INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 15, Issue 12, (2025) E-ISSN: 2222-6990

Risk Management in Information Systems and Technology Trends: A Bibliographic Perspective

Nina Fadilah Najwa[1*], Suraya Miskon[2] and Okfalisa[3]

[1*]Department of Information Systems, Universiti Teknologi Malaysia, Malaysia and Politeknik Caltex Riau, Indonesia, [2]Department of Information Systems, Universiti Teknologi Malaysia, Malaysia,[3]Department of Informatics Engineering, Universitas Islam Negeri Sultan Syarif Kasim, Indonesia

Email: nina@pcr.ac.id

[1*]Corresponding Author Email: nina@graduate.utm.my

DOI Link: http://dx.doi.org/10.6007/IJARBSS/v15-i12/27294

Published Date: 22 December 2025

Abstract

Information security becomes an object in IS/IT risk management. Organizations' technology and information systems have been embedded into business processes and become competitive advantage strategies. However, many threats and cybercrime are behind the benefits of IS/IT adoption. This study examines trends and research opportunities related to IS/IT risk management from a bibliography perspective. The research stages consist of four stages: identification, screening, eligibility, and sorting. The 289 papers were obtained from 2020 to 2025 and processed using the VosViewer application to map the bibliography network. The results are 145 terms, and 7 clusters have occurrence values and links to relevance. The Top 3 Terms with the highest occurrence level are terms "project," "assessment," and "threat." IS/IT risk management in enterprises will have different results depending on the conditions of each case. Further research can examine the trends, network of terms, recommendation paper, and gaps presented in this paper.

Keywords: IS/IT Risk Management, Cyber Security, Information Security, Risk Assessment

Introduction

Information is an essential asset that needs to be protected because the value of information depends on the type and scale of the business and its role in delivering services (Muhammad et al., 2025). Information security becomes an object in IS/IT risk management in maintaining confidentiality, integrity, and availability of crucial organizational data (Alotaibi et al., 2023). Current technological developments mean that data centers have even become big data, which has become an asset for organizations to continue to survive and grow.

Organizations' technology and information systems have been embedded into business processes and become competitive advantage strategies. However, behind the benefits of

IS/IT adoption, many threats have impact levels ranging from small, medium, to severe. Organizational business risks are currently faced with cyber risks, loss or leakage of company data, loss exposure, and other risks arising from vulnerabilities and incorrect IS/IT risk management (Arista & Ngafidin, 2022). Organizations need to carry out IS/IT risk management on an ongoing basis. The risk management process helps identify risks and their factors to minimize risks (Taherdoost, 2021). Risk management has become one of the success factors for organizational growth. At the same time is a challenge for organizations so that risk mitigation is carried out at the right risk value (Berrada et al., 2021).

This research will discuss from a bibliographic perspective to answer two research questions: (1) What are the variables or domains related to IT/IS Risk Management research? (2) What is the IT/IS Risk Management research gap? The research stages consist of four stages: identification, screening, eligibility, and sorting. The usefulness of this research is to get an overview of research trends in the IS/IT Risk Management field as well as further research opportunities.

Research Methodology

This study examines trends and research opportunities related to IS/IT risk management. A systematic stage was conducted to obtain research papers based on the scope of the study to answer the research question (RQ) (Magabaleh et al., 2024). Two RQs were formulated for this review: (1) What are the variables or domains related to IT/IS Risk Management research? (2) What is the IT/IS Risk Management research gap? The research stages consist of four stages: identification, screening, eligibility, and sorting. In this identification stage, the keywords used are related to the scope of the study of information systems and technology and risk management. The query formulation is (“information system” OR "information technology" OR "Information security") AND ("Risk Management" OR "Risk Framework" OR "Risk Methodology" OR "Risk Method"). Furthermore, the query is used in the Scopus and Web of Science databases on April 23, 2025. There are the following search criteria: (1) range publication from 2020 to 2025, (2) English paper, (3) journal and article type papers, and (4) Subject area selection. The second stage is screening the paper to detect whether there is duplication or incomplete data by using the Mendeley reference manager application. The third stage is to assess the eligibility of the paper to be reviewed. After that, all selected papers are imported into the Vosviewer application. The fourth stage is to analyze the bibliography results and answer the research questions.

