KMAN PUBLISHING INSTITUTE

Article history:
Received 28 August 2026
Revised 29 October 2026
Accepted 04 November 2026
Initial Publish 25 November 2026
Published online 01 January 2028

Journal of Resource Management and Decision Engineering

Volume 7, Issue 1, pp 1-19



Designing a Meta-Synthesis Model for Identifying Risks in Knowledge-Based Companies Based on Information Technology

Asdollah. Honardoost[1], Amir. Mohammadzadeh[2*], Mohsen. Torabian[3]

[1] Ph.D of Student, Industrial Management, Qa.c., Islamic Azad University, Qazvin, Iran
[2] Professor, Department of Finacial Management, Qa.c., Islamic Azad University, Qazvin, Iran
[3] Associate Professor, Department of Mathematics, Qa.c., Islamic Azad University, Qazvin, Iran

*** Corresponding author email address**: amir126@iau.ac.ir

A r t i c l e I n f o

Article type:
Original Research

How to cite this article:
Honardoost, A., Mohammadzadeh, A., & Torabian, M. (2028). Designing a Meta-Synthesis Model for Identifying Risks in Knowledge-Based Companies Based on Information Technology. *Journal of Resource Management and Decision Engineering*, *7*(1), 1-19.
https://doi.org/10.61838/kman.jrmde.476

© 2028 the authors. Published by KMAN Publication Inc. (KMANPUB). This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

A B S T R A C T

This study aimed to design an integrated meta-synthesis model for identifying the major risks confronting knowledge-based companies from an information-technology perspective. This qualitative study employed a meta-synthesis design to integrate and reinterpret findings from previous research on information technology, knowledge management, organizational risk, cybersecurity, innovation, and knowledge-based enterprises. An initial search identified 436 potentially relevant documents from major national and international academic databases. After duplicate removal, title and abstract screening, full-text assessment, and methodological appraisal based on predefined inclusion and exclusion criteria, 42 studies were retained for final analysis. Data were extracted using a researcher-designed document-review form and analyzed through iterative coding, constant comparison, conceptual integration, and progressive abstraction. The analytical process involved identifying meaningful statements, generating primary codes, merging conceptually similar codes, forming subcategories, and synthesizing them into higher-order risk dimensions until theoretical saturation was achieved. The meta-synthesis yielded 118 primary codes organized into 28 subcategories and eight overarching dimensions: technological and digital infrastructure risk, cybersecurity and information security risk, strategic and innovation risk, organizational and operational risk, knowledge and human capital risk, financial and economic risk, legal and regulatory risk, and environmental, market, and ecosystem risk. The findings indicated that these dimensions were strongly interconnected rather than independent. Information technology emerged simultaneously as an independent source of risk, a transmission mechanism capable of amplifying risks across organizational domains, and a capability for mitigating uncertainty through improved governance, analytics, knowledge integration, and monitoring. Technological vulnerabilities were particularly linked to operational disruption, financial exposure, knowledge loss, legal liability, and weakened innovation capacity. The proposed model demonstrates that risk identification in knowledge-based companies requires a systemic and multidimensional approach in which technological, organizational, knowledge-related, financial, legal, and environmental risks are assessed jointly, enabling managers to identify interdependencies and design more coordinated risk-management strategies.

Keywords: *Knowledge-Based Companies; Information Technology; Meta-Synthesis; Risk Identification; Knowledge Management; Cybersecurity; Innovation Risk; Organizational Risk*

1. Introduction

Knowledge-based companies have become increasingly central to contemporary economic development because their competitive advantage depends less on tangible resources and more on the creation, acquisition, integration, protection, and commercialization of knowledge. These companies typically operate in environments characterized by technological intensity, rapid innovation, high uncertainty, reliance on specialized human capital, and continuous interaction with digital infrastructures. Their organizational value is therefore strongly associated with intellectual assets, technological capabilities, information systems, data resources, innovative competencies, and knowledge networks. In such firms, information technology is not merely a supporting function but constitutes a fundamental infrastructure for knowledge creation, knowledge sharing, organizational learning, product development, collaboration, decision-making, and market responsiveness. Recent developments in digital technologies have further expanded the strategic role of information technology by enabling organizations to exploit artificial intelligence, big data analytics, intelligent assistants, blockchain, cloud-based platforms, and advanced digital knowledge systems. At the same time, these technologies have created new organizational dependencies and sources of uncertainty that require more sophisticated approaches to risk identification and management. The growing use of large language models, for example, is transforming the ways organizations search for, create, transfer, revise, and even forget knowledge, thereby creating new opportunities for organizational learning while simultaneously introducing risks related to knowledge quality, reliability, dependence, and governance (Wiesenfeld & Kellogg, 2026). Similarly, the development of personal intelligent assistants indicates that knowledge-management activities are becoming increasingly automated and personalized, with potentially significant implications for decision-making, professional expertise, data governance, and organizational control (Vedapradha et al., 2024). These developments suggest that the risk profile of knowledge-based companies is becoming increasingly multidimensional and closely intertwined with technological change.

Information technology can improve organizational agility, efficiency, innovation capacity, and access to knowledge; however, it can also generate systemic vulnerabilities when technological capabilities are poorly governed, inadequately integrated, or insufficiently aligned with organizational objectives. Technology-based small and medium-sized enterprises increasingly rely on digital capabilities to balance exploratory and exploitative innovation, indicating that digital competence is closely related to organizational adaptability and innovation performance (Wang et al., 2024). Entrepreneurial culture and knowledge-management mechanisms likewise contribute to technological innovation by helping organizations recognize, interpret, and exploit emerging opportunities (Padhy, 2024). Yet the same dependence on digital capabilities creates exposure to technology failure, digital disruption, insufficient expertise, cybersecurity threats, inappropriate technology selection, and ineffective transformation initiatives. Studies of digital transformation demonstrate that knowledge management plays an important role in enabling organizations to convert technological investment into organizational value, particularly where transformation requires the integration of technological platforms with existing knowledge structures and managerial practices (Elgargouh et al., 2024). The implementation of information technology systems also depends on organizational acceptance, effective knowledge transfer, user readiness, governance structures, and the ability to institutionalize new practices, as illustrated by research on knowledge-management-system adoption and implementation (Istyanto & Nasrullah, 2022). Accordingly, risk in knowledge-based companies cannot be conceptualized solely as the probability of technical failure; rather, it involves the interaction of technological, organizational, strategic, human, knowledge-related, financial, and external factors.

Knowledge management is particularly important in understanding these risks because knowledge represents both a strategic resource and a source of organizational vulnerability. The competitive position of knowledge-intensive companies depends substantially on their ability to generate, retain, share, and apply knowledge more effectively than competitors. In small and medium-sized enterprises, knowledge-management capability may function as a source of competitive advantage by strengthening organizational learning, improving decision quality, supporting innovation, and reducing informational asymmetries (Bernal et al., 2023). At the same time, weaknesses in knowledge processes may expose organizations to knowledge loss, leakage, obsolescence, fragmentation, duplication, and inappropriate use. The relationship between knowledge risks and knowledge

vulnerabilities has been shown to extend across multiple stages of knowledge processes, demonstrating that vulnerabilities may emerge during knowledge creation, storage, transfer, retrieval, and application (Neştian et al., 2024). Internal and external knowledge-management risks may include employee turnover, ineffective knowledge transfer, inadequate documentation, organizational silos, insufficient protection of knowledge assets, and exposure to external environmental changes (Dodla & Jones, 2023). Such risks are especially serious in knowledge-based firms because a relatively small number of specialists may hold critical technical or commercial knowledge, making the organization vulnerable to employee departure, inadequate succession, and failure to codify tacit expertise. Consequently, identifying risk requires an understanding of how information technology interacts with the organizational processes through which knowledge is generated and protected.

The increasing digitalization of knowledge also creates significant security and governance risks. Knowledge assets are now frequently stored, transmitted, and processed through interconnected digital systems, making them susceptible to unauthorized access, data leakage, cyberattacks, manipulation, and loss. The relationship between knowledge-management systems and national digital security illustrates the broader strategic importance of securing information infrastructures and organizational knowledge resources (Adejumo, 2023). Integrated approaches to security risk analysis have therefore become necessary because technological risks often span multiple domains and cannot be effectively managed through isolated controls (Santos-Olmo et al., 2023). The integration of knowledge capabilities with information technology governance further demonstrates that sustainable IT governance depends not only on technical policies but also on organizational knowledge, employee competence, and institutional learning (Hammami et al., 2022). In knowledge-intensive settings, information security thus becomes inseparable from knowledge governance. A breach of information systems can simultaneously result in loss of intellectual property, disruption of business continuity, reputational damage, regulatory exposure, and weakening of organizational learning. The growth of data-intensive technologies makes these issues even more complex. Big-data quality, for instance, influences the reliability and usefulness of knowledge-management processes, and poor data quality may propagate inaccurate conclusions throughout organizational decision systems (Ravikumar et al., 2023). The emergence of artificial intelligence, big data, and generative technologies further challenges conventional assumptions about knowledge ownership, validity, traceability, and control (Sumbal et al., 2024).

