Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P8074-cd

Third-Party Risk in Research: A Literature Review

Julija Saveljeva

Department of Economics and Finance, BA School of Business and Finance, Latvia. E-mail: julija.saveljeva@ba.lv

Third-party risk management is crucial for organizations to manage potential risks associated with outsourcing and supply chain operations. While the topic of third-party risk management has been widely discussed in professional literature and regulatory papers, it remains an emerging area of research in scientific literature.
The purpose of this theoretical paper is to examine the overall landscape of research devoted to the third-party risk topic and to answer key questions: 1. What is the definition of third-party risk in scientific research? 2. What types of risks are managed within third-party risk management frameworks, and 3. What is the essential difference between third-party risk, vendor risk, and supplier risk concepts?
To achieve this goal, a systematic literature review using the PRISMA 2020 methodology was conducted. A total of 107 unique publications were identified in the Scopus and Web of Science databases using the keyword "third-party risk" and analyzed using a two-stage approach: first through an abstract review, followed by a full-text analysis. The papers included in the final set were further analyzed using bibliometric and content analysis methods. From a theoretical perspective, the research findings provide a comprehensive overview of previous work on the topic of third-party risk, highlighting future research opportunities. From a practitioner's perspective, this research helps clarify the conceptual differences between vendor risk, supplier risk, and third-party risk, supporting the development of a more effective organizational risk management program.

Keywords: third-party risk, operational risk, supplier risk, vendor risk, risk management, systematic literature review, risk governance.

1. Introduction

Modern business ecosystems depend heavily on third-party relationships, meaning that most business processes cannot operate without products or services provided by external parties. This reliance makes the risks associated with external parties more significant (Ramasubramaniam and Singh 2020; Keskin et al. 2021).

In recent years, regulators have paid more attention to third-party oversight, motivating organizations to improve their third-party risk management practices (Ramasubramaniam and Singh 2020). One important regulation in this area is the European Union's Digital Operational Resilience Act (DORA), which came into effect on January 16, 2023, and will apply to the entire financial sector starting January 17, 2025. Among other aspects of digital resilience, DORA focuses on ICT third-party risk, defined as "ICT risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers or by subcontractors of the latter, including through outsourcing arrangements" (European Commission 2022).

While the regulation introduces the principle of proportionality - stating that financial entities should manage ICT third-party risks based on how critical certain services are and their impact on financial service continuity - it does not provide a detailed framework or specify the types of risks to be managed.

This paper explores several key research questions:

RQ1: What is the definition of third-party risk in scientific research?

RQ2: What types of risks are managed within third-party risk management frameworks?

RQ3: What is the essential difference between the concepts of third-party risk, vendor risk, and supplier risk?

Since the author's first language is not English, the text has been proofread using OpenAI GPT-4o and Grammarly to correct any spelling or grammar errors. The author has reviewed the text after using these tools and takes full responsibility for the content of the publication.

2. Research Design and Methodology

A systematic literature review was conducted following the PRISMA 2020 methodology (Page et al. 2021) to address the research questions. The keyword "third-party risk" was searched on October 12, 2024, focusing on papers' titles, abstracts, and keywords. The search was carried out in the Scopus (Elsevier, n.d.) and Web of Science (Clarivate, n.d.) databases, resulting in 108 sources from Scopus and 26 sources from Web of Science. After removing duplicates, 107 unique papers were identified.

The identified papers reveal a growing interest in the third-party risk topic over time. Before the year 2000, the interest was minimal, with no publications or just 1–2 documents. A gradual increase began after 2000, with significant growth in publications starting around 2015. The interest peaked in 2024, with 15 publications recorded within an incomplete year. The trend in the number of publications over time is illustrated in Figure 1 below.