Results and Discussions

Findings and Analysis

The topic area of IS/IT risk management research from 2020 to 2024 is increasingly trending and still a hot topic (Figure 1). In 2025, because the search was carried out until April, the graph is still decreasing because it has not been a full year of calculation. From the initial search and filter results, the results of the papers found were 615 paper. Furthermore, incomplete and data duplication were detected in as many as 130 papers. After the selection process, 289 papers were obtained, then process with VosViewer applications. The final terms amounted to 145. Terms are divided into 7 clusters marked with different colors for each cluster (Figure 3).

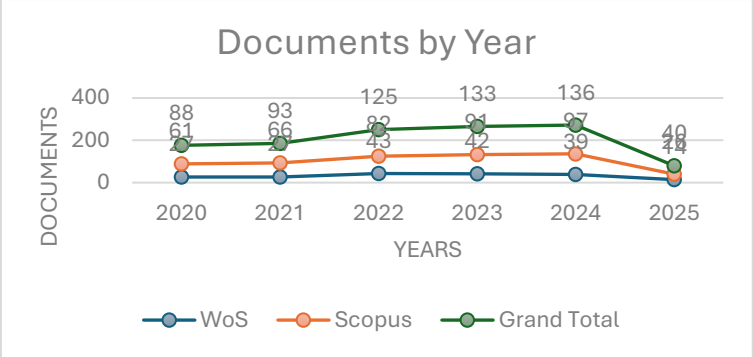

Figure 1. Research Trend by Year

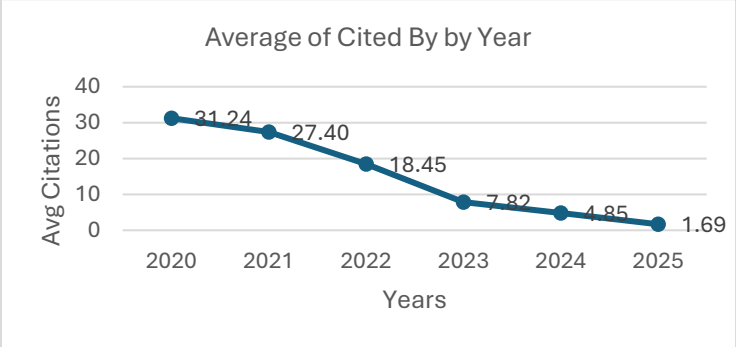

Figure 2. Average of Cited Trend by Year

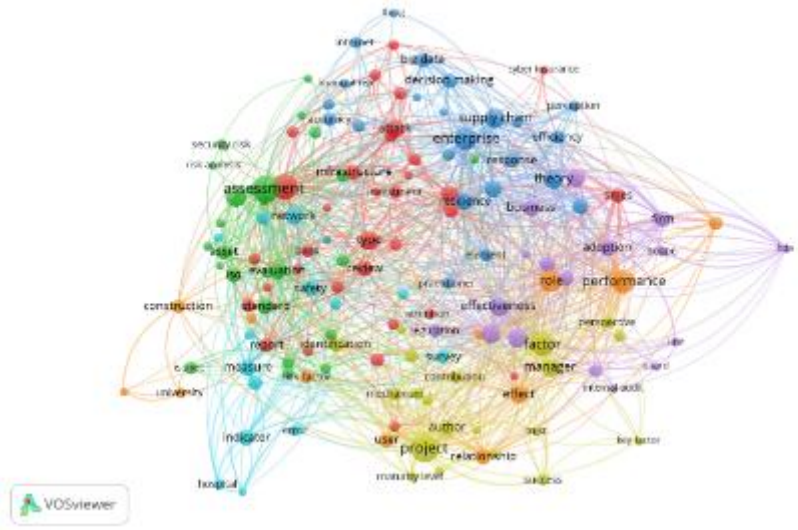

Figure 3. Network Map of Terms

Based on the results, the average number of citations of research papers each year has decreased significantly (Figure 2). With the rising number of studies, there will be competition in the number of citations, especially in new studies that need several years to get this research citation. This study provides seven recommendations for papers with the most citations on the research topic of IS/IT Risk Management (Table 1).

