable B and variable B is related to variable C, then variable A is necessarily related to variable C. This leads to the development of a final RM;
- Final RM is partitioned into several levels;
- ISM model is developed based on the contextual relationships given above and then transitive links are removed;
- Developed ISM model is reviewed to ensure that any conceptual inconsistencies and necessary modifications are considered.

3.2. Cross-Impact Matrix Multiplication Applied to Classification (MICMAC) Analysis

Duperrin and Godet (1973) proposed MICMAC analysis for assessing indirect relation- ships among system elements. Among managers, it is also considered useful for in-depth analysis of a system (Elmsalmi and Hachicha 2013). In this study, we used the MICMAC analysis to classify the identified key drivers of knowledge leakage in collaborative agreements according to their driving power (DrP) and dependence power (DeP). According to Figure 1, the MICMAC graph is derived from the final RM, by summing across the rows and columns of the final RM to determine each driver's driving power and dependence power. The drivers were then classified into four clusters (Wu et al. 2022):

- Autonomous drivers (Cluster I) possess weak driving and dependence powers. These drivers are often referred to as excluded drivers due to their limited influence.
- Dependent drivers (Cluster II) possess weak driving power but strong dependence power. For decision makers, these drivers represent an unfavourable outcome.
- Linkage drivers (Cluster III) possess strong driving and dependence powers. Typically, these drivers are unstable.
- Independent drivers (Cluster IV) possess strong driving power but weak dependence power. They are generally considered to be the most important drivers and are accorded the highest priority.

4. Model Development and Validation

Based on the research methodology presented earlier, we developed an integrated ISM-MICMAC model, which was validated through a case firm. To maintain the firm's anonymity, we used Alpha as a pseudonym. Alpha is a leader in the magnet technology market based in Germany. It provides sophisticated and customised magnetic products to its clients, making it a firm with a high level of expertise. As Alpha's production of magnetic products is dependent upon raw materials imported from outside Europe, it belongs to a global supply chain network. For this reason, Alpha engages in a wide variety of collaborative agreements. As a result, there is a high risk of knowledge leakage, especially when dealing with their partners and business-to-business clients. As mentioned previously, due to Alpha's knowledge-intensive nature and external collaborations, it was viewed as an appropriate case firm to validate a model regarding knowledge leakage.

4.1. Application of Integrated ISM-MICMAC Model

4.1.1. Structural Self-Interaction Matrix (SSIM)

Following the identification of the nine drivers that influence knowledge leakage in collaborative agreements through the literature review and their validation based upon opinions obtained from employees of the case firm, in the next step contextual relationships were determined. The

contextual relationship is one of the steps in the ISM modelling that heavily relies on the inputs from the involved participants (Foli 2022; Ramos et al. 2021). Through multiple discussions and reflections, the employees were able to establish relationships among the nine drivers identified. As a guideline, we adopted the following four conventional symbols as widely used in the literature (e.g., Sushil 2012) to assign relationships among the drivers:

- *V* for a forward relation of driver *i* to *j* (driver *i* will influence driver *j*/*i* → *j*);
- *A* for backward relation of driver *i* to *j* (driver *j* will influence driver *i*/*j* → *i*);
- *X* for a bidirectional relation of drivers *i* and *j* (drivers *i* and *j* will influence each other */i* ←→ *i)*; and
- *O* for no relation exists between drivers *i* and *j* (drivers *i* and *j* have no influence on each other).

Based on contextual relationships, the SSIM is derived by using the symbols as cell entries as shown in Table 2.

Table 2. Structural self-interaction matrix (SSIM).

Drivers	D01	D02	D03	D04	D05	D06	D07	D08	D09
D01		A	O	O	O	X	A	X	O
D02			O	O	O	V	V	V	V
D03				V	V	X	X	V	O
D04					X	V	O	O	O
D05						V	X	V	A
D06							X	A	A
D07								X	A
D08									X
D09									

4.1.2. Reachability Matrix (RM)

As a next step, the SSIM derived in the previous section was transformed into an initial reachability matrix. To do this, we converted each cell entry in the SSIM into binary, i.e., 0's and 1's, where zero represents no interrelationship between the drivers, whereas one indicates there is an interrelationship between them. Since these cell entries are symbols, we transformed them according to the following rules (Bux et al. 2020; Foli 2022):

- For SSIM cell entries *(i, j)* denoted by *V*, the initial reachability matrix cell entries *(i, j)* become *1* and *(j, i)* become *0*;
- For SSIM cell entries *(i, j)* denoted by *A*, the initial reachability matrix cell entries *(i, j)* become *0* and *(j, i)* become *1*;
- For SSIM cell entries *(i, j)* denoted by *X*, the initial reachability matrix cell entries *(i, j)* and *(j, i)* become *1*; and

- For SSIM cell entries *(i, j)* denoted by *O*, the initial reachability matrix cell entries *(i, j)* and *(j, i)* become *0*.

Upon application of the rules, the initial reachability matrix was determined as shown in Table 3. The initial reachability matrix is then used to determine the final reachability matrix. The final reachability matrix (see Table 4) is constructed based on the transitivity rule, which states that if driver i influences driver *j* and driver *j* influences driver *k*, then driver *i* has an influence on driver *k*.

Table 3. Initial reachability matrix.

Drivers	D01	D02	D03	D04	D05	D06	D07	D08	D09
D01	1	0	0	0	0	1	0	1	0
D02	1	1	0	0	0	1	1	1	1
D03	0	0	1	1	1	1	1	1	0
D04	0	0	0	1	1	1	0	0	0
D05	0	0	0	1	1	1	1	1	0
D06	1	0	1	0	0	1	1	0	0
D07	1	0	1	0	1	1	1	1	0
D08	1	0	0	0	0	1	1	1	0
D09	0	0	0	0	1	1	1	0	1

Table 4. Final reachability matrix.

Drivers	D01	D02	D03	D04	D05	D06	D07	D08	D09	DrP
D01	1	0	1 *	1 *	1 *	1	1 *	1	0	7
D02	1	1	1 *	1 *	1 *	1	1	1	1	9
D03	1 *	0	1	1	1	1	1	1	0	7
D04	1 *	0	1 *	1	1	1	1 *	1 *	0	7
D05	1 *	0	1 *	1	1	1	1	1	0	7
D06	1	0	1	1 *	1 *	1	1	1 *	0	7
D07	1	0	1	1 *	1	1	1	1	0	7
D08	1	0	1 *	1 *	1 *	1	1	1	0	7
D09	1 *	0	1 *	1 *	1	1	1	1 *	1	8
DeP	9	1	9	9	9	9	9	9	2	

* denotes transitivity relationship.

4.1.3. Level Partitions

In this step, the final reachability matrix was systematically partitioned into different levels, using the sets of reachability, antecedents, and intersections from the final reachability matrix. A reachability set (Rsi) was obtained for each driver across the final reachability matrix in the horizontal direction with cell entries "1". The antecedent set (Asi) was similarly derived for each driver across the final reachability matrix in the vertical direction with cell entries "1". As for the intersection set, it was derived through an iterative partitioning process. For example, as shown in Table 5, drivers D01, D03, D04, D05, D06, D07, and D08 are assigned to Level 1 since their Rsi intersected with their Asi exhaustively, while the rest did not. This process was repeated until all the drivers had been partitioned.

4.1.4. Formation of ISM Model

The ISM model of the drivers was derived from the final reachability matrix. It is important to note that the final reachability matrix includes transitivity relationships; these transitivity relationships were removed in order to maintain only direct interrelationships. As demonstrated in Figure 2, the interrelationships between drivers are indicated by arrows. In the case of D08 and D01, for example, there are two arrows at the end, which indicates that D01 exerts a direct influence on D08 and vice versa.

Table 5. Level partition for the drivers.

D0′s	Reachability Set (Rsi)	Antecedent Set (Asi)	Intersection Set (Isi)	Level
Iteration 1				
D01	1,3,4,5,6,7,8	1,2,3,4,5,6,7,8,9	1,3,4,5,6,7,8	I
D02	1,2,3,4,5,6,7,8,9	2	2	
D03	1,3,4,5,6,7,8	1,2,3,4,5,6,7,8,9	1,3,4,5,6,7,8	I
D04	1,3,4,5,6,7,8	1,2,3,4,5,6,7,8,9	1,3,4,5,6,7,8	I
D05	1,3,4,5,6,7,8	1,2,3,4,5,6,7,8,9	1,3,4,5,6,7,8	I
D06	1,3,4,5,6,7,8	1,2,3,4,5,6,7,8,9	1,3,4,5,6,7,8	I
D07	1,3,4,5,6,7,8	1,2,3,4,5,6,7,8,9	1,3,4,5,6,7,8	I
D08	1,3,4,5,6,7,8	1,2,3,4,5,6,7,8,9	1,3,4,5,6,7,8	I
D09	1,3,4,5,6,7,8,9	2,9	9	
Iteration 2				
D02	2,9	2	2	
D09	9	2,9	9	II
Iteration 3				
D02	2	2	2	III

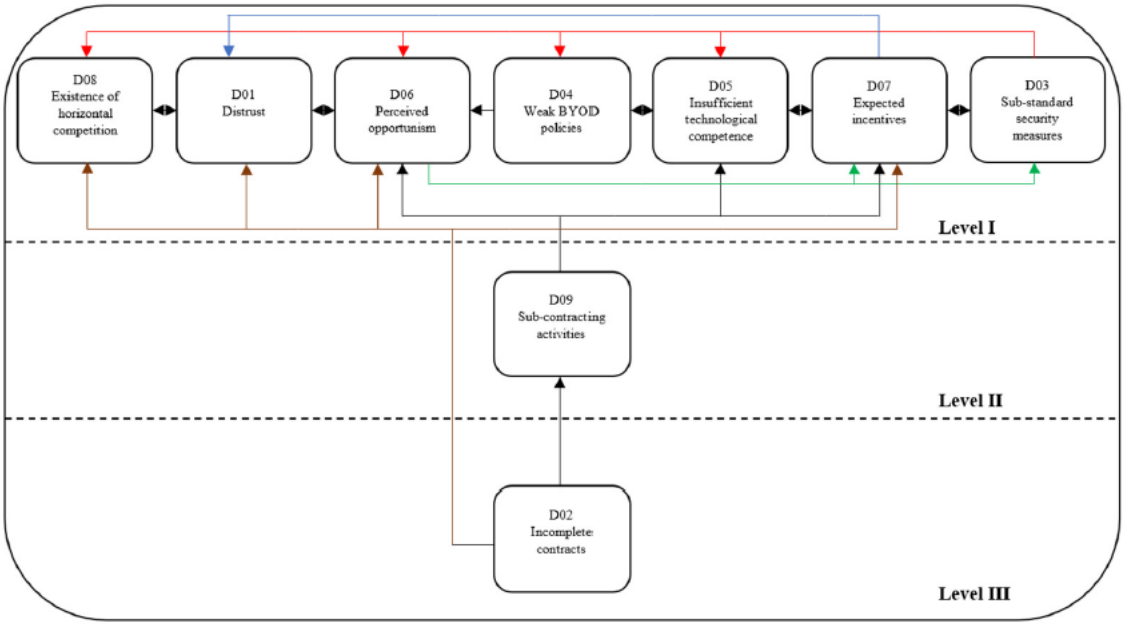


Figure 2. ISM model.

Moreover, the ISM provides a detailed representation of the drivers based on their level partitions. In the model, D01, D03, D04, D05, D06, D07, and D08 were structurally placed at the top, followed by D02 and D09.

4.1.5. MICMAC Analysis

Finally, we used the MICMAC analysis to classify the drivers into clusters. The result of the analysis generated two clusters—the Independent cluster and the Linkage cluster (Figure 3). No driver was placed under the Autonomous or the Dependent cluster.

Considering that D02 and D09 have a high driving power, but a low dependent power, they were assigned to the Independent cluster. Whereas D01, D03, D04, D05, D06, D07, and D08 were classified under the Linkage cluster since they possess a high degree of driving and dependence.

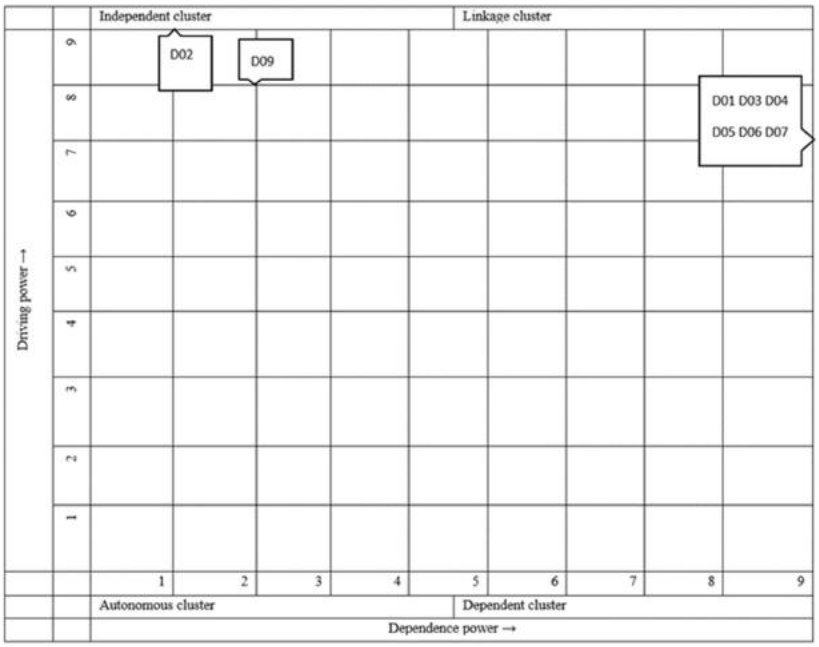


Figure 3. MICMAC analysis.

5. Discussion

Our research revealed nine key drivers of knowledge leakage in collaborative agreements. Besides the relevance of the identified drivers in the literature, employees including the CEO of the case firm confirmed their practicality at the collaborative level. Consequently, our findings regarding the drivers of knowledge leakage in collaborative agreements are in line with those found in the literature. As an example, distrust as a driver of knowledge leakage is consistent with studies from Fawad Sharif et al. (2020b, 2022) which found that distrust significantly influenced knowledge leakage in collaborative projects. Our findings also support previous studies (e.g., Jiang et al. 2013) that found incomplete contracts to be associated with knowledge leakage in similar collaborative settings. The validation of substandard security measures, weak BYOD policies, insufficient technological competence, perceived opportunism, expected incentives, the existence of horizontal competition, and sub-contracting activities as contributing factors to knowledge leakage is consistent with various findings in the literature (e.g., Serna et al. 2017; Zeiringer and Thalmann 2022).

The results of the ISM model indicate that there are three partitions among the nine identified drivers, which are hierarchical in nature and have several interdependencies. It is clear from this that knowledge leakage is a complex issue (Kaiser et al. 2021) and therefore requires a more holistic approach (Durst and Zieba 2019). Further, we observe that an incomplete contract in collaborative agreements contributes significantly to knowledge leakage, as it forms the foundation of the ISM hierarchy. Considering the fact that most previous studies (e.g., Jiang et al. 2013; Fawad Sharif et

al. 2020b) have reached similar conclusions, this is not surprising. Additionally, the ISM model indicates that incomplete contracts are associated with perceived opportunism. The reason for this can be explained in the context of a given collaborative project in which the contractual binding involving firms is not comprehensive. This paves the way for opportunistic behaviour to prevail and thrive, resulting in knowledge leakage. It is also found that an incomplete contract is directly linked to distrust. In a similar vein, when partners demonstrate a lack of commitment in a collaborative agreement, it is likely to result in distrust among them. Likewise, Fawad Sharif et al. (2020b) conclude that the existence of more complete contract can lead to higher levels of trust. It is clear from the above that contract design has an important role to play in minimising knowledge leakage (knowledge protection), confirming previous research. It also underlines the need for understanding the link between trust and formal contracts with regard to knowledge leakage (Jiang et al. 2013).

Despite the benefits of subcontracting, such as reduced costs, improved service quality, and more time to focus on the core business, it is also considered to be a significant driver of knowledge leakage in collaborative agreements. As shown in the ISM model, subcontracting activities have a direct correlation with perceived opportunism, insufficient technological competence, and expected incentives. As tasks are outsourced outside of a project, external collaboration is necessary, either in the form of sharing insight and knowledge about the project with subcontractors or third parties. In turn, such external collaboration can result in vertical relationships (Nishat Faisal et al. 2007) that breed opportunistic behaviour among partners. In relation to the correlation between subcontracting activities and insufficient technological competence, Durst and Zieba (2019) argue that the more firms outsource, the more they tend to rely on their contractors, consequently losing the necessary skills and capacities to operate the business. These skills could be technical capabilities to protect key organisational assets such as knowledge.

The upper hierarchy of the ISM model consists of the existence of horizontal competition, distrust, perceived opportunism, weak BYOD policies, insufficient technological competence, expected incentives, and substandard security measures. Among the drivers, substandard security measure is the most interconnected. It is directly associated with horizontal competition, perceived opportunism, weak BYOD policies, insufficient technological competence, and expected incentives. Thus, it implies that, without measures like security, many drivers may emerge and contribute to knowledge leakage (Altukruni et al. 2021). As well, it is important to note that even though substandard security measure has numerous connections, it is less influential due to their lower driving power when compared to subcontracting activities and incomplete contracts.

Finally, the MICMAC findings indicate that the nine key drivers of knowledge leakage in collaborative agreements can be classified into two main clusters. Based on the results, incomplete contracts and sub-contracting activities are placed under the Independent cluster. This indicates that incomplete contracts and subcontracting activities have a strong driving force, but a weak dependence power. This confirms their position at the bottom of the ISM hierarchy. A well-written contract, according to Qiu and Haugland (2019), specifies each company's rights and

responsibilities, along with the primary motive of the collaboration. In this regard, if a contract such as this is not available, it may lead to undesirable behaviours and traits, such as opportunism (Fawad Sharif et al. 2020a) and distrust (Fawad Sharif et al. 2022; Yang et al. 2019). It is therefore understandable why incomplete contracts attained the highest driving power as far as knowledge leakage in collaborative agreements is concerned. The remaining drivers, which include the existence of horizontal competition, distrust, perceived opportunism, insufficient technological expertise, expected incentives, and substandard security measures, are included in the Linkage cluster, which implies that they possess strong driving and dependence powers. Based on our findings, it appears that the drivers in the Linkage cluster have a relatively lower driving power than those in the Independent cluster, as this explains why the seven drivers in the Linkage cluster are placed at the top of the ISM hierarchy.

5.1. Implications

This study specifically contributes to the knowledge leakage research field by establishing interrelationships among drivers of knowledge leakage in collaborative agreements, in contrast to previous studies that have primarily focused on mediation-moderation relationships. This was achieved by first proposing an integrated ISM-MICMAC model and then by validating the model using a single case. Therefore, it can be argued that this study is one of those first attempts to integrate the ISM technique and MICMAC analysis to analyse knowledge leakage drivers. Further, the authors have attempted to answer calls for robust approaches in understanding the phenomenon of knowledge leakage by using a modelling research design approach (e.g., Li and Li 2021; Wu et al. 2021).

For practitioners, the study offers decision makers such as CEOs, managers, and directors a better understanding of the complexity of knowledge leakage when engaging in collaborative projects. Additionally, the findings provide risk managers in smaller businesses in particular with a list of key drivers of knowledge leakage that have been validated based upon opinions obtained from employees of the case firm in likely similar industries. It is also possible that these findings may be useful and relevant to risk managers working in other contexts. Moreover, it seems beneficial for project managers involved in collaborative projects to develop strategies for successfully implementing projects in response to the identified driver to minimise knowledge leakage concerns. In addition, the proposed integrated ISM-MICMAC model would also serve as a useful tool for managers to support their existing risk management frameworks.

6. Conclusions

In this study, drivers of knowledge leakage in collaborative agreements were analysed using an integrated ISM-MICMAC model validated by employees including the CEO of a magnetic processing firm located in Germany. Based on a literature review and supported by inputs obtained

from employees of the case firm, nine key drivers were identified and validated. Through the application of the ISM-MICMAC model, hierarchical interrelationships and classification of the drivers were achieved. While the ISM technique was helpful in establishing interrelationships, the MICMAC analysis assisted in classifying them according to their driving and dependence powers.

Hence, the major contribution of this study to theory is the development of the integrated ISM-MICMAC model, by fulfilling the proposed objectives. As a result, the study has attempted to answer the "what", "how", and "why" questions, which are fundamental to theory building (Whetten 1989). The "what" question has been answered by identifying drivers of knowledge leakage from the literature and validated based upon opinions obtained from employees of the case firm. By demonstrating the strength and power of these drivers through interpretive analysis, the "how" and "why" questions have also been addressed.

6.1. Limitation and Future Research Directions

Since the ISM-MICMAC model is based on a single firm (i.e., the small magnetic processing firm), it may be biased and limited in its application to one industry. It is therefore recommended that future research consider different contexts, including various types of industries and SMEs, in order to strengthen the generalisability of the findings. As nine drivers were identified for the development and validation of the model, future work may consider exploring additional drivers. From our findings, we discovered a few relationships among the drivers that we could not compare and contrast with literature since there were no studies regarding their nature; therefore, we may use system dynamics modelling (SDM) or statistical methods such as structural equation modelling (SEM) to verify these relationships in future studies. Finally, it may be worthwhile to employ longitudinal studies in the future to investigate the phenomenon of knowledge leakage over time, given its complexity.

References

Ahlfänger, Marcel, Hans Georg Gemünden, and Jens Leker. 2022. Balancing knowledge sharing with protecting: The efficacy of formal control in open innovation projects. International Journal of Project Management 40: 105–19. [CrossRef]

Ahmad, Atif, Rachelle Bosua, and Rens Scheepers. 2014. Protecting organizational competitive advantage: A knowledge leakage perspective. Computers & Security 42: 27–39. [CrossRef]

Ali, Sikandar, Samad Baseer, Irshad Ahmed Abbasi, Bader Alouffi, Wael Alosaimi, and Jiwei Huang. 2022. Analyzing the interactions among factors affecting cloud adoption for software testing: A two-stage ISM-ANN approach. Soft Computing 26: 8047–75. [CrossRef]

Altukruni, Hibah, Sean B. Maynard, Moneer Alshaikh, and Atif Ahmad. 2021. Exploring Knowledge Leakage Risk in Knowledge- Intensive Organisations: Behavioural aspects and key controls. arXiv arXiv:2104.07140.