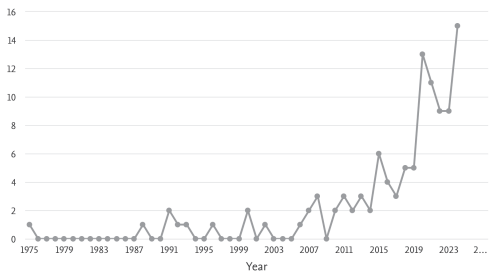

Fig. 1. Number of conference proceedings and research papers containing the keyword "third-party risk" in the abstract, title, or keywords published per year (Elsevier, n.d.)

The abstracts of the identified papers were further analyzed using the following inclusion criteria:

(i) The research should explicitly address third-party risk.
(ii) The term "third-party risk" must be applied within an operational risk management context of organization.

For example, it was observed that in the field of aviation (n=34 from the retrieved papers), third-party risk is often discussed in the context of "safety (risk) for the people on the ground, who are involuntarily exposed to an aircraft accident" (Aalmoes et al., 2015), therefore such papers were excluded from the analysis. Another exclusion criterion was the focus on risks to a third party, rather than risks originating from third parties.

Based on the inclusion and exclusion criteria, 31 papers were selected for further analysis. Of these, five papers were unavailable to the author, leaving 26 papers for detailed review. After applying the criteria to the full texts, 10 papers were excluded, resulting in a final set of 16 papers included in this analysis. The process of paper selection and analysis is depicted in Figure 2 below.

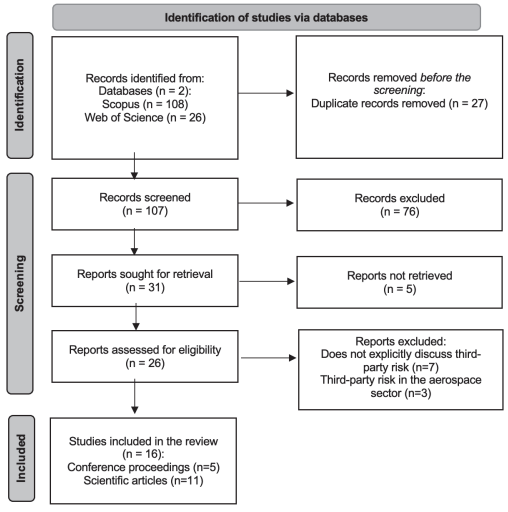

Fig. 2. Systematic literature review process

3. Research Findings

3.1. *Bibliometric analysis results*

The analysis included a total of 16 publications, comprising five conference proceedings and 11 scientific articles. The topic, in the reviewed context, first appeared in publications in 2016. It began to gain more attention in 2019 and reached its peak in 2024, with five papers published.

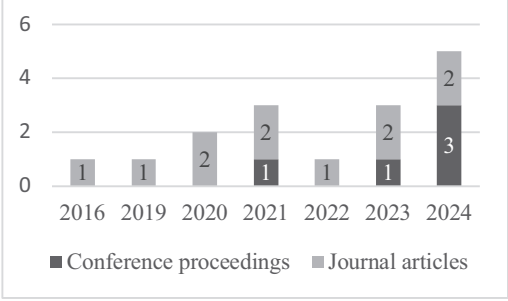

Fig. 3. Papers included in the analysis based on publication type and year (Author's research)

The analysis revealed no recurring authors or publication sources among the papers. Two of the analyzed papers did not include the author's affiliation. For the remaining 14 papers, authors from 18 different countries contributed to the research on third-party risks. The most represented country was India, with four papers, followed by the United States of America and the United Kingdom, each with two publications.

A full-count co-occurrence keyword analysis was conducted using the VOSviewer tool ("VOSviewer," n.d.), which analyzed 63 keywords from the reviewed papers. Among these, 13 keywords were interconnected, resulting in the identification of three thematic clusters, as shown in Figure 4:

- Cluster 1 (keywords: blockchain technology, encryption, internet of things, privacy, security) focusing on technological solutions to third-party risk.
- Cluster 2 (keywords: information, risk, self-assessment) highlighting a process-oriented perspective on third-party risk.
- Cluster 3 (keywords: construction, engineering, integrity, risk-based due diligence, third-party) emphasizing third-party risk management within specific industry settings.