Risk in knowledge-based companies also emerges from the processes of innovation and commercialization. Innovation is inherently uncertain because the technical success of an idea does not necessarily guarantee market success, financial sustainability, or strategic fit. Artificial intelligence and blockchain technologies can encourage greater organizational risk-taking by expanding perceived opportunities and enabling new business models, particularly among small and medium-sized enterprises operating in highly digitalized environments (Polas et al., 2022). However, the adoption of advanced technologies may simultaneously increase exposure to unfamiliar technological, financial, strategic, and regulatory risks. Research examining the “dark side” of knowledge management in innovation forecasting demonstrates that knowledge-intensive decision systems can themselves produce new forms of risk when organizational models depend heavily on data, algorithms, or imperfect representations of innovation dynamics (Figueiredo et al., 2023). Similarly, knowledge management can influence organizational risk through the way firms interpret and respond to technological uncertainty, especially when implementing environmentally oriented technologies or other novel production systems (Alam et al., 2023). Knowledge-based enterprises therefore require risk-identification mechanisms capable of capturing not only identifiable operational hazards but also emerging risks associated with innovation uncertainty, technology substitution, commercialization failure, and dependence on new digital capabilities.

The strategic significance of knowledge and technology extends beyond individual organizations to collaborative and network-based relationships. Knowledge-based companies frequently depend on universities, research institutions, technology suppliers, venture partners, digital platforms, consultants, and specialized service providers. Such networks provide access to complementary expertise and resources but also create relational and governance risks. In industry–university collaborative projects, risk management and knowledge-management capabilities interact in ways that can materially influence project performance, indicating that collaborative success depends on both knowledge exchange and effective management of uncertainty (Daradkeh, 2023). Similar dynamics can be

observed in supply chains, where relational risk may reduce effective knowledge sharing and organizational resilience, while blockchain and relational governance mechanisms can complement one another in managing uncertainty (Pu, 2024). Knowledge management is also a critical component of resilient supply-chain systems because organizations require dynamic capabilities to acquire, interpret, and mobilize knowledge when disruptions occur (Sumbal et al., 2022). These findings are especially relevant to knowledge-based companies, which are often embedded in complex innovation ecosystems and may depend heavily on external providers of technology, infrastructure, intellectual resources, and market access. Consequently, risk identification must account for dependencies extending beyond organizational boundaries.

The complexity of organizational risk has encouraged greater use of knowledge-based and intelligent technologies for risk identification. In construction and engineering environments, ontology-based approaches have been employed to infer quality risks by structuring and formalizing domain knowledge (Jiang & Cao, 2025). Knowledge management has also been integrated with Building Information Modeling to improve the identification of safety risks, demonstrating the value of combining codified organizational knowledge with digital information models (Chen et al., 2022). Similarly, knowledge bases integrated with digital modeling environments have been used to identify automated inspection risks and support design-for-safety processes (Liu et al., 2023). Broader reviews of intelligent risk management show increasing reliance on artificial intelligence, machine learning, knowledge representation, predictive analytics, and integrated digital systems to improve the identification and assessment of project risk (Chenya et al., 2022). Ontology-based knowledge-management tools likewise facilitate structured organizational knowledge sharing and can improve the accessibility and interpretability of complex knowledge resources (Osman et al., 2022). These developments demonstrate that information technology can serve both as a source of risk and as an instrument for identifying and managing risk. However, most existing applications have been developed within specific sectors or operational contexts and do not necessarily provide an integrated framework suitable for knowledge-based companies.

Another critical area concerns intellectual property and knowledge protection. Knowledge-based organizations often derive substantial portions of their value from patents, software, proprietary processes, trade secrets, technical designs, databases, and other intangible assets. As a result, intellectual property risk can directly threaten their competitive advantage and long-term survival. Knowledge management has been shown to contribute to the prevention of intellectual property risks by improving the organization, sharing, control, and protection of strategic knowledge resources (Jiang et al., 2022). Nevertheless, the expansion of digital collaboration and cloud-based environments has made organizational boundaries increasingly porous, raising the possibility of inadvertent disclosure, unauthorized reuse, ambiguous ownership, and cross-organizational leakage of knowledge. The risks are further intensified in collaborative innovation projects, where multiple actors may contribute to the development of knowledge assets, making ownership, confidentiality, and exploitation rights more difficult to define. Consequently, intellectual-property risk should be considered alongside cybersecurity, human-capital, governance, and collaboration risks rather than treated as an isolated legal issue.

Knowledge-based risk is also closely associated with organizational performance and institutional development. The role of knowledge management in organizational development has been demonstrated in different institutional contexts, including sports organizations, where the effective acquisition and application of organizational knowledge can support managerial development and performance improvement (Saati, 2023). Complex organizational systems similarly require formalized knowledge-management models to coordinate distributed information, decision-making structures, and control mechanisms (Rodríguez-Páez et al., 2024). These findings reinforce the idea that organizational risk is often rooted in deficiencies in knowledge flows and information coordination. In complex systems, localized failures in information sharing may produce broader organizational consequences because decision-makers depend on timely, accurate, and contextually relevant knowledge. For knowledge-based companies, this challenge is amplified by fast decision cycles, high innovation intensity, specialized expertise, and dependence on digital systems. Risk identification therefore requires an approach capable of recognizing interdependencies among organizational structures, technological platforms, knowledge processes, and decision mechanisms.

Despite the substantial literature on information technology risk, knowledge management, organizational resilience, innovation, cybersecurity, intellectual property,

and intelligent risk-identification systems, the evidence remains fragmented across disciplinary and sectoral boundaries. Existing studies have often focused on a specific type of risk, such as security, supply-chain disruption, innovation failure, intellectual property, or project risk, rather than developing an integrated framework for knowledge-based enterprises. Some studies emphasize technology governance and information systems, while others address knowledge vulnerabilities, organizational learning, innovation, or interorganizational relationships. Although each stream offers important insights, the absence of an integrated model makes it difficult to determine how different risk categories relate to one another and how information technology contributes simultaneously to the creation, transmission, amplification, and mitigation of risk. This fragmentation is particularly problematic because contemporary knowledge-based companies operate within interconnected digital environments in which technological, strategic, organizational, financial, human, legal, and ecosystem risks frequently reinforce one another. Effective risk identification therefore requires a synthesis capable of integrating heterogeneous findings and revealing recurring conceptual patterns across prior studies.

Meta-synthesis provides an appropriate methodological approach for addressing this problem because it enables the systematic integration and reinterpretation of findings from multiple studies into a higher-order conceptual structure. Rather than merely aggregating prior results, meta-synthesis allows researchers to identify conceptual similarities, differences, recurring themes, and underlying relationships across a body of literature. This is particularly valuable in emerging and multidisciplinary fields in which evidence is dispersed across different sectors and methodological traditions. By integrating findings on technological risk, knowledge-management vulnerabilities, cybersecurity, innovation uncertainty, governance, collaboration, intellectual property, and organizational resilience, a meta-synthesis can provide a more comprehensive understanding of the risk landscape confronting knowledge-based firms. It can also clarify the dual role of information technology as both an enabling capability and a source of organizational vulnerability. Such an integrated model may provide a stronger conceptual basis for subsequent risk assessment, prioritization, control design, and organizational decision-making in technology-intensive firms.

Accordingly, the aim of this study was to design a meta-synthesis model for identifying risks in knowledge-based companies based on information technology.

2. Methods and Materials

This study employed a qualitative research design based on the meta-synthesis approach to develop an integrated model for identifying risks in knowledge-based companies with an emphasis on information technology. Meta-synthesis was selected because it provides a systematic procedure for integrating, interpreting, and reconceptualizing findings from previous qualitative and conceptual studies and enables the researcher to move beyond simple aggregation of prior results toward the development of a coherent and higher-order conceptual framework. The research population consisted of scientific articles, conference papers, dissertations, research reports, and other credible academic documents related to organizational risk, information technology risk, knowledge-based firms, technology-oriented enterprises, innovation-driven companies, knowledge management, cybersecurity, digital infrastructure, strategic risk, operational risk, and related dimensions. An initial search identified 436 potentially relevant documents. After removing duplicate records and screening titles and abstracts, 127 documents remained for full-text assessment. The full texts were then evaluated according to predefined inclusion and exclusion criteria, including direct relevance to risk identification in knowledge-intensive or technology-based organizations, sufficient methodological transparency, availability of analyzable findings, publication in reputable scientific sources, and substantive connection with information technology or digitally enabled organizational processes. Studies with insufficient conceptual relevance, weak methodological quality, duplicated findings, unavailable full texts, or an exclusive focus on sectors unrelated to knowledge-based enterprises were excluded. Following the final appraisal process, 42 studies were retained as the final sample for meta-synthesis. These 42 studies constituted the analytical corpus of the research and provided the empirical and conceptual basis for extracting primary codes, organizing categories, identifying higher-order dimensions, and developing the final risk-identification model. The study followed an iterative review procedure in which study selection and conceptual saturation were considered simultaneously so that the final body of evidence was sufficiently diverse to represent technological, organizational, strategic, financial, human, legal, security-related, and environmental risk domains affecting knowledge-based companies.