Appio, Francesco Paolo, Federico Frattini, Antonio Messeni Petruzzelli, and Paolo Neirotti. 2021. Digital Transformation and Innovation Management: A Synthesis of Existing Research and an Agenda for Future Studies. Journal of Product Innovation Management 38: 4–20. [CrossRef]

Bakker, Elmer, Helen Walker, Fredo Schotanus, and Christine Harland. 2008. Choosing an organisational form: The case of collaborative procurement initiatives. International Journal of Procurement Management 1: 297–317.

Belderbos, René, Martin Carree, Bert Diederen, Boris Lokshin, and Reinhilde Veugelers. 2004. Heterogeneity in R&D cooperation strategies. International Journal of Industrial Organization 22: 1237–63. [CrossRef]

Belderbos, René, Martin Carree, Boris Lokshin, and Juan Fernández Sastre. 2015. Inter-temporal patterns of R&D collaboration and innovative performance. The Journal of Technology Transfer 40: 123–37. [CrossRef]

Bond-Barnard, Taryn Jane, Lizelle Fletcher, and Herman Steyn. 2018. Linking trust and collaboration in project teams to project management success. International Journal of Managing Projects in Business 11: 432–57. [CrossRef]

Bux, Hussain, Zhe Zhang, and Naveed Ahmad. 2020. Promoting sustainability through corporate social responsibility implementation in the manufacturing industry: An empirical analysis of barriers using the ISM-MICMAC approach. Corporate Social Responsibility and Environmental Management 27: 1729–48. [CrossRef]

Christina, Sarigianni, Thalmann Stefan, and Manhart Markus. 2016. Protecting Knowledge in the Financial Sector: An Analysis of Knowledge Risks Arising from Social Media. Paper presented at the 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, January 5–8.

Deniaud, Ioana Filipas, François Marmier, Didier Gourc, and Sophie Bougaret. 2016. A Risk Management Approach for Collaborative NPD Project. Paper presented at the 2016 International Conference on Industrial Engineering, Management Science and Application (ICIMSA), Jeju, Korea, May 23–26.

dos Santos Gonçalves, Paulo Vitor, and Lucila M. S. Campos. 2022. A systemic review for measuring circular economy with multi-criteria methods. Environmental Science and Pollution Research 29: 31597–611. [CrossRef] [PubMed]

Duperrin, Jean-Claude, and Michel Godet. 1973. Hierarchization Method for the Elements of a System. An Attempt to Forecast a Nuclear Energy System in Its Societal Context (CEA-R-4541),

France. Available online: https://inis.iaea.org/search/search.aspx? orig_q=RN:05115595 (accessed on 31 August 2022).

Durst, Susanne. 2020. Knowledge Risk Management in Organizations: Findings from Latin America. Multidisciplinary Business Review 15: 11–19. [CrossRef]

Durst, Susanne, and Helio Aisenberg Ferenhof. 2014. Knowledge Leakages and Ways to Reduce Them in Small and Medium-Sized Enterprises (SMEs). Information 5: 440–50. [CrossRef]

Durst, Susanne, and Malgorzata Zieba. 2019. Mapping knowledge risks: Towards a better understanding of knowledge management. Knowledge Management Research & Practice 17: 1–13. [CrossRef]

Durst, Susanne, Lena Aggestam, and Helio Aisenberg Ferenhof. 2015. Understanding knowledge leakage: A review of previous studies. VINE 45: 568–86. [CrossRef]

Dye, Ronald A., and Sri S. Sridhar. 2003. Investment Implications of Information Acquisition and Leakage. Management Science 49: 767–83. [CrossRef]

Elmsalmi, Manel, and Wafik Hachicha. 2013. Risks prioritization in global supply networks using MICMAC method: A real case study.

Paper presented at the 2013 International Conference on Advanced Logistics and Transport, Sousse, Tunisia, May 29–31.

Estrada, Isabel, Dries Faems, and Pedro de Faria. 2016. Coopetition and product innovation performance: The role of internal knowledge sharing mechanisms and formal knowledge protection mechanisms. Industrial Marketing Management 53: 56–65. [CrossRef]

Fang, Eric, Jongkuk Lee, Robert Palmatier, and Zhaoyang Guo. 2016. Understanding the Effects of Plural Marketing Structures on Alliance Performance. Journal of Marketing Research 53: 628–45. [CrossRef]

Fawad Sharif, Sayed Muhammad, Yang Naiding, Atiq Ur Rehman, Umar Farooq Sahibzada, and Fouzia Kanwal. 2020a. From partners' learning intent to knowledge leakage: The role of contract and trust. Knowledge Management Research & Practice 1–12. [CrossRef] Fawad Sharif, Sayed Muhammad, Yang Naiding, Yan Xu, and Atiq ur Rehman. 2020b. The effect of contract completeness on knowledge leakages in collaborative construction projects: A moderated mediation study. Journal of Knowledge Management 24: 2057–78. [CrossRef]

Fawad Sharif, Sayed Muhammad, Yang Naiding, and Sayed Kifayat Shah. 2022. Restraining knowledge leakage in collaborative projects through HRM. Vine Journal of Information and Knowledge Management Systems, ahead-of-print. [CrossRef]

Foli, Samuel. 2022. Total interpretive structural modelling (TISM) and MICMAC approach in analysing knowledge risks in ICT- supported collaborative project. Vine Journal of Information and Knowledge Management Systems 52: 394–410. [CrossRef]

Frishammar, Johan, Kristian Ericsson, and Pankaj C. Patel. 2015. The dark side of knowledge transfer: Exploring knowledge leakage in joint R&D projects. Technovation 41–42: 75–88. [CrossRef]

Galati, Francesco, Barbara Bigliardi, Alberto Petroni, Giorgio Petroni, and Giovanna Ferraro. 2019. A framework for avoiding knowledge leakage: Evidence from engineering to order firms. Knowledge Management Research & Practice 17: 340–52. [CrossRef] Garousi Mokhtarzadeh, Nima, Hannan Amoozad Mahdiraji, Ismail Jafarpanah, Vahid Jafari-Sadeghi, and Stefano Bresciani. 2021.

Classification of inter-organizational knowledge mechanisms and their effects on networking capability: A multi-layer decision making approach. Journal of Knowledge Management 25: 1665–88. [CrossRef]

Goel, Pankaj, Raman Kumar, Harish Kumar Banga, Swapandeep Kaur, Rajesh Kumar, Danil Yurievich Pimenov, and Khaled Giasin. 2022. Deployment of Interpretive Structural Modeling in Barriers to Industry 4.0: A Case of Small and Medium Enterprises. Journal of Risk and Financial Management 15: 171. [CrossRef]

Goi, Hoe Chin, Muhammad Mohsin Hakeem, and Frendy. 2022. Bridging Academics' Roles in Knowledge Diffusion in Sustainability- Driven Public-Private Partnerships: A Case Study of the SDGs Workshop in Central Japan. Sustainability 14: 2378. [CrossRef]

Govier, Trudy. 1994. Is It a Jungle Out There? Trust, Distrust and the Construction of Social Reality. Dialogue 33: 237–52. [CrossRef] Guo, Min, Naiding Yang, and Yanlu Zhang. 2021. Focal enterprises' control and knowledge transfer risks in R&D networks. European Journal of Innovation Management 24: 870–92. [CrossRef]

Guo, Wenyu, Jianjun Yang, Dan Li, and Chongchong Lyu. 2020. Knowledge sharing and knowledge protection in strategic alliances: The effects of trust and formal contracts. Technology Analysis & Strategic Management 32: 1366–78. [CrossRef]

Haleem, Abid, Sunil Luthra, Bisma Mannan, Sonal Khurana, Sanjay Kumar, and Sirajuddin Ahmad. 2016. Critical factors for the successful usage of fly ash in roads & bridges and embankments: Analyzing indian perspective. Resources Policy 49: 334–48. [CrossRef]

Hislop, Donald, Rachelle Bosua, and Remko Helms. 2018. Knowledge Management in Organizations: A Critical Introduction. Oxford: Oxford University Press.

Ho, Hillbun, and Shankar Ganesan. 2013. Does Knowledge Base Compatibility Help or Hurt Knowledge Sharing between Suppliers in Coopetition? the Role of Customer Participation. Journal of Marketing 77: 91–107. [CrossRef]

Hoffmann, Werner, Dovev Lavie, Jeffrey J. Reuer, and Andrew Shipilov. 2018. The interplay of competition and cooperation. Strategic Management Journal 39: 3033–52. [CrossRef]

Huo, Lisha, Yunfei Shao, Yi Jin, and Weijia Kong. 2022. Alliance coopetition and breakthrough innovation: The contributory roles of resources integration and knowledge ambiguity. Technology Analysis & Strategic Management 1–15. [CrossRef]

Hurmelinna-Laukkanen, Pia. 2011. Enabling collaborative innovation—Knowledge protection for knowledge sharing. European Journal of Innovation Management 14: 303–21. [CrossRef]

Jakhar, Suresh Kumar, and Mukesh Kumar Barua. 2014. An integrated model of supply chain performance evaluation and decision- making using structural equation modelling and fuzzy AHP. Production Planning & Control 25: 938–57. [CrossRef]

Jiang, Xu, Mei Li, Shanxing Gao, Yongchuan Bao, and Feifei Jiang. 2013. Managing knowledge leakage in strategic alliances: The effects of trust and formal contracts. Industrial Marketing Management 42: 983–91. [CrossRef]

Jiang, Xu, Yongchuan Bao, Yan Xie, and Shanxing Gao. 2016. Partner trustworthiness, knowledge flow in strategic alliances, and firm competitiveness: A contingency perspective. Journal of Business Research 69: 804–14. [CrossRef]

Jung, Seoyoung, Seulki Lee, and Jungho Yu. 2021. Identification and Prioritization of Critical Success Factors for Off-Site Construction Using ISM and MICMAC Analysis. Sustainability 13: 8911. [CrossRef]

Kaiser, Rene, Stefan Thalmann, and Viktoria Pammer-Schindler. 2021. An investigation of knowledge protection practices in inter- organisational collaboration: Protecting specialised engineering knowledge with a practice based on grey-box modelling. Vine Journal of Information and Knowledge Management Systems 51: 713–31. [CrossRef]

Kleber, Matheus, Néstor Fabián Ayala, Marie-Anne Le Dain, Érico Marcon, and Alejandro Germán Frank. 2019. Knowledge sharing in collaborative new product development: A study of grey box supplier involvement configuration. Production 29: e20180071. [CrossRef]

Kunttu, Leena, and Yrjö Neuvo. 2019. Balancing learning and knowledge protection in university-industry collaborations. The Learning Organization 26: 190–204. [CrossRef]

Lee, Hau L. 2002. Aligning Supply Chain Strategies with Product Uncertainties. California Management Review 44: 105–19. [CrossRef] Li, Qian, and Yuanfei Kang. 2019. Knowledge Sharing Willingness and Leakage Risk: An Evolutional Game Model. Sustainability 11: 596. [CrossRef]

Li, Xingong, and Xiaokai Li. 2021. The impact of different internet application contexts on knowledge transfer between enterprises. Systems 9: 87. [CrossRef]

Mathiyazhagan, Kaliyan, Kannan Govindan, A.Noorul Haq, and Yong Geng. 2013. An ISM approach for the barrier analysis in implementing green supply chain management. Journal of Cleaner Production 47: 283–97. [CrossRef]

Nishat Faisal, Mohd, Devinder Kumar Banwet, and Ravi Shankar. 2007. Information risks management in supply chains: An assessment and mitigation framework. Journal of Enterprise Information Management 20: 677–99. [CrossRef]

Norman, Patricia M. 2002. Protecting knowledge in strategic alliances: Resource and relational characteristics. The Journal of High Technology Management Research 13: 177–202. [CrossRef]

Oxley, Joanne E., and Rachelle C. Sampson. 2004. The Scope and Governance of International R&D Alliances. Strategic Management Journal 25: 723–49.

Oxley, Joanne, and Tetsuo Wada. 2009. Alliance Structure and the Scope of Knowledge Transfer: Evidence from U.S.-Japan Agreements. Management Science 55: 635–49. [CrossRef]

Papadas, Karolos-Konstantinos, George J. Avlonitis, Marylyn Carrigan, and Lamprini Piha. 2019. The interplay of strategic and internal green marketing orientation on competitive advantage. Journal of Business Research 104: 632–43. [CrossRef]

Pateman, Hilary, Stephen Cahoon, and Shu-Ling Chen. 2016. The Role and Value of Collaboration in the Logistics Industry: An Empirical Study in Australia. The Asian Journal of Shipping and Logistics 32: 33–40. [CrossRef]

Qiu, Xinlu, and Sven A. Haugland. 2019. The role of regulatory focus and trustworthiness in knowledge transfer and leakage in alliances. Industrial Marketing Management 83: 162–73. [CrossRef]

Ramos, Edgar, Timothy J. Pettit, Mamun Habib, and Melissa Chavez. 2021. A model ISM-MICMAC for managing risk in agri-food supply chain: An investigation from the Andean region of Peru. International Journal of Value Chain Management 12: 62–85. [CrossRef]

Ravi, V., and Ravi Shankar. 2005. Analysis of interactions among the barriers of reverse logistics. Technological Forecasting and Social Change 72: 1011–29. [CrossRef]

Raza-Ullah, Tatbeeq. 2021. When does (not) a coopetitive relationship matter to performance? An empirical investigation of the role of multidimensional trust and distrust. Industrial Marketing Management 96: 86–99. [CrossRef]

Raza-Ullah, Tatbeeq, and Jessica Eriksson. 2017. Knowledge Sharing and Knowledge Leakage in Dyadic Coopetitive Alliances Involving SMEs. In Global Opportunities for Entrepreneurial

Growth: Coopetition and Knowledge Dynamics within and across Firms. Edited by Stavros Sindakis and Panagiotis Theodorou. Bradford: Emerald Publishing Limited, pp. 229–52.

Ritala, Paavo, Heidi Olander, Snejina Michailova, and Kenneth Husted. 2015. Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study. Technovation 35: 22–31. [CrossRef]

Scaliza, Janaina Aparecida Alves, Daniel Jugend, Charbel Jose Chiappetta Jabbour, Hengky Latan, Fabiano Armellini, David Twigg, and Darly Fernando Andrade. 2022. Relationships among organizational culture, open innovation, innovative ecosystems, and performance of firms: Evidence from an emerging economy context. Journal of Business Research 140: 264–79. [CrossRef]

Serna, Carlos Andrés González, Rachelle Bosua, Atif Ahmad, and Sean B. Maynard. 2017. Strategies to Mitigate Knowledge Leakage Risk caused by the use of mobile devices: A Preliminary Study. Paper presented at the 38th International Conference on Information Systems (ICIS 2017), Seoul, Korea, December 10–13; pp. 1–24.

Shabtai, Asaf, Yuval Elovici, and Lior Rokach. 2012. A Survey of Data Leakage Detection and Prevention Solutions. New York: Springer Science & Business Media.

Singh, Mahipal, Pankaj Kumar, and Rajeev Rathi. 2019. Modelling the barriers of Lean Six Sigma for Indian micro-small medium enterprises. The TQM Journal 31: 673–95. [CrossRef]

Sushil, S. 2012. Interpreting the Interpretive Structural Model. Global Journal of Flexible Systems Management 13: 87–106. [CrossRef] Tan, Kim Hua, Wai Peng Wong, and Leanne Chung. 2016. Information and Knowledge Leakage in Supply Chain. Information Systems Frontiers 18: 621–38. [CrossRef]

Taylor, Andrew. 2005. An operations perspective on strategic alliance success factors. International Journal of Operations & Production Management 25: 469–90. [CrossRef]

Tidd, Joe, and Yasuhiko Izumimoto. 2002. Knowledge exchange and learning through international joint ventures: An Anglo-Japanese experience. Technovation 22: 137–45. [CrossRef]

Troche-Escobar, Jorge Arnaldo, Herman Augusto Lepikson, and Francisco Gaudêncio Mendonça Freires. 2018. A Study of Supply Chain Risk in the Brazilian Wind Power Projects by Interpretive Structural Modeling and MICMAC Analysis. Sustainability 10: 3442. [CrossRef]

Vafaei-Zadeh, Ali, Thurasamy Ramayah, Haniruzila Hanifah, Sherah Kurnia, and Imran Mahmud. 2020. Supply chain information integration and its impact on the operational performance of manufacturing firms in Malaysia. Information & Management 57: 103386. [CrossRef]

Wagner, Stephan M., and Nikrouz Neshat. 2010. Assessing the vulnerability of supply chains using graph theory. International Journal of Production Economics 126: 121–29. [CrossRef]

Wang, Lei, Jun Li, and Shengjun Wang. 2021. Rivalling firms' absorptive capacity congruence in coopetition relationships: The reciprocal effects on firms' innovation performance. Knowledge Management Research & Practice, 1–16. [CrossRef]

Warfield, John N. 1973. On Arranging Elements of a Hierarchy in Graphic Form. IEEE Transactions on Systems, Man, and Cybernetics SMC-3: 121–32. [CrossRef]

Wayne Gould, Robert. 2012. Open innovation and stakeholder engagement. Journal of Technology Management & Innovation 7: 1–11. Wei, Zelong, Zhanhe Du, and Yongchuan Bao. 2018. Outsourcer Knowledge Protection, Psychological Contract Schema, and Project Performance: A Vendor's Perspective. IEEE Transactions on Engineering Management 65: 128–40. [CrossRef]

Whetten, David A. 1989. What Constitutes a Theoretical Contribution? The Academy of Management Review 14: 490–95. [CrossRef]

Williamson, Oliver E. 1975. Markets and hierarchies: Analysis and antitrust implications: A study in the economics of internal organization. In University of Illinois at Urbana-Champaign's Academy for Entrepreneurial Leadership Historical Research Reference in Entrepreneurship. New York: Free Press.

Wu, Haizhen, Zhao'an Han, and Yong Zhou. 2021. Optimal degree of openness in open innovation: A perspective from knowledge acquisition & knowledge leakage. Technology in Society 67: 101756. [CrossRef]

Wu, Zezhou, Kaijie Yang, Hong Xue, Jian Zuo, and Shenghan Li. 2022. Major barriers to information sharing in reverse logistics of construction and demolition waste. Journal of Cleaner Production 350: 131331. [CrossRef]

Yang, Miaomiao, Juanru Wang, and Xiaodi Zhang. 2021. Boundary-spanning search and sustainable competitive advantage: The mediating roles of exploratory and exploitative innovations. Journal of Business Research 127: 290–99. [CrossRef]

Yang, Qian, Yi Liu, and Yuan Li. 2019. How do an alliance firm's strategic orientations drive its knowledge acquisition? Evidence from Sino-foreign alliance partnership. Journal of Business & Industrial Marketing 34: 505–17. [CrossRef]

Zeiringer, Johannes P., and Stefan Thalmann. 2022. Knowledge sharing and protection in data-centric collaborations: An exploratory study. Knowledge Management Research & Practice 20: 436–48. [CrossRef]

Zhang, Da Yong, Yong Zeng, Lingyu Wang, Hongtao Li, and Yuanfeng Geng. 2011. Modeling and evaluating information leakage caused by inferences in supply chains. Computers in Industry 62: 351–63. [CrossRef]

Zhao, Guohao, Rahil Irfan Ahmed, Naveed Ahmad, Cheng Yan, and Muhammad Shahjahan Usmani. 2021. Prioritizing critical success factors for sustainable energy sector in China: A DEMATEL approach. Energy Strategy Reviews 35: 100635. [CrossRef]

Zhao, Xiaoting, and Liang Liang. 2011. The impact of openness on innovation performance of China's firms: From the perspective of knowledge attributes. Paper presented at the 2011 IEEE International Conference on Industrial Engineering and Engineering Management, Singapore, December 6–9.

Zhao, Xiande, Jinxing Xie, and W. J. Zhang. 2002. The impact of information sharing and ordering co-ordination on supply chain performance. Supply Chain Management: An International Journal 7: 24–40. [CrossRef]

Zhou, Jia, Aifang Guo, Yutao Chen, and Jin Chen. 2022. Original Innovation through Inter-Organizational Collaboration: Empirical Evidence from University-Focused Alliance Portfolio in China. Sustainability 14: 6162. [CrossRef]

Zieba, Malgorzata, Susanne Durst, and Christoph C. Hinteregger. 2022. The impact of knowledge risk management on sustainability. Journal of Knowledge Management 26: 234–58. [CrossRef]

5. Development and validation of the framework

In this chapter, a complementary study is presented, focusing on the development of the TISM-DEMATEL-PROMETHEE framework. The goal of this chapter - serving as a step toward achieving the overall aim of the thesis - is to develop an integrated framework by adapting the models introduced in *Article I*, *Article II*, and *Article III*, and combining them with the PROMETHEE model. This integrated framework is then validated using a case company.

To build a clear understanding of the proposed framework, the subsequent sections provide a detailed explanation of each model, starting with TISM, followed by DEMATEL and PROMETHEE. Next, the proposed framework is presented and discussed, and in the final section, a case company validation is presented.

5.1. Development of TISM-DEMATEL-PROMETHEE framework

In this section, the steps involved in developing the framework are explained in greater detail. Given that assessing (knowledge) risks can be viewed as an integral part of risk management activities, the framework is designed with a generic approach but is specifically tailored to address knowledge risks.

5.1.1. Steps in TISM

The TISM is an extension of the ISM, which was originally developed by Warfield in the 1970s. TISM builds upon the foundations of ISM by incorporating an interactive learning process to derive logical insights from complex systems and support theory building (Menon and Suresh, 2020). The key difference between ISM and TISM is that TISM not only identifies the elements within a system but also demonstrates both direct and transitive relationships between them, resulting in a fully interpretive structural model (Obi et al., 2020; Sushil, 2012). This allows for a more comprehensive understanding of the interconnections and dependencies within the system.

In this case, TISM is employed to understand the interrelations between threats/risk factors associated with the knowledge risks under study. The estimates of these risks are then used to predict the interrelationships among their respective knowledge risk factors. Incorporating this interrelationship information into the risk analysis expands the criteria and provides deeper insights

into the nature and characteristics of these knowledge risk factors. The various steps involved in TISM are presented below, providing valuable insights for developing the final framework:

Step 1: Establish and define the risk factors.