Although the number of analyzed papers is relatively small, the results illustrate that the topic of third-party risk in scientific research extends beyond a single domain. The findings reflect a multi-dimensional approach, addressing the topic from practical, technical, and systematic perspectives.

3.2. *Context analysis results*

The analyzed papers were further studied using context analysis to identify the primary focus areas of prior research on third-party risk.

From an industry perspective, five papers are not linked to any specific industry, focusing on general research. The remaining papers explore specific sectors, with manufacturing, construction, finance, and technology each being covered twice. Other industries, such as healthcare, pharmacy, and smart cities, appear only once. This distribution aligns with the balance of conceptual and empirical studies among the analyzed papers: six are conceptual or theoretical, while 10 are empirical.

Fig. 4. Keywords co-occurrence clustering results ("VOSviewer," n.d.)

The conceptual papers can be categorized into two groups:

- Four papers focus on innovative methods and tools for improving third-party risk management (Ramasubramaniam and Singh 2020; Fortner 2021; Mohta, Singh, and Arya 2024; Agrawal et al. 2024).
- Two papers highlight existing gaps and propose strategic roadmaps for industry and policymakers. One discusses prior research in operational risk management (Jadwani, Parkhi, and Mitra 2024), while the other provides a comparative gap analysis between DORA and ISO 27001:2013 standard (Neumannová, Bernroider, and Elshuber 2023).

The 10 empirical papers focus on the following areas:

(i) Three papers propose new risk management frameworks, either concentrating on (Aliane and Zakariya 2023; Vitunskaite et al. 2019) or including

(Tang et al. 2024) third-party risk management.

(ii) Two papers introduce new tools designed for risk management, including third-party risks (Abbasi et al. 2023; Jallan and Ashuri 2020).

(iii) Three papers either propose new procedural approaches for third-party risk management (Sehgal and Ambili 2024; Roy et al. 2022) or enhance existing ones (Monev 2021).

(iv) Two papers focus on evaluating current methods. One analyzes solutions for managing cyber third-party risks (Keskin et al. 2021), while the other examines the correlation between responsible purchasing and improved supply chain risk management (Kähkönen et al. 2016).

3.2.1. *Definition of third-party risk*

Only six of the analyzed papers provided definitions of third-party risk, which are listed in Table 1. Among these, only one definition specifically addressed risks in the IT domain (Ramasubramaniam and Singh 2020), while the others do not explicitly relate to a particular operational area of third parties.

Table 1. Definitions of third-party risks

Nr.	Definition
1	"In less mature third-party risk management programs, the scope of third parties is restricted to typical IT service providers. In some cases, the scope is extended to include business process outsourcing arrangements" (Ramasubramaniam and Singh 2020).
2	"Third-Party Risk Management (TPRM) is the process used by companies to monitor and manage interactions with all external parties, particularly their vendors" (Keskin et al. 2021).
3	"Third-party risk involves assessing and managing the risks associated with external entities such as sales agents, lobbyists, business development, consultants, customs or visa agents, joint venture and consortium partners, etc" (Roy et al. 2022).
4	"The risks associated with utilizing external suppliers and service providers for business operations" (Mohta, Singh, and Arya 2024).
5	Risks related to disruption for the organizations arising from the relationships with third-party providers – *definition summarized by the author of the research* (Jadwani, Parkhi, and Mitra 2024)
6	"Risk related to dealings with third parties, subcontractors, and joint venture" (Jallan and Ashuri 2020).

The definitions reveal a lack of a unified view of what constitutes third parties and the risks they pose to organizations. Consolidating the various perspectives, third parties can broadly include service providers (such as IT service and outsourcing providers), vendors, suppliers, partners, subcontractors, consultants, or any other external entity interacting with an organization.

This gap creates challenges for organizations in establishing consistent third-party risk management frameworks. Differing interpretations across organizations or sectors can lead to inconsistencies in risk assessment and mitigation. On the other hand, customizing the scope is essential, considering the industry in which the organization operates and its specific operational needs.

