

# Mapping the Landscape of Information Security Risk Management Research: A Bibliometric Analysis Using VOS Viewer and Power BI

Norshima Humaidi\*, Nurhafizah Zainal and Amirul Afif Muhamat

<sup>1</sup> Faculty of Business and Management, Universiti Teknologi MARA (UiTM) Selangor, Puncak Alam Campus, Malaysia

\*Corresponding author: norshima958@uitm.edu.my

**Abstract:** Effective risk management is crucial for businesses to mitigate a wide array of threats. This paper conducts a bibliometric analysis of information security risk management literature spanning two decades, from 2000 to early 2025. Using the Web of Science (WoS) database, 418 English-language journal articles were reviewed. Visualizations using VOS viewer and Power BI offer insights into publication trends, co-citations, keywords, authors, journals and contributing countries. The analysis identifies four thematic clusters reflecting key areas in information security risk management research. The findings highlight significant growth in this field over the past 25 years, with expectations for continued international expansion and knowledge advancement.

**Keywords:** Bibliometrics, Information Security, Risk Management, WoS, VOS viewer, Power BI

## 1 Introduction

In today's interconnected business environment, information is recognized as one of the most valuable assets for organizations. The quality, authenticity, relevance, and uniqueness of information significantly influence a business's competitive standing and operational success. However, the increasing intricacy of digital ecosystems has amplified the exposure of information assets to risks, making effective management of information security a top priority for organizations. According to the World Economic Forum [1], complexity in cybersecurity reduces visibility and increases vulnerability to human error and attacks. Consolidating security tools into a unified platform is crucial for eliminating blind spots and improving efficiency. Additionally, the rise in cyber threats is a significant concern, as highlighted by Malaysia's Prime Minister Datuk Seri Anwar Ibrahim, who cited that 93% of cyber leaders believe geopolitical instabilities will likely lead to a catastrophic cyber event in the next two years [2].

Therefore, effectively managing information security risks is essential for safeguarding organizational information assets. This process not only protects sensitive data but also reinforces an organization's corporate image, which is a vital component of its branding and reputation [3]. A strong corporate image enables organizations to respond effectively to dynamic external factors, such as evolving cyber threats and regulatory requirements.

Moreover, a well-managed information security strategy enhances organizational resilience and competitiveness [4]. By addressing potential risks and ensuring the integrity of information systems, companies can adapt quickly to changing conditions, strengthen stakeholder trust, and achieve sustainable growth. Additionally, a secure and trustworthy information environment supports diversification efforts, empowering enterprises to explore new markets and expand their product offerings without compromising their operational integrity.

Although various analysis tools are available, as listed in Table 1, this study employs bibliometric analysis using VOS viewer to offer a comprehensive overview of the research landscape, identify research gaps, highlight trends, and suggest future directions in information security risk management. The study also provides a detailed analysis using VOS viewer related to key authors, institutions,

journals, publications and citation and co-citation analysis on the topic. The bibliometric analysis of managing information security risk also provides important insights to policymakers and practitioners to make informed decisions with regards to resource allocation and value creation. Moreover, using bibliometric analysis on managing information security risk provides valuable insights into the current state of research in the field and highlights research gaps, research trends, future directions, themes and informed policy decisions related to managing information security risk. As the field of risk management in the context of information security continues to evolve, new research questions and perspectives emerge, which may require updated bibliometric analyses to fully understand the current state of the field.

Furthermore, the study aims to analyse various aspects of scholarly publications from the Web of Science (WoS) database. This includes analysing patterns, trends, authorships relationships within and between bibliographic data, citation and co-citation analysis and collaborations. By analysing patterns in publication and citation data, bibliometric reviews can provide insights into the impact and influence of researchers, institutions and even entire fields of study. The analysis would help future researchers in conducting quantitative or qualitative research on risk management related to information security. The articles used in the study are retrieved from WoS data which shows only 14 articles for risk management related to information security from 2000 to 2007 and which increases to 404 results by 2008 as shown in Table 2.