Table 1
Publication and Citation of Top Seven Authors

Authors	Year	Cited by
(Gu et al., 2021)	2021	387
(Sobb et al., 2020).	2020	222
(Rodríguez-Espíndola et al., 2022)	2022	217
(Kulathunga et al., 2020)	2020	211
(Kamiya et al., 2021)	2021	184
(Culot et al., 2021)	2021	141
(Gordon et al., 2020)	2020	131

Analysis of the Most Relevant and Important Keywords in Each Cluster

The Top 5 Terms with the highest occurrence level are Terms project (119), assessment (109), threat (91), enterprise (82), performance (76) (Figure 4). However, these clusters are also grouped based on their links and relevance levels so that cluster 1 is more relevant and followed by the next cluster in sequence. Cluster are formed automatically using the VosViewer clustering algorithm based on co-occurrence relationship between keywords.

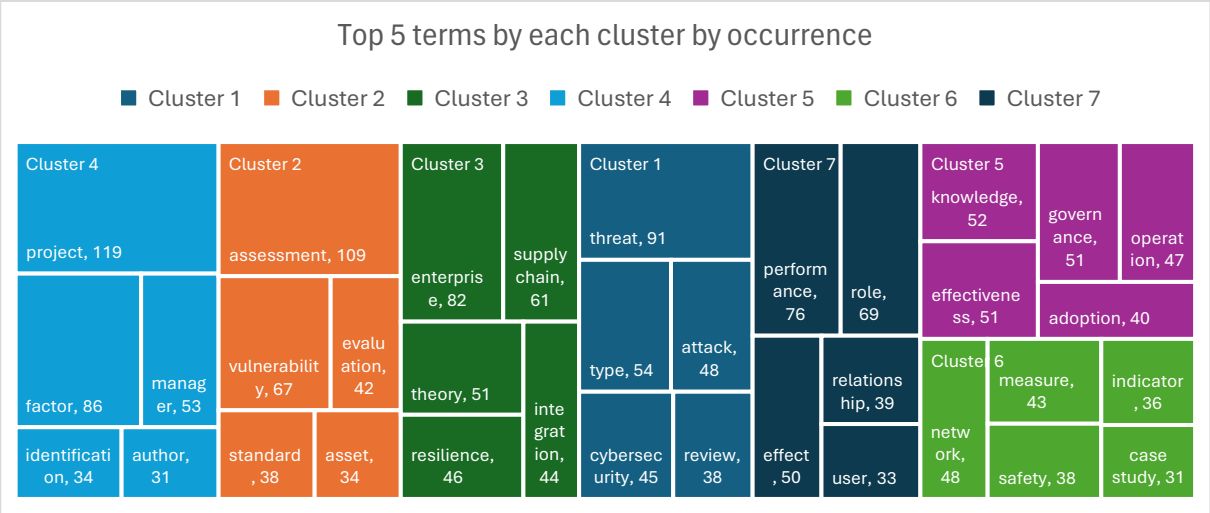

Figure 4. The top five terms by each cluster by occurrence level

Cluster 1: Threat, Cyber Security

In cluster 1, 33 items of terms were obtained that were interrelated. The most frequently appearing term was a threat. Threats can be defined as phenomena that harm protected assets or objects (Kopencova et al., 2021). Information security in organizations faces various threats from internal and external organizations. Threats from internal organizations are challenging to manage because irresponsible people can easily access information (Sektas-Bilusich et al., 2020). As security threats increase, so does the vulnerability of businesses and organizations to attack by cybercriminals (Abdymanapov et al., 2021). Cybersecurity threats such as malware, phishing, and others are increasingly occurring (Althobaiti, 2021). Based on the results of the study (Chundu et al., 2025) that the main pillars of cyber security are confidentiality, integrity, availability, authentication, authorization, and non-repudiation.

Cluster 2: Risk Assessment, Standard

In cluster 2, The total terms in cluster 2 are 25 terms. The most frequently appearing is assessment terms. Many types of standards related to risk management are generally associated with information security, but few are related to IT Risk management (Berrada et al., 2021). The growth of cybercrime with various incidents shows that traditional approaches to information security are no longer relevant (Abdymanapov et al., 2021). Risk assessment helps organizations to identify weaknesses and threats and recommend appropriate mitigation solutions for those risks (Shakibazad & Rashidi, 2020). There needs to be a calculation mechanism that helps make decisions objectively (Kozlov & Noga, 2021). IT risk management standards or frameworks do not include mechanisms to measure the maturity level (Fauzi & Lubis, 2021).