3.2.2. *Types of third-party risks*

Nine papers addressed the types of third-party risks, offering varying levels of detail. Some papers categorized the risks broadly, while others provided more specific examples or focused on particular aspects of risks that may arise from external parties. In total, six categories of third-party risks were identified, offering a comprehensive overview of the potential range of these risks.

(i) **Regulatory and Compliance.** This category includes compliance and regulatory risks, such as conformity to tax laws, sanctions, and legal aspects (Ramasubramaniam and Singh 2020; Roy et al. 2022; Mohta, Singh, and Arya 2024).

(ii) **Operational.** This category can be divided into three subcategories:

a. General Operational Risks: Risks associated with managing a third-party governance framework

(Ramasubramaniam and Singh 2020; Mohta, Singh, and Arya 2024).

b. Supply Chain and Partner-Process Issues: Includes risks such as supply chain disruptions, siloed processes, hindered visibility, onboarding risks, and inefficient collaboration (Fortner 2021; Kähkönen et al. 2016). It also addresses such supplier-related factors as geographical location, industry type, partner profile, proximity to officials, reasons for partnership, and contract complexity (Roy et al. 2022; Kähkönen et al. 2016). Additionally, it includes fourth-party and nth-party risks associated with suppliers and sub-contractors in the extended supply chain (Ramasubramaniam and Singh 2020; Fortner 2021).

c. Concentration Risk and Contingency Planning: Risks arising from over-reliance on specific third parties or a lack of contingency measures (Jadwani, Parkhi, and Mitra 2024; Abbasi et al. 2023).

(iii) **Financial.** This category includes financial risks such as high intermediary fees and cost exposures (Abbasi et al. 2023; Kähkönen et al. 2016; Mohta, Singh, and Arya 2024).

(iv) **Security and Privacy** category, which can be divided into:

a. Vendor and Supply Chain Cybersecurity Risks: Risks related to the cybersecurity vulnerabilities of vendors and supply chains (Keskin et al. 2021; Mohta, Singh, and Arya 2024; Jadwani, Parkhi, and Mitra 2024).

b. Data Privacy Risks: Risks such as data security breaches, leakage, and sovereignty issues 01/01/25 1:45:00 PM.

(v) **Strategic**. This category includes strategic risks related to alignment with business objectives and frameworks, such as outsourcing strategies (Neumannová, Bernroider, and Elshuber 2023; Ramasubramaniam and Singh 2020).

(vi) **Ethical and Social** category, which is represented by:

a. Reputational risks and conflict of interest, both including risks of corruption, bribery, and collusion (Roy et al. 2022).

b. Corporate social responsibility. Risks involving human rights and other social responsibility aspects (Roy et al. 2022; Kähkönen et al. 2016).

The variety of identified third-party risks reflects the complexity and breadth of issues organizations must address in their third-party risk management practices. While some risks, such as regulatory compliance and operational concerns, are widely acknowledged across industries, others, like ethical, social, or cyber risks, are context-specific and often industry-dependent.

The inclusion of security and privacy risks in seven out of nine papers highlights the increasing relevance of digital threats in today's interconnected environments, where vulnerabilities in third-party systems can have significant consequences. Similarly, the identification of fourth-party and nth-party risks underscores the growing need for organizations to extend their risk management practices beyond direct partners to include the entire supply chain.

3.2.3. *Third-party risk differentiation from vendor and supplier risks*

While examining the definitions of third-party risks, it may seem that they are synonymous with supplier or vendor risks. Some authors support this perspective, stating that third-party risks can be used interchangeably with vendor risks and supply chain risks (Schelegia and Fleşer 2021; Keskin et al. 2021).

However, a closer look at the definitions does not support such a position. The definition of third-party risk proposed by Keskin et al. (2021) already included the vendor as one of the external party types that requires a specific focus.