**Table 1.** Analysis Tools for Bibliometric Research

| No. | Criteria      | VOS viewer                                                                                                                        | CiteSpace                                                                                               | Power BI                                                                                                                                                                                                      | Gephi                                                                                                |
|-----|---------------|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| 1.  | Purpose       | Primarily used for constructing and visualizing bibliometric networks, such as citation, co-citation, and co-authorship networks. | An open-source software for network visualization and analysis.                                         | A business analytics tool by Microsoft, used for data visualization and business intelligence.                                                                                                                | An open-source software for network visualization and analysis.                                      |
| 2.  | Strength      | Preferably for text mining and creating co-occurrence networks of terms from scientific literature.                               | Suitable for detecting emerging trends and sudden bursts of activity in research.                       | Integrates well with various data sources, provides robust data analysis, and interactive dashboards.                                                                                                         | Supports large-scale network analysis and offers various layout algorithms for better visualization. |
| 3.  | Visualisation | Offers detailed and interactive visualizations of bibliometric maps.                                                              | Provides temporal visualizations and cluster views, highlighting key areas of research.                 | It offers a variety of visualization options that can be combined into interactive dashboards, allowing users to explore the data dynamically and gain deeper insights into bibliometric patterns and trends. | Highly versatile with numerous options for editing and customizing network visualizations.           |
| 4.  | Customisation | Customized visualizations to highlight important nodes and connections.                                                           | Tailored visualizations to emphasize co-citation networks, keyword co-occurrences, and citation bursts. | Power BI allows extensive customization for business reports and dashboards, while Gephi offers detailed options for visualizing complex network structures.                                                  | Rank nodes by metrics such as degree centrality or PageRank.                                         |

Source: Authors

**Table 2.** Usage of the Risk Management Related to Information Security Term In the Academic Writings

| Used in Title                            | Source | Total of Academic Writings |             |             |             |            |
|------------------------------------------|--------|----------------------------|-------------|-------------|-------------|------------|
|                                          |        | 2000 - 2005                | 2006 - 2011 | 2012 - 2017 | 2018 - 2023 | 2024 -2025 |
| Information Security AND Risk Management | WoS    | 14                         | 74          | 112         | 180         | 38         |

Source: Authors

## 2 Literature Review

### 2.1 Information security threats in digital business environments

As a desirable intangible resource, information is increasingly vulnerable to a range of threats, including cybersecurity risks and intellectual property misappropriation [5]. The growing reliance on digital platforms has heightened the exposure of intangible assets to various risks, making their protection a strategic priority for organizations. Recent study has demonstrated the importance of intangible assets for various dimensions of firm's economic performance [6]. However, the protection of these assets is inadequate; only 19% of organizations insure their intangible assets compared to 60% for tangible assets [7]. This disparity highlights the need for businesses to recognize and mitigate the risks associated with their intangible resources.

Cybersecurity threats are particularly pronounced, as they pose the primary risk to intangible assets in modern enterprises. Companies often lack awareness of the value of their intangible resources, leading to insufficient protective measures against potential breaches [5]. Furthermore, the phenomenon of key personnel taking proprietary information when transitioning to new roles exacerbates the leakage of valuable intangible assets. Moreover, threats can be categorized in various ways depending on the framework of scientific investigation and the format in which informational resources are maintained [8]. According to Pawel [9], threats can be classified as follow:

- i. Threats associated with the use of information technology (IT) and techniques.
- ii. Threats related to the IT model used in the business entity.
- iii. Threats caused by the human factor, directly related to deliberate and non-deliberate human actions, both in the area of techniques, technologies, and the IT model.

Nowadays, modern information resources are mostly stored in digital form. A document is a sequence of bits with specific informational content [10]. Consequently, new IT techniques and technologies are employed to manage, process, and archive information. This development arises both from the capabilities provided by modern IT solutions, such as artificial intelligence, data analysis, visualization, and archiving and the necessity to handle the growing volume of information [11].

Threats arising from information sharing on the Internet have driven the evolution of research in information security management. The rise of the IT market has led to the emergence of various threats that can compromise information resources. These threats encompass a wide range of areas where vulnerabilities may occur, highlighting the need for businesses to be vigilant in protecting their intangible assets. With the continuous development of technology, newer methods to seize or irreparably damage information resources are increasingly observed. This evolution has resulted in the formation of new and previously unrecognized sub-areas that require focused attention regarding the safeguarding of intangible assets that engenders a security culture [12].