Data were collected through a structured document-review protocol developed specifically for the meta-synthesis process. The primary data collection instrument was a researcher-designed extraction form used to record bibliographic characteristics, study objectives, research context, methodological approach, major findings, reported risk factors, conceptual categories, definitions, organizational consequences, and information-technology-related dimensions from each selected document. The search process was conducted using combinations of relevant keywords and equivalent expressions, including "knowledge-based companies," "knowledge-intensive firms," "technology-based firms," "information technology risk," "IT risk," "digital risk," "cybersecurity risk," "organizational risk," "strategic risk," "operational risk," "innovation risk," "knowledge management risk," "technology infrastructure," "digital transformation," and "risk identification." Boolean operators such as AND and OR were used to combine the search terms and increase retrieval accuracy. Searches were conducted in major scholarly databases and academic repositories, including Scopus, Web of Science, ScienceDirect, SpringerLink, Emerald, IEEE Xplore, ProQuest, Google Scholar, and relevant national academic databases. To ensure systematic selection of studies, the researchers applied predefined inclusion and exclusion criteria throughout the screening process. Methodological quality and relevance were assessed through a critical appraisal checklist covering clarity of research objectives, adequacy of the research design, appropriateness of the study context, transparency of data collection and analysis procedures, consistency between evidence and conclusions, and the explicit contribution of the study to the identification or explanation of risk. Each selected source was read repeatedly, and all statements, concepts, themes, and findings directly associated with potential risks in knowledge-based companies were entered into the extraction form. Particular attention was paid to risks arising from information systems, technological dependence, cybersecurity threats, data governance, digital infrastructure, technological obsolescence, innovation uncertainty, intellectual property, human resources, organizational knowledge, financial constraints, regulatory conditions, and external environmental changes. Data extraction continued until all relevant concepts had been captured and no substantively new risk categories emerged from the selected literature.

Data were analyzed using a systematic meta-synthesis procedure based on iterative coding, constant comparison, conceptual integration, and abstraction of findings across the 42 selected studies. In the first stage, the full texts of all included documents were examined line by line and meaningful statements related to risks, vulnerabilities, threats, sources of uncertainty, organizational weaknesses, and information-technology-related challenges were identified as initial analytical units. These statements were converted into primary codes while preserving their original conceptual meaning as closely as possible. Similar or conceptually overlapping codes were then compared across studies, and redundant or synonymous codes were merged. In the next stage, the refined codes were grouped into subcategories according to conceptual similarity and their relationship to common sources or mechanisms of risk. The subcategories were subsequently compared at a higher level of abstraction and organized into broader categories representing the principal domains of risk in knowledge-based companies. Through repeated movement between the original studies, primary codes, subcategories, and higher-order categories, the researchers developed an integrated interpretive structure that explained how different types of risk emerge, interact, and influence knowledge-based firms in environments characterized by technological dependence and rapid digital change. Particular attention was given to identifying relationships among information technology risks and other organizational domains so that technology-related factors were not treated as isolated technical variables but as interconnected drivers of strategic, operational, financial, legal, human-resource, knowledge, and reputational risks. To improve analytical credibility, coding decisions were repeatedly reviewed and compared, ambiguous codes were reconsidered in relation to their original textual context, and categories were revised until internal coherence and conceptual distinctiveness were achieved. The final model was generated through synthesis of the stabilized categories and their interrelationships, with information technology considered both as an independent source of risk and as a cross-cutting factor capable of intensifying or mitigating other organizational risks. The analytical process continued until theoretical saturation was reached and no new higher-order category emerged from further comparison of the included studies. The resulting conceptual model therefore represented an evidence-based synthesis of the dominant risk dimensions and their underlying components in knowledge-based companies operating in technology-intensive environments.

3. Findings and Results

The final analytical corpus consisted of 42 studies that met all methodological and conceptual inclusion criteria and were retained for the meta-synthesis. Examination of the publication characteristics showed that the literature was concentrated predominantly in the more recent period, reflecting the growing importance of information technology, digital transformation, cybersecurity, innovation, and technology-dependent organizational risks in knowledge-based enterprises. Of the 42 studies, 4 studies (9.52%) were published before 2015, 9 studies (21.43%) were published between 2015 and 2018, 13 studies (30.95%) were published between 2019 and 2021, and 16 studies (38.10%) were published from 2022 onward. In terms of publication type, 32 studies (76.19%) were peer-reviewed journal articles, 4 studies (9.52%) were conference papers, 4 studies (9.52%) were doctoral dissertations or postgraduate theses, and 2 studies (4.76%) were institutional or specialized research reports. With respect to methodological orientation, 18 studies (42.86%) employed qualitative methods, 12 studies (28.57%) used quantitative methods, 7 studies (16.67%) adopted mixed-method designs, and 5 studies (11.90%) were conceptual, systematic, or framework-development studies. Regarding geographical coverage, 17 studies (40.48%) were conducted in Asian countries, 10 studies (23.81%) in European countries, 6 studies (14.29%) in North America, 3 studies (7.14%) in the Middle East outside the separately classified national studies, and 6 studies (14.29%) had multinational or non-country-specific scopes. Analysis of the organizational settings further indicated that 15 studies (35.71%) focused directly on knowledge-based or knowledge-intensive firms, 10 studies (23.81%) examined technology-based enterprises and digital businesses, 7 studies (16.67%) investigated innovative small and medium-sized enterprises, 5 studies (11.90%) addressed research-and-development-intensive organizations, and 5 studies (11.90%) examined broader organizational contexts from which findings directly transferable to knowledge-based companies could be extracted. The screening and synthesis process initially generated 286 raw conceptual statements. After eliminating repetitions, merging semantically overlapping expressions, and refining conceptually similar findings, 118 primary codes remained. These codes were subsequently organized into 28 subcategories and finally synthesized into eight overarching risk dimensions. The eight dimensions were technological and digital infrastructure risk, cybersecurity and information security risk, strategic and innovation risk, organizational and operational risk, knowledge and human capital risk, financial and economic risk, legal and regulatory risk, and environmental, market, and ecosystem risk.

Table 1

Final Meta-Synthesis Structure of Risks in Knowledge-Based Companies

Category	Subcategories	Representative Risk Components	Number of Primary Codes
Technological and Digital Infrastructure Risk	Technology obsolescence; system reliability and continuity; technological dependency; integration and interoperability	Rapid obsolescence of software and hardware, inappropriate technology selection, infrastructure failure, system downtime, dependence on specific platforms, vendor lock-in, incompatibility among systems, weak scalability, inadequate backup infrastructure	18
Cybersecurity and Information Security Risk	Cyber threats; data security and privacy; access and identity management	Malware, ransomware, phishing, unauthorized access, data leakage, weak encryption, privacy violations, insecure remote access, inadequate authentication, insider cyber threats, insufficient monitoring	16
Strategic and Innovation Risk	Strategic alignment; innovation uncertainty; commercialization and business-model risk	Misalignment between IT and corporate strategy, unsuccessful technology investment, uncertain innovation outcomes, product-development failure, market timing errors, weak commercialization capability, inappropriate digital business models	17
Organizational and Operational Risk	Process vulnerability; governance and decision-making; project and service continuity	Weak internal controls, process disruption, unclear responsibilities, poor IT governance, delayed technology projects, project cost overruns, inadequate continuity planning, insufficient incident response, inefficient digital workflows	17
Knowledge and Human Capital Risk	Knowledge loss and transfer; skills and competence; human behavior and culture	Loss of key experts, inadequate knowledge sharing, tacit knowledge dependency, shortage of digital skills, resistance to technology, low cybersecurity awareness, employee turnover, weak learning culture	15
Financial and Economic Risk	Funding and investment; cost volatility; financial return uncertainty	Limited access to finance, high technology acquisition costs, unexpected maintenance costs, uncertain return on IT investment, cash-flow pressures, exchange-rate exposure, R&D financing constraints	12

Legal and Regulatory Risk	Compliance; intellectual property; contractual and digital legal risk	Data protection non-compliance, regulatory uncertainty, intellectual property infringement, software licensing disputes, contractual ambiguity, digital transaction risks, legal liability arising from technology failures	11
Environmental, Market, and Ecosystem Risk	Market dynamics; competitive and ecosystem dependence; external disruptions	Rapid customer preference changes, intense technological competition, supplier dependency, platform ecosystem instability, disruption in technology supply chains, macroeconomic shocks, geopolitical restrictions, external technological discontinuities	12
Total	28 subcategories	Integrated risk factors extracted through meta-synthesis	118

As shown in Table 1, the meta-synthesis resulted in a multidimensional structure comprising eight main dimensions, 28 subcategories, and 118 primary codes. Technological and digital infrastructure risk represented the largest individual dimension with 18 codes, followed by strategic and innovation risk and organizational and operational risk, each containing 17 codes. Cybersecurity and information security risk included 16 primary codes, while knowledge and human capital risk comprised 15 codes. Financial and economic risk and environmental, market, and ecosystem risk each contained 12 codes, whereas legal and regulatory risk comprised 11 codes. The distribution of the extracted codes indicates that risk in knowledge-based companies cannot be reduced to technical malfunction or cybersecurity incidents alone. Instead, information technology operates as an interconnected organizational infrastructure whose risks extend into strategic decision-making, innovation, knowledge retention, financial sustainability, regulatory compliance, operational continuity, and relationships with external technological ecosystems. The findings further demonstrate that the technological dimension occupies a central position in the model because weaknesses in infrastructure, system architecture, compatibility, technological updating, or vendor dependence can generate secondary consequences in nearly all other dimensions. Similarly, cybersecurity risks were identified not merely as technical threats but as sources of financial loss, reputational damage, legal liability, operational interruption, and potential loss of strategic knowledge. The eight-dimensional structure therefore suggests that effective risk identification in knowledge-based enterprises requires an integrated rather than fragmented perspective in which information technology is simultaneously understood as a source of risk, a transmission mechanism through which other risks intensify, and an organizational capability that may be used to mitigate them.