A review of vendor risk definitions demonstrates variability in focus and scope:

(i) "Efficient management of third-party vendor risks entails evaluating and addressing possible security breaches linked to technological solutions or services rendered to financial institutions" (Wang et al. 2024).

(ii) "Vendor risk concerns the possibility that the seller is fictitious or otherwise invalid" (Mascha, Miller, and Janvrin 2011).

(iii) "Vendor risks are the risks that the client bears when contracting the project to an external vendor rather than conducting it in-house. Vendor risks are unique to outsourced IT projects and are not applicable to in-house projects" (Natovich 2003).

(iv) "Degree to which individuals believe that if they purchase products or services through the Internet, they will suffer losses caused by Internet vendors" (Herrero and San Martín 2012).

From the above list of definitions, it may be concluded that there is no unified view of vendor risk definitions, as the interpretations vary significantly. Vendor risk can be analyzed from two main perspectives: that of an organization or an individual customer. Additionally, the scope of risks associated with vendors is often narrower compared to the broader concept of third-party risks. Furthermore, vendor risks are frequently associated with IT service vendors, reflecting their differentiated position in risk management frameworks.

The term "supplier risk" is strongly linked to "supply chain risk" and is often used interchangeably in research. Examples of definitions include:

(i) "This paper considers the risks of two types of poor supplier performance: late delivery and poor quality supply. This paper refers to these risks as supplier risks" (Zhou et al. 2022).

(ii) "Supplier risk deals with their short-and long-term capability to deliver products, parts, and services in accordance to the requirements" (Phusavat et al. 2015).

(iii) "Supplier risk profiles consist of risk events that can have an adverse impact on buyer organizations. Risk events are incidents whose occurrences result in the disruption of overall supply chain performance" (Lockamy 2011).

(iv) "Perceived supplier risk (or supplier risk) refers to the buyer's expectation of probable disruption on the supplier's side that causes loss to the buyer due to unavailability of a sourced item (Nguyen et al. 2017).

As with vendor risks, supplier risks lack a universal definition, and authors often propose definitions tailored to the specific objectives of their studies.

The differences outlined above confirm that third-party, vendor, and supplier risks are separate concepts rather than interchangeable terms. While third-party risks encompass a broader range of external relationships, vendor risks are typically associated with specific contractual relationships and are often linked to the technological context of the provided products or services. Supplier risks, by contrast, are closely tied to supply chain performance and operational reliability.

4. Discussion and Conclusions

Third-party risk is an emerging topic that continues to gain increasing attention in academic research year by year. While the definitions of third-party risk show some variation, they are relatively homogenous compared to the definitions of vendor and supplier risks, which remain fragmented and require further exploration to standardize and clearly distinguish these terms.

Additionally, further research should focus on analyzing the differences among third-party, vendor, and supplier risks, going beyond the comparison of the definitions to the comparison of types of risks included in each category. Another area of exploration is the evaluation of existing tools and frameworks for third-party risk management, assessing their effectiveness, and identifying areas for improvement. Despite the progress in identifying and categorizing third-party risks, gaps remain in the standardization of these classifications across industries. This would help organizations adapt to the evolving risk landscape and ensure a consistent approach to third-party risk management practices.

Addressing these challenges would contribute to the development of more robust, unified, and actionable third-party risk management approaches, supporting both academic advancements and practical applications in this critical area.

Acknowledgement

This research is supported by the grant received within a project nr. 5.2.1.1.i.0/2/24/I/CFLA/007 “Internal and External Consolidation of the University of Latvia”.

References

Abbasi, M., J. Prieto, A. Shahraki, and J.M. Corchado. 2023. “Industrial Data Monetization: A Blockchain-Based Industrial IoT Data Trading System.” *Internet of Things (Netherlands)* 24. https://doi.org/10.1016/j.iot.2023.100959.