The initial step in the TISM process, akin to ISM, involves identifying and defining the knowledge risk factors. Begin by reviewing relevant literature to identify potential knowledge risk factors. Subsequently, validate these factors through consultations with stakeholders, experts, or participants via surveys or focus group discussions to establish their relevance.

Step 2: Development of the contextual relationship

The contextual relationship is then established by incorporating inputs from involved participants or experts, which may include academics and industry professionals. This process utilises a guideline of four conventional symbols, widely used in the literature (e.g., Sushil, 2012), to assign relationships among the knowledge risk factors:

- *V* for a forward relation from knowledge risk factor *i* to *j* (knowledge risk *i* will influence knowledge risk factor *j*, $i \rightarrow j$).
- *A* for a backward relation from knowledge risk factor *i* to *j* (risk j will influence knowledge risk factor *i*, $j \rightarrow i$).
- *X* for a bidirectional relation between knowledge risk factors *i* and *j* (knowledge risk factors i and j will influence each other, $i \leftrightarrow j$).
- for no relation existing between knowledge risk factors *i* and *j* (knowledge risk factors *i* and *j* have no influence on each other).

Step 3: Structural self-interaction matrix (SSIM)

With the contextual relationships established, the inputs are presented in the form of a matrix known as SSIM, as shown in **Table 6** as illustration.

Table 6 Structured Self-Interaction Matrix

	R_1	R_2	R_3	. . . .	R_j
R_1		V	V	V V V	V
R_2			V	V V V	V

.				V	V	V	V
.					V	V	V
.						V	V
							V
R_i							

Step 4: Reachability matrix (RM)

The subsequent step involves transforming the SSIM derived in the previous section into an initial reachability matrix (RM). To achieve this, each cell entry in the SSIM is converted into binary representation, using 0's and 1's. A cell entry with zero signifies no interrelationship between the knowledge risk factors, while a cell entry with one indicates the presence of an interrelationship between them. To perform this transformation, the following rules (adapted from Bux et al., 2020) are applied:

- For SSIM cell entries (i, j) denoted by V, the initial RM cell entries (i, j) become 1, and (j, i) become 0.
- For SSIM cell entries (i, j) denoted by A, the initial RM cell entries (i, j) become 0, and (j, i) become 1.
- For SSIM cell entries (i, j) denoted by X, the initial RM cell entries (i, j) and (j, i) both become 1.
- For SSIM cell entries (i, j) denoted by O, the initial RM cell entries (i, j) and (j, i) both become 0.

After applying these rules, the initial reachability matrix is determined. This initial reachability matrix is then used to determine the final reachability matrix based on the transitivity rule. The transitivity rule dictates that if knowledge risk factor *i* influences knowledge risk factor *j* and knowledge risk factor *j* influences knowledge risk factor *k*, then knowledge risk factor *i* also has an influence on knowledge risk factor *k*. With the final reachability matrix in hand, the dependent and driving power of each knowledge risk can be computed and derived for utilisation in the PROMETHEE model.

5.1.2. Steps in DEMATEL

The DEMATEL approach is utilised to determine the weights of various criteria relevant to the study. The selection of criteria is tailored to the specific risk factors being analysed. In traditional risk assessment frameworks, probability (likelihood of occurrence) and impact (extent of potential damage) are often the primary criteria used to assess risks. These metrics offer a simple yet effective method for evaluating both the likelihood of a risk event and the potential severity of its consequences.

The DEMATEL procedure, as adapted from Chang et al. (2011), and Shieh et al. (2010), is summarised as follows:

Step 1: Develop a direct relation matrix.

A direct-relation matrix is computed by seeking evaluations from each respondent regarding the direct influence between any two criteria. Respondents use a linguistic scale with integer scores ranging from 1 to 5, representing 'equal importance', 'moderate importance', 'strong importance', 'very important', and 'extremely important', respectively.

The notation of $\otimes Z_{ij}$ indicates the degree to which the respondent believes criterion *i* is important in relation to criterion *j*. For cases where *i*=*j*, the diagonal elements are set to 1. For each respondent, a matrix is established as:

$$X^k = [X_{ij}^k]$$

Where k is the number of respondents with $1 \leq k \leq H$, and n is the number of criteria. Thus, $X^1, X^2, \ldots, X^H$ are the matrices corresponding to H respondents. To combine all the inputs from these respondents, the average matrix $Z = [\otimes Z_{ij}]$ can be constructed as follows:

$$\otimes Z_{ij} = \frac{1}{H}\sum_{k=1}^{H} X_{ij}^k$$

Step 2: Formulate the normalised direct relation matrix.

The overall relation matrix is transformed into the normalised direct-relation matrix *N* using Equations (1) – (3).

$$\otimes s = \left[\underline{s}, \underline{s}\right] = \frac{1}{\frac{max}{1\leq i\leq n} = \sum_{j=1}^{n} \otimes Z_{ij}} \quad i, j = 1,2,3, \ldots n \qquad (1)$$

$$N = \otimes s * Z \quad (2)$$

$$\otimes n_{ij}[\underline{s} * \otimes z_{ij}\ ,\ \underline{s} * \otimes z_{ij}\ ] \quad (3)$$

Step 3: Compute the total relation matrix.

The total relation matrix *T* is determined by using Equation (4):

$$T = N(I - N)^{-1} \quad (4)$$

Where *I* if the identity matrix

Step 4: Compute the causal parameters.

The causal parameter is determined using Equations (5) and (6):

$$\otimes R_i = \sum_{j=1}^{n} t_{ij}\ \Theta_i \quad (5)$$

$$\otimes C_j = \sum_{i=1}^{n} t_{ij}\ \Theta_j \quad (6)$$

$\otimes R_i$ represents the direct and indirect influence of criterion *i* on the other criteria, while $\otimes C_j$ represents the influence received by criterion *j* from the other criteria.

Step 5: Calculate the prominence (P_i)

The prominence (P_i) of the criteria is determined using Equations (*7*):

$$\otimes P_i = \otimes R_i + \otimes C_i\ ,\ i = j \quad (7)$$

5.1.3. Steps in PROMETHEE

Lastly, the PROMETHEE approach, as an outranking method, is employed to rank the risk factors understudy. According to Altun et al. (2019), the algorithm's process involves the following steps:

Step 1: Calculate the deviations from the comparison of two knowledge risk factors based on the j-th criterion, using equation (8):

$$(a, b) = f_j(a) - f_j(b)\ j = 1, 2, \ldots . k \quad (8)$$

where j represents the j-th criterion, and k is the total number of criteria considered. Additionally, $f_j(a)$ denotes the value of the j-th criterion for risk "a."

Step 2: Determine the preference function using equations (9) and (10):

$$(a, b) = F_j(a, b) \; j = 1, 2, \ldots . k \quad (9)$$

$$0 \leq P_j \leq 0 \; j = 1, 2, \ldots . k \quad (10)$$

where $P_j \; (a, b)$ defines the preference degree value of the j-th criterion for risks "a" and "b."

Step 3: Calculate the aggregated preference degrees for each possible pair of criteria using equation (11):

$$\pi(a, b) = \sum_{j=1}^{k}(a, b) \quad j = 1, 2, \ldots . k \quad (11)$$

Here, W_j represents the weight of the j-th criterion.

Step 4: In this step, calculate the values of outranking flows for all possible risks using equations (12) and (13). In these equations, "A" represents the set of risks, and the value of *Phi* + indicates the preference of the considered risk over other risks, while *Phi* - indicates the preference of other knowledge risk factors over the considered knowledge risk factor.

$$Þ^{+}(a) = \sum_{x \epsilon A} \pi(x, a) \quad (12)$$

$$Þ^{-}(a) = \sum_{x \epsilon A} \pi(a, x) \quad (13)$$

Step 5: Calculate the value of the net flow Þ(a), which represents the difference between the values of *Phi* + and *Phi* -. The higher the net Phi value, the better the option and the higher its rank. The value of Þ(a) is defined as follows:

$$Þ(a) = Þ^{+}(a) + Þ^{-}(a) \quad (14)$$

To achieve the overarching aim of this doctoral thesis, the study integrates the three models – TISM, DEMATEL, and PROMETHEE – into a unified framework designed to address the complex and interrelated nature of knowledge risks. This integrated framework leverages the strengths of each individual approach: TISM for capturing the interdependencies among knowledge risks and knowledge risk factors, DEMATEL for estimating the weights of the criteria, and PROMETHEE for prioritising and evaluating the knowledge risk factors. The combined models provide a comprehensive framework for assessing knowledge risks in an organisational setting. A visual representation of the proposed framework is provided in **Figure 9**.

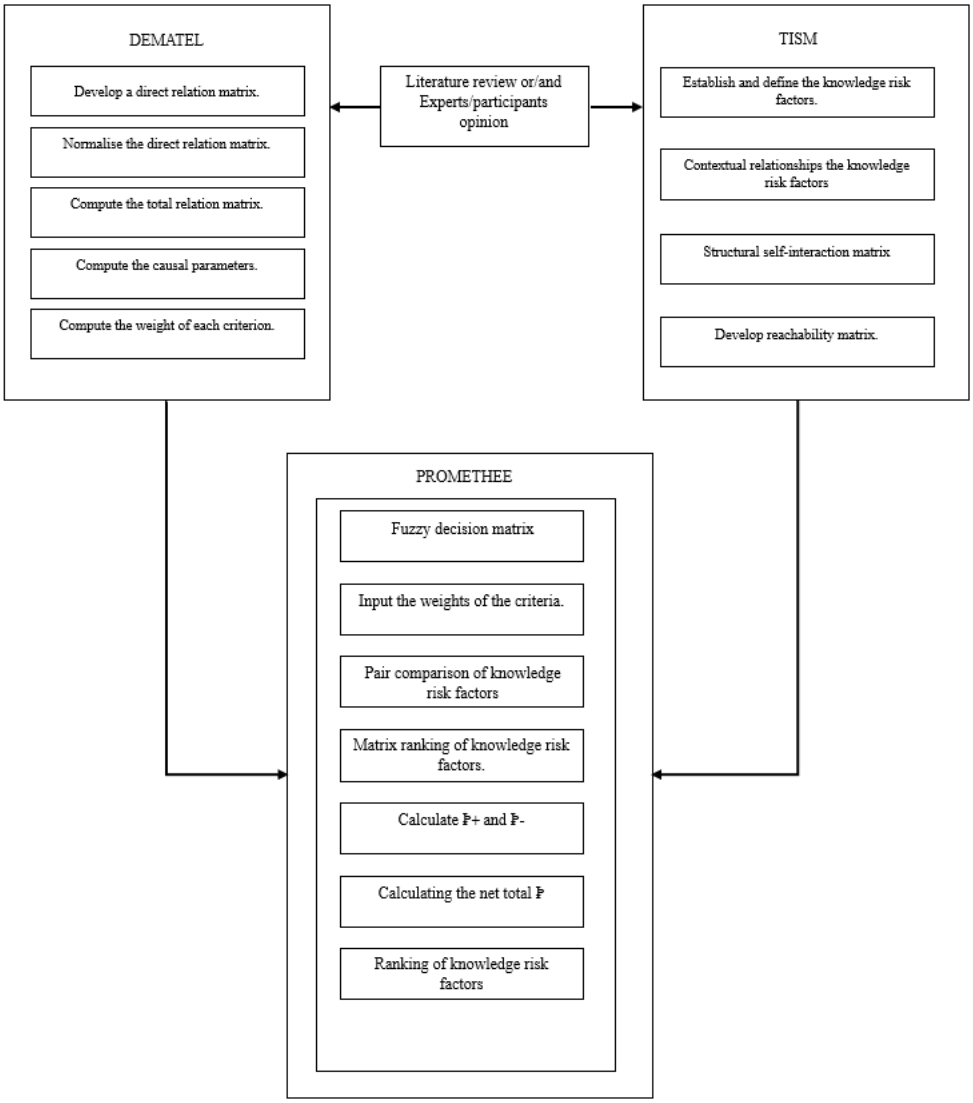


Figure 9 The proposed framework for assessment of knowledge risks.

5.2. Application of the proposed framework

This section demonstrates the application of the proposed TISM-DEMATEL-PROMETHEE framework, with a specific focus on assessing knowledge leakage risks within a consulting firm, which serves as the case company. By applying the framework in this context, the study aims to highlight how the framework can identify, analyse, and prioritise knowledge leakage risks, providing actionable insights for managing these risks in an organisational setting. The consulting firm, referred to hereafter by the pseudonym ABC Company, was selected due to its reliance on

knowledge as a critical asset, making it a suitable context for testing the framework's relevance and practical utility.

5.2.1. Context of the study

ABC Company, located in Malta, is a consultancy firm that specialises in providing support and guidance to organisations looking to engage in strategic project investments. The company operates through several divisions, with the Advisory arm playing a major role. This includes services such as corporate valuations, internal audits, tailored business re-engineering using lean methodologies, assistance with securing funding (such as EU grants), human resource consulting, cost-benefit analysis and feasibility studies. This company was selected for the study due to its knowledge-intensive operations and reliance on intellectual capital, which are critical to its competitive advantage and service delivery. The nature of its work, which involves managing sensitive information and leveraging expert-driven solutions, makes it an ideal setting for evaluating the proposed framework's ability to assess knowledge leakage risks.

Access to ABC Company was facilitated through the researcher's position as an employee within the organisation. This role provided an in-depth understanding of the company's processes, challenges, and knowledge flows, as well as the opportunity to engage with key stakeholders, including employees and senior management. This unique insider perspective ensured access to relevant data and meaningful insights, allowing for a thorough application and validation of the proposed framework.

Currently, through its Advisory arm, ABC Company is engaged in a project for a public-private agency in Malta. The project involves a detailed market study aimed at identifying business opportunities, collaboration avenues, investment prospects, and growth potential within the financial services sector in Malta and a targeted Asian nation.

The project presents particular challenges due to tight timelines and the requirement to engage multiple local and international stakeholders, as well as the need for close collaboration with subject matter experts essential to its delivery. Despite these challenges, the advisory team is actively working to keep the project objectives on course. However, management is concerned about the risk of knowledge leakage, as the skills, frameworks, methodologies, and insights

developed during the project could potentially be appropriated by external subject matter experts, partners, or other third-party entities involved.

To address management's concerns, the researcher proposed and applied the TISM-DEMATEL-PROMETHEE framework to assess the risk of knowledge leakage, enabling the implementation of tailored safeguards/controls to protect proprietary knowledge throughout the course of the project.

5.2.2. Approach adopted

To assess the risk of knowledge leakage, this study first identifies potential threats that could lead to unauthorised use or disclosure of ABC's proprietary knowledge assets, including skills, frameworks, methodologies, and insights developed during the project. These threats, referred to as risk factors in this study.

The identification of these risk factors[8] builds upon the analysis conducted in Article II of this thesis, where risk factors relevant to knowledge leakage were identified. A summary of these identified risk factors is presented in **Table 7**.

Table 7 List of knowledge leakage risk factors

Codes	Risk factors	Descriptions	References
RF01	Distrust	Neither of the partners involved in collaborative agreements can be relied upon by the other.	Qiu and Haugland (2019), Jiang et al. (2016), Yang et al. (2019), Taylor (2005), Guo et al. (2020), Deniaud et al. (2016), Fawad Sharif et al. (2020, 2024), Vafaei-Zadeh et al. (2020)
RF02	Incomplete contracts	Weak or no legal contract in place to protect the core knowledge of partners involved in the collaboration.	Jiang et al. (2013), Yang et al. (2019), Taylor (2005), Guo et al. (2020), Ahlfänger et al. (2022), Deniaud et al. (2016), Fawad Sharif et al. (2020)
RF03	Substandard security measures	Lack or inadequate security guidelines to oversee knowledge exchange between partners in collaborative arrangements.	Hislop et al. (2018), Durst and Zieba (2019), Frishammar et al. (2015), Altukruni et al. (2021)

[8] [8] Please refer to Article III

RF04	Weak Bring your own device (BYOD) policies	A lack of strict rules underpinning BYOD policies could expose the focal and partner firms' core knowledge to cyberattacks (third party).	Serna et al. (2017), Shabtai et al. (2012), Altukruni et al. (2021)
RF05	Insufficient technological competence	Emerging technologies used in collaborative arrangements put a firm's core knowledge at risk of leakage due to a lack of tech know-how.	Ahmad et al. (2014), Hislop et al. (2018), Jiang et al. (2013), Sarigianni et al. (2016), Altukruni et al. (2021), Zeiringer and Thalmann (2022)
RF06	Perceived opportunism	Partners attempt to gain an advantage by misappropriating the core knowledge of the focal firm.	Estrada et al. (2016), Norman (2002), Oxley and Wada (2009), Fawad Sharif et al. (2023, 2024)
RF07	Expected incentives	The act of exposing core knowledge to a partner or external party for an incentive by a player in collaborative arrangements.	Tan et al. (2016)
RF08	Existence of horizontal competition	Cooperation encourages partners to take advantage of exposed core knowledge.	Lee (2002), Zhao et al. (2002)
RF09	Sub-contracting activities	Cooperation agreements between firms often result in subcontracting activities rather than collaborations, which often result in unknowingly transferred core knowledge.	Tan et al. (2016), Foli (2022), Nishat Faisal et al. (2007), Dye and Sridhar (2003), Zhang et al. (2011)

With these identified knowledge risk factors, a discussion session was conducted to refine and validate them with the project participants. These participants were actively engaged in the project through activities such as kick-off meetings, regular team discussions, idea exchanges, and task execution.

During the session, participants reviewed the list of risk factors to ensure alignment with the project's specific context and challenges. Based on their input, the risk factor "Expected incentives" was excluded, as it was considered less relevant to knowledge leakage in this case. "Informal knowledge sharing" and "Lack of continuous monitoring" were added to the list. **Table 8** presents the finalised and refined list of knowledge leakage risk factors along with remarks.

Table 8 Final list of knowledge leakage risk factors

Codes	Risk factors	Remarks
RF01	Distrust among partners	Participants noted that a lack of trust between the company and external collaborators could result in cautious behaviour, with some parties withholding information. Conversely, distrust could also lead to opportunistic behaviour, where collaborators might exploit the company's methodologies, increasing the risk of proprietary insights being misappropriated.
RF02	Incomplete contracts	Several participants expressed concerns about contracts that did not clearly define intellectual property ownership, confidentiality terms, or usage limitations on the company's proprietary knowledge. They felt that such gaps could provide opportunities for external collaborators to exploit or copy unique insights and processes developed by the company.
RF03	Substandard security measures	Participants pointed out that inadequate security measures could expose proprietary data to unauthorised access by third parties. They highlighted that the lack of robust security protocols increases the risk of knowledge leakage.
RF04	Weak BYOD policies	The participants discussed the risks associated with allowing external collaborators to use their personal devices to access sensitive project data. They noted that without stringent security measures, this practice could lead to accidental leaks of proprietary research methodologies or frameworks, especially when multiple stakeholders are involved.
RF05	Insufficient technological competence	Some participants raised concerns that external partners lacking technological competence might mishandle sensitive information or fail to use secure platforms. This, they noted, could unintentionally expose the company's proprietary knowledge to third parties.
RF06	Perceived opportunism among external partners	Participants expressed worries that external partners perceived as opportunistic might exploit their access to the company's methodologies, frameworks, or insights for their own benefit. This could happen without regard for contractual or ethical obligations, leading to the misuse of proprietary knowledge.
RF07	Existence of horizontal competition	Participants noted the risk posed by working with collaborators from the same industry. They expressed concern that competitors might gain access to the company's proprietary research processes and methodologies and potentially replicate them to enhance their own competitive position.

RF08	Subcontracting activities	Several participants highlighted the risks associated with subcontracting portions of the project. They emphasised that subcontractors who are not bound by strict confidentiality agreements or who lack proper oversight might inadvertently or intentionally misuse the company's proprietary methodologies in other projects.
RF09	Informal knowledge sharing	Participants discussed the potential for unintentional knowledge leakage during informal conversations, meetings, or calls with external stakeholders. They highlighted that unstructured sharing of proprietary insights in such settings could result in sensitive information being disclosed.
RF10	Lack of continuous monitoring	Some participants raised concerns about the absence of continuous monitoring of external partners' access to proprietary knowledge throughout the project lifecycle. Without this oversight, there is a heightened risk of unauthorised replication or misuse of the company's methodologies and frameworks.

Following the validation of the risk factors, the next step involved applying Total Interpretive Structural Modelling (TISM) to model these factors, with a focus on estimating and understanding their interrelationships.

Phase I. Determining the risk factor's dependence and driving power.

In this phase, the computation of driving and dependency values for each risk factor was carried out. The process began with the development of a questionnaire (see **Appendix A2**) in the form of a matrix, designed to assess the pairwise relationships between the identified risk factors, specifically evaluating whether one factor influences another.

The participants' responses were aggregated and are presented in **Appendix A3**. This aggregated matrix served as the foundation for constructing the initial reachability matrix (IRM), which identifies and maps the direct relationships between the risk factors.

Subsequently, the final reachability matrix was computed, incorporating both direct and indirect relationships between the risk factors. This matrix was iteratively refined to capture all transitive

relationships, ensuring that both direct and indirect influences between the factors were accurately represented.

The final step in this phase involved calculating the driving power and dependent power for each risk factor. Driving power reflects the extent to which a risk factor influences others, while dependent power measures how much a risk factor is influenced by other factors. The driving power and dependent power for each risk factor are presented in the table below:

Table 9 Final reachability matrix

	RF1	RF2	RF3	RF4	RF5	RF6	RF7	RF8	RF9	RF10	Driving Power
RF1	1	1	1	1	1	1	1	1	1	1	**10**
RF2	0	1	0	1	1	0	1	1	1	1	**7**
RF3	0	1	1	1	1	0	1	1	1	1	**8**
RF4	0	1	0	1	1	0	1	1	1	1	**7**
RF5	0	0	0	0	1	0	0	0	0	0	**1**
RF6	1	1	1	1	1	1	1	1	1	1	**10**
RF7	0	1	0	1	1	0	1	1	1	1	**7**
RF8	0	1	0	1	1	0	1	1	1	1	**7**
RF9	0	0	0	0	0	0	0	0	1	0	**1**
RF10	0	1	0	1	1	0	1	1	1	1	**7**
Dependency Power	**2**	**8**	**3**	**8**	**9**	**2**	**8**	**8**	**9**	**8**	

These values will be used in the PROMETHEE analysis in Phase III. The next phase involves determining the weights for the criteria of these risk factors.