Cluster 3: Enterprise and Big Data

The total terms in cluster 3 are 24 terms. Big data technology supports more modern, easier, and more efficient IT governance than traditional governance (Yang, 2022). Big data analysis systems can monitor and identify risks in real-time using network analysis algorithms and machine learning (Li & Zhang, 2025). Big data helps provide data that supports decisions in depth, easy to handle financial problems, and can carry out an early warning system (Ren, 2022). The role of IS/IT risk management in an organization is not only the task of the IT department but is the role and responsibility of all organizational stakeholders (Alshahrani et al., 2022). It is necessary to adjust standards and frameworks according to the organization needs, such as combining more dynamic, responsive, and holistic methods for IT risk management (AL-Dosari & Fetais, 2023). Implementing cyber insurance policies in SMEs can be applied to manage security risks arising from the rapid digitalization process. With this policy, SMEs will feel safer investing their money using information systems and technology more widely. This policy can provide a reference for an effective and efficient mitigation process (Taskin et al., 2025).

Cluster 4: Successful Project

The total terms in cluster 4 are 20 terms. There is a relationship between project success and the accuracy of the risk identification, analysis, and measurement process (Selvakumar et al., 2024). Project managers are found to have difficulty managing risks because they are individually responsible for identifying, analyzing, and monitoring risks (Soares et al., 2020). Project managers can use the analytic hierarchy hybrid process (AHP) and artificial neural networks (ANN) to predict the biggest risk factors and strategic decision making in the risk management process (Lin et al., 2022) or with a fuzzy approach (Androshchuk et al., 2020). Based on research (Flyvbjerg et al., 2022) that the risk in terms of cost is higher in IT projects compared to decision makers in organizations and academics.

Cluster 5: Knowledge

In the IS/IT risk management concept, this knowledge is needed to analyze risks, especially in risk assessment and prioritization. Cluster 5 has 17 interrelated terms. This knowledge term can also be associated with research (Hammami et al., 2022). The study conducted knowledge management in health organizations that implement IT. The results of this study indicate that individual knowledge significantly affects IT risk management in the IT governance dimension. The organization needs to understand the importance of knowledge related to cyber risk, security policies, and mitigation (Adriko & Nurse, 2024). The organization also needs to

calculate the optimal IT investment value and, at the same time, consider IT security insurance (Biswas et al., 2024).

Cluster 6: Network, Information Security

In cluster 6, there are 12 interrelated terms. Developing networks in IS/IT elements has provided much space for system users to express their opinions and access information easily (Liu & Wu, 2023). Both physical and social networks must be included in the IS/IT risk management scope (Richter & Ammenwerth, 2023). In cybersecurity, focusing on network monitoring is vital in protecting system security from various incidents. So, there are cyber security standards such as the International Society of Automation/International Electrotechnical Commission (ISA/IEC) 62443 (Pochmara & Świetlicka, 2024).

Cluster 7: Risk Management Performance

In cluster 7, 12 terms were obtained. Based on the researched by (Moreira et al., 2021), which evaluates the performance of the National Institute of Standards and Technology (NIST) framework for IS/IT risk management. Research related to measuring the performance of risk management frameworks in information security is still very challenging because many frameworks have not been tested in many organizations (Prislan et al., 2020). Many other studies have implemented this IS/IT risk management because it improves the organization's performance (Kulathunga et al., 2020).

Research Gap based on Network Map

The recommendations for case studies that can be implemented widely in IS/IT risk management, namely hospitals, banks, and universities (Figure 5). On average, studies related to hospital risks are related to disease risks, medical device risks, etc. The research created by (Wang et al., 2024) shows hospital-based fall inpatient risk management information systems for incident prevention and improving medical team performance. The use of IS/IT in the financial sector is increasingly widespread. The research (Arim & Wamema, 2022) created an improvement framework for e-risk management in Ugandan banks. Investigating information security risk management is also a challenge for banks (Al-Khulaidi et al., 2024). Information security in the education sector is also interesting to discuss further. The research by (Sikorska et al., 2020) created a risk measurement tool for collaboration between industry and universities. Information security at universities is closely related to student profile data, which is the target of the breach (Arista & Ngafidin, 2022).