Agrawal, P., P. Durge, R.K. Kushwaha, G. Kaur, G.K. Gupta, and S. Maheshwari. 2024. “Securing the Internet of Things: A Blockchain Paradigm.” In *Int. Conf. Innov. Challenges Emerg. Technol., ICICET*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICICET59348.2024.10616308.

Aliane, N., and A. Zakariya. 2023. “Enhancing Cyber Security Resilience in the Industrial Sector: A Comprehensive Framework for Third-Party Risk Management.” *International Journal of Cyber Criminology* 17 (2): 262–83. https://doi.org/10.5281/zenodo.4766716.

Clarivate. n.d. “Web of Science.” Accessed November 18, 2024. https://www.webofscience.com.

Elsevier. n.d. “Scopus.” Accessed November 18, 2024. https://www.scopus.com.

European Commission. 2022. “Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA Relevance).” https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554.

Fortner, Z.A. 2021. “Mitigating Third-Party Risks: The Benefits of Extending Quality to the Supply Chain.” *Pharmaceutical Technology Europe* 45 (9): 56–60.

Herrero, A., and H. San Martín. 2012. “Effects of the Risk Sources and User Involvement on E-Commerce Adoption: Application to Tourist Services.” *Journal of Risk Research* 15 (7): 841–55. https://doi.org/10.1080/13669877.2012.666758.

Jadwani, B., S. Parkhi, and P.K. Mitra. 2024. “Operational Risk Management in Banks: A Bibliometric Analysis and Opportunities for Future Research.” *Journal of Risk and Financial Management* 17 (3). https://doi.org/10.3390/jrfm17030095.

Jallan, Y., and B. Ashuri. 2020. “Text Mining of the Securities and Exchange Commission Financial Filings of Publicly Traded Construction Firms Using Deep Learning to Identify and Assess Risk.” *Journal of Construction Engineering and Management* 146 (12). https://doi.org/10.1061/(ASCE)CO.1943-7862.0001932.

Kähkönen, A.-K., K. Lintukangas, J. Hallikas, and P. Evangelista. 2016. “Responsible Buying Practices in Supply Risk Management.” *International Journal of Integrated Supply Management* 10 (3–4): 309–29. https://doi.org/10.1504/IJISM.2016.081282.

Keskin, O.F., K.M. Caramancion, I. Tatar, O. Raza, and U. Tatar. 2021. “Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports.” *Electronics (Switzerland)* 10 (10). https://doi.org/10.3390/electronics10101168.

Lockamy, III A. 2011. “Benchmarking Supplier Risks Using Bayesian Networks.” *Benchmarking* 18 (3): 409–27. https://doi.org/10.1108/14635771111137787.

Mascha, M.F., C.L. Miller, and D.J. Janvrin. 2011. “The Effect of Encryption on Internet Purchase Intent in Multiple Vendor and Product Risk Settings.” *Electronic Commerce Research* 11 (4): 401–19. https://doi.org/10.1007/s10660-011-9080-6.

Mohta, Y., U. Singh, and A. Arya. 2024. “NLP-Enabled Bot for Managing Third-Party Risk.” In *Proc. - Int. Conf. Comput. Intell. Comput. Appl., ICCICA*, edited by Gupta S.C., Gandhi A.B., Mehla S., and Lakhina U., 131–35. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICCICA60014.2024.10584983.

Monev, V. 2021. “The ‘Self-Assessment’ Method within a Mature Third-Party Risk Management Process in the Context of Information Security.” In *Int. Conf. Inf. Technol., InfoTech - Proc.* Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/InfoTech52438.2021.9548373.

Natovich, J. 2003. “Vendor Related Risks in IT Development: A Chronology of an Outsourced Project Failure.” *Technology Analysis and Strategic Management* 15 (4): 409–19.

https://doi.org/10.1080/09537320300013601 5.

Neumannová, A., E.W.N. Bernroider, and C. Elshuber. 2023. "The Digital Operational Resilience Act for Financial Services: A Comparative Gap Analysis and Literature Review." In *Vienna University of Economics & Business*, edited by Papadaki M., Rupino da Cunha P., Themistocleous M., and Christodoulou K., 464 LNBIP:570–85. Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-30694-5_40.