Phase II. Calculating the weights of the criteria.

As mentioned earlier, risk assessment frameworks, traditionally, often rely on likelihood and severity as primary criteria for assessing risks. Building upon this foundation and recognising from Phase I that knowledge risks often exhibit interconnections - where risk factors may influence one another - this study introduces two additional criteria: driving power and dependency power. These added criteria are essential for examining both the individual behaviours of risk factors and the ways in which they interact with and affect one another. As a result, the following six criteria are included using DEMATEL to calculate their weights: probability, severity, driving power, and dependency power. The definitions of these criteria are presented in **Table 10.**

Table 10 Criteria definition

Criteria	**Definition**
Likelihood	The likelihood or frequency of the risk factor leading to knowledge leakage.
Severity	The potential impact or damage caused by knowledge leakage when the risk occurs.
Dependency power	The extent to which a risk factor is influenced or dependent on other risk factors.
Driving power	The degree to which a risk factor drives or influences other risk factors.

In this phase, the objective was to assign weights to each criterion, recognising that their relevance may differ. To achieve this, data was collected using a linguistic scale through discussions among the project members. The linguistic scale is presented in **Table 11**.

Table 11 Linguistic scale

Scale value	**Description**
1	Both criteria are equally important.
3	One criterion is moderately more important.
5	One criterion is significantly more important.

7	One criterion is much more important than the other.
9	One criterion is of utmost importance over the other.
2,4,6	Intermediate levels

Based on the responses collected, a pairwise comparison matrix was constructed to reflect the relative importance of each criterion against the others. Each entry in this matrix indicates how one criterion compares to another in terms of importance, as rated by the participants. Once the pairwise comparison matrix was established, it underwent normalisation to ensure that all values were proportionally adjusted, making the matrix consistent and comparable. From this normalised matrix, a total relation matrix was derived, capturing the overall influence each criterion has, both directly and indirectly, on every other criterion. The results for these matrices are provided in **Appendix A4** for reference.

The prominence values (Ri + Ci) for each criterion—calculated as the sum of the Ri and Ci values from the total relation matrix—were determined. Using these prominence values, the weights for each criterion were computed and are presented in **Table 12**.

Table 12 Final weights for each criterion

	Ri	**Ci**	**Prominence**	**Weight**
Likelihood	46.73	20.08	66.81	0.39
Severity	18.92	21.75	40.67	0.24
Dependency power	8.25	22.11	30.36	0.17
Driving power	11.93	21.90	33.84	0.20

Phase III. Computing the Phi value each of the risk factors.

In this final phase, the weights of each criterion from Phase II, combined with the driving and dependency power values determined in Phase I, as well as additional data on the likelihood and severity of each risk factor, are input into the PROMETHEE software[9] for analysis.

To gather the data, a meeting was held with nine participants, including the firm's senior partner. During this session, participants collaboratively discussed and assigned likelihood and severity values to each risk factor using the linguistic scales outlined in **Table 13** and **Table 14**, respectively.

Table 13 Likelihood linguistic scale

Qualitative descriptors	**Description**	**Range**
Very unlikely	Extremely low chance of occurrence; highly improbable	0.0-1.0
Unlikely	Low chance of occurrence but still possible.	0.5-2.0
Fairly unlikely	A reasonable possibility, but still less than likely.	1.5-3.5
Likely	Expected to happen with some regularity; more likely than not.	3.0-4.5
Very likely	Almost certain; expected to happen frequently.	4.0-5.0

Table 14 Severity linguistic scale

Qualitative descriptors	**Description**	**Range**
Negligible	Minimal impact with no significant consequences	0.0-1.0
Minor	Slight impact with minor effects	0.5-2.0
Moderate	Noticeable impact with potential operational disruption	1.5-3.5
Major	Significant impact with substantial effects.	3.0-4.5

[9] PROMETHEE Software. Available at http://www.promethee-gaia.net/phone/visual-promethee.html

Catastrophic	Severe impact with critical consequences	4.0-5.0

These responses are then consolidated and presented in **Table 15** below:

Table 15 Summary of the likelihood and severity of each risk factor

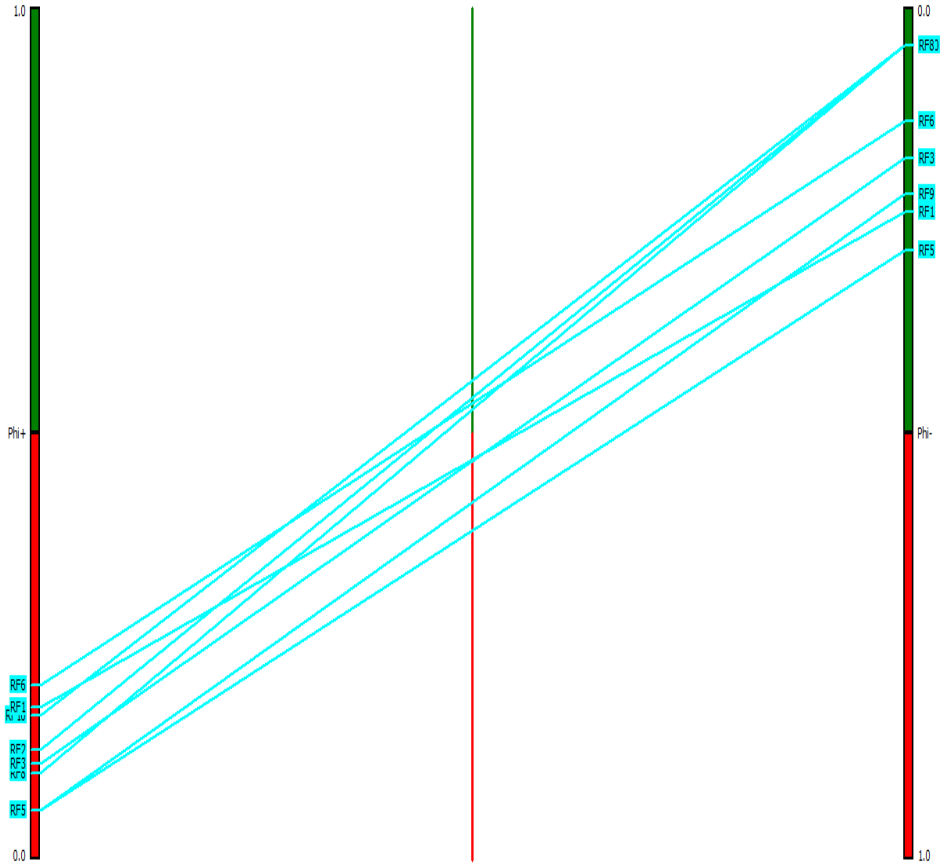
Risk factor	**Severity**	**Probability**
Distrust among partners	2.5 (Moderate)	2.5 (Fairly unlikely)
Incomplete contracts	4.0 (Major)	3.5 (Likely)
Substandard security measures	4.5 (Catastrophic)	3.5 (Likely)
Weak BYOD policies	3.5 (Major)	2.5 (Fairly unlikely)
Insufficient technological competence	2.5 (Moderate)	2.5 (Fairly unlikely)
Perceived opportunism among partners	4.0 (Major)	3.5 (Likely)
Existence of horizontal competition	4.5 (Catastrophic)	3.5 (Likely)
Subcontracting activities	3.5 (Major)	2.5 (Fairly unlikely)
Informal knowledge sharing	3.0 (Moderate)	3.5 (Likely)
Lack of continuous monitoring	4.5 (Catastrophic)	3.5 (Likely)

The PROMETHEE analysis was then conducted, resulting in the calculation of Phi, Phi+, and Phi- values for each risk, as presented in **Table 16**. The Phi value is obtained by subtracting Phi- from Phi+. Higher Phi values indicate a higher rank, with *RF07* and *RF10* both attaining the top Phi value of 0.1233, placing them first. *RF02* follows with a Phi value of 0.0833, with the third rank, and RF06 ranks fourth with a Phi value of 0.0722. On the other hand, *RF05* recorded the lowest Phi values of -0.2278, with the lowest rank.

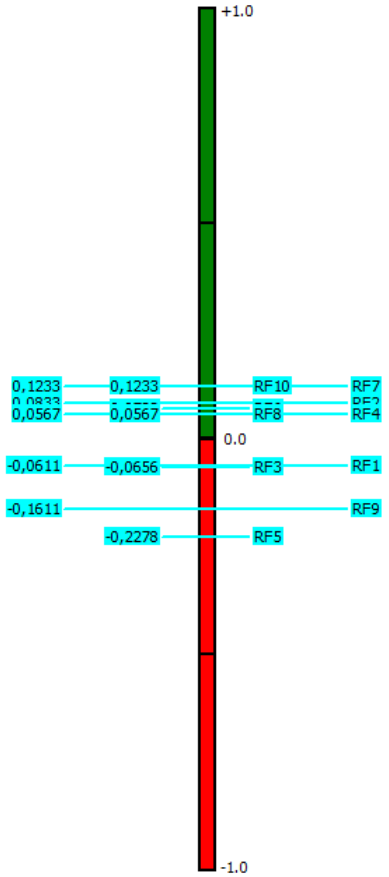
Table 16 Ranking, Phi, Phi- and Ph+ values for each risk

Rank	Risk	Phi	Phi+	Phi-
1	RF07	0,1233	0,1678	0,0444
1	RF10	0,1233	0,1678	0,0444
3	RF02	0,0833	0,1278	0,0444
4	RF06	0,0722	0,2044	0,1322
5	RF04	0,0567	0,1011	0,0444
5	RF08	0,0567	0,1011	0,0444
7	RF01	-0,0611	0,1778	0,2389
8	RF03	-0,0656	0,1111	0,1767
9	RF09	-0,1611	0,0567	0,2178
10	RF05	-0,2278	0,0567	0,2844

For visual analysis of the risk factors, both PROMETHEE I (partial ranking) and PROMETHEE II (complete ranking) are employed (see **Figure 10**). In PROMETHEE I, the left side presents the Phi+ values, which reflect the strengths or positive contributions of each risk factor. *RF06* holds the highest influence, followed by *RF01*. On the right side, the Phi- values highlight the weaknesses or negative contributions, with *RF08* and other risk factors with a Phi- of 0.0444 appearing at the top. This split helps identify which factors contribute positively or negatively to the overall evaluation. In PROMETHEE II, the complete ranking combines both Phi+ and Phi- values to create a single priority list. Here, *RF07* and *RF10* emerge as the top-ranked risk factors, followed closely by *RF02*.



PROMETHEE I (Partial ranking)



PROMETHEE II (Full ranking)

Figure 10 PROMETHEE ranking

Alternatively, the PROMETHEE diamond is used to visualise the proximity between Phi+ and Phi- scores, providing a two-dimensional joint representation of both PROMETHEE I and II rankings. From **Figure 11**, it is evident that *RF10* and *RF7*, exhibit a net positive preference, signifying they are prioritised higher in the ranking. Conversely, factors near the bottom, like *RF05* and *RF09*, display a net negative preference, placing them lower in priority.

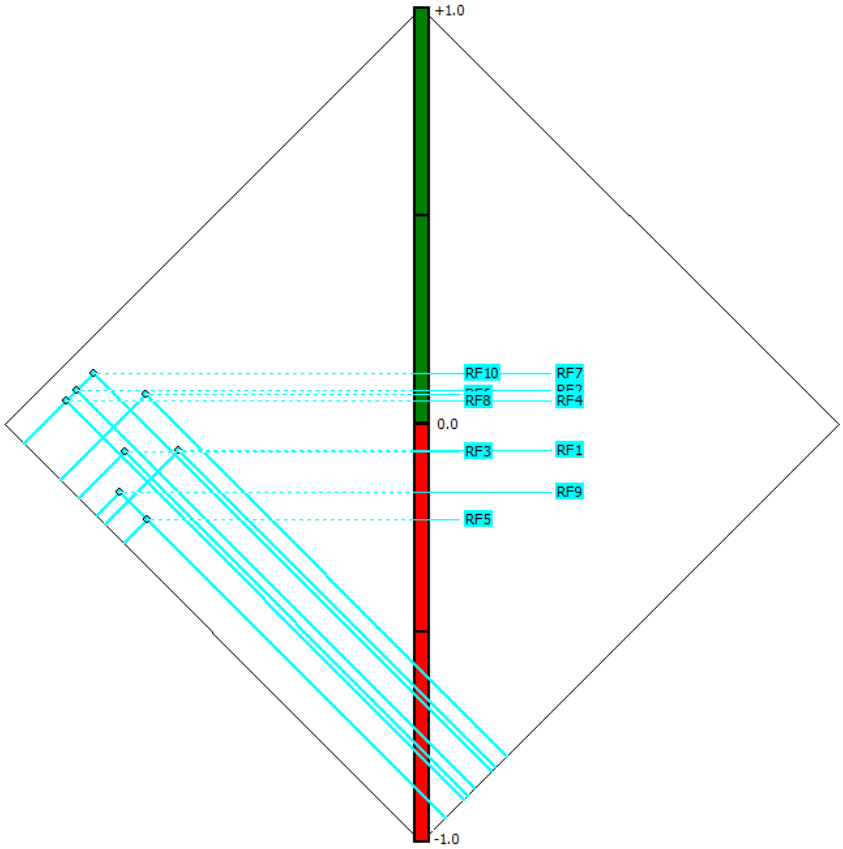


Figure 11 PROMETHEE diamond

Performing a criteria-risk analysis

The GAIA plane, incorporated into the visual PROMETHEE software, proves to be a valuable instrument for conducting criteria-risk assessment. This approach offers an optimal two-dimensional representation based on the U and V components, where U represents the primary principal component with the highest probable information values, while V signifies the secondary principal component that contributes maximum orthogonal supplementary information. It is worth

noting that the GAIA analysis[10] attains reliability when the quality threshold reaches approximately 70%. The present study achieves a quality level of 91.5%, emphasising the robustness of the outcomes obtained through this approach.

At its core, the GAIA plane maps each risk factor onto a distinct point. The placement of these points corresponds to the respective evaluations of risk factors across a defined set of criteria, thereby positioning risk factors with analogous attributes in closer proximity. In the illustrated **Figure 12**, for instance, *RF07 and RF10* overlap, and both appear close to *RF02* and *RF08*, indicating shared characteristics between these particular risk factors.

Turning to the criteria dimension, each criterion - such as severity, likelihood, dependency power, and driving power - influences the positioning and prioritisation of risk factors on the GAIA plane. The likelihood criterion, centrally located on the plane, moderately affects the various risk factors, with its direction suggesting a balanced impact across both positive and negative influences. Risk factors located closer to a criterion vector are notably influenced by that criterion. For instance, the dependency power criterion, positioned to the left of the GAIA plane, impacts *RF10*, *RF02*, and *RF08*, emphasising the degree to which these factors are dependent on other risks or conditions, thus making their evaluation sensitive to changes in dependency power. In contrast, *RF09* and *RF05* perform sub optimally across all criteria.

In addition, a red line on the GAIA plane represents the "preference direction," which indicates the optimal alignment of risk factors to maximise preference or minimise risk factor. The orientation of this line points toward the ideal direction for criteria influence, serving as a guide for prioritising risk factors effectively.

[10] Visual PROMETHEE Manual. Available at http://www.promethee-gaia.net/FR/assets/vpmanual.pdf

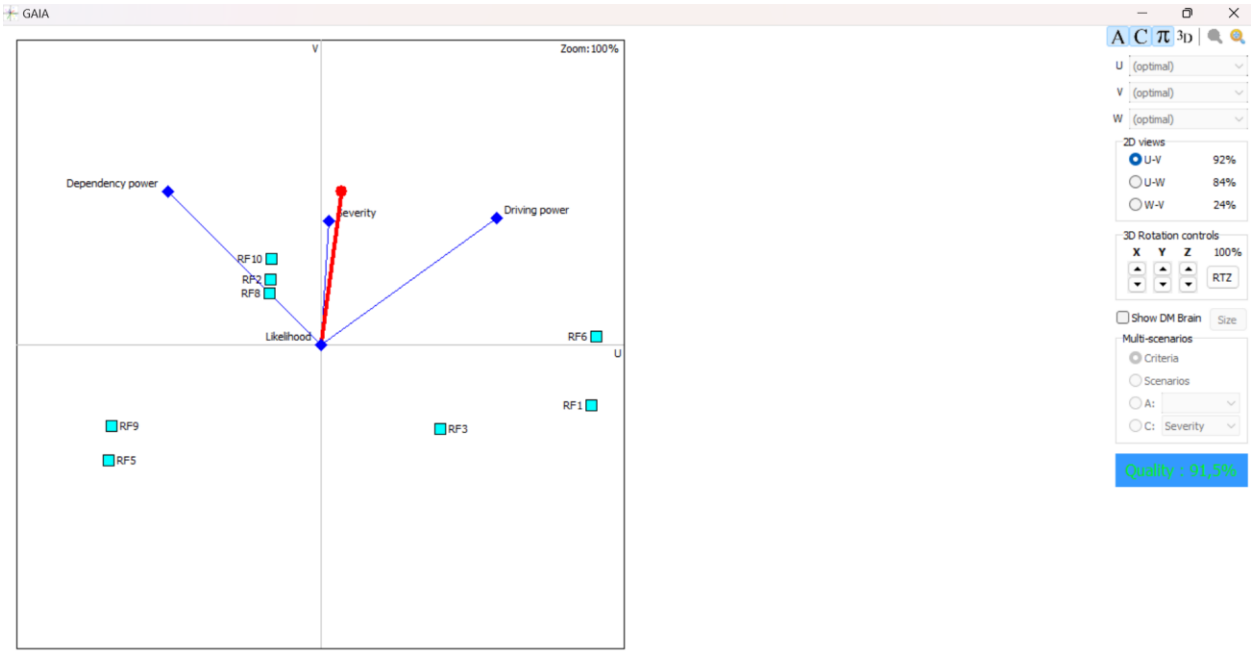
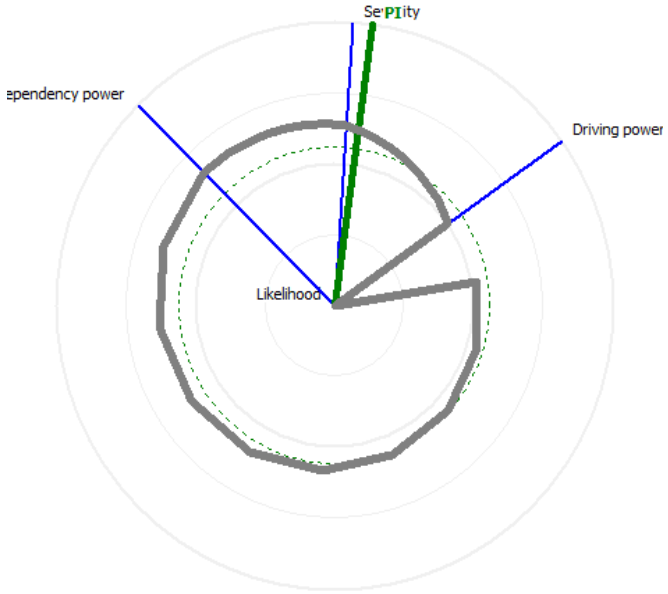


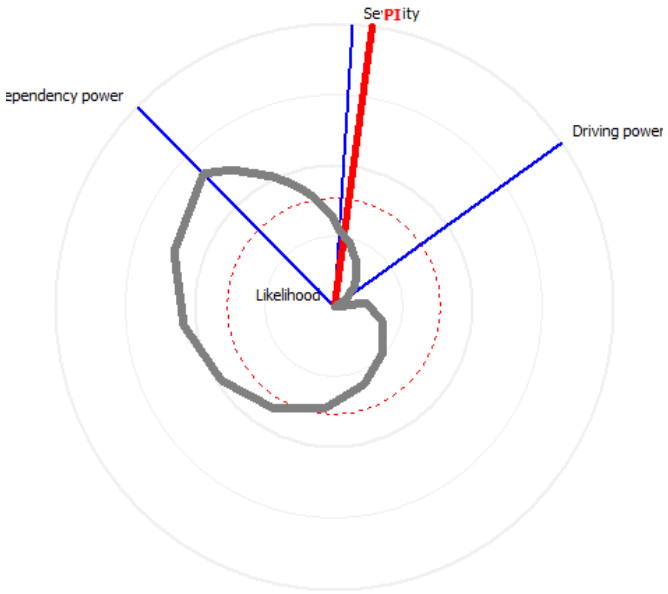
Figure 12 GAIA plane analysis

Figure 13 illustrates the GAIA web plane depicting an assessment of selected risk factors, namely *RF07*, *RF10*, and *RF05*. This visual framework enables a comparative analysis by illustrating the evaluation of criteria for each risk factor. *RF07* and *RF10* share a similar shape on the plane, indicating comparable performance across all four criteria, with a slightly higher rating in the dependency power criterion. Conversely, *RF05* demonstrates lower performance across all criteria, with only a marginally better score in dependency power.

RF07



RF10



RF05

Figure 13 GAIA web plane

5.3. Comparison of proposed framework with NIST and ISO framework

This section presents a comparative analysis of the proposed TISM-DEMATEL-PROMETHEE framework with NIST SP 800-30 and ISO/IEC 27001, focusing on their respective risk assessment phases. NIST SP 800-30 and ISO/IEC 27001 were chosen for comparison because they are widely recognised and respected as standards in risk management, each providing established methodologies for conducting risk assessments.

The purpose of this comparison is not to question the validity or comprehensiveness of the NIST and ISO frameworks, but rather to contextualise how the proposed framework aligns with and diverges from these standards in addressing a specific knowledge risk - namely, knowledge leakage. While NIST and ISO frameworks address a broad spectrum of risk management activities, the TISM-DEMATEL-PROMETHEE framework is tailored specifically to the assessment of knowledge risks. Therefore, this comparison focuses solely on the risk assessment phases of NIST SP 800-30 and ISO/IEC 27001 to highlight where the proposed framework complements or extends existing processes.