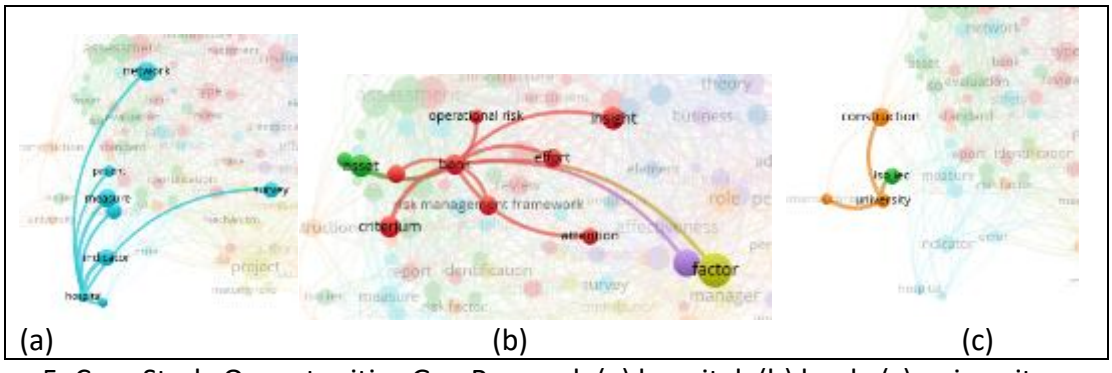

Figure 5. Case Study Opportunities Gap Research (a) hospital, (b) bank, (c) university

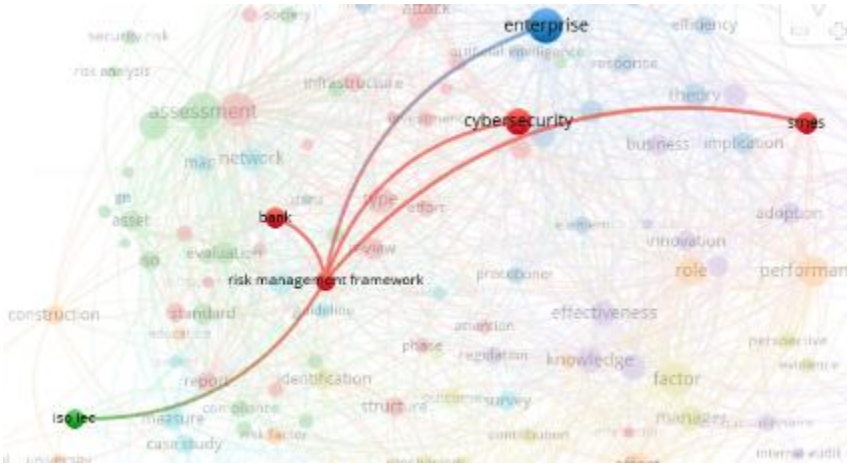

Figure 6. Risk management Framework Connection with Other Terms

Organizations can implementing various methodologies and standards, for example the international organization for standardization (ISO) 27001 (Kitsios et al., 2023), evaluating the Information Security Index (KAMI) (Savitri & Hasibuan, 2024), ISO 31000 (Berrada et al., 2021; Pertiwi & Kusumah, 2023; Sahibu et al., 2024; Sanjaya et al., 2020). Organizations must be able to understand and define the main problems that must be monitored related to cybersecurity culture, planning cyber threat-based risk management, flexibility, and updates in implementing various types of risk management framework that are suitable for application to the organization (Melaku, 2023) (Figure 6).

Conclusions

This research is a literature review that looks at the perspective of a bibliography. Risk management is a framework that can generally be used in various scientific fields to measure multiple types of risks. Therefore, a systematic stage is carried out in finding papers genuinely relevant to IS/IT risk management. 145 terms and 7 clusters have occurrence values and relevance links. The suggestion for previous research is to conduct a trial of the IS/IT risk management framework with a broader scope of case studies and to deepen the existing research. Furthermore, it is necessary to examine further the combination of IS/IT risk management tools with standards, methods, or other tools to improve the quality of the results and performance of the framework.