Table 2

Technological, Infrastructure, and Cybersecurity Risk Components

Main Category	Subcategory	Extracted Risk Components	Interpretation in Knowledge-Based Companies
Technological and Digital Infrastructure Risk	Technology obsolescence	Rapid software obsolescence; hardware aging; unsupported technologies; delayed upgrading; inappropriate technology adoption	Knowledge-based firms may lose technological competitiveness and encounter rising maintenance, compatibility, and security problems when digital assets become obsolete.
Technological and Digital Infrastructure Risk	System reliability and continuity	System downtime; server failure; network interruption; insufficient backup; disaster recovery weakness; capacity limitations	Because core knowledge processes are digitally mediated, infrastructure interruptions may directly halt research, development, collaboration, service delivery, and decision-making.
Technological and Digital Infrastructure Risk	Technological dependency	Vendor lock-in; dependence on proprietary systems; dependence on cloud providers; shortage of alternative providers	Excessive dependency limits organizational flexibility and increases exposure to price changes, service discontinuation, vendor failure, or restrictive contractual conditions.
Technological and Digital Infrastructure Risk	Integration and interoperability	Incompatible applications; fragmented databases; legacy-system integration problems; poor API compatibility; data inconsistency	Lack of integration reduces information quality, creates duplicate processes, delays decision-making, and weakens the organization's ability to exploit knowledge across functional boundaries.
Cybersecurity and Information Security Risk	External cyber threats	Malware; ransomware; phishing; denial-of-service attacks; exploitation of vulnerabilities	Digitally intensive firms are attractive targets because they hold valuable intellectual assets, customer data, proprietary algorithms, and commercially sensitive knowledge.
Cybersecurity and Information Security Risk	Data security and privacy	Data leakage; loss of confidential information; inadequate encryption; privacy breaches; insecure data storage	Compromise of sensitive information may lead to legal sanctions, loss of trust, competitive disadvantage, and erosion of intellectual capital.
Cybersecurity and Information Security Risk	Identity and access management	Weak authentication; excessive access privileges; compromised passwords; unauthorized access; insecure remote access	Inadequate access governance increases the probability of both external intrusion and internal misuse of critical systems and organizational knowledge.

Cybersecurity and Information Security Risk	Internal security vulnerabilities	Insider threats; employee negligence; poor security awareness; unauthorized copying; insecure personal devices	Human behavior remains a major security vulnerability, particularly in organizations characterized by intensive collaboration and flexible access to information.
Cybersecurity and Information Security Risk	Monitoring and response	Delayed threat detection; inadequate logging; absence of security monitoring; weak incident response	Failure to detect and contain incidents rapidly may transform limited technical events into major organizational crises.

Table 2 demonstrates that technological and cybersecurity risks form the most immediate information-technology-related layer of the proposed model. The technological dimension encompasses not only failures in hardware or software but also structural weaknesses associated with technology life cycles, interoperability, capacity, continuity, and dependence on external technology providers. Technology obsolescence emerged as a particularly important concern because knowledge-based firms typically compete through speed of innovation and the exploitation of advanced technological capabilities. When organizations rely on outdated applications, unsupported platforms, or aging infrastructure, they face simultaneously increasing maintenance costs, compatibility problems, cybersecurity vulnerabilities, and declining technological competitiveness. System reliability and continuity were also repeatedly emphasized because interruption of networks, servers, cloud services, databases, or digital collaboration platforms can immediately affect core knowledge activities. Integration and interoperability problems represented another significant source of risk, especially where organizations used multiple disconnected systems that generated inconsistent data or fragmented organizational knowledge. The cybersecurity dimension showed similarly broad consequences. External cyber threats, including ransomware, phishing, malware, service-disruption attacks, and vulnerability exploitation, were important because knowledge-based firms possess high-value intangible assets such as research data, intellectual property, product designs, proprietary source code, algorithms, and customer information. At the same time, the synthesis highlighted internal vulnerabilities, including employee negligence, inappropriate privilege allocation, insecure remote working practices, and insufficient security awareness. These findings suggest that cybersecurity should not be treated exclusively as the responsibility of technical personnel. Instead, it must be embedded in governance arrangements, employee behavior, data management, operational continuity, legal compliance, and strategic risk management. The relationship among infrastructure instability, security weaknesses, and data governance further indicates that technological risk is cumulative: weaknesses in one area frequently magnify vulnerabilities in another. For example, delayed software upgrading may increase cyber exposure, whereas fragmented systems may make access control and incident monitoring more difficult. Accordingly, the technological and cybersecurity layer constitutes the operational foundation of the meta-synthesis model.

Table 3

Strategic, Innovation, Organizational, and Operational Risk Components

Main Category	Subcategory	Extracted Risk Components	Interpretation in Knowledge-Based Companies
Strategic and Innovation Risk	IT-strategy alignment	Misalignment between business strategy and IT strategy; inappropriate technology priorities; weak executive support; fragmented digital investments	Technology investments that are disconnected from strategic objectives may consume resources without improving organizational competitiveness or innovation capability.
Strategic and Innovation Risk	Innovation uncertainty	Failure of R&D projects; technological uncertainty; uncertain feasibility; unsuccessful experimentation; inability to scale innovations	Innovation inherently involves uncertain outcomes, and technology-intensive firms face substantial risks in converting technical ideas into sustainable organizational value.
Strategic and Innovation Risk	Commercialization	Weak market adoption; ineffective commercialization; poor market timing; inability to transform knowledge into marketable products	Scientific or technological competence does not necessarily translate into commercial success, making commercialization a major strategic risk.
Strategic and Innovation Risk	Business-model risk	Unsustainable digital business models; inappropriate revenue models; platform dependency; inability to adapt value propositions	Rapid technological change may render existing revenue and value-creation mechanisms obsolete.
Strategic and Innovation Risk	Technology investment decisions	Overinvestment; underinvestment; incorrect technology selection; uncertain IT returns	Inaccurate investment decisions can lock firms into costly technologies or leave them technologically underdeveloped.
Organizational and Operational Risk	Governance and accountability	Unclear IT responsibilities; weak governance structures; inadequate risk ownership; poor management oversight	Ambiguous authority and accountability reduce the organization's capacity to identify and respond to interconnected technology risks.

Organizational and Operational Risk	Process vulnerability	Inefficient digital processes; excessive process dependence on IT; workflow disruption; poor process standardization	Digitization can improve efficiency but may also amplify disruption if critical processes become dependent on vulnerable systems.
Organizational and Operational Risk	Project management	Delayed projects; budget overruns; scope creep; weak requirements definition; implementation failure	Technology and innovation projects frequently involve uncertain requirements and complex coordination, increasing implementation risk.
Organizational and Operational Risk	Business continuity	Inadequate continuity plans; weak disaster recovery; lack of alternative processes; inadequate crisis preparation	Failure to plan for technological interruptions can produce prolonged organizational inactivity and loss of critical knowledge.
Organizational and Operational Risk	Decision quality	Inaccurate information; weak analytics; poor data quality; algorithmic bias; excessive reliance on automated decisions	Strategic and operational decisions may deteriorate when data or automated decision-support systems are inaccurate, incomplete, or insufficiently governed.

As presented in Table 3, strategic, innovation, organizational, and operational risks constitute the second major layer of the model and show how information technology becomes embedded in managerial and competitive processes. The synthesis indicated that strategic risk frequently originated from weak alignment between technology investment and organizational objectives. Knowledge-based enterprises often invest in advanced technologies because of competitive pressure or expectations regarding digital transformation, but such investments become risky when they are not based on a clear strategic rationale, appropriate organizational capabilities, or realistic assessment of expected value. Innovation uncertainty was another recurring theme. Knowledge-based companies depend heavily on research, experimentation, product development, and continuous technological renewal, yet these activities are characterized by uncertain technical feasibility, uncertain customer acceptance, and uncertain economic returns. The findings therefore distinguish between invention or technical development and successful commercialization. A technically successful innovation may still fail because of weak market timing, inadequate customer demand, ineffective commercialization capability, inappropriate pricing, or an unsustainable business model. Organizational and operational risks were similarly interconnected with information technology. Weak governance structures, unclear allocation of responsibility, and inadequate managerial oversight reduced the organization's capacity to identify emerging risks and coordinate responses across departments. Technology project failure was associated with incomplete requirements, uncontrolled changes in project scope, unrealistic schedules, inadequate communication between technical and managerial teams, and poor resource allocation. Furthermore, increasing digital dependence creates operational concentration risk because failure of a small number of systems may interrupt a large proportion of organizational processes. Decision-quality risk was particularly important because knowledge-based organizations increasingly depend on digital analytics, data-driven management, artificial intelligence, and automated decision-support systems. Poor data quality, algorithmic bias, incomplete datasets, or excessive managerial dependence on automated outputs may therefore affect not only operational decisions but also strategic resource allocation and long-term organizational positioning. Collectively, these findings demonstrate that information technology risk should be evaluated at the level of strategic management and organizational design, rather than being confined to infrastructure or technical functions.