Nguyen, H.V., H.T. Nguyen, S. Deligonul, and S.T. Cavusgil. 2017. "Developing Visibility to Mitigate Supplier Risk: The Role of Power-Dependence Structure." *Asia-Pacific Journal of Business Administration* 9 (1): 69–82. https://doi.org/10.1108/apjba-05-2016-0052.

Page, Matthew J., Joanne E. McKenzie, Patrick M. Bossuyt, Isabelle Boutron, Tammy C. Hoffmann, Cynthia D. Mulrow, Larissa Shamseer, et al. 2021. "The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews." *Systematic Reviews* 10 (1): 89. https://doi.org/10.1186/s13643-021-01626-4.

Phusavat, K., P. Anussornnitisarn, T. Pongrakhananon, and Z. Pastuszak. 2015. "Applications of Benchmarking and Classification Framework for Supplier Risk Management." *BENCHMARKING-AN INTERNATIONAL JOURNAL* 22 (2): 275–99. https://doi.org/10.1108/BIJ-12-2012-0085.

Ramasubramaniam, V., and A.K. Singh. 2020. "Addressing Key Pain Points to Develop a Mature Third-Party Risk Management Program." *ISACA Journal* 3:46–52.

Roy, V., D. Desjardins, C. Fertel, and C. Ouellet-Plamondon. 2022. "Methodology for Conducting Third-Party Risk-Based Due Diligence in the Construction and Civil Engineering Industry." *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction* 14 (4). https://doi.org/10.1061/(ASCE)LA.1943-4170.0000553.

Schelegia, E.P., and T. Fleşer. 2021. "Automated Supplier Risk Evaluation System." In *J. Phys. Conf. Ser.*, edited by Sandu A.V., Abdullah M.M.A.B., Vizureanu P., Nabialek M., Ghazali C.M.R., and Sandu I. Vol. 1960. IOP Publishing Ltd. https://doi.org/10.1088/1742-6596/1960/1/012003.

Sehgal, V.V., and P.S. Ambili. 2024. "A Taxonomy and Survey of Software Bill of Materials (SBOM) Generation Approaches." In *Commun. Comput. Info. Sci.*, edited by Dhar S., Goswami S., Dinesh Kumar U., Bose I., Dubey R., and Mazumdar C., 2008:40–51. Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-50815-8_3.

Tang, J., Q.-H. Zheng, W.-Z. Wang, M. Deveci, N. Bacanin, and A.A. Zaidan. 2024. "Analyzing Information Security Factors in Adoption of Intelligent Technologies for Medical Waste Management Systems." *IEEE Transactions on Consumer Electronics* 70 (1): 2066–77. https://doi.org/10.1109/TCE.2023.3347650.

Vitunskaite, M., Y. He, T. Brandstetter, and H. Janicke. 2019. "Smart Cities and Cyber Security: Are We There yet?A Comparative Study on the Role of Standards, Third Party Risk Management and Security Ownership." *Computers and Security* 83 (June):313–31. https://doi.org/10.1016/j.cose.2019.02.009.

"VOSviewer." n.d. VOSviewer. Accessed April 26, 2024. https://www.vosviewer.com//.

Wang, S., M. Asif, M.F. Shahzad, and M. Ashfaq. 2024. "Data Privacy and Cybersecurity Challenges in the Digital Transformation of the Banking Sector." *Computers and Security* 147. https://doi.org/10.1016/j.cose.2024.104051.

Zhou, R., T.H. Bhuiyan, H.R. Medal, M.D. Sherwin, and D. Yang. 2022. "A Stochastic Programming Model with Endogenous Uncertainty for Selecting Supplier Development Programs to Proactively Mitigate Supplier Risk." *OMEGA-INTERNATIONAL JOURNAL OF MANAGEMENT SCIENCE* 107 (February). https://doi.org/10.1016/j.omega.2021.102542.