References

Abdymanapov, S. A., Muratbekov, M., Altynbek, S., & Barlybayev, A. (2021). Fuzzy Expert System of Information Security Risk Assessment on the Example of Analysis Learning Management Systems. *IEEE ACCESS*, *9*, 156556–156565. https://doi.org/10.1109/ACCESS.2021.3129488

Adriko, R., & Nurse, J. R. C. (2024). Cybersecurity, cyber insurance and small-to-medium-sized enterprises: a systematic Review. *INFORMATION AND COMPUTER SECURITY*, *32*(5), 691–710. https://doi.org/10.1108/ICS-01-2024-0025

AL-Dosari, K., & Fetais, N. (2023). Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. *Electronics (Switzerland)*, *12*(17). https://doi.org/10.3390/electronics12173629

Al-Khulaidi, A. A. G., Nasser, A. A., Al-Ashwal, M. H. Y., Al-Ashwal, M. M. Y., & Altayeb, A. M. (2024). Investigating information security risk management in Yemeni banks: An CILOS-TOPSIS approach. *Multidisciplinary Science Journal*, *6*(9). https://doi.org/10.31893/multiscience.2024175

Alotaibi, F. M., Al-Dhaqm, A., Yafooz, W. M. S., & Al-Otaibi, Y. D. (2023). A Novel Administration Model for Managing and Organising the Heterogeneous Information Security Policy Field. *Applied Sciences (Switzerland)*, *13*(17). https://doi.org/10.3390/app13179703

Alshahrani, H. M., Alotaibi, S. S., Ansari, M. T. J., Asiri, M. M., Agrawal, A., Khan, R. A., Mohsen, H., & Hilal, A. M. (2022). Analysis and Ranking of IT Risk Factors Using Fuzzy TOPSIS-Based Approach. *Applied Sciences (Switzerland)*, *12*(12). https://doi.org/10.3390/app12125911

Althobaiti, M. M. (2021). Assessing user's susceptibility and awareness of cybersecurity threats. *Intelligent Automation and Soft Computing*, *28*(1), 167–177. https://doi.org/10.32604/iasc.2021.016660

Androshchuk, A., Yevseiev, S., Melenchuk, V., Lemeshko, O., & Lemeshko, V. (2020). Improvement of project risk assessment methods of implementation of automated information components of non-commercial organizational and technical systems. *EUREKA, Physics and Engineering*, *2020*(1), 48–55. https://doi.org/10.21303/2461-4262.2020.001131

Arim, A., & Wamema, J. (2022). Towards an Improved Framework for E-Risk Management for Digital Financial Services (DFS) in Ugandan Banks: A Case of Bank of Africa (Uganda) Limited. *JOURNAL OF INFORMATION AND ORGANIZATIONAL SCIENCES*, *46*(1), 103–127. https://doi.org/10.31341/jios.46.1.6

Arista, A., & Ngafidin, K. N. M. (2022). An Information System Risk Management of a Higher Education Computing Environment. *International Journal on Advanced Science, Engineering and Information Technology*, *12*(2), 557–564. https://doi.org/10.18517/ijaseit.12.2.13953

Berrada, H., Boutahar, J., & Houssaini, S. E. G. E. (2021). Simplified IT Risk Management Maturity Audit System based on "COBIT 5 for Risk." *International Journal of Advanced Computer Science and Applications*, *12*(8), 641–652. https://doi.org/10.14569/IJACSA.2021.0120875

Biswas, B., Mukhopadhyay, A., Kumar, A., & Delen, D. (2024). A hybrid framework using explainable AI (XAI) in cyber-risk management for defence and recovery against phishing attacks. *DECISION SUPPORT SYSTEMS*, *177*. https://doi.org/10.1016/j.dss.2023.114102

Chundu, B., Masamha, T., & Sifile, O. (2025). Cyber-security governance framework pillars for Zimbabwean local authorities. *COGENT SOCIAL SCIENCES*, *11*(1). https://doi.org/10.1080/23311886.2025.2453094

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *TQM JOURNAL*, *33*(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202

Fauzi, R., & Lubis, M. (2021). Assessment Framework for Defining the Maturity of Information Technology within Enterprise Risk Management (ERM). *International Journal of Advanced Computer Science and Applications*, *12*(10), 680–689. https://doi.org/10.14569/IJACSA.2021.0121075