Table 4

Knowledge, Human Capital, Financial, and Economic Risk Components

Main Category	Subcategory	Extracted Risk Components	Interpretation in Knowledge-Based Companies
Knowledge and Human Capital Risk	Knowledge retention	Loss of key experts; employee turnover; retirement of specialists; dependence on individuals; loss of tacit knowledge	Knowledge loss may directly reduce innovation capability because critical expertise often resides in specialized employees rather than formal documentation.
Knowledge and Human Capital Risk	Knowledge transfer and sharing	Knowledge hoarding; weak documentation; ineffective knowledge repositories; poor cross-unit communication; limited organizational learning	Failure to transfer knowledge increases duplication, slows innovation, and creates dependence on isolated individuals or teams.
Knowledge and Human Capital Risk	Digital competence	Shortage of IT skills; insufficient analytical capability; weak cybersecurity competence; lack of emerging-technology expertise	Skill gaps may prevent organizations from exploiting new technologies safely and efficiently.
Knowledge and Human Capital Risk	Resistance and organizational culture	Resistance to change; technology avoidance; weak learning culture; low innovation acceptance; lack of security culture	Organizational culture can delay digital transformation and undermine implementation of risk-control measures.

Knowledge and Human Capital Risk	Human error	Incorrect data entry; accidental disclosure; configuration errors; inappropriate system use; failure to follow procedures	Human errors can generate technical, security, operational, and legal consequences simultaneously.
Financial and Economic Risk	Financing constraints	Limited access to external finance; shortage of venture capital; insufficient R&D funding; credit constraints	Knowledge-based firms often require substantial investment before innovations generate stable revenues.
Financial and Economic Risk	Technology costs	High acquisition costs; maintenance expenses; licensing costs; cybersecurity expenditure; cloud and infrastructure costs	Technology expenditure may become financially burdensome, particularly for smaller knowledge-based firms.
Financial and Economic Risk	Return on investment	Uncertain IT returns; delayed payback; unsuccessful digital investments; difficulty measuring intangible returns	The value of information technology and knowledge assets is often difficult to quantify, complicating investment decisions.
Financial and Economic Risk	Economic volatility	Inflation; exchange-rate fluctuations; interest-rate changes; recession; declining investment capacity	Macroeconomic instability can increase the cost of imported technology and reduce the firm's capacity to sustain innovation expenditures.
Financial and Economic Risk	Revenue and cash-flow instability	Uncertain sales; delayed commercialization revenue; high burn rate; dependence on limited clients	Financial instability may force organizations to reduce R&D, postpone technology upgrades, or abandon promising innovations.

Table 4 indicates that knowledge and human capital risks are fundamental to the risk architecture of knowledge-based companies because their competitive advantage is derived primarily from specialized expertise, intellectual capabilities, learning processes, and the capacity to transform information into innovation. Loss of key employees emerged as a major risk because essential knowledge may remain tacit, individualized, and insufficiently documented. When a specialist leaves the organization, the resulting loss may not be limited to technical expertise but may also include customer relationships, project history, problem-solving routines, and informal knowledge regarding organizational systems. Weak knowledge-sharing mechanisms further intensify this risk by concentrating expertise within isolated individuals or teams. Digital competence was another central factor because knowledge-based organizations increasingly require combined expertise in information technology, cybersecurity, data analytics, artificial intelligence, digital collaboration, and innovation management. A shortage of these competencies may reduce both technological performance and the effectiveness of risk controls. Cultural resistance to technological change was likewise identified as a significant barrier because employees may resist new systems, fail to adopt secure practices, or continue using informal workarounds that reduce the effectiveness of digital transformation initiatives. The financial dimension was closely linked to these human and technological challenges. Knowledge-based firms frequently operate under conditions of high initial investment, uncertain revenue, substantial R&D expenditure, and delayed commercialization. Consequently, limitations in financing can interrupt technological development before innovations reach market maturity. Technology acquisition, software licensing, cybersecurity, infrastructure maintenance, cloud services, specialist employment, and compliance requirements may create substantial recurring costs. Moreover, return on investment is difficult to estimate because many benefits of digital systems and knowledge assets are intangible, delayed, or distributed across multiple organizational processes. The findings therefore indicate a reciprocal relationship between financial capability and technological resilience. Firms with limited financial resources may postpone system upgrading, cybersecurity investment, employee development, and business continuity measures, thereby increasing technological and operational vulnerability. Conversely, technological failure or unsuccessful innovation may intensify financial pressure by generating direct losses and reducing future revenue. This reciprocal relationship supports the integrated nature of the proposed risk model.

Table 5

Legal, Regulatory, Environmental, Market, and Ecosystem Risk Components

Main Category	Subcategory	Extracted Risk Components	Interpretation in Knowledge-Based Companies
Legal and Regulatory Risk	Data and privacy compliance	Non-compliance with data protection requirements; inappropriate personal-data processing; inadequate consent management; cross-border data issues	Knowledge-based firms may face penalties, litigation, restrictions, and reputational loss if digital information is processed unlawfully.

Legal and Regulatory Risk	Intellectual property	Patent infringement; copyright violations; trade-secret leakage; unclear ownership of software or research outputs	Intellectual property is often a principal asset of knowledge-based firms, making ownership and protection central legal risks.
Legal and Regulatory Risk	Technology contracts	Ambiguous service agreements; weak vendor contracts; software licensing disputes; inadequate service-level provisions	Poor contractual arrangements can increase dependency and reduce legal protection when technology providers fail to perform.
Legal and Regulatory Risk	Regulatory uncertainty	Rapid regulatory changes; unclear digital regulations; emerging AI regulations; sector-specific compliance changes	Rapid technological development often outpaces legislation, creating uncertainty regarding permissible practices and future compliance costs.
Legal and Regulatory Risk	Technology-related liability	Liability for system failures; cybersecurity incidents; defective digital products; automated decision errors	Technology failures may create civil, contractual, administrative, or professional liability.
Environmental, Market, and Ecosystem Risk	Market volatility	Rapid shifts in customer preferences; demand uncertainty; shortening product life cycles; technology substitution	Fast-moving markets can rapidly reduce the commercial value of technological innovations.
Environmental, Market, and Ecosystem Risk	Competitive intensity	Aggressive technology competition; entry of global competitors; imitation; rapid innovation by rivals	Knowledge-based companies may lose competitive position when competitors innovate more rapidly or possess superior resources.
Environmental, Market, and Ecosystem Risk	Supplier and partner dependency	Dependence on technology suppliers; cloud providers; research partners; outsourcing firms; platform operators	External dependencies transmit risk from ecosystem partners into the focal company.
Environmental, Market, and Ecosystem Risk	Technology supply chain	Hardware shortages; component unavailability; service disruptions; import restrictions; infrastructure dependency	Disruption in technology supply chains may delay development, maintenance, and commercialization.
Environmental, Market, and Ecosystem Risk	Macroeconomic and geopolitical environment	Sanctions; trade restrictions; political instability; global economic shocks; restrictions on technology transfer	External political and economic conditions can limit access to technologies, markets, investment, and specialized knowledge.
Environmental, Market, and Ecosystem Risk	Technological discontinuity	Emergence of disruptive technologies; replacement of existing platforms; ecosystem restructuring	Radical technological change may make existing competencies, products, and investments obsolete.

Table 5 presents the external and institutional layer of the risk model and demonstrates that knowledge-based companies operate within legal, regulatory, competitive, and technological ecosystems that can generate risks beyond the direct control of the organization. Legal and regulatory risks were particularly associated with the increasing digitalization of business activities. Data protection and privacy requirements create obligations regarding collection, processing, storage, transfer, and protection of information, and non-compliance may result in penalties, litigation, reputational damage, and restrictions on business activities. Intellectual property risk was especially prominent because patents, software, proprietary algorithms, research outputs, trade secrets, databases, and specialized technical knowledge represent a substantial proportion of the value of knowledge-based enterprises. Failure to establish ownership, protect intellectual property, or prevent unauthorized disclosure can directly undermine competitive advantage. Contractual risks also emerged in relation to outsourcing, cloud computing, software licensing, platform participation, and technology procurement. Poorly structured contracts may increase vendor dependence, weaken service guarantees, create ambiguity regarding data ownership, and limit the organization's ability to obtain compensation after disruption or security incidents. Regulatory uncertainty adds another layer of risk because digital technologies, artificial intelligence, automated decision systems, cybersecurity, and cross-border data flows are developing more rapidly than many regulatory frameworks. The external environment similarly exposes knowledge-based firms to rapid changes in customer demand, competitive intensity, supply-chain conditions, and technological standards. Because many such companies depend on specialized vendors, cloud platforms, research partners, digital marketplaces, component manufacturers, or external infrastructure providers, disruption affecting one ecosystem participant may propagate throughout the firm's operations. Technological discontinuity represents a particularly important strategic threat because the emergence of a disruptive technology can reduce the value of existing capabilities and investments within a short period. Macroeconomic and geopolitical conditions may further constrain access to capital, imported technologies, global markets, or international knowledge networks. These findings show that external risk is not independent of internal capability: firms with diversified suppliers, strong legal governance, flexible technological architectures, effective environmental scanning, and adaptive innovation capabilities are better positioned to absorb external shocks.