This analysis aims to provide insights into the unique contributions of the TISM-DEMATEL-PROMETHEE framework in the context of knowledge risk assessment, while acknowledging the established principles and practices outlined by the NIST and ISO standards.

5.3.1. ISO IEC/27001 framework

ISO/IEC 27001 is an internationally recognised standard for Information Security Management Systems (ISMS), emphasising the protection of information assets to ensure their confidentiality, integrity, and availability. It offers a comprehensive framework for managing information security risks. According to ISO/IEC 27001, the standard outlines a five-step process for risk assessment:

1. **Risk identification**: Identify assets, threats, and vulnerabilities.
2. **Assigning risk owners**: Designate individuals responsible for each risk.
3. **Risk analysis**: Evaluate the consequences and likelihood of each risk.
4. **Risk calculation**: Determine the overall risk level by scoring identified criteria.

5. **Risk evaluation**: Accept or mitigate risks based on predefined criteria.

Comparison with TISM-DEMATEL-PROMETHEE Framework

The ISO/IEC 27001 framework and the TISM-DEMATEL-PROMETHEE framework share common ground in their approach to risk assessment, particularly in the early stages of identifying risk factors and criteria. Both frameworks emphasise the importance of a systematic process for risk identification, which helps organisations recognise and categorise potential risks based on specific factors. However, while these initial steps in both frameworks overlap, significant differences arise as the processes advance into risk analysis, calculation, and evaluation.

A distinct feature of the ISO/IEC 27001 framework is its emphasis on assigning specific risk owners for each identified risk. This step is crucial in ISO/IEC 27001, as it ensures accountability by clearly designating individuals responsible for managing specific risks, thus providing a structured approach to oversight and monitoring. In contrast, the TISM-DEMATEL-PROMETHEE framework does not explicitly designate risk ownership as a separate step. Instead, accountability is addressed implicitly within the broader framework. While this indirect approach does not negate accountability, it may lack the formalisation ISO/IEC 27001 achieves through specific assignments, potentially affecting clarity in larger organisations with complex structures.

The primary divergence between the two frameworks becomes evident in the risk analysis and calculation stages. ISO/IEC 27001 typically assesses risk levels by calculating a composite score, derived either through multiplication (product) or addition (summation) of values assigned to each risk criterion. This straightforward scoring approach is designed to yield an overall risk level, making it accessible and practical for a wide range of organisational settings. For example, in contrast to the results generated by the PROMETHEE method in **Table 16**, ISO/IEC 27001 calculates risk levels by applying numerical values to the criteria, resulting in a simple and clear metric for prioritisation. This process can be visualised in **Table 17**, which illustrates the calculation of risk levels based on the product of severity and probability.

Table 17 Severity x probability

Risk factor	Severity	Probability	Score
Substandard security measures	4.5 (Catastrophic)	3.5 (Likely)	15.75

Existence of horizontal competition	4.5 (Catastrophic)	3.5 (Likely)	15.75
Lack of continuous monitoring	4.5 (Catastrophic)	3.5 (Likely)	15.75
Incomplete contracts	4.0 (Major)	3.5 (Likely)	14
Perceived opportunism among partners	4.0 (Major)	3.5 (Likely)	14
Informal knowledge sharing	3.0 (Moderate)	3.5 (Likely)	10.5
Weak BYOD policies	3.5 (Major)	2.5 (Fairly Unlikely)	8.75
Subcontracting activities	3.5 (Major)	2.5 (Fairly Unlikely)	8.75
Distrust among partners	2.5 (Moderate)	2.5 (Fairly Unlikely)	6.25
Insufficient technological competence	2.5 (Moderate)	2.5 (Fairly Unlikely)	6.25

On the other hand, the TISM-DEMATEL-PROMETHEE framework takes a more complex approach to risk analysis and calculation. TISM are used to estimate relationships among risk factors, offering a nuanced view of interdependencies. This model allows for a detailed analysis of how risks influence each other, which can be particularly valuable in complex environments where risks are highly interconnected. PROMETHEE further enhances this analysis by providing a multi-criteria decision-making approach, helping organisations rank risks based on a broader range of criteria. This advanced combination of methods provides a more comprehensive assessment, particularly useful for organisations needing to prioritise among competing risks with intricate interdependencies.

In the evaluation phase, ISO/IEC 27001 uses a structured matrix to guide decisions on risk mitigation based on the organisation's risk appetite and tolerance. This standardised approach aids in consistency and aligns with broader corporate governance standards, making it especially suitable for organisations with established risk tolerance thresholds. Decisions are typically binary—either accepting a risk if it falls within an acceptable range or implementing controls to mitigate it if it exceeds predefined limits.

Conversely, the TISM-DEMATEL-PROMETHEE framework's evaluation process is less prescriptive, allowing for greater flexibility and granularity in decision-making. The combination of DEMATEL and PROMETHEE enables a layered evaluation process, where risks are not only

ranked but are also evaluated on their influence and interdependence with other risks. This approach allows decision-makers to consider both direct and indirect effects of risk mitigation strategies, supporting a more dynamic form of risk prioritisation and response. Organisations that operate in fast-changing environments or deal with complex, evolving risk landscapes may find this approach more adaptable to their needs, as it facilitates a nuanced and responsive risk management strategy.

5.3.2. NIST SP 800-30 framework

NIST SP 800-30, similarly, provides a structured approach to assess organisational information systems, with a primary focus on information security risks, such as threats to data confidentiality, integrity, and availability. According to NIST SP 800-30, the framework follows these steps:

1. **Identify threat sources**: Identify both adversarial (e.g., cyber-attacks) and non-adversarial sources.
2. **Identify threat events**: Determine events triggered by each threat source.
3. **Identify vulnerabilities and predisposing conditions**: Assess factors that increase susceptibility to threats.
4. **Determine likelihood**: Estimate the probability of risk scenarios based on frequency and event impact.
5. **Determine impact**: Evaluate the potential consequences of risk events.
6. **Determine risk**: Calculate risk levels based on impact and likelihood matrices.

Comparison with TISM-DEMATEL-PROMETHEE Framework

The NIST SP 800-30 and TISM-DEMATEL-PROMETHEE frameworks both emphasise comprehensive risk assessment, yet they approach the process in distinctive ways, particularly in addressing complex, interdependent risks such as those involving organisational knowledge. A comparative analysis of these frameworks reveals differences in their approaches to threat identification, vulnerability analysis, risk evaluation, and prioritisation, highlighting strengths and potential limitations in each.

Both NIST SP 800-30 and TISM-DEMATEL-PROMETHEE emphasise thorough identification of threats as an initial step in the risk assessment process. NIST SP 800-30, however, differentiates explicitly between threat sources and threat events. This separation enables a more granular approach, where threat sources (such as unauthorised users or natural disasters) are individually identified and analysed alongside specific threat events (such as data breaches or system failures) that may arise from these sources. This structured distinction helps organisations isolate the root causes of potential risks, allowing for targeted risk mitigation strategies.

In contrast, the TISM-DEMATEL-PROMETHEE framework treats threats as general risk factors without distinguishing between sources and events. This more generalised approach is advantageous for a high-level analysis but may lack the depth needed for isolating specific sources of risk. While the TISM-DEMATEL-PROMETHEE framework's focus on interdependent factors provides a more interconnected view of risks, it may not offer the specific clarity NIST achieves in identifying and responding to individual threats.

NIST SP 800-30 includes a distinct phase for vulnerability identification, which plays a critical role in identifying weaknesses within systems and processes that may expose an organisation to risk. This phase is key to isolating and addressing both immediate threats and underlying vulnerabilities, thus allowing for a proactive risk management approach that strengthens defences against potential risk factors.

The TISM-DEMATEL-PROMETHEE framework, while accounting for vulnerabilities as part of its risk assessment criteria, does not treat them as a separate phase. Vulnerabilities are embedded within the broader criteria rather than being explicitly identified and analysed as unique points of concern. Although this integration may streamline the assessment process, it can limit the framework's ability to isolate vulnerabilities as distinct factors, potentially hindering a focused approach to risk mitigation.

Both frameworks employ likelihood and impact evaluations as core components of their risk analysis. NIST SP 800-30 calculates risk levels by combining the likelihood of a risk event occurring with the potential impact of that event, providing organisations with a straightforward method for assessing the severity of each identified risk. This risk quantification helps establish priorities based on the probability and potential consequences of each threat, which is beneficial in environments where risk needs to be assessed quickly and comprehensively.

However, the TISM-DEMATEL-PROMETHEE framework introduces an additional layer of complexity by incorporating MCDM through PROMETHEE, which considers interdependencies between risk criteria. This preference-based analysis enables a nuanced ranking of risks by accounting for the relative influence and interaction between different factors. For example, knowledge risks in an organisation often have complex interdependencies; the risk of employee turnover may heighten the risk of knowledge leakage, which can in turn lead to outdated knowledge within the organisation. The TISM-DEMATEL-PROMETHEE framework's ability to model these interdependencies provides a more comprehensive view of knowledge risks, which can be particularly valuable in understanding how various risks reinforce or mitigate one another.

NIST SP 800-30, by contrast, does not incorporate modelling techniques such as TISM or DEMATEL that allow for this level of analysis. As a result, it may be less effective in capturing the dynamic interactions and cascading effects that can occur between related risks, such as those found in knowledge risk scenarios.

A notable limitation of NIST SP 800-30 lies in its lack of advanced prioritisation mechanisms for strategic decision-making. Although it evaluates risks based on likelihood and impact, it does not incorporate sophisticated prioritisation tools like PROMETHEE or other multi-criteria decision-making techniques, which are critical for complex risks. For organisations facing intricate knowledge risks – such as those that affect intellectual capital, competitive advantage, or alignment with strategic goals – simple likelihood-impact matrices may be insufficient for effective prioritisation.

The TISM-DEMATEL-PROMETHEE framework, on the other hand, provides a multi-criteria ranking capability through PROMETHEE, which is particularly advantageous for prioritising risks in line with organisational objectives. This feature allows for a more strategic approach to risk management, enabling organisations to allocate resources and focus efforts on high-priority risks that directly impact their core knowledge assets. For instance, an organisation could prioritise risks related to proprietary knowledge over those with less direct influence on its competitive position, thereby strengthening its resilience against the most strategically relevant risks.

Building on the above discussion, the table below highlights the key similarities and differences among the frameworks:

Table 18 Summary of key similarities and differences

Aspect	TISM-DEMATEL-PROMETHEE	ISO/IEC 27001	NIST SP 800-30
Risk identification	Identifies risk factors directly	Identifies assets, threats, and vulnerabilities	Identifies threat sources and events
Assigning risk owners	Not explicitly stated	Specifies risk owners	Not explicitly stated
Risk analysis	Uses multi-criteria evaluation	Analyses consequences and likelihood	Uses impact and likelihood matrices
Risk calculation	Based on interdependencies and preferences	Summation of criteria scores	Combines impact and likelihood matrices
Vulnerability identification	Implicit in criteria	Embedded in asset and threat identification	Separate step
Risk evaluation	Preference-based prioritisation	Ranking by score for acceptance or treatment	Matrix-based risk level calculation
Focus on threat events	General treatment of threats	Not explicitly segmented	Differentiates threat sources and events

6. Discussion

This chapter presents and discusses the main findings from the three articles, along with those from the complementary study, in alignment with the research questions.

6.1. What are the components required to develop a comprehensive framework for the assessment of knowledge risks in organisations?

The findings across the articles collectively identified key components required for developing a comprehensive framework for assessing knowledge risks. These components were derived from the application of various models, each contributing unique insights into the hierarchical and causal relationships among knowledge risks.

In the first article, Foli (2022) applied TISM and MICMAC analysis to assess knowledge risks in ICT-supported collaborative projects, focusing on risks such as cybercrime, digitalisation, social network sites (SNSs), outsourcing, espionage, communication risks, and outmoded technologies. The TISM model positioned cybercrime and espionage as dependent risks, meaning these risks were influenced by other foundational or driving risks like digitalisation and outsourcing. According to the findings, risks to digitalisation, SNSs, outsourcing, communication, and outmoded technology collectively drove the occurrence of risks to cybercrime and espionage in ICT environments. This finding aligned with Zeiringer and Thalmann's (2022) study on knowledge risks in data-centric environments, where digitalisation and outdated technologies emerged as critical risks compounding the threat of cybercrime.

The MICMAC analysis further refined this understanding by categorising cybercrime and espionage within the dependent cluster, indicating that they had high dependency but low driving power. This suggested that, while cybercrime and espionage were serious concerns in ICT-supported collaborative projects, they were largely reactive risks, triggered by the presence and interaction of driving risks like digitalisation, outsourcing, and SNSs. The model thus emphasised the importance of managing foundational risks to indirectly mitigate dependent risks such as cybercrime and espionage. This interrelation aligned with prior research, which had found that risks

like espionage were more likely to emerge within networked systems (Whitman and Mattord, 2019). In these environments, the digitalised platforms facilitating collaboration also introduced vulnerabilities exploitable by third parties, especially when these platforms were not adequately secured against contemporary cyber threats (Durst and Zieba, 2019).

Furthermore, outmoded technologies posed a unique risk by leaving security gaps that could be exploited by external agents, facilitating cybercrime and espionage. These findings were corroborated by studies such as those by Freet and Agrawal (2017), and Gragido and Pirc (2011), which highlighted the relationship between outdated infrastructure and increased vulnerability to espionage and cyber threats. By structuring these interdependencies, TISM and MICMAC allowed organisations to visualise and prioritise risks based on their systemic influence, highlighting the importance of addressing driving risks to mitigate dependent ones effectively.

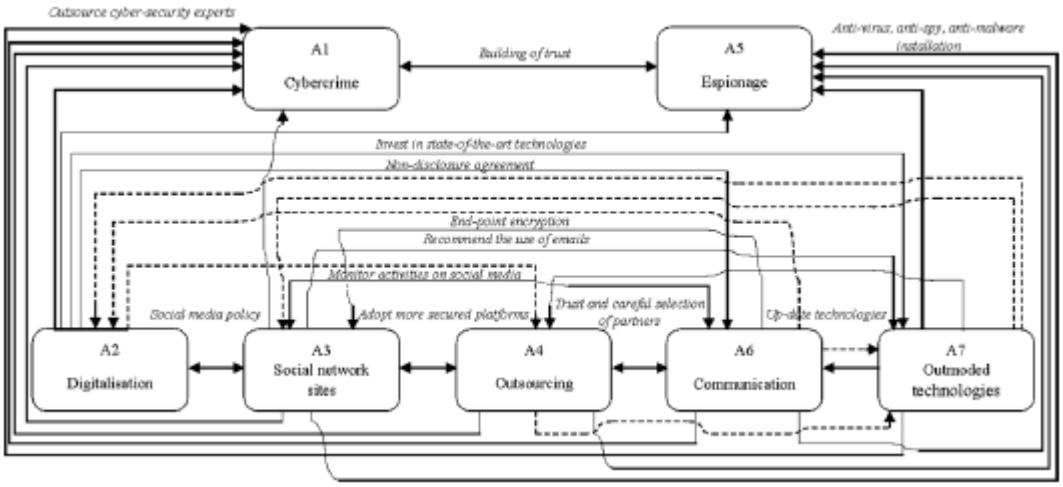


Figure 14 TISM (Source: *Article I*)

The third article by Foli and Durst (2022) also utilised ISM to explore knowledge leakage risks within collaborative agreements, a context where knowledge exchange was necessary but risky. This study identified seven primary risk factors for knowledge leakage: incomplete contracts, subcontracting activities, distrust among partners, perceived opportunism, insufficient technological competence, weak bring-your-own-device (BYOD) policies, substandard security measures, expected incentives, and horizontal competition.

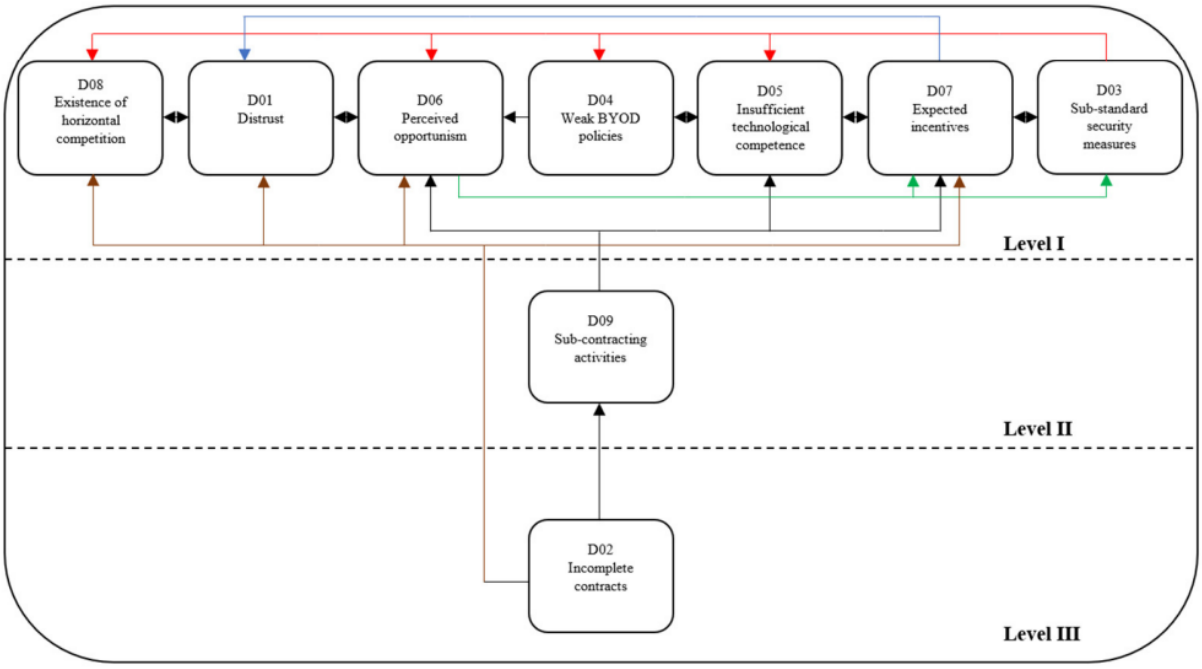


Figure 15 ISM (Source: *Article III*)

In this case, ISM delineated the interrelationships among these risks, with incomplete contracts and subcontracting identified as foundational risks. The model showed that these foundational risks drove other risks like distrust, perceived opportunism, and substandard security measures. For instance, incomplete contracts created ambiguities in collaborative agreements, leading to knowledge misuse or opportunistic behaviour by partners. The lack of contractual clarity also fostered distrust, as partners felt less secure in knowledge-sharing arrangements, increasing the likelihood of knowledge leakage (Jiang et al., 2013; Fawad Sharif et al., 2020).

The ISM model further illustrated that subcontracting as a driving risk had a direct influence on insufficient technological competence and weak BYOD policies, both of which were related to a firm's capacity to protect knowledge in a networked environment. Studies by Durst and Zieba (2019) supported this observation, highlighting that firms heavily relying on subcontracting often faced skill gaps in protecting their knowledge assets, thereby exposing them to knowledge leakage. By establishing these hierarchical relationships, ISM helped practitioners in collaborative settings prioritise risk mitigation strategies, focusing first on strengthening contracts and reducing subcontracting dependencies to minimise overall knowledge leakage.

The second article (Foli et al., 2023) applied the Grey DEMATEL technique, a model particularly well-suited for environments where data might be incomplete or uncertain, to assess operational knowledge risks in small and medium-sized enterprises (SMEs). This technique identified key risks like outsourcing risks, communication risks, knowledge waste, the risk of using obsolete or unreliable knowledge, and knowledge gaps.

In the DEMATEL model, outsourcing risks and communication risks emerged with strong driving influences on other risks, positioning them as primary factors shaping the risk landscape in SMEs. Outsourcing risks, for example, exposed SMEs to potential knowledge loss or leakage as third-party contractors gained access to sensitive information. Similarly, communication risks could lead to misunderstandings and misinterpretations, resulting in knowledge waste or the propagation of outdated information across the organisation. This emphasis on outsourcing aligned with previous research, which found that SMEs often lacked the resources to manage outsourcing risks effectively, thereby exposing themselves to significant operational vulnerabilities (Durst and Zieba, 2019; Ahmad et al., 2014).

Grey DEMATEL enabled SMEs to quantify and prioritise these risks based on their causal relationships, highlighting outsourcing and communication risks as the most critical areas for intervention. By focusing on managing these driving risks, SMEs could more effectively prevent secondary risks, such as knowledge gaps or the use of unreliable information, from impacting their operations. The study's findings reinforced the value of DEMATEL in resource-constrained environments, as it allowed SMEs to make informed decisions despite limited data, ensuring that efforts to manage knowledge risks were both targeted and impactful.

6.2. How can improved risk assessment tools be integrated into the framework to address the complex nature of knowledge risks?

The research question focuses on identifying how improved risk assessment tools can be integrated into a framework to effectively address the complex nature of knowledge risks. In this study, the tools are represented by models – TISM, DEMATEL, and PROMETHEE – for assessing and prioritising knowledge risks. These models, when combined, act as complementary tools that overcome the limitations of individual methods and provide a comprehensive risk assessment

process. As noticed in *Article I*, *II* and *III*, the models, such as (T)ISM and DEMATEL, have been instrumental in this regard. However, each model has inherent limitations that can impede comprehensive risk assessment and prioritisation. Integrating these models with the PROMETHEE can address these shortcomings, leading to a more effective framework for knowledge risk assessment.

TISM is suitable at identifying the structural interdependencies among various knowledge risks, providing a hierarchical framework that maps out how each risk influences others. This structural insight is crucial for understanding the complex web of risk interactions. However, TISM does not quantify the strength of these relationships, limiting its ability to assess the intensity of each risk factor's impact. This absence of quantitative data hinders the prioritisation of risks based on their significance or likelihood, which is essential for informed decision-making. As noted by Sushil (2012), while TISM offers a clear depiction of dependencies, it lacks the capability to measure the magnitude of these influences.

DEMATEL excels in identifying and analysing cause-and-effect relationships among knowledge risks, assigning weights that quantify the influence of each risk factor. This quantitative approach aids in understanding the prominence and causal relationships between risks. However, DEMATEL does not inherently provide a hierarchical or structural model, making it challenging to visualise the overall influence patterns and dependencies among risks. This limitation can obscure the intricate interdependencies that are vital for a holistic understanding of knowledge risks. Wu and Lee (2007) highlight that while DEMATEL effectively captures direct and indirect influences, it does not offer a structural hierarchy of factors.