Flyvbjerg, B., Budzier, A., Lee, J. S., Keil, M., Lunn, D., & Bester, D. W. (2022). The Empirical Reality of IT Project Cost Overruns: Discovering A Power-Law Distribution. *JOURNAL OF MANAGEMENT INFORMATION SYSTEMS*, *39*(3), 607–639. https://doi.org/10.1080/07421222.2022.2096544

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost-benefit analysis into the NIST Cybersecurity Framework via the Gordon-Loeb Model. *JOURNAL OF CYBERSECURITY*, *6*(1). https://doi.org/10.1093/cybsec/tyaa005

Gu, M. H., Yang, L., & Huo, B. F. (2021). The impact of information technology usage on supply chain resilience and performance: An ambidexterous view. *INTERNATIONAL JOURNAL OF PRODUCTION ECONOMICS*, *232*. https://doi.org/10.1016/j.ijpe.2020.107956

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

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability (Switzerland)*, *15*(7). https://doi.org/10.3390/su15075828

Kopencova, D., Rak, R., & Hudecova, V. (2021). Global phenomenon of threats and risk management in management and information technologies. *Issues in Information Systems*, *22*(1), 75–83. https://doi.org/10.48009/1_iis_2021_75-83

Kozlov, A., & Noga, N. (2021). About Some Risks Associated with Subjective Factors, and the Methodology for their Assessment. *Review of Business and Economics Studies*, *9*(3), 94–102. https://doi.org/10.26794/2308-944X-2021-9-3-94-102

Kulathunga, K., Ye, J. M., Sharma, S., & Weerathunga, P. R. (2020). How Does Technological and Financial Literacy Influence SME Performance: Mediating Role of ERM Practices. *INFORMATION*, *11*(6). https://doi.org/10.3390/info11060297

Li, P., & Zhang, L. M. (2025). Application of big data technology in enterprise information security management. *SCIENTIFIC REPORTS*, *15*(1). https://doi.org/10.1038/s41598-025-85403-6

Lin, C.-L., Fan, C.-L., & Chen, B.-K. (2022). Hybrid Analytic Hierarchy Process–Artificial Neural Network Model for Predicting the Major Risks and Quality of Taiwanese Construction Projects. *Applied Sciences (Switzerland)*, *12*(15). https://doi.org/10.3390/app12157790

Liu, Z., & Wu, X. (2023). Structural Analysis of the Evolution Mechanism of Online Public Opinion and its Development Stages Based on Machine Learning and Social Network

Analysis. *International Journal of Computational Intelligence Systems*, *16*(1). https://doi.org/10.1007/s44196-023-00277-8

Magabaleh, A. A., Ghraibeh, L. L., Audeh, A. Y., Albahri, A. S., Deveci, M., & Antucheviciene, J. (2024). Systematic review of software engineering uses of multi-criteria decision-making methods: Trends, bibliographic analysis, challenges, recommendations, and future directions. In *Applied Soft Computing* (Vol. 163). Elsevier Ltd. https://doi.org/10.1016/j.asoc.2024.111859

Melaku, H. M. (2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. *Risks*, *11*(6). https://doi.org/10.3390/risks11060101

Moreira, F. R., Da Silva Filho, D. A., Nze, G. D. A., De Sousa Junior, R. T., & Nunes, R. R. (2021). Evaluating the Performance of NIST's Framework Cybersecurity Controls through a Constructivist Multicriteria Methodology. *IEEE Access*, *9*, 129605–129618. https://doi.org/10.1109/ACCESS.2021.3113178

Muhammad, A. H., Nasiri, A., & Harimurti, A. (2025). Machine learning methods for classification and prediction information security risk assessment. *IAES International Journal of Artificial Intelligence*, *14*(1), 457–465. https://doi.org/10.11591/ijai.v14.i1.pp457-465

Pertiwi, D. E., & Kusumah, L. H. (2023). Identification of operational risk of embedded Subscriber Identity Module (SIM) technology based on ISO 31000: Systematic Literature Review. *Sinergi (Indonesia)*, *27*(2), 193–200. https://doi.org/10.22441/sinergi.2023.2.007

Pochmara, J., & Świetlicka, A. (2024). Cybersecurity of Industrial Systems—A 2023 Report. *Electronics (Switzerland)*, *13*(7). https://doi.org/10.3390/electronics13071191