Overall synthesis of the findings produced an integrated meta-synthesis model in which the eight identified risk dimensions are not interpreted as isolated categories but as

mutually reinforcing components of a dynamic risk system. The highest concentration of codes occurred in technological and digital infrastructure risk, strategic and innovation risk, organizational and operational risk, and cybersecurity and information security risk, demonstrating the centrality of technology to the overall risk architecture of knowledge-based enterprises. Nevertheless, the findings also showed that purely technical interpretations are insufficient. Technological vulnerabilities may generate operational interruption, financial loss, legal liability, knowledge leakage, and reputational damage; strategic misalignment may lead to ineffective technological investment and reduced competitiveness; human capital deficiencies may undermine cybersecurity and innovation; financing constraints may delay critical system upgrades; and regulatory or ecosystem changes may make existing technologies commercially or legally unsustainable. The synthesis therefore indicates that information technology performs three simultaneous roles within the model. First, it constitutes an independent risk domain through infrastructure failure, technological obsolescence, system incompatibility, and technological dependency. Second, it acts as a transmission channel through which risks originating in one organizational area can influence other areas, as illustrated by cyber incidents that become financial, legal, operational, and reputational crises. Third, information technology can function as a risk-management capability when supported by appropriate governance, reliable infrastructure, analytical systems, cybersecurity controls, organizational learning, and adaptive strategic planning. Accordingly, the final model conceptualizes risk identification in knowledge-based companies as a multidimensional and interconnected process in which technological, security, strategic, operational, knowledge-related, human, financial, legal, market, and environmental factors must be evaluated jointly. This integrated structure provides the conceptual basis for prioritizing risks and designing coordinated risk-management mechanisms in knowledge-based companies operating under conditions of rapid technological change, high innovation intensity, dependence on intangible assets, and considerable environmental uncertainty.

4. Discussion and Conclusion

The present meta-synthesis was conducted to develop an integrated model for identifying risks in knowledge-based companies from an information-technology perspective. The findings demonstrated that the risk architecture of knowledge-based companies is multidimensional and consists of eight interrelated dimensions: technological and digital infrastructure risk, cybersecurity and information security risk, strategic and innovation risk, organizational and operational risk, knowledge and human capital risk, financial and economic risk, legal and regulatory risk, and environmental, market, and ecosystem risk. These dimensions were derived from 28 subcategories and 118 primary codes, indicating that the risks confronting knowledge-based companies cannot be adequately understood through a narrow technological or financial perspective. The findings instead suggest that information technology has a cross-cutting role in contemporary knowledge-intensive organizations: it is simultaneously a strategic resource, an infrastructure for knowledge processes, a potential source of vulnerability, and a mechanism through which risks originating in one organizational area may propagate to other areas. This interpretation is consistent with the broader literature showing that digital technologies increasingly reshape organizational knowledge creation, transfer, utilization, and learning while also changing the nature of organizational dependence and uncertainty (Wiesenfeld & Kellogg, 2026). Similarly, research on technology-based SMEs has demonstrated that digital capabilities are closely associated with innovation and organizational adaptability, reinforcing the idea that technological capability and organizational risk are structurally interconnected rather than independent phenomena (Wang et al., 2024).

The first major finding concerned technological and digital infrastructure risk, which contained the largest number of primary codes in the proposed model. The results indicated that technology obsolescence, system reliability, continuity, technological dependence, and interoperability constitute fundamental sources of vulnerability for knowledge-based companies. This finding is understandable because the basic activities of these companies, including research and development, knowledge sharing, collaboration, customer interaction, data analysis, and innovation management, increasingly depend on stable digital infrastructures. When key systems become obsolete, fragmented, incompatible, or dependent on a limited number of vendors, technological weaknesses can immediately influence organizational performance. The result is consistent with studies emphasizing that sustainable technology implementation requires organizational knowledge, governance capabilities, and effective

integration of technological resources (Hammami et al., 2022). It is also aligned with research on digital transformation indicating that knowledge management plays an important role in converting technological infrastructures into meaningful organizational capabilities (Elgargouh et al., 2024). The importance of interoperability and structured technological knowledge is further supported by studies of ontology-based knowledge-management tools, which show that organizational knowledge becomes more usable when information is formally structured, accessible, and integrated across systems (Osman et al., 2022). Accordingly, infrastructure risk in knowledge-based companies should be interpreted not merely as the probability of hardware or software failure, but as the possibility that technological architecture will become incapable of supporting the organization's knowledge-intensive and innovation-oriented processes.

Cybersecurity and information security emerged as a second major dimension and were closely related to technological infrastructure, data governance, and human behavior. The findings showed that malware, ransomware, unauthorized access, data leakage, inadequate identity management, insider threats, and insufficient monitoring can threaten both technological assets and strategic knowledge. This result is consistent with the growing recognition that digital security and knowledge management are inseparable in knowledge-intensive environments. Adejumo emphasized the relationship between knowledge-management systems and digital security, demonstrating that the integrity of knowledge resources depends substantially on the security of the technological environments through which those resources are stored and exchanged (Adejumo, 2023). Similarly, integrated security-risk frameworks emphasize that information-security risks should be analyzed systematically rather than through disconnected technical controls (Santos-Olmo et al., 2023). The current findings extend these arguments by indicating that cyber incidents in knowledge-based companies may simultaneously create operational, financial, legal, intellectual-property, and reputational consequences. The growing organizational reliance on data analytics also increases the importance of information quality and integrity. Research has shown that the quality of big-data analytics affects the value generated through knowledge-management systems (Ravikumar et al., 2023); therefore, threats to data confidentiality, availability, or accuracy may weaken both decision-making and organizational learning. The emergence of generative artificial intelligence further expands these concerns because organizations must increasingly govern the reliability, ownership, security, and provenance of machine-generated or machine-mediated knowledge (Sumbal et al., 2024).

Strategic and innovation risk constituted another prominent dimension of the model. The findings demonstrated that misalignment between IT and organizational strategy, uncertainty in innovation outcomes, weak commercialization capability, inappropriate business models, and poor technology-investment decisions can threaten the sustainability of knowledge-based companies. This result reflects the specific nature of knowledge-based firms, whose competitive position frequently depends on transforming specialized knowledge into commercially viable products or services. Innovation therefore involves not only technological uncertainty but also uncertainty regarding demand, timing, scalability, resource availability, and strategic fit. The finding is supported by research showing that entrepreneurial culture and knowledge-management processes can shape technological innovation by influencing how organizations recognize and exploit opportunities (Padhy, 2024). Studies of artificial intelligence and blockchain adoption have similarly suggested that new digital technologies can alter organizational risk-taking behavior and encourage firms to pursue new opportunities under conditions of uncertainty (Polas et al., 2022). However, technological sophistication does not automatically guarantee successful innovation. The risks associated with knowledge-intensive innovation have also been highlighted through research on the darker dimensions of knowledge management and predictive systems, showing that inappropriate use of organizational knowledge or analytical models may introduce additional uncertainty into innovation decisions (Figueiredo et al., 2023). The present findings therefore indicate that strategic risk management should incorporate technology selection, innovation governance, commercialization capability, and organizational learning within one coherent decision framework.

The results also identified organizational and operational risk as a major component of the model. Weak governance, unclear accountability, inefficient processes, project failure, inadequate continuity planning, and poor decision quality were among the most important subcategories. This finding indicates that information technology risks become organizational risks when technological systems are embedded in poorly governed structures. The relevance of governance is evident in prior research showing that knowledge capabilities are necessary to sustain effective

information-technology governance (Hammami et al., 2022). Moreover, the adoption of organizational knowledge-management systems depends substantially on implementation quality, user acceptance, institutional support, and alignment between technological design and organizational requirements (Istyanto & Nasrullah, 2022). The findings regarding operational and project risks are also consistent with studies of intelligent risk management, where digital systems, machine learning, and structured knowledge have been increasingly applied to improve risk identification and project control (Chenya et al., 2022). Likewise, the integration of knowledge management with Building Information Modeling has been used to identify safety risks more effectively, demonstrating that combining organizational knowledge with digital information structures can strengthen preventive decision-making (Chen et al., 2022). The current model extends these insights beyond project-based environments by suggesting that knowledge-based companies require integrated governance mechanisms through which technological, operational, and strategic risks are jointly monitored.