To overcome these limitations, in the complementary study, an integrated framework that combines TISM, DEMATEL, and PROMETHEE is proposed. This composite approach leverages the strengths of each model to provide a comprehensive assessment of knowledge risks. The process begins with TISM to identify and map the interrelationships and dependencies among knowledge risks. By creating a structured model, TISM helps explain how each risk influences others, establishing a clear hierarchy of dependencies. This structural mapping is important for understanding the foundational and dependent risks within the organisation.

Following the structural mapping, DEMATEL is employed to assign quantitative weights to the relationships identified by TISM. By evaluating the driving power and dependency of each risk,

DEMATEL quantifies the influence of each factor, providing a clearer picture of the intensity of these relationships. This quantitative data addresses TISM's limitation by offering measurable insights into the strength of each risk's impact. For example, DEMATEL can quantify how significantly outsourcing influences knowledge leakage, allowing organisations to gauge the severity of this risk (Foli et al., 2023).

The final step involves integrating the structural insights from TISM and the quantitative weights from DEMATEL into the PROMETHEE model. PROMETHEE facilitates the prioritisation of risks by evaluating them based on their overall impact and likelihood. By synthesising the hierarchical structure and quantified influences, PROMETHEE generates a ranked list of risks, enabling decision-makers to focus on the most critical areas. This prioritisation is essential for developing effective mitigation strategies and allocating resources efficiently. As Brans and Mareschal (2005) discuss, PROMETHEE provides a clear and rational ranking of alternatives, making it a valuable tool for decision-making.

The integration of TISM, DEMATEL, and PROMETHEE offers several key benefits. Combining structural mapping with quantitative analysis and prioritisation provides a holistic view of knowledge risks, capturing both the interrelationships and the strength of influences. The framework equips decision-makers with actionable insights, allowing for informed prioritisation and the development of targeted mitigation strategies. Additionally, this integrated approach is adaptable to various organisational contexts and can be tailored to assess diverse knowledge risks across different industries.

By addressing the individual limitations of TISM and DEMATEL and incorporating the prioritisation capabilities of PROMETHEE, this integrated framework enhances the improvement of knowledge risk assessment. It enables organisations to not only identify and understand the complex web of knowledge risks but also to quantify their impacts and prioritise them effectively, leading to more informed and strategic decision-making.

6.3. How does the proposed knowledge risk assessment framework, when applied in an organisational setting, improve the identification, analysis, and evaluation of knowledge risks?

In the complementary study, the proposed framework was validated, revealing critical insights into the factors contributing to knowledge leakage risks within the case company. The findings indicate that horizontal competition, coupled with inadequate continuous monitoring, poses the most significant threats to knowledge security. This aligns with prior research (e.g., Serna, 2023; Serna et al., 2017), which emphasises the vulnerability of organisations to knowledge leakage in environments with highly competitive pressures and insufficient control mechanisms.

In highly competitive industries, companies face increased pressures to innovate, frequently necessitating the sharing of critical knowledge across various departments and external partners. However, horizontal competition, particularly when organisations operate in the same or overlapping markets, intensifies this risk as employees or collaborators might be incentivised to transfer knowledge to competitors. Husted and Michailova (2002) discuss how knowledge leakage is exacerbated in situations where companies share similar market objectives, thus rendering internal knowledge highly attractive to potential competitors.

The lack of continuous monitoring further compounds this vulnerability, as it limits the organisation's ability to track and control knowledge flows effectively. Alhawari et al. (2012) argue that robust monitoring mechanisms are essential in knowledge-intensive environments to mitigate risks associated with knowledge transfer and retention. Without such mechanisms, organisations may struggle to detect when knowledge is misappropriated or unintentionally shared beyond its intended scope. Furthermore, the study's outcomes highlight the importance of implementing proactive measures to manage knowledge risks. Strategies such as establishing rigorous internal protocols, enhancing employee awareness of knowledge security, and fostering a culture of knowledge protection have been recommended to address these challenges (Pérez-Aróstegui et al., 2015). These measures, combined with continuous monitoring systems, are likely to provide a more secure environment that minimises the threats associated with both horizontal competition and knowledge leakage.

The proposed knowledge risk assessment framework improves how organisations identify, analyse, and prioritise knowledge risks. By combining a detailed literature review with discussions among

stakeholders, it identifies risks such as knowledge leakage and its causes, including horizontal competition and poor monitoring. This approach ensures the risks are not only based on theory but also relevant to the organisation's specific challenges, like informal knowledge sharing.

For analysing risks, the framework uses TISM and DEMATEL. TISM provides a structural mapping of risks, distinguishing between foundational risks – like inadequate monitoring – and dependent risks, thereby clarifying how these vulnerabilities interconnect. DEMATEL complements this by assigning weights to various risk criteria, enabling a more precise evaluation of their significance. These models work together to provide a clear and thorough understanding of these risks.

Finally, the framework prioritises risks using the PROMETHEE. This model combines insights from TISM and DEMATEL to rank risks by their impact and likelihood. This helps organisations focus resources on the most serious risks, such as inadequate monitoring and competition. Overall, the framework gives organisations a clear, practical way to manage knowledge risks and reduce potential threats effectively.

7. Conclusions

In conclusion, this doctoral thesis proposes an integrated framework to improve knowledge risk assessment in organisations. Developed using TISM, DEMATEL, and PROMETHEE models, the framework was validated through a case company, revealing key insights: the most critical risks related to knowledge leakage stem from horizontal competition and inadequate continuous monitoring. While tested within a consulting firm, this framework is adaptable across diverse organisational contexts, including multi-stakeholder projects. This thesis's contributions, both methodological and practical, are discussed in subsequent sections, along with limitations and recommendations for future research.

7.1. Methodological contributions

This doctoral thesis makes a methodological contribution to the field of KRM, by introducing an integrated framework for assessing knowledge risks. This framework addresses a gap identified in

the Systematic Literature Review (SLR), which emphasised the absence of comprehensive frameworks for systematically evaluating knowledge risks. The proposed framework is novel in its combination of three established models – Total Interpretive Structural Modelling (TISM), Decision-Making Trial and Evaluation Laboratory (DEMATEL), and Preference Ranking Organisation Method for Enrichment Evaluation (PROMETHEE).

What sets this framework apart is its ability to assess potential knowledge risks, such as knowledge leakage, not only in terms of traditional parameters like probability and severity but also through the incorporation of driving power and dependency power. These additional parameters enhance the reliability and precision of the knowledge risk assessment process. Driving and dependency power values, derived through TISM, allow for an advanced analysis of how risks influence one another and the system as a whole. By enabling experts to provide crisp values, ranges, or subjective judgements based on their expertise, TISM ensures flexibility in capturing nuanced insights.

In parallel, DEMATEL plays a critical role in calculating and estimating the weights of criteria such as probability, severity, driving power, and dependency power, adding depth to the analysis. This integration allows for a multidimensional evaluation of knowledge risks, where the interconnections and influence among factors are assessed. PROMETHEE further refines this process by offering a systematic prioritisation of risks, making the framework adaptable for organisational decision-making.

7.2. Practical contributions

This thesis has important implications for risk managers seeking a better understanding of knowledge risks and a better means for assessing them. First, the framework developed in this research provides a clear and systematic set of steps that facilitates easy implementation. This aspect of the framework is particularly valuable, as it enables practitioners to readily appreciate the process of modelling and understand how it can be applied to the assessment of knowledge risks, as well as risks in general. The step-by-step approach outlined in the framework serves as a valuable guide for managers, allowing them to navigate the intricacies of risk assessment with confidence and precision.

The integration of the PROMETHEE model further strengthens the framework by enhancing its analytical precision and efficiency. PROMETHEE equips decision-makers with tools for preference modelling, visual representations, and streamlined decision-making processes. This addition enables a deeper analysis of the complex challenges associated with knowledge risks, empowering managers to make more informed decisions. As a result, decision-makers can optimise risk mitigation strategies and resource allocation, ultimately improving knowledge risk management outcomes.

7.3. Limitations and future research directions

As with any research study, this thesis possesses several limitations that are important to acknowledge. First, the field of knowledge risks spans multiple disciplines, including KM, information management, information systems, and, to a certain extent, computer science. Given this interdisciplinary nature, conducting a systematic literature review in this field presents inherent challenges. Although efforts were made to extend the SLR beyond the core domain of KM, which remains the main focus of the study, some relevant articles may have been unintentionally omitted. This limitation stems from the expansive scope of the field and the difficulty of capturing all relevant literature. Despite an extensive search process, including supplementary searches on Google Scholar and a review of references within the selected papers, certain works that could further inform this study's findings might not have been included. Thus, it is worth acknowledging that.

Another significant limitation lies in the case study approach used to validate the framework. This study tested the integrated TISM-DEMATEL-PROMETHEE framework within a single consulting firm, which, while providing valuable insights, may limit the generalisability of the findings. Knowledge risks can vary substantially across organisations and industries, and what is deemed a high-priority risk in one firm might be less critical in another. For example, in a consulting firm, client-related knowledge leaks and strategic misalignments might be of high concern, whereas in a manufacturing setting, intellectual property theft or operational disruptions might take precedence. Although the proposed framework is designed with a level of adaptability, the specific risk factors and priorities identified in this study may not translate directly to other industries. Future research should address this limitation by applying the framework to a variety of organisational contexts,

including manufacturing, healthcare, and technology sectors. Conducting comparative studies across different industries could provide a more comprehensive understanding of how knowledge risks manifest and offer insights into the universal applicability and necessary modifications of the framework across diverse settings.

Finally, while this study has contributed to advancing the field by integrating TISM, DEMATEL, and PROMETHEE into a single, cohesive framework, there remains an opportunity to improve the model's flexibility and scalability for real-time decision-making. Future research could explore the development of an automated or semi-automated version of this framework, potentially leveraging artificial intelligence or machine learning algorithms. Such an enhancement would enable continuous monitoring and dynamic adjustment of risk assessments, thereby enhancing the framework's responsiveness to emerging risks. In addition, incorporating data analytics techniques might allow for the integration of real-time data, which would provide a more accurate and timely assessment of risks as they evolve within an organisation.

References

Ahlfänger, M., Gemünden, H. G., & Leker, J. (2022). Balancing knowledge sharing with protecting: The efficacy of formal control in open innovation projects. *International Journal of Project Management*, *40*(2), 105-119.

Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers & Security*, *42*, 27-39.

Ahmad, M. S., Fei, W., Shoaib, M., & Ali, H. (2024). Identification of Key Drivers for Performance Measurement in Sustainable Humanitarian Relief Logistics: An Integrated Fuzzy Delphi-DEMATEL Approach. *Sustainability*, *16*(11), 4412.

Aladayleh, K. J., & Aladaileh, M. J. (2024). Applying Analytical Hierarchy Process (AHP) to BIM-Based Risk Management for Optimal Performance in Construction Projects. *Buildings*, *14*(11), 3632.

Alavi, M., & Leidner, D. (1999). Knowledge management systems: issues, challenges, and benefits. *Communications of the Association for Information systems*, *1*(1), 7.

Alavi, M., & Leidner, D. E. (2001). Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS quarterly*, 107-136.

Albadvi, A., Chaharsooghi, S. K., & Esfahanipour, A. (2007). Decision making in stock trading: An application of PROMETHEE. *European journal of operational research*, *177*(2), 673-683.

Alberts, C. J., Behrens, S. G., Pethia, R. D., & Wilson, W. R. (1999). Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, Version 1.0.

Albert, C., Dorofee, A. J., Stevens, J. F., & Woody, C. C. (2005). OCTAVE-S Implementation Guide, Version 1.

Alhawari, S., Karadsheh, L., Talet, A. N., & Mansour, E. (2012). Knowledge-based risk management framework for information technology project. *International Journal of Information Management*, *32*(1), 50-65.

Alojaiman, B. (2023). A Multi-Criteria Decision-Making Process for the Selection of an Efficient and Reliable IoT Application. *Processes*, *11*(5), 1313.

Altukruni, H., Maynard, S. B., Alshaikh, M., & Ahmad, A. (2021). Exploring knowledge leakage risk in knowledge-intensive organisations: behavioural aspects and key controls. *arXiv preprint arXiv:2104.07140*.

Altun, F., Şahin, R., & Güler, C. (2020). Multi-criteria decision making approach based on PROMETHEE with probabilistic simplified neutrosophic sets. *Soft Computing*, *24*(7), 4899-4915. https://doi.org/10.1007/s00500-019-04244-4

Andersen, H. K., & Mitchell, S. D. (2023). Pragmatism for Philosophy of Science. *The Pragmatist Challenge: Pragmatist Metaphysics for Philosophy of Science*, 1.

Aven, T. (2011). On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. *Risk Analysis: An International Journal*, *31*(4), 515-522.

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European journal of operational research*, *253*(1), 1-13.

Baafi, M. A., Xin-Ying, J., & Mills, E. F. E. A. (2021). Critical diversity dimensions influencing effective diverse workforce: a grey-DEMATEL approach. *International Journal of Applied Decision Sciences*, *14*(5), 498-517.

Baseer, M., Ghiaus, C., Viala, R., Gauthier, N., & Daniel, S. (2023). pELECTRE-Tri: Probabilistic ELECTRE-Tri Method—Application for the Energy Renovation of Buildings. *Energies*, *16*(14), 5296.

Bayer, F., & Maier, R. (2006, September). Knowledge risks in inter-organizational knowledge transfer. In *Proceedings of I-Know* (Vol. 6, pp. 6-8).

Behzadian, M., Otaghsara, S. K., Yazdani, M., & Ignatius, J. (2012). A state-of the-art survey of TOPSIS applications. *Expert Systems with applications*, *39*(17), 13051-13069.

Bell, E., Bryman, A., & Harley, B. (2022). *Business research methods*. Oxford university press.

Belton, V., & Stewart, T. (2012). *Multiple criteria decision analysis: an integrated approach*. Springer Science & Business Media.

Bhandari, S., & Hallowell, M. R. (2021). Identifying and Controlling Biases in Expert-Opinion Research: Guidelines for Variations of Delphi, Nominal Group Technique, and Focus Groups. *Journal of Management in Engineering*, *37*(3), 04021015. https://doi.org/doi:10.1061/(ASCE)ME.1943-5479.0000909

Biedenbach, T., & Müller, R. (2011). Paradigms in project management research: examples from 15 years of IRNOP conferences. *International Journal of Managing Projects in Business*, 4(1), 82-104. https://doi.org/10.1108/17538371111096908

Blaikie, N. (2007). Approaches to social enquiry: *Advancing knowledge*. Polity.

Blomqvist, K., & Kianto, A. (2007). Knowledge-based view of the firm–theoretical notions and implications for management. *Department of Business Administration and Technology Business Research Center, Lappeenranta University of Technology*.

Boehm, B. W. (1991). Software risk management: principles and practices. *IEEE software*, *8*(1), 32-41.

Bottani, E., & Rizzi, A. (2006). A fuzzy TOPSIS methodology to support outsourcing of logistics services. *Supply Chain Management: An International Journal*, *11*(4), 294-308.

Brans, J.-P., Nadeau, R., & Landry, M. (1982). L'ingénierie de la décision. *Elaboration d'instruments d'aide à la décision. La méthode PROMETHEE. In l'Aide à la Décision: Nature, Instruments et Perspectives d'Avenir*, 183-213.

Brans, J.-P., Vincke, P., & Mareschal, B. (1986). How to select and how to rank projects: The PROMETHEE method. *European journal of operational research*, *24*(2), 228-238.

BrĂTianu, C. (2018). A Holistic Approach to Knowledge Risk. *Management Dynamics in the Knowledge Economy*, *6*(4), 593-607. https://www.managementdynamics.ro/index.php/journal/article/view/280

Bratianu, C., Neştian, A. Ş., Tiţã, S. M., Voda, A. I., & Guţã, A. L. (2020). The impact of knowledge risk on sustainability of firms. *Amfiteatru Economic*, *22*(55), 639-652.

Bratianu, C., & Bejinaru, R. (2022). Exploring vulnerabilities and risks related to knowledge management systems. In *17th International Forum for Knowledge Asset Dynamics, SUPSI University, Lugano, Switzerland*, June (pp. 20-22).

Breiman, L. (2001). Statistical modeling: The two cultures (with comments and a rejoinder by the author). *Statistical science*, *16*(3), 199-231.

Brunold, J., & Durst, S. (2012). Intellectual capital risks and job rotation. *Journal of Intellectual Capital*, *13*(2), 178-195. https://doi.org/10.1108/14691931211225021

Bux, H., Zhang, Z., & Ahmad, N. (2020). Promoting sustainability through corporate social responsibility implementation in the manufacturing industry: An empirical analysis of barriers using the ISM-MICMAC approach. *Corporate Social Responsibility and Environmental Management*, *27*(4), 1729-1748. https://doi.org/https://doi.org/10.1002/csr.1920

Chang, B., Chang, C.-W., & Wu, C.-H. (2011). Fuzzy DEMATEL method for developing supplier selection criteria. *Expert Systems with Applications*, *38*(3), 1850-1858. https://doi.org/https://doi.org/10.1016/j.eswa.2010.07.114

Chen, Y., Yu, J., & Khan, S. (2013). The spatial framework for weight sensitivity analysis in AHP-based multi-criteria decision making. *Environmental modelling & software*, *48*, 129-140.

Coleman, L., & Casselman, R. M. (2016). Optimizing decisions using knowledge risk strategy. *Journal of Knowledge Management*, *20*(5), 936-958. https://doi.org/10.1108/JKM-11-2015-0465

Collins, T. R., Rossetti, M. D., Nachtmann, H. L., & Oldham, J. R. (2006). The use of multi-attribute utility theory to determine the overall best-in-class performer in a benchmarking study. *Benchmarking: An International Journal*, *13*(4), 431-446.

Connelly, C. E., Zweig, D., Webster, J., & Trougakos, J. P. (2012). Knowledge hiding in organizations. *Journal of Organizational Behavior*, *33*(1), 64-88. https://doi.org/https://doi.org/10.1002/job.737

Coşkun, C. (2019). *Development of a risk assessment method for sustainable construction of megaprojects* (Master's thesis, Middle East Technical University).

Cox, R. (2009). *Risk analysis of complex and uncertain systems* (Vol. 129). Springer Science & Business Media.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Crossan, M. M., & Apaydin, M. (2010). A multi-dimensional framework of organizational innovation: A systematic review of the literature. *Journal of management studies*, *47*(6), 1154-1191.

Daghfous, A., Qazi, A., & Khan, M. S. (2021). Incorporating the risk of knowledge loss in supply chain risk management. *The International Journal of Logistics Management*, *32*(4), 1384-1405.

Das, D., Datta, A., Kumar, P., Kazancoglu, Y., & Ram, M. (2022). Building supply chain resilience in the era of COVID-19: An AHP-DEMATEL approach. *Operations Management Research*, *15*(1), 249-267.

Davenport, T. H., De Long, D. W., & Beers, M. C. (1998). Successful knowledge management projects. *MIT Sloan management review*, *39*(2), 43.

Delak, B., & Damij, N. (2015). Knowledge risk assessments. European Conference on Knowledge Management.

Deniaud, I. F., Marmier, F., Gourc, D., & Bougaret, S. (2016, May). A risk management approach for collaborative NPD project. In *2016 International Conference on Industrial Engineering, Management Science and Application (ICIMSA)* (pp. 1-5). IEEE.

Dye, R. A., & Sridhar, S. S. (2003). Investment implications of information acquisition and leakage. *Management Science*, *49*(6), 767-783.

Disterer, G. (2001, January). Individual and social barriers to knowledge transfer. In *Proceedings of the 34th annual Hawaii international conference on system sciences* (pp. 7-pp). IEEE.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(2).

Dodgson, J. S., Spackman, M., Pearman, A., & Phillips, L. D. (2009). Multi-criteria analysis: a manual.

Dubois, É., Heymans, P., Mayer, N., & Matulevičius, R. (2010). A systematic approach to define the domain of information system security risk management. *Intentional perspectives on information systems engineering*, 289-306.

Durst, S. (2013). An exploratory study of intangibles risk disclosure in annual reports of banking companies from the UK, US, Germany and Italy-Some descriptive insights. *Financial reporting*, (2013/1).

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

Durst S. (2021). Knowledge risk management in organisations: Findings from Latin America. *Multidisciplinary Business Review*.

Durst, S., Aggestam, L., & Ferenhof, H. A. (2015). Understanding knowledge leakage: a review of previous studies. *Vine*, *45*(4), 568-586.

Durst, S., Bruns, G., & Henschel, T. (2018). The management of knowledge risks: what do we really know? In *Global business expansion: Concepts, methodologies, tools, and applications* (pp. 258-269). IGI Global.

Durst, S., Edvardsson, I. R., & Foli, S. (2023). Knowledge management in SMEs: a follow-up literature review. *Journal of Knowledge Management*, *27*(11), 25-58. https://doi.org/10.1108/JKM-04-2022-0325

Durst, S., & Ferenhof, H. A. (2014). Knowledge Leakages and Ways to Reduce Them in Small and Medium-Sized Enterprises (SMEs). *Information*, *5*(3), 440-450. https://www.mdpi.com/2078-2489/5/3/440

Durst, S., & Ferenhof, H. A. (2016). Knowledge risk management in turbulent times. In *Competitive strategies for small and medium enterprises* (pp. 195-209). Springer.

Durst, S., Foli, S., La Torre, M., & Borgia, M. (2023). Knowledge risk management in banks-An area for improving organizational performance. *Heliyon*, *9*(11).

Durst, S., Foli, S., & Edvardsson, I. R. (2024). A systematic literature review on knowledge management in SMEs: current trends and future directions. *Management Review Quarterly*, *74*(1), 263-288.

Durst, S., Heinze, I., Henschel, T., & Nawaz, N. (2020). Unlearning: a systematic literature review. *International Journal of Business and Globalisation*, *24*(4), 472-495.

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/https://doi.org/10.1016/j.jbusres.2019.08.002

Durst, S., & Wilhelm, S. (2011). Knowledge management in practice: insights into a medium-sized enterprise's exposure to knowledge loss. *Prometheus*, *29*(1), 23-38.