The global trend in information protection is increasingly characterized by a continuous “virtual struggle” between employees developing security solutions and those attempting to breach them [13]. This dynamic reflects the evolving landscape of cybersecurity, where organizations must remain vigilant against a backdrop of sophisticated threats. The perception of information security is closely linked to the IT model employed by a specific business entity. Until the early 21st century, the predominant method for managing digital information involved establishing an internal IT infrastructure within enterprises [13]. This infrastructure encompassed all devices necessary for the storage, archiving, and processing of digital resources, along with application solutions that included both general components (such as operating systems, email systems, and office software) and sector-specific applications (like CAD, graphic design, financial, and accounting software). This approach is commonly referred to in the literature as the traditional model.

In this traditional model, particularly among larger enterprises, dedicated IT departments were responsible for managing these internal IT facilities. This management included overseeing hardware and software installations, ensuring data security, and maintaining operational efficiency. However, this model often operated under a “castle-and-moat” philosophy, where external threats were kept at bay through perimeter defences such as firewalls and intrusion detection systems. While this approach provided a sense of security for internal resources, it also created vulnerabilities, particularly regarding insider threats and lateral movements by cyber attackers once they breached the perimeter defences [14 – 15].

As businesses evolve and increasingly adopt cloud-based solutions and hybrid environments, the limitations of the traditional IT model become more apparent. The shift towards cloud computing necessitates a re-evaluation of security strategies to address new challenges posed by remote access and mobile workforces. Consequently, organizations must adapt their information security practices to align with contemporary technological advancements while safeguarding their digital assets effectively.

The traditional IT model has played a significant role in shaping the perception of information security within enterprises. However, as the landscape continues to change with technological advancements, businesses must reconsider their approaches to information management and security to remain resilient against emerging threats.

## 2.2 *The role of risk management in reducing information security threats*

Information security encompasses the processes and methodologies aimed at safeguarding sensitive information from unauthorized access, ensuring its confidentiality, integrity, and availability—commonly referred to as the CIA triad [16 – 17]. This triad serves as a cornerstone of information security, emphasizing three critical objectives: protecting data from unauthorized disclosure (confidentiality), maintaining the accuracy and reliability of information (integrity), and ensuring that information is accessible to authorized users when needed (availability) [18].

Information security risk management is a critical component of a comprehensive information security program. It is a systematic process encompassing the identification, analysis, and response to potential threats to organizational information assets [16]. This process involves evaluating the likelihood and potential impact of security threats and implementing appropriate strategies, such as mitigation, transfer, acceptance, or avoidance, to manage those risks. Within an information security program, risk management plays a pivotal role, often aligning with the principles of the CIA triad (Confidentiality, Integrity, and Availability) to guide organizations in prioritizing threats and vulnerabilities.

Furthermore, risk management provides a structured framework for evaluating and prioritizing threats based on their potential impact and likelihood of occurrence [19]. This enables efficient resource allocation, focusing on mitigating the most critical risks. For example, risk assessments can identify system vulnerabilities, such as outdated software, unprotected endpoints, or inadequate access controls, enabling the implementation of targeted solutions like regular patch management, advanced threat detection systems, or multi-factor authentication. Critically, risk management also facilitates compliance with industry best practices and regulatory requirements, thereby minimizing the risk of penalties.

The iterative nature of risk management also fosters adaptability. As new cyber threats emerge, organizations can continuously update their risk assessments and security measures, staying ahead of potential adversaries and safeguarding sensitive information. By identifying vulnerabilities before they are exploited, risk management reduces the probability of severe incidents such as data breaches, ransomware attacks, or insider threats [17]. It also minimizes the financial and operational impact of security incidents through pre-established mitigation strategies, such as disaster recovery plans and incident response protocols [19]. For instance, implementing real-time monitoring and early warning systems can help organizations detect and respond to threats before they escalate into major crises. Moreover, risk management provides a clear understanding of acceptable risk levels, enabling businesses to avoid excessive risk-taking and make informed decisions about their cybersecurity investments [20].

A well-implemented risk management strategy not only strengthens security but also protects an organization's reputation. Data breaches or security failures can erode customer trust, damage relationships with stakeholders, and lead to significant financial and legal repercussions. Conversely, demonstrating a commitment to robust security through proactive risk management enhances customer confidence and positions the organization as a reliable and trustworthy partner [20].