Knowledge and human capital risk constituted another central dimension. The findings demonstrated that knowledge loss, insufficient knowledge transfer, shortage of digital competencies, resistance to technological change, weak learning cultures, and human error can significantly increase organizational vulnerability. This result is particularly important because knowledge-based companies derive much of their competitive value from specialized expertise that may be difficult to replace or codify. The relationship between knowledge processes and organizational vulnerabilities has been emphasized in previous research showing that knowledge risks may arise throughout the processes of knowledge acquisition, storage, sharing, and utilization (Neştian et al., 2024). Similarly, internal and external knowledge-management risks include loss of expertise, weak transfer mechanisms, inadequate documentation, and failures in knowledge retention (Dodla & Jones, 2023). These findings support the present conclusion that human capital should not be treated merely as a staffing resource but as a critical risk-bearing component of the organization. Knowledge management has also been described as an important source of competitive advantage for SMEs because it supports organizational learning, innovation, and adaptability (Bernal et al., 2023). Consequently, employee turnover, inadequate learning mechanisms, or insufficient digital skills may directly weaken the strategic capacity of knowledge-based companies. The increasing use of intelligent assistants and automated knowledge systems further suggests that human competence must evolve alongside technology so that employees can critically interpret, supervise, and integrate machine-supported knowledge rather than merely consume it (Vedapradha et al., 2024).

Financial and economic risk was also identified as a separate but strongly interconnected dimension. The findings showed that restricted access to finance, high technology costs, uncertainty regarding return on investment, economic volatility, and unstable cash flows can constrain technological development and risk-management capacity. Although knowledge-based companies may possess substantial intellectual capital, many face significant financial pressure because innovation requires investment before commercial returns become predictable. This finding is consistent with the broader literature emphasizing that technological and innovation activities involve uncertainty and may alter organizational willingness to undertake risk (Polas et al., 2022). Financial constraints may also affect the firm's ability to invest in cybersecurity, technological upgrading, specialist personnel, data infrastructure, and business continuity mechanisms. Thus, financial weakness can indirectly amplify technological and operational risks. Conversely, technological failures or unsuccessful commercialization can intensify financial instability. The relationship between knowledge management and performance in collaborative innovation projects further illustrates the importance of coordinating knowledge and risk-management capabilities when resources are limited and project outcomes uncertain (Daradkeh, 2023). Therefore, the proposed model conceptualizes financial risk as both an independent category and an amplifier of other organizational vulnerabilities.

Legal and regulatory risks formed another important dimension, particularly in relation to data protection, intellectual property, technology contracts, regulatory uncertainty, and technology-related liability. The finding regarding intellectual-property risk is strongly supported by previous research demonstrating that knowledge-management processes can contribute to the prevention of intellectual-property risks in strategically important and technology-intensive industries (Jiang et al., 2022). This issue is particularly important for knowledge-based companies because their economic value may depend heavily on patents, software, proprietary databases, algorithms, technical designs, and trade secrets. Digitalization increases the ease with which such assets can

be transferred, duplicated, or disclosed, thereby intensifying legal and competitive vulnerability. The increasing use of artificial intelligence and advanced data technologies also introduces uncertainty regarding ownership, accountability, privacy, and acceptable use. Research on generative organizational learning illustrates that emerging technologies alter traditional processes of knowledge creation and forgetting and may therefore challenge established governance arrangements (Wiesenfeld & Kellogg, 2026). Accordingly, the present findings suggest that legal and regulatory risk management should be integrated into technological and knowledge governance from the earliest stages of innovation rather than addressed only after commercialization.

The final principal dimension consisted of environmental, market, and ecosystem risks, including rapid changes in customer preferences, competitive intensity, supplier dependency, technological supply-chain disruption, macroeconomic and geopolitical uncertainty, and technological discontinuity. This finding reflects the increasingly networked structure of knowledge-based competition. Firms seldom operate independently; they rely on cloud providers, research partners, technology vendors, universities, digital platforms, component suppliers, and external knowledge networks. The importance of such relationships is supported by evidence demonstrating that relational risk and knowledge sharing influence supply-chain resilience and that technological and relational governance can operate complementarily (Pu, 2024). Similarly, knowledge management and dynamic capabilities play important roles in strengthening supply-chain resilience under disruptive conditions (Sumbal et al., 2022). The current findings indicate that external ecosystem risks can be transmitted into the focal company through technological and knowledge dependencies. A disruption affecting a major digital platform, supplier, or research partner may therefore produce consequences extending beyond procurement to knowledge access, innovation, customer relationships, and operational continuity. This reinforces the need for knowledge-based companies to monitor not only internal risk indicators but also the resilience of their wider technological and collaborative ecosystems.

Taken together, the findings demonstrate that information technology occupies a dual and, in some cases, paradoxical position within knowledge-based companies. It generates substantial organizational value by facilitating knowledge creation, analytical decision-making, digital collaboration, innovation, and organizational learning, yet it simultaneously creates new forms of dependency and vulnerability. The use of ontology-based reasoning for engineering quality risk management illustrates how digital knowledge structures can improve the systematic identification of risk (Jiang & Cao, 2025), while the integration of knowledge bases and digital models has also been shown to support automated safety-risk identification (Liu et al., 2023). Complex organizational systems similarly benefit from structured knowledge-management models that integrate information flows and decision structures (Rodríguez-Páez et al., 2024). These studies reinforce the central proposition of the present model: information technology should not be treated only as a risk object but also as a risk-management capability. When supported by appropriate governance, high-quality data, organizational learning, cybersecurity, and human competence, digital technologies can increase visibility into emerging threats and improve organizational response. When such supporting conditions are absent, however, the same technologies may intensify uncertainty and interdependence.

The integrated nature of the proposed model is therefore one of the most important contributions of this study. Previous studies have often examined individual domains, including intellectual-property risk, cybersecurity, project risk, supply-chain resilience, or knowledge vulnerabilities, whereas the present meta-synthesis demonstrates that these domains are structurally interconnected. Knowledge management may contribute to safer technological implementation (Alam et al., 2023), strengthen organizational development (Saati, 2023), facilitate collaborative performance (Daradkeh, 2023), and contribute to the resilience of external networks (Sumbal et al., 2022). At the same time, weak knowledge processes can expose companies to internal and external threats (Dodla & Jones, 2023). These apparently different findings can be interpreted coherently through the proposed eight-dimensional structure. A cybersecurity incident, for example, may originate in technological or human vulnerability but subsequently generate operational disruption, financial loss, legal liability, intellectual-property leakage, and reputational consequences. Similarly, financial constraints may delay system upgrading, which increases security vulnerabilities and ultimately threatens innovation capability. The principal implication is that risk identification in knowledge-based companies should be systemic, relational, and dynamic rather than based on isolated risk registers organized according to conventional departmental boundaries.

The findings of this study should be interpreted in light of several limitations. First, because the study employed a meta-synthesis design, the resulting model depended on the scope, quality, and conceptual emphases of the studies available for inclusion. Certain emerging risks may therefore have received less attention because they remain underrepresented in the existing literature. Second, the included studies were conducted across different industries, countries, institutional settings, and organizational sizes, which increased the conceptual breadth of the synthesis but may also have reduced contextual specificity. Third, the coding and categorization process necessarily involved interpretive judgment when conceptually similar findings were merged into higher-order categories, despite the systematic procedures used to improve analytical consistency. Fourth, the model identifies dimensions and relationships conceptually but does not determine their relative weights, causal strength, probability, or severity. Finally, the rapid development of artificial intelligence, cybersecurity threats, cloud technologies, platform ecosystems, and digital regulations means that the risk landscape of knowledge-based companies is continuously changing, and some technology-related risks may evolve more rapidly than systematic academic evidence can document them.

Future studies should empirically validate the proposed model in different types of knowledge-based companies and examine whether the eight dimensions retain the same structure across industries, firm sizes, technological maturity levels, and institutional environments. Quantitative studies can develop measurement instruments based on the identified dimensions and test their reliability, validity, relative importance, and interrelationships using exploratory factor analysis, confirmatory factor analysis, structural equation modeling, or partial least squares methods. Future research should also prioritize the identified risks by combining probability, severity, detectability, interdependence, and organizational exposure rather than relying exclusively on frequency of occurrence in the literature. Longitudinal research would be particularly valuable for examining how risk profiles change as companies progress through different stages of growth, digital transformation, commercialization, and internationalization. Further studies can also investigate the network structure of the identified risks to determine which factors function as central nodes capable of propagating disruption across multiple dimensions. Special attention should be given to emerging risks associated with generative artificial intelligence, autonomous decision systems, cloud concentration, algorithmic dependence, digital intellectual-property leakage, third-party platforms, and technology-related regulatory change. Comparative research across countries could also clarify the influence of institutional environments, regulatory structures, financing systems, and innovation ecosystems on the relative importance of individual risk dimensions.