Durst, S., & Wilhelm, S. (2013). Do you know your knowledge at risk? *Measuring Business Excellence*, *17*(3), 28-39. https://doi.org/10.1108/MBE-08-2012-0042

Durst, S., & Zieba, M. (2017). Knowledge risks-towards a taxonomy. *International Journal of Business Environment*, *9*(1), 51-63.

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

Easterby-Smith, M., & Prieto, I. M. (2008). Dynamic capabilities and knowledge management: an integrative role for learning?. *British journal of management*, *19*(3), 235-249.

Elias, N., & Wright, A. (2006). Using knowledge management systems to manage knowledge resource risks. In *Advances in Management Accounting* (pp. 195-227). Emerald Group Publishing Limited.

El Khatib, R. A., Ali, A. A., & Mostapha, N. (2021). A review of knowledge risk conception. *BAU Journal-Creative Sustainable Development*, *3*(1), 9.

El Khatib, R. A., & Ali, A. A. (2022). Evaluating the effect of knowledge risks on sustainability: the mediating role of organizational performance. *Journal of Management Development*, *41*(9/10), 496-513. https://doi.org/10.1108/JMD-01-2022-0006

El Khatib, R. E., & Abbas, A. (2023). Knowledge risks and business sustainability: the role of organisational performance as a mediating factor. *Middle East Journal of Management*, *10*(5), 523-550.

Engemann, K. J., & Henderson, D. M. (2014). *Business continuity and risk management: essentials of organizational resilience*. Rothstein Publishing.

Erickson, G. S., & Rothberg, H. N. (2010). Strategic knowledge management in a low-risk environment. In *Proceedings of the 11th European Conference on Knowledge Management: ECKM*. Academic Conferences Limited.

Estrada, I., Faems, D., & de Faria, P. (2016). Coopetition and product innovation performance: The role of internal knowledge sharing mechanisms and formal knowledge protection mechanisms. *Industrial Marketing Management*, *53*, 56-65.

Fawad Sharif, S. M., Naiding, Y., Ur Rehman, A., Sahibzada, U. F., & Kanwal, F. (2023). From partners' learning intent to knowledge leakage: the role of contract and trust. Knowledge Management Research & Practice, 21(1), 107-118.

Fawad Sharif, S. M., Naiding, Y., Xu, Y., & Rehman, A. U. (2020). The effect of contract completeness on knowledge leakages in collaborative construction projects: a moderated mediation study. *Journal of Knowledge Management*, *24*(9), 2057-2078.

Fawad Sharif, S. M., Naiding, Y., & Kifayat Shah, S. (2024). Restraining knowledge leakage in collaborative projects through HRM. *VINE Journal of Information and Knowledge Management Systems*, *54*(3), 493-509.

Ferenhof, H. A. (2016). Recognizing Knowledge Leakage and Knowledge Spillover and Their Consequences. *International Journal of Knowledge and Systems Science (IJKSS)*, *7*(3), 46-58. https://doi.org/10.4018/IJKSS.2016070104

Figueira, J. R., Greco, S., Roy, B., & Słowiński, R. (2010). ELECTRE methods: Main features and recent developments. *Handbook of multicriteria analysis*, 51-89.

Figueira, J. R., Greco, S., Roy, B., & Słowiński, R. (2013). An overview of ELECTRE methods and their recent extensions. *Journal of Multi-Criteria Decision Analysis*, *20*(1-2), 61-85.

Fink, A. (2019). *Conducting research literature reviews: From the internet to paper*. Sage publications.

Foli, S. (2022). Total interpretive structural modelling (TISM) and MICMAC approach in analysing knowledge risks in ICT-supported collaborative project. *VINE Journal of Information and Knowledge Management Systems*, *52*(3), 394-410.

Foli, S., & Durst, S. (2022). Analysing drivers of knowledge leakage in collaborative agreements: A magnetic processing case firm. *Journal of Risk and Financial Management*, *15*(9), 389.

Foli, S., Durst, S., & Romero, E. D. (2023). Evaluation of operational knowledge risks in SMEs–Using a Grey-DEMATEL technique. *Journal of Information & Knowledge Management*, *22*(06), 2350071.

Fontela, E., & Gabus, A. (1974). DEMATEL, innovative methods.

Freet, D., & Agrawal, R. (2017, March). A virtual machine platform and methodology for network data analysis with IDS and security visualization. In *SoutheastCon 2017* (pp. 1-8). IEEE.

Frishammar, J., Ericsson, K., & Patel, P. C. (2015). The dark side of knowledge transfer: Exploring knowledge leakage in joint R&D projects. *Technovation*, *41*, 75-88.

Fruhwirth, M., Pammer-Schindler, V., & Thalmann, S. (2024). Knowledge Leaks in Data-Driven Business Models? Exploring Different Types of Knowledge Risks and Protection Measures. *Schmalenbach Journal of Business Research*, *76*(3), 357-396.

Galway, L. (2004). Quantitative risk analysis for project management. *A Critical Review, WR-112-RC, http://www. rand. org/pubs/working_papers/2004/RAND_WR112. pdf*.

Gerst, K. J. (2011). *Evaluating the impact of government energy R&D investments through a multi-attribute utility-based decision tool* (Doctoral dissertation, Massachusetts Institute of Technology).

Ghauri, P., Grønhaug, K., & Strange, R. (2020). *Research methods in business studies*. Cambridge University Press.

Gheorghe, M. (2012). The Risk Associated To The Knowledge Transfer At Organizational Level. In *Proceedings of the INTERNATIONAL MANAGEMENT CONFERENCE* (Vol. 6, No. 1, pp. 570-576). Faculty of Management, Academy of Economic Studies, Bucharest, Romania.

Gheorghioiu, N. (2020). Knowledge risk management in aviation. Proceedings of the International Conference on Business Excellence.

Gold, A. H., Malhotra, A., & Segars, A. H. (2001). Knowledge management: An organizational capabilities perspective. *Journal of management information systems*, *18*(1), 185-214.

Govindan, K., Khodaverdi, R., & Vafadarnikjoo, A. (2016). A grey DEMATEL approach to develop third-party logistics provider selection criteria. *Industrial Management & Data Systems*, *116*(4), 690-722. https://doi.org/10.1108/IMDS-05-2015-0180

Goyal, T., & Kaushal, S. (2017). An intelligent scheduling scheme for real-time traffic management using Cooperative Game Theory and AHP-TOPSIS methods for next generation telecommunication networks. *Expert Systems with Applications*, *86*, 125-134.

Gragido, W., & Pirc, J. (2011). *Cybercrime and espionage: An analysis of subversive multi-vector threats*. Newnes.

Graham, J. D., & Wiener, J. B. (2024). Co-Benefits, Countervailing Risks, and Cost–Benefit Analysis. *Human and Ecological Risk Assessment: Theory and Practice*, 2, 1167-1188.

Grant, R. M. (1996). Toward a knowledge-based theory of the firm. *Strategic Management Journal*, *17*(S2), 109-122. https://doi.org/https://doi.org/10.1002/smj.4250171110

Guo, W., Yang, J., Li, D., & Lyu, C. (2020). Knowledge sharing and knowledge protection in strategic alliances: the effects of trust and formal contracts. *Technology Analysis & Strategic Management*, *32*(11), 1366-1378.

Hammoda, B., & Durst, S. (2022). A taxonomy of knowledge risks for healthcare organizations. *Vine Journal of Information and Knowledge Management Systems*, *52*(3), 354-372. https://doi.org/10.1108/VJIKMS-07-2021-0114

Henn, M., Weinstein, M., & Foard, N. (2005). *A short introduction to social research*. Sage.

Hillson, D. (2016). Enterprise risk management: Managing uncertainty and minimising surprise. In *Advising Upwards* (pp. 57-86). Routledge.

Hislop, D., Bosua, R., & Helms, R. (2018). *Knowledge management in organizations: A critical introduction*. Oxford university press.

Ho, C. T. (2009). The relationship between knowledge management enablers and performance. *Industrial Management & Data Systems*, *109*(1), 98-117. https://doi.org/10.1108/02635570910926618

Hosseinzadeh Lotfi, F., Allahviranloo, T., Pedrycz, W., Shahriari, M., Sharafi, H., & Razipour GhalehJough, S. (2023). Simple Additive Weighting (SAW) Method in Fuzzy Environment. In *Fuzzy Decision Analysis: Multi Attribute Decision Making Approach* (pp. 117-140). Cham: Springer International Publishing.

Husted, K., & Michailova, S. (2002). Diagnosing and fighting knowledge-sharing hostility. *Organizational dynamics*, *31*(1), 60-73.

Hutchins, G. (2018). *ISO 31000: 2018 enterprise risk management*. Greg Hutchins.

Hwang C. L., & Yoon K. (1981). *Multiple Attribute Decision Making. Methods and Applications*, Springer, Berlin.

Iivari, J., & Venable, J. R. (2009). Action research and design science research-Seemingly similar but decisively dissimilar.

Ilvonen, I., Jussila, J. J., & Kärkkäinen, H. (2015). Towards a business-driven process model for knowledge security risk management: Making sense of knowledge risks. *International Journal of Knowledge Management (IJKM)*, *11*(4), 1-18.

Inkpen, A. C., & Tsang, E. W. (2005). Social capital, networks, and knowledge transfer. *Academy of management review*, *30*(1), 146-165.

International Organization for Standardization. (2018). *ISO 30401:2018 Knowledge management systems – Requirements*. International Organization for Standardization – ISO`.

International Organization for Standardization. (2018). Proposals for management system standards (ISO/IEC Directives Part 1 and Consolidated ISO Supplement, Annex SL). International Organization for Standardization – ISO.

International Organization for Standardization. (2022). *Information Security, Cybersecurity and Privacy Protection-Information Security Management Systems-Requirements*. ISO.

Ishizaka, A., Balkenborg, D., & Kaplan, T. (2011). Does AHP help us make a choice? An experimental evaluation. *Journal of the Operational Research Society*, *62*(10), 1801-1812.

Jabbarzadeh, A. (2018). Application of the AHP and TOPSIS in project management. *Journal of Project Management*, *3*(2), 125-130.

Jackson, T., Shen, J., Nikolic, S., & Xia, G. (2020). Managerial factors that influence the success of knowledge management systems: A systematic literature review. *Knowledge and Process Management*, *27*(2), 77-92. https://doi.org/https://doi.org/10.1002/kpm.1622

Jafari, M., Rezaeenour, J., Mahdavi Mazdeh, M., & Hooshmandi, A. (2011). Development and evaluation of a knowledge risk management model for project-based organizations. *Management Decision*, *49*(3), 309-329. https://doi.org/10.1108/00251741111120725

Järvinen, P. (2007). Action research is similar to design science. *Quality & quantity*, *41*, 37-54.

Jennex, M. E., & Durcikova, A. (2013, January). Assessing knowledge loss risk. In 2013 46th Hawaii International Conference on System Sciences (pp. 3478-3487). IEEE.

Jennex, M. E., & Durcikova, A. (2020a). Creating sustainable knowledge systems: towards a risk and threat assessment framework. *Journal of Strategic Innovation and Sustainability*, *15*(4), 138-152.

Jennex, M. E., & Durcikova, A. (2020b). Knowledge systems and risk management: Towards a risk and threat assessment framework. In *Current issues and trends in knowledge management, discovery, and transfer* (pp. 367-385). IGI Global.

Jesson, J. (2011). *Doing your literature review: Traditional and systematic techniques*. Sage.

Jiang, X., Li, M., Gao, S., Bao, Y., & Jiang, F. (2013). Managing knowledge leakage in strategic alliances: The effects of trust and formal contracts. *Industrial Marketing Management*, *42*(6), 983-991.

Jiang, X., Bao, Y., Xie, Y., & Gao, S. (2016). Partner trustworthiness, knowledge flow in strategic alliances, and firm competitiveness: A contingency perspective. *Journal of business research*, *69*(2), 804-814.

Jozi, S. A., & Majd, N. M. (2014). Health, safety, and environmental risk assessment of steel production complex in central Iran using TOPSIS. *Environmental monitoring and assessment*, *186*, 6969-6983.

Kabassi, K. (2009). Fuzzy simple additive weighting for evaluating a personalised geographical information system. In *New Directions in Intelligent Interactive Multimedia Systems and Services-2* (pp. 275-284). Berlin, Heidelberg: Springer Berlin Heidelberg.

Kailiponi, P. (2010). Analyzing evacuation decisions using multi-attribute utility theory (MAUT). *Procedia Engineering*, *3*, 163-174.

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk analysis*, *1*(1), 11-27.

Keeney, R. L. (1993). *Decisions with multiple objectives: preferences and value trade-offs*. Cambridge university press.

Kent, C. W., & Allen, F. W. (2014). An overview of risk-based priority setting at EPA. *Worst things first*, 47-68.

Knight, F. H. (1921). Risk, uncertainty and profit. *Hart, Schaffner and Marx*.

Kogut, B., & Zander, U. (1992). Knowledge of the Firm, Combinative Capabilities, and the Replication of Technology. *Organization Science*, *3*(3), 383-397. http://www.jstor.org/stable/2635279

Kovács, G., & Spens, K. M. (2005). Abductive reasoning in logistics research. *International Journal of Physical Distribution & Logistics Management*, *35*(2), 132-144.

Kuo, T. (2017). A modified TOPSIS with a different ranking index. *European journal of operational research*, *260*(1), 152-160.

Kwak, Y. H., & Ingall, L. (2007). Exploring Monte Carlo simulation applications for project management. *Risk management*, 9, 44-57.

Leflar, J., & Siegel, M. (2013). Organizational Resilience. *Managing the Risks of Disruptive Events–A practitioner's Guide. Boca Raton, FL: CRC PressTaylor & Francis Group*.

Lee, H. L. (2002). Aligning supply chain strategies with product uncertainties. *California management review*, *44*(3), 105-119.

Lee, S., Suh, E., & Lee, M. (2014). Measuring the risk of knowledge drain in communities of practice. *Journal of Knowledge Management*, *18*(2), 382-395.

Lee, R. W., Yip, J. Y., & Shek, V. W. (2021). Assessment of Knowledge Risks. In *Knowledge Risk and its Mitigation: Practices and Cases* (pp. 15-40). Emerald Publishing Limited.

Li, J., & Xiao, Y. (2024). Analysis of influencing factors on review efficiency of multidisciplinary scientific research projects using DEMATEL with a 5-point scale. *PloS one*, *19*(12), e0315349.

Loomba, A. P. (2006). A FRAMEWORK FOR KNOWLEDGE RISK MANAGEMENT. Proceedings of the 11th Annual Conference of Asia Pacific Decision Sciences Institute.

Macharis, C., Springael, J., De Brucker, K., & Verbeke, A. (2004). PROMETHEE and AHP: The design of operational synergies in multicriteria analysis.: Strengthening PROMETHEE with ideas of AHP. *European journal of operational research*, *153*(2), 307-317.

Macharis, C., Mareschal, B., Waaub, J. P., & Milan, L. (2015). PROMETHEE–GDSS revisited: applications so far and new developments. *International Journal of Multicriteria Decision Making*, *5*(1-2), 129-151.

Madi, E. N., Garibaldi, J. M., & Wagner, C. (2016, July). An exploration of issues and limitations in current methods of TOPSIS and fuzzy TOPSIS. In *2016 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* (pp. 2098-2105). IEEE.

Maleki, H., & Zahir, S. (2013). A comprehensive literature review of the rank reversal phenomenon in the analytic hierarchy process. *Journal of Multi-Criteria Decision Analysis*, *20*(3-4), 141-155.

Manhart, M., & Thalmann, S. (2015). Protecting organizational knowledge: a structured literature review. *Journal of Knowledge Management*, *19*(2), 190-211.

Manjunatheshwara, K. J., & Vinodh, S. (2018). Application of TISM and MICMAC for analysis of influential factors of sustainable development of tablet devices: a case study. *International Journal of Sustainable Engineering*, *11*(5), 353-364.

Marabelli, M., & Newell, S. (2012). Knowledge risks in organizational networks: The practice perspective. *The Journal of Strategic Information Systems*, *21*(1), 18-30. https://doi.org/https://doi.org/10.1016/j.jsis.2011.11.002

Mascitelli, R. (2000). From experience: harnessing tacit knowledge to achieve breakthrough innovation. *Journal of Product Innovation Management: an International Publication of the Product Development & Management Association*, *17*(3), 179-193.

Massaro, M., Dumay, J., & Guthrie, J. (2016). On the shoulders of giants: undertaking a structured literature review in accounting. *Accounting, Auditing & Accountability Journal*, *29*(5), 767-801.

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

Massingham, P. R. (2018). Measuring the impact of knowledge loss: a longitudinal study. *Journal of Knowledge Management*, *22*(4), 721-758. https://doi.org/10.1108/JKM-08-2016-0338

Massingham, P. (2014). An evaluation of knowledge management tools: Part 1–managing knowledge resources. *Journal of knowledge management*, *18*(6), 1075-1100.

Massingham, P. R., & Massingham, R. K. (2014). Does knowledge management produce practical outcomes? *Journal of Knowledge Management*, *18*(2), 221-254. https://doi.org/10.1108/JKM-10-2013-0390

McDermott, R., & O'dell, C. (2001). Overcoming cultural barriers to sharing knowledge. *Journal of knowledge management*, *5*(1), 76-85.

Menghwar, P. S., & Daood, A. (2021). Creating shared value: A systematic review, synthesis and integrative perspective. *International Journal of Management Reviews*, *23*(4), 466-485. https://doi.org/https://doi.org/10.1111/ijmr.12252

Menon, S., & Suresh, M. (2020). Total interpretive structural modelling: evolution and applications. In *Innovative Data Communication Technologies and Application: ICIDCA 2019* (pp. 257-265). Springer International Publishing.

Migdadi, M. M. (2022). Knowledge management processes, innovation capability and organizational performance. *International Journal of Productivity and Performance Management*, *71*(1), 182-210. https://doi.org/10.1108/IJPPM-04-2020-0154

Müller, F., & Mueller, A. (2019). Knowledge Risk Manangement–How to Manage Future Knowledge Loss. HICSS.

Munier, N., Hontoria, E., Munier, N., & Hontoria, E. (2021). Shortcomings of the AHP Method. *Uses and Limitations of the AHP Method: A Non-Mathematical and Rational Analysis*, 41-90.

Nafisur Rahman, N. (2024). Multi-Criteria Decision-Making for Information Science Program Ranking Using the ELECTRE Method. *Library Progress International*, *44*(3), 17266-17273.

National Institute of Standards and Technology (NIST). (2012). Guide for conducting risk assessments.

Neef, D. (2005). Managing corporate risk through better knowledge management. *The Learning Organization*, *12*(2), 112-124.

Nikou, T., & Klotz, L. (2014). Application of multi-attribute utility theory for sustainable energy decisions in commercial buildings: A case study. *Smart and Sustainable Built Environment*, *3*(3), 207-222.

Nishat Faisal, M., Banwet, D. K., & Shankar, R. (2007). Information risks management in supply chains: an assessment and mitigation framework. *Journal of Enterprise Information Management*, *20*(6), 677-699.

Nonaka, I. (1991). The knowledge-creating company Harvard business review November-December.

Nonaka, L., Takeuchi, H., & Umemoto, K. (1996). A theory of organizational knowledge creation. *International journal of technology Management*, *11*(7-8), 833-845.

Nonaka, I., & Toyama, R. (2003). The knowledge-creating theory revisited: knowledge creation as a synthesizing process. *Knowledge management research & practice*, *1*(1), 2-10.

Norman, P. M. (2002). Protecting knowledge in strategic alliances: Resource and relational characteristics. *The Journal of High Technology Management Research*, *13*(2), 177-202.

North, K., De Carvalho, A. B., Braccini, A. M., Durst, S., Carvalho, J. Á., Gräslund, K., & Thalmann, S. (2020). 4.1 Knowledge risks in supply chain interactions of SMEs: An exploratory study. 2019 Knowledge Management in Digital Work Environments, State-of-the-Art and Outlook, WM 2019, Potsdam, Germany, 18 March 2019 through 20 March 2019, Code 166782,

Obi, L., Hampton, P., & Awuzie, B. (2020). Total Interpretive Structural Modelling of Graduate Employability Skills for the Built Environment Sector. *Education Sciences*, *10*(12), 369. https://www.mdpi.com/2227-7102/10/12/369

Oxley, J., & Wada, T. (2009). Alliance structure and the scope of knowledge transfer: Evidence from US-Japan agreements. *Management science*, *55*(4), 635-649.

Padyab, A. M., Päivärinta, T., & Harnesk, D. (2015). Genre-based approach to assessing information and knowledge security risks. In *Transportation Systems and Engineering: Concepts, Methodologies, Tools, and Applications* (pp. 1237-1253). IGI Global.

Papathanasiou, J., Ploskas, N., Papathanasiou, J., & Ploskas, N. (2018). *Topsis* (pp. 1-30). Springer International Publishing.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, *24*(3), 45-77.

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC press.

Pereira, V., Mellahi, K., Temouri, Y., Patnaik, S., & Roohanifar, M. (2019). Investigating dynamic capabilities, agility and knowledge management within EMNEs-longitudinal evidence from Europe. *Journal of Knowledge Management*, *23*(9), 1708-1728. https://doi.org/10.1108/JKM-06-2018-0391

Pérez-Aróstegui, M. N., Bustinza-Sánchez, F., & Barrales-Molina, V. (2015). Exploring the relationship between information technology competence and quality management. *BRQ Business Research Quarterly*, *18*(1), 4-17.

Perrott, B. E. (2007). A strategic risk approach to knowledge management. *Business Horizons*, *50*(6), 523-533. https://doi.org/https://doi.org/10.1016/j.bushor.2007.08.002

Piri, M., Zahedi, M. R., Vaziri Goodarzi, E., & Mohammadpanah, M. (2021). Proposing a model for dynamical computing the risk of knowledge domains in the organizational knowledge map. *Vine Journal of Information and Knowledge Management Systems*, *51*(2), 259-270. https://doi.org/10.1108/VJIKMS-07-2019-0110

Polanyi, M. (1966). The logic of tacit inference. *Philosophy*, *41*(155), 1-18.

Power, M. (2004). The risk management of everything. *The Journal of Risk Finance*, *5*(3), 58-65.

Qiu, X., & Haugland, S. A. (2019). The role of regulatory focus and trustworthiness in knowledge transfer and leakage in alliances. *Industrial Marketing Management*, *83*, 162-173.