Moreover, effective cybersecurity risk management enhances an organization's ability to manage incidents transparently and professionally, thereby mitigating reputational damage. For example, a timely and well-coordinated response to a breach, supported by pre-established risk management protocols, can reassure stakeholders and preserve the organization's integrity in the market. Based on above reviews, it is shown that risk management serves as a critical mechanism for improving cybersecurity protection, reducing major risks, and safeguarding business reputation. By systematically addressing vulnerabilities and preparing for potential threats, organizations can build a resilient security infrastructure that not only protects sensitive information but also supports long-term business growth and stakeholder trust.

## 2.3 *Bibliometric Studies on Information Security (2020–2025)*

In recent years, several studies have used bibliometric analysis to map the intellectual landscape of information security and cybersecurity research. Such analyses apply tools like VOS viewer, CiteSpace and bibliometric to large publication datasets (e.g., from WoS or Scopus) to identify

research trends, prolific authors, collaboration networks and emerging themes. This study summarizes five bibliometric analyses conducted between 2020 and 2025, focusing on information security and cybersecurity. It outlines key details such as the title, year, authors, focus, methodologies, data sources, significant findings, and identified research gaps or future directions. A summary of these studies is presented in Table 3.

**Table 3.** Summarise of Bibliometric Studies on Information Security

| Study (Reference)                                                              | Focus/Scope                                                                                                                       | Bibliometric Methods/Tools                                                                                                                                                                                | Data Source                                                                                  | Key Findings / Trends                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Research Gaps / Future Directions                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sharma et al. 2023 [21]<br><i>Cybersecurity &amp; Forensics</i>                | Cybersecurity and cyber forensics research (2011–2021); mapping a decade of digital security literature.                          | Co-authorship, co-citation, citation and keyword analysis using full vs. fractional counting; timeline trends and burst detection (CiteSpace-like approach).                                              | Web of Science (WoS), 2011–2021 publications.                                                | Steady growth in cybersecurity/forensics publications over the decade.<br>Top contributors identified: key authors, institutions, countries leading the field.<br>Major topics include anomaly detection, malware analysis, cyber-attacks, machine learning in security.<br>Collaboration networks show global research clusters (with certain countries forming hubs).                                                                                                                                                                                        | Points out under-investigated areas at the intersection of cybersecurity and forensics.<br>Emphasizes need for future work linking preventative security and post-incident forensics.<br>Provides a decade-long baseline to guide future research directions in emerging cybersecurity threats.                                                                                                          |
| Arroyabe et al. 2024 [22]<br><i>Cybersecurity &amp; Digitalization in SMEs</i> | Intersection of SME digitalization and cybersecurity – how digital transformation in small businesses relates to security issues. | Bibliometric (R) used for co-occurrence (keyword) clustering and citation analysis. Four main thematic clusters identified via co-word analysis.                                                          | WoS + Scopus (417 papers, up to ~2022) on “SMEs + cybersecurity/digitalization”.             | Research splits into 4 clusters: (1) Industry 4.0 & smart factories, (2) Industry 4.0 & SMEs, (3) SMEs & cybersecurity practices, (4) SME digitalization & entrepreneurship.<br>Increasing digitalization - higher cyber risk for SMEs, but current literature often treats these topics separately (tech adoption vs. security).<br>Few studies integrate business innovation and security preparedness, indicating a silo effect.                                                                                                                            | Identifies a gap: lack of integrated studies on SME digitalization and security.<br>Predicts cybersecurity in SMEs will emerge as its own research stream, distinct from general digitalization research.<br>Recommends bridging the gap by focusing future research on security as an integral part of SME digital transformation strategies.                                                           |
| Guembe et al. 2025 [23]<br><i>AI for Cyberattack Detection</i>                 | Artificial Intelligence in cybersecurity, specifically AI-driven cyberattack and intrusion detection (2014–2024).                 | Comprehensive bibliometric review using Bibliometric/Bibliophagy (R). Co-authorship networks, keyword co-occurrence maps, and citation metrics analysed. Also used dominance factor for author influence. | Scopus (2014–2024): 2,338 documents (journals, conferences, etc.) on AI-based cyber defence. | Machine learning & deep learning are the dominant approaches in cybersecurity, showing rapid growth in research interest.<br>USA is the top-producing country, with India, China and others also major contributors. Strong collaboration networks among leading countries (USA–China–Europe etc.).<br>High impact work from countries like Canada and Italy despite fewer