Managers of knowledge-based companies should use the proposed model as an integrated risk-identification framework rather than managing technological, financial, human, legal, and strategic risks through isolated organizational functions. Risk assessment should begin with a comprehensive inventory of critical digital systems, knowledge assets, intellectual property, specialized human competencies, external technological dependencies, and business processes whose interruption could materially affect organizational continuity. Companies should establish clear ownership for each major risk category while creating cross-functional mechanisms that connect information technology, cybersecurity, knowledge management, finance, human resources, legal affairs, innovation management, and senior leadership. Particular attention should be paid to reducing single points of failure, including dependence on individual experts, specific technology vendors, unique infrastructure providers, or undocumented knowledge. Organizations should strengthen backup and recovery capabilities, cybersecurity monitoring, access governance, knowledge documentation, succession planning, workforce digital competence, contractual safeguards, and intellectual-property controls. Technology investments should also be evaluated not only in terms of expected efficiency or innovation benefits but according to their effects on organizational dependency, interoperability, security, maintainability, and long-term strategic flexibility. Finally, risk registers should be treated as dynamic management instruments and reviewed continuously so that emerging technological, regulatory, market, and ecosystem changes can be incorporated before they develop into major organizational disruptions.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethics Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were considered.

References

Adejumo, D. A. (2023). Review of Issues on Knowledge Management System and Country's Digital Security: a Study of Nigeria. *International Journal of Complementary & Alternative Medicine*, *16*(2), 55-62. https://doi.org/10.15406/ijcam.2023.16.00633

Alam, S., Zhang, J., & Ali, A. (2023). Mechanism of Knowledge Management Process Towards Minimizing Manufacturing Risk Under Green Technology Implementation: An Empirical Assessment. *Environmental Science and Pollution Research*, *30*(18), 51977-51994. https://doi.org/10.1007/s11356-023-25945-2

Bernal, Ó. A. V., Peinado, W. F., & Laverde, W. E. M. (2023). Knowledge Management as a Competitive Advantage an SMEs: A Theoretical Exploration. https://doi.org/10.46254/na8.20230055

Chen, D., Zhou, J., Duan, P., & Zhang, J. (2022). Integrating Knowledge Management and BIM for Safety Risk Identification of Deep Foundation Pit Construction. *Engineering Construction & Architectural Management*, *30*(8), 3242-3258. https://doi.org/10.1108/ecam-10-2021-0934

Chenya, L., Aminudin, E. B., Mohd, S., & Yap, L. S. (2022). Intelligent Risk Management in Construction Projects: Systematic Literature Review. *IEEE Access*, *10*, 72936-72954. https://doi.org/10.1109/access.2022.3189157

Daradkeh, M. K. (2023). Exploring the Influence of Risk Management on the Performance Of industry–university Collaborative Projects: The moderating Role of Knowledge Management Capabilities. *Journal of Organizational Effectiveness People and Performance*, *11*(3), 723-748. https://doi.org/10.1108/joepp-03-2023-0098

Dodla, T. R., & Jones, L. A. (2023). Mitigating Knowledge Management Internal and External Risk Factors: A Literature Review of Best Practices. *Scientific Bulletin*, *28*(1), 44-54. https://doi.org/10.2478/bsaft-2023-0005

Elgargouh, Y., Louhdi, M. R. C., Zemmouri, E. M., & Behja, H. (2024). Knowledge Management for Improved Digital Transformation in Insurance Companies: Systematic Review and Perspectives. *Informatics*, *11*(3), 60. https://doi.org/10.3390/informatics11030060

Figueiredo, R., Ferreira, J. J., Camargo, M. E., & Dorokhov, O. (2023). Applying Deep Learning to Predict Innovations in Small and Medium Enterprises (SMEs): The Dark Side of Knowledge Management Risk. *VINE Journal of Information and Knowledge Management Systems*, *53*(5), 941-962. https://doi.org/10.1108/vjikms-09-2022-0294

Hammami, S., Durrah, O., Jamil, S. A., & Eltigani, M. (2022). Engaging Knowledge Capabilities to Sustain the Application of Information Technology Governance in Healthcare Institutions. *Sage Open*, *12*(4). https://doi.org/10.1177/21582440221132783

Istyanto, N. P., & Nasrullah, M. (2022). Development of I-Graciass Adoption and Implementation Model at Telkom Education Foundation Lemdikti Knowledge Management Systems Based. *Journal of Information Systems and Informatics*, *4*(3), 753-771. https://doi.org/10.51519/journalisi.v4i3.321

Jiang, S. J. Y. G., & Cao, X. (2025). Rule Inferring for Engineering Quality Risk Management Based on Ontology in Housing Construction. *Sustainability*, *17*(4), 1643. https://doi.org/10.3390/su17041643

Jiang, Y., Ma, Z., & Wang, X. (2022). The Impact of Knowledge Management on Intellectual Property Risk Prevention: Analysis From China's Strategic Emerging Industries. *Journal of Knowledge Management*, *27*(1), 197-207. https://doi.org/10.1108/jkm-03-2022-0216

Liu, P., Shang, Y., & Zhang, L. (2023). A Design for Safety (DFS) Framework for Automated Inspection Risks in Metro Stations by Integrating a Knowledge Base and Building Information Modeling. *International journal of environmental research and public health*, *20*(6), 4765. https://doi.org/10.3390/ijerph20064765

Neştian, A. Ș., Guță, A. L., & Tiță, S.-M. (2024). Correlations Between Knowledge Risks and Knowledge Vulnerabilities Along Knowledge Processes. https://doi.org/10.24818/imc/2023/02.06

Osman, M. A., Noah, S. A. M., & Saad, S. (2022). Ontology-Based Knowledge Management Tools for Knowledge Sharing in Organization—A Review. *IEEE Access*, *10*, 43267-43283. https://doi.org/10.1109/access.2022.3163758

Padhy, P. C. (2024). Navigating Innovation Highways: Unraveling the Entrepreneurial Culture's Role With Knowledge Management as the Mediator in Automotive Technology Innovations. *Qubahan Academic Journal*, *4*(1), 190-200. https://doi.org/10.48161/qaj.v4n1a290

Polas, M. R. H., Jahanshahi, A. A., Kabir, A. I., Sohel-Uz-Zaman, A. S. M., Osman, A., & Karim, R. (2022). Artificial Intelligence, Blockchain Technology, and Risk-Taking Behavior in the 4.0IR Metaverse Era: Evidence From Bangladesh-Based SMEs. *Journal of Open Innovation Technology Market and Complexity*, *8*(3), 168. https://doi.org/10.3390/joitmc8030168

Pu, G. (2024). Relational Risk, Knowledge Sharing and Supply Chain Resilience: The Complementary Role of Blockchain Governance and Relational Governance. *Journal of Knowledge Management*, *29*(2), 301-341. https://doi.org/10.1108/jkm-12-2023-1244

Ravikumar, R., Kitana, A. F., Taamneh, A., Aburayya, A., Shwedeh, F., Salloum, S. A., & Shaalan, K. F. (2023). The Impact of Big Data Quality Analytics on Knowledge

Management in Healthcare Institutions: Lessons Learned From Big Data's Application Within the Healthcare Sector. *South Eastern European Journal of Public Health*. https://doi.org/10.56801/seejph.vi.309

Rodríguez-Páez, F. G., Diego Rafael Roberto Cabrera, M., & Herrera, J. (2024). Proposal of a Knowledge Management Model for Complex Systems: Case of the Supervision and Control Subsystem of the Colombian Health System. *Journal of Market Access & Health Policy*, *12*(3), 224-251. https://doi.org/10.3390/jmahp12030019

Saati, N. (2023). The Role of Knowledge Management in the Development of Sports Clubs in the Kingdom of Saudi Arabia. *International Journal of Advances in Computer Science and Technology*, *12*(1), 20-36. https://doi.org/10.30534/ijacst/2023/0411212023

Santos-Olmo, A., Sánchez, L., Rosado, D. G., Serrano, M., Blanco, C., Mouratidis, H., & Fernández-Medina, E. (2023). Towards an Integrated Risk Analysis Security Framework According to a Systematic Analysis of Existing Proposals. *Frontiers of Computer Science*, *18*(3). https://doi.org/10.1007/s11704-023-1582-6

Sumbal, M. S., Amber, Q., Tariq, A., Raziq, M. M., & Tsui, E. (2024). Wind of Change: How ChatGPT and Big Data Can Reshape the Knowledge Management Paradigm? *Industrial Management & Data Systems*, *124*(9), 2736-2757. https://doi.org/10.1108/imds-06-2023-0360

Sumbal, M. S., Khurshid, F., & Chan, F. T. (2022). Toward a Resilient Supply Chain Model: Critical Role of Knowledge Management and Dynamic Capabilities. *Industrial Management & Data Systems*, *122*(5), 1153-1182. https://doi.org/10.1108/imds-06-2021-0356

Vedapradha, R., Ravi, H., Sudha, E., Divyashree, V. R., & Ponnusamy, M. (2024). Future of Knowledge Management in Investment Banking: Role of Personal Intelligent Assistants. *Methodological Innovations*, *17*(4), 229-247. https://doi.org/10.1177/20597991241287118

Wang, X., Wu, K., He, J., Ma, X., Zhou, Q., & Chen, X. (2024). Digital Capabilities and Ambidextrous Innovation: Evidence From Chinese Technology-Based SMEs. *Sustainability*, *16*(23), 10611. https://doi.org/10.3390/su162310611

Wiesenfeld, B. M., & Kellogg, K. C. (2026). Generative Organizational Learning: Affordances for New Modes of Knowledge Search, Creation, Transfer, and Forgetting With LLMs. *Strategic Organization*, *24*(2), 256-284. https://doi.org/10.1177/14761270251408580