Rahim, A. A., Musa, S. N., Ramesh, S., & Lim, M. K. (2021). Development of a fuzzy-TOPSIS multi-criteria decision-making model for material selection with the integration of safety, health

and environment risk assessment. *Proceedings of the Institution of Mechanical Engineers, Part L: Journal of Materials: Design and Applications*, *235*(7), 1532-1550.

Rajesh, R., & Ravi, V. (2017). Analyzing drivers of risks in electronic supply chains: a grey–DEMATEL approach. *The International Journal of Advanced Manufacturing Technology*, *92*(1), 1127-1145. https://doi.org/10.1007/s00170-017-0118-3

Rehman, Z., & Kifor, C. V. (2015). Risk management in perspective of knowledge management a brief survey. *Acta Universitatis Cibiniensis. Technical Series*, *67*(1), 191-194.

Rehman, S. U., Bresciani, S., Ashfaq, K., & Alam, G. M. (2022). Intellectual capital, knowledge management and competitive advantage: a resource orchestration perspective. *Journal of Knowledge Management*, *26*(7), 1705-1731. https://doi.org/10.1108/JKM-06-2021-0453

Ross, R. S., & Johnson, L. A. (2010). Guide for applying the risk management framework to federal information systems: A security life cycle approach.

Ross, R. S. (2014). Guide for applying the Risk Management Framework to federal information systems: A security life cycle approach.

Roy, B. (1991). The outranking approach and the foundations of ELECTRE methods. *Theory and decision*, 31, 49-73.

Saaty, T. L. (1980). The analytic hierarchy process (AHP). *The Journal of the Operational Research Society*, *41*(11), 1073-1076.

Saaty, T. L. (2016). The analytic hierarchy and analytic network processes for the measurement of intangible criteria and for decision-making. *Multiple criteria decision analysis: state of the art surveys*, 363-419.

Sarigianni, C., Thalmann, S., & Manhart, M. (2016, January). Protecting knowledge in the financial sector: An analysis of knowledge risks arising from social media. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4031-4040). IEEE.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students*. Pearson education.

Saunders, M., Lewis, P., & Thornhill, A. (2019). Research Onion. Research methods for business students. In: USA: Routledge. doi. org/10.1007/s13398-014-0173-7.2.

Serna, C. A. A. (2023). Mitigating the Risk of Knowledge Leakage in Knowledge Intensive Organizations: a Mobile Device Perspective. arXiv preprint arXiv:2308.09229.

Serna, C. A., Bosua, R., Ahmad, A., & Maynard, S. (2017). Strategies to Mitigate Knowledge Leakage Risk caused by the use of mobile devices: A Preliminary Study.

Shabtai, A., Elovici, Y., & Rokach, L. (2012). A Survey of Data Leakage Detection and Prevention Solutions.

Shao, J., Taisch, M., & Ortega-Mier, M. (2016). A grey-DEcision-MAking Trial and Evaluation Laboratory (DEMATEL) analysis on the barriers between environmentally friendly products and consumers: practitioners' viewpoints on the European automobile industry. *Journal of Cleaner Production*, *112*, 3185-3194. https://doi.org/https://doi.org/10.1016/j.jclepro.2015.10.113

Shieh, J.-I., Wu, H.-H., & Huang, K.-K. (2010). A DEMATEL method in identifying key success factors of hospital service quality. *Knowledge-Based Systems*, *23*(3), 277-282. https://doi.org/https://doi.org/10.1016/j.knosys.2010.01.013

Shujahat, M., Akhtar, A., Nawaz, F., Wang, M., & Sumbal, M. S. (2020). Knowledge Risk Management in two-tier HRM structures. *Knowledge risk management: from theory to praxis*, 49-68.

Si, S. L., You, X. Y., Liu, H. C., & Zhang, P. (2018). DEMATEL technique: a systematic review of the state-of-the-art literature on methodologies and applications. *Mathematical problems in Engineering*, *2018*(1), 3696457.

Siddiqui, A. A., Lahmar, A., Singh, P., Arora, K., Samadhiya, A., & Kumar, A. (2024). Unlocking circular supply chain 4.0: identifying key barriers through bibliometrics and TISM-MICMAC. *Benchmarking: an International Journal*.

Singh, N., Dixit, A., & Ashish, D. K. (2024). Modelling of critical success factors to improve the supply chain resilience for sustainable construction sector. *Smart and Sustainable Built Environment*.

Slovic, P. (1987). Perception of risk. *science*, *236*(4799), 280-285.

Smith, E. A. (2001). The role of tacit and explicit knowledge in the workplace. *Journal of knowledge Management*, *5*(4), 311-321.

Sodhi, M. S., Son, B. G., & Tang, C. S. (2012). Researchers' perspectives on supply chain risk management. *Production and operations management*, *21*(1), 1-13.

Sommestad, T., Ekstedt, M., & Holm, H. (2012). The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. *IEEE Systems Journal*, *7*(3), 363-373.

Sotamaa, T., Reiman, A., & Kauppila, O. (2024). Manufacturing SME risk management in the era of digitalisation and artificial intelligence: a systematic literature review. *Continuity & Resilience Review*.

Souto, L. F., & Bruno-Faria, M. d. F. (2022). Knowledge loss risk management in a Brazilian public company: the case of AMAZUL. *Knowledge Management Research & Practice*, 1-12. https://doi.org/10.1080/14778238.2022.2125848

Spender, J.-C. (1996). Making knowledge the basis of a dynamic theory of the firm. *Strategic Management Journal*, *17*(S2), 45-62. https://doi.org/https://doi.org/10.1002/smj.4250171106

Sumbal, M. S., Tsui, E., Durst, S., Shujahat, M., Irfan, I., & Ali, S. M. (2020). A framework to retain the knowledge of departing knowledge workers in the manufacturing industry. *VINE Journal of Information and Knowledge Management Systems*, *50*(4), 631-651.

Sushil. (2012). Interpreting the Interpretive Structural Model. *Global Journal of Flexible Systems Management*, *13*(2), 87-106. https://doi.org/10.1007/s40171-012-0008-3

Sushil, & Dinesh, K. K. (2022). Structured literature review with TISM leading to an argumentation based conceptual model. *Global Journal of Flexible Systems Management*, *23*(3), 387-407.

Taherdoost, H. (2023). Analysis of Simple Additive Weighting Method (SAW) as a Multi-Attribute Decision-Making Technique: A Step-by-Step. *Taherdoost, H*, 21-24.

Tan, K. H., Wong, W. P., & Chung, L. (2016). Information and knowledge leakage in supply chain. *Information Systems Frontiers*, *18*, 621-638.

Tanţău, A. D., & Paicu, E. L. (2013). Managing knowledge risks in intrapreneurial environment. *The International Journal of Management Science and Information Technology (IJMSIT)*(10-(Dec)), 4-25.

Taylor, A. (2005). An operations perspective on strategic alliance success factors: An exploratory study of alliance managers in the software industry. *International Journal of Operations & Production Management*, *25*(5), 469-490.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic management journal*, *18*(7), 509-533.

Teece, D. J. (2000). Strategies for managing knowledge assets: the role of firm structure and industrial context. *Long range planning*, *33*(1), 35-54.

Temel, S., & Vanhaverbeke, W. (2020). Knowledge risk management during implementation of open innovation. *Knowledge Risk Management: From Theory to Praxis*, 207-227.

Temel, S., & Durst, S. (2021). Knowledge risk prevention strategies for handling new technological innovations in small businesses. *Vine Journal of Information and Knowledge Management Systems*, *51*(4), 655-673. https://doi.org/10.1108/VJIKMS-10-2019-0155

Thalmann, S., Manhart, M., Ceravolo, P., & Azzini, A. (2014). An integrated risk management framework: measuring the success of organizational knowledge protection. *International Journal of Knowledge Management (IJKM)*, *10*(2), 28-42.

Thalmann, S., Maier, R., Remus, U., & Manhart, M. (2024). Connect with care: informal knowledge protection practices to enhance knowledge sharing in networks of organizations. *VINE Journal of Information and Knowledge Management Systems*, (ahead-of-print).

Thakkar, J. J., & Thakkar, J. J. (2021). Decision-making trial and evaluation laboratory (DEMATEL). *Multi-criteria decision making*, 139-159.

Timiyo, A. J., & Foli, S. (2023). Knowledge leakage through social networks: a review of existing gaps, strategies for mitigating potential risk factors and future research direction. *VINE Journal of Information and Knowledge Management Systems*.

Torabi, F., & El-Den, J. (2017). The impact of Knowledge Management on Organizational Productivity: A Case Study on Koosar Bank of Iran. *Procedia Computer Science*, *124*, 300-310. https://doi.org/https://doi.org/10.1016/j.procs.2017.12.159

Torbacki, W. (2021). A hybrid MCDM model combining DANP and PROMETHEE II methods for the assessment of cybersecurity in industry 4.0. *Sustainability*, *13*(16), 8833.

Triantaphyllou, E., & Triantaphyllou, E. (2000). *Multi-criteria decision making methods* (pp. 5-21). Springer Us.

Trkman, P., & Desouza, K. C. (2012). Knowledge risks in organizational networks: An exploratory framework. *The Journal of Strategic Information Systems*, *21*(1), 1-17. https://doi.org/https://doi.org/10.1016/j.jsis.2011.11.001

Tsang, H. W. C., & Lee, R. W. (2018). Mitigation of knowledge risks in open innovation. In Open innovation and knowledge management in small and medium enterprises (pp. 183-203).

Tubigi, M., & Alshawi, S. (2015). The impact of knowledge management processes on organisational performance. *Journal of Enterprise Information Management*, *28*(2), 167-185. https://doi.org/10.1108/JEIM-01-2014-0003

Ursache, V. M. (2023, March). Knowledge Vulnerabilities Scoring System and the Knowledge Economy. In *International Conference on Business Excellence* (pp. 341-359). Cham: Springer Nature Switzerland.

Vafaei-Zadeh, A., Ramayah, T., Hanifah, H., Kurnia, S., & Mahmud, I. (2020). Supply chain information integration and its impact on the operational performance of manufacturing firms in Malaysia. *Information & Management*, *57*(8), 103386.

Venable, J., & Baskerville, R. (2012). Eating our own cooking: Toward a more rigorous design science of research methods. *Electronic Journal of Business Research Methods*, *10*(2), pp141-153.

Vlasov, M., & Panikarova, S. (2019). Management of knowledge generation risk: Empirical research of the industrial enterprises. Academic Conferences Limited.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Vose, D. (2008). *Risk analysis: a quantitative guide*. John Wiley & Sons.

Waddell, D., & Stewart, D. (2008). Knowledge management as perceived by quality practitioners. *The TQM Journal*, *20*(1), 31-44. https://doi.org/10.1108/09544780810842884

Walsh, J. P., & Ungson, G. R. (1991). Organizational memory. *Academy of management Review*, *16* (1), 57–91.

Warfield J, N. (1982). Interpretive structural modeling. *Group planning and problem solving methods in engineering management*. https://cir.nii.ac.jp/crid/1572824501228254976

Whitman, M. E., & Mattord, H. J. (2019). *Management of information security*. Cengage Learning.

Wu, W. W., & Lee, Y. T. (2007). Developing global managers' competencies using the fuzzy DEMATEL method. *Expert systems with applications*, *32*(2), 499-507.

Yang, Q., Liu, Y., & Li, Y. (2019). How do an alliance firm's strategic orientations drive its knowledge acquisition? Evidence from Sino-foreign alliance partnership. *Journal of Business & Industrial Marketing*, *34*(2), 505-517.

Yarovenko, H., Bilan, Y., Lyeonov, S., & Mentel, G. (2021). Methodology for assessing the risk associated with information and knowledge loss management. *JOURNAL OF BUSINESS ECONOMICS AND MANAGEMENT*, *22*(2), 369-387.

Yin, R. K. (2009). *Case study research: Design and methods* (Vol. 5). sage.

Zaku, A., & Uysal, F. (2022). Decision Tree Analysis in Project Risk Management: A Systematic Review. *the specific publication details need to be added*.

Zeiringer, J. P., & Thalmann, S. (2022). Knowledge sharing and protection in data-centric collaborations: An exploratory study. *Knowledge Management Research & Practice*, *20*(3), 436-448. https://doi.org/10.1080/14778238.2021.1978886

Zeiringer, J. P., Fleiß, J., & Thalmann, S. (2024). Data Anonymization as Instrument to manage Knowledge Risks in Supply Chains.

Zekhnini, K., Chaouni Benabdellah, A., Bag, S., & Gupta, S. (2024). Supply chain 5.0 digitalization: an integrated approach for risk assessment. *Management Decision*.

Zhao, X., Xie, J., & Zhang, W. J. (2002). The impact of information sharing and ordering co-ordination on supply chain performance. *Supply Chain Management: an international journal*, *7*(1), 24-40.

Zhang, D. Y., Zeng, Y., Wang, L., Li, H., & Geng, Y. (2011). Modeling and evaluating information leakage caused by inferences in supply chains. *Computers in Industry*, *62*(3), 351-363.

Zieba, M., & Bongiovanni, I. (2022). Knowledge management and knowledge security—Building an integrated framework in the light of COVID-19. *Knowledge and Process Management*, *29*(2), 121-131. https://doi.org/https://doi.org/10.1002/kpm.1707

Zięba, M., Durst, S., & Gonsiorowska, M. (2021). Knowledge Risks in the COVID-19 Pandemic.

Zieba, M., Durst, S., & Gonsiorowska, M. (2022a, August). A new Critical risk on the Block: Cyber Risks as an Example of Technical Knowledge Risks in Organizations. In *European Conference on Knowledge Management* (Vol. 23, No. 2, pp. 1269-1276).

Zieba, M., Durst, S., & Hinteregger, C. (2022b). 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

Zieba, M. (2023). Emotions and Their Relation with Knowledge Risks in Organizations. In *The Future of Knowledge Management: Reflections from the 10th Anniversary of the International Association of Knowledge Management (IAKM)* (pp. 169-184). Cham: Springer Nature Switzerland.

Appendix

Appendix A1

Table 19 List of papers included in the systematic literature review

Author(s)	Title of Journal/Conference/Book	Type	Methodology
Jennex and Durcikova (2020a)	International Journal of Knowledge Management	Article	Qualitative
Jennex and Durcikova (2020b)	Journal of Strategic Innovation and Sustainability	Article	Conceptual paper
Yarovenko et al. (2021)	Journal of Business Economics and Management	Article	Quantitative
Lee et al. (2021)	N/A	Book chapter	Quantitative
Lee et al. (2014)	Journal of Knowledge Management	Article	Quantitative
Piri et al. (2021)	Vine Journal of Information and Knowledge Management Systems	Article	Quantitative
Ursache et al. (2023)	International Conference on Business Excellence	Conference paper	Qualitative
Thalmann et al. (2014)	International Journal of Knowledge Management	Article	Quantitative
Delak and Damij (2015)	European Conference on Knowledge Management (ECKM)	Conference paper	Quantitative
Neef (2005)	The Learning Organisation: An International Journal	Article	Conceptual paper
Massingham (2010)	Journal of Knowledge Management	Article	Quantitative
Jafari et al. (2011)	Management Decision	Article	Quantitative
Tanţău and Paicu (2013)	The International Journal of Management Science and Information Technology (IJMSIT)	Article	Qualitative
Massingham (2014)	Journal of Knowledge Management	Article	Qualitative
Durst et al. (2019)	Journal of Business Research	Article	Quantitative
Gheorghioiu (2020)	International Conference on Business Excellence	Conference paper	Conceptual paper
Zieba et al. (2021)	European Conference on Knowledge Management (ECKM)	Conference paper	Quantitative
Zieba et al. (2022b)	Journal of Knowledge Management	Article	Quantitative
Zieba and Bongiovanni (2022)	Knowledge and Process Management	Article	Qualitative
Zieba (2023)	N/A	Book chapter	Conceptual paper
Durst et al. (2023)	Heliyon	Article	Quantitative

El Khatib and Abbas (2023)	Middle East Journal of Management	Article	Quantitative
Bratianu et al. (2020)	Amfiteatru Economic	Article	Quantitative
El Khatib and Ali (2022)	Journal of Management Development	Article	Quantitative
Zeiringer et al. (2024)	Hawaii International Conference on System Sciences (HICSS)	Conference paper	Qualitative
Bayer and Maier (2006)	International Conference on Knowledge Management and Knowledge Technologies	Conference paper	Conceptual paper
Loomba (2006)	Conference of Asia Pacific Decision Sciences Institute	Conference paper	Qualitative
Erickson and Rothberg (2010)	European Conference on Knowledge Management (ECKM)	Conference paper	Qualitative
Sarigianni et al. (2016)	Hawaii International Conference on System Sciences (HICSS)	Conference paper	Qualitative
Gheorghe (2012)	International Management Conference	Conference paper	Qualitative
Von Solms and Van Niekerk (2013)	Computers & Security	Article	Qualitative
Padyab et al. (2015)	Hawaii International Conference on System Sciences (HICSS)	Conference Paper	Qualitative
Manhart and Thalmann (2015)	Journal of Knowledge Management	Article	Qualitative
Peltier (2016)	N/A	Book chapter	Conceptual paper
Müller and Mueller (2019)	Hawaii International Conference on System Sciences (HICSS)	Conference paper	Quantitative
Vlasov and Panikarova (2019)	European Conference on Knowledge Management (ECKM)	Conference paper	Quantitative
North et al. (2019)	N/A	Book chapter	Qualitative
Shujahat et al. (2020)	N/A	Book chapter	Qualitative
Daghfous et al. (2021)	The International Journal of Logistics Management	Article	Conceptual paper
Zeiringer and Thalmann (2022)	Journal of Knowledge Management Research & Practice	Article	Qualitative
Souto and Bruno-Faria (2022)	Knowledge Management Research & Practice	Article	Qualitative
Souto and Bruno-Faria (2023)	Knowledge Management Research & Practice	Article	Qualitative
Elias and Wright (2006)	Advances In Management Accounting, Vol 15	Article	Qualitative
Rehman and Kifor (2015)	Acta Universitatis Cibiniensis. Technical Series	Article	Qualitative
Durst and Zieba (2019)	Knowledge Management Research & Practice	Article	Conceptual paper
El Khatib et al. (2021)	BAU Journal-Creative Sustainable Development	Article	Conceptual paper

Bratianu and Bejinaru (2022)	International Forum on Knowledge Asset Dynamics (IFKAD)	Article	Qualitative
Hammoda and Durst (2022)	VINE Journal of Information and Knowledge Management Systems	Article	Conceptual paper
Fruhwirth et al. (2023)	Schmalenbach Journal of Business Research	Article	Qualitative
TrKMan et al. (2012)	Journal of Strategic Information Systems	Article	Qualitative
Coleman and Casselman (2016)	Journal of Knowledge Management	Article	Qualitative
Durst et al. (2018)	Journal of Knowledge Management	Article	Qualitative
Temel and Vanhaverbeke (2020)	N/A	Book chapter	Conceptual paper
Zieba et al. (2022a)	European Conference on Knowledge Management	Conference Paper	Quantitative
Temel and Durst (2021)	VINE Journal of Information and Knowledge Management Systems	Article	Conceptual paper
Thalmann and Ilvonen (2020)	Hawaii International Conference on System Sciences (HICSS)	Conference paper	Qualitative
Thalmann et al. (2024)	VINE Journal of Information and Knowledge Management Systems	Article	Qualitative
Tsang and Lee (2018)	N/A	Book chapter	Qualitative

Appendix A2

Questionnaire

Instructions: For each pair of risk factors, please indicate whether risk factor "X" influences or drives risk factor "Y." Use the following scale:

- 1: Risk factor "X" influences or drives risk factor "Y."
- 0: Risk factor "X" does not influence or drive risk factor "Y."

Y **X**	Distrust Among Partners	Incomplete Contracts	Substandard Security Measures	Weak BYOD Policies	Insufficient Technological Competence	Perceived Opportunism	Horizontal Competition	Subcontracting Activities	Informal Knowledge Sharing	Lack of Continuous Monitoring
Distrust Among Partners	—									
Incomplete Contracts		—								
Substandard Security Measures			—							
Weak BYOD Policies				—						

Insufficient Technological Competence					—					
Perceived Opportunism						—				
Horizontal Competition							—			
Subcontracting Activities								—		
Informal Knowledge Sharing									—	
Lack of Continuous Monitoring										—

Appendix A3

Aggregated matrix

	Distrust Among Partners	Incomplete Contracts	Substandard Security Measures	Weak BYOD Policies	Insufficient Technological Competence	Perceived Opportunism	Horizontal Competition	Subcontracting Activities	Informal Knowledge Sharing	Lack of Continuous Monitoring
Distrust Among Partners	1	1	1	1	0	1	1	1	1	1
Incomplete Contracts	0	1	0	0	1	0	1	0	0	0
Substandard Security Measures	0	0	1	1	1	0	0	1	1	1
Weak BYOD Policies	0	0	0	1	1	0	0	0	0	1
Insufficient Technological Competence	0	0	0	0	1	0	0	0	0	0
Perceived Opportunism	1	0	0	0	0	1	1	0	0	1
Horizontal Competition	0	0	0	1	1	0	1	1	0	1

Subcontracting Activities	0	1	0	1	1	0	0	1	1	1
Informal Knowledge Sharing	0	0	0	0	0	0	0	0	1	0
Lack of Continuous Monitoring	0	1	0	0	1	0	0	0	1	1

Appendix A4

Pairwise comparison matrix

	Likelihood	Severity	Dependency Power	Driving Power
Likelihood	1	3	5	4
Severity	1/3	1	4	2
Dependency Power	1/5	1/4	1	1/2
Driving Power	1/4	1/2	2	1

Normalised matrix

	Likelihood	Severity	Dependency Power	Driving Power
Likelihood	0.513	0.632	0.417	0.533
Severity	0.171	0.211	0.333	0.267
Dependency Power	0.102	0.053	0.083	0.067
Driving Power	0.128	0.105	0.167	0.133

Total relation matrix

	Likelihood	Severity	Dependency Power	Driving Power
Likelihood	11.676	11.692	11.683	11.681
Severity	4.123	5.497	4.707	4.591
Dependency Power	1.724	1.819	2.870	1.842
Driving Power	2.555	2.742	2.848	3.789