Prislan, K., Mihelič, A., & Bernik, I. (2020). A real-world information security performance assessment using a multidimensional socio-technical approach. *PLoS ONE*, *15*(9 September). https://doi.org/10.1371/journal.pone.0238739

Ren, S. (2022). Optimization of Enterprise Financial Management and Decision-Making Systems Based on Big Data. *Journal of Mathematics*, *2022*. https://doi.org/10.1155/2022/1708506

Richter, S., & Ammenwerth, E. (2023). IT risk management for medical devices in hospital IT networks: a catalogue of measures and indicators. *BMJ Health and Care Informatics*, *30*(1). https://doi.org/10.1136/bmjhci-2022-100639

Rodríguez-Espíndola, O., Chowdhury, S., Dey, P. K., Albores, P., & Emrouznejad, A. (2022). Analysis of the adoption of emergent technologies for risk management in the era of digital manufacturing. *Technological Forecasting and Social Change*, *178*, 121562. https://doi.org/10.1016/j.techfore.2022.121562

Sahibu, S., Sakti, A., & Iskandar, A. (2024). Risk Management Analysis of SMK Telkom Makassar's Integrated Academic Information System in Compliance with ISO 31000 Standards. *Ingenierie Des Systemes d'Information*, *29*(1), 205–218. https://doi.org/10.18280/isi.290121

Sanjaya, I. G. A. S., Sasmita, G. M. A., & Sri Arsa, D. M. (2020). Information technology risk management using ISO 31000 based on issaf framework penetration testing (Case study: Election commission of x city). *International Journal of Computer Network and Information Security*, *12*(4), 30–40. https://doi.org/10.5815/ijcnis.2020.04.03

Savitri, R., & Hasibuan, M. S. (2024). Information Security Measurement using INDEX KAMI at Metro City. *Journal of Applied Data Sciences*, *5*(1), 33–45. https://doi.org/10.47738/jads.v5i1.152

Sektas-Bilusich, D., Nunes-Vaz, R. A., Chim, L., & Lord, S. (2020). A risk-based framework to inform prioritisation of security investment for insider threats. *International Journal of Safety and Security Engineering*, *10*(1), 49–57. https://doi.org/10.18280/ijsse.100107

Selvakumar, J. J., Suganya, G., Arthi, T. S., & Pachiyappan, S. (2024). Does risk management components influence on project success? Evidence from IT sector. *Journal of Project Management (Canada)*, *9*(3), 269–276. https://doi.org/10.5267/j.jpm.2024.4.001

Shakibazad, M., & Rashidi, A. J. (2020). New method for assets sensitivity calculation and technical risks assessment in the information systems. *IET Information Security*, *14*(1), 133–145. https://doi.org/10.1049/iet-ifs.2018.5390

Sikorska, J., Bradley, S., Hodkiewicz, M., & Fraser, R. (2020). DRAT: Data risk assessment tool for university-industry collaborations. *Data-Centric Engineering*, *1*(2). https://doi.org/10.1017/dce.2020.13

Soares, R. A., Chaves, M. S., & Pedron, C. D. (2020). W4RM: A prescriptive framework based on a wiki to support collaborative risk management in information technology projects. *International Journal of Information Systems and Project Management*, *8*(1), 67–83. https://doi.org/10.12821/ijispm080104

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions. *ELECTRONICS*, *9*(11). https://doi.org/10.3390/electronics9111864

Taherdoost, H. (2021). A Review on Risk Management in Information Systems: Risk Policy, Control and Fraud Detection. *Electronics*, *10*(24), 3065. https://doi.org/10.3390/electronics10243065

Taskin, N., Özkeleş Yıldırım, A., Ercan, H. D., Wynn, M., & Metin, B. (2025). Cyber Insurance Adoption and Digitalisation in Small and Medium-Sized Enterprises. *Information (Switzerland)*, *16*(1). https://doi.org/10.3390/info16010066

Wang, Y., Jiang, M. Y., He, M., & Du, M. J. (2024). Design and Implementation of an Inpatient Fall Risk Management Information System. *JMIR MEDICAL INFORMATICS*, *12*. https://doi.org/10.2196/46501

Yang, X. (2022). Judgment of Social Governance System Risk Based on Big Data Analysis. *Mobile Information Systems*, *2022*. https://doi.org/10.1155/2022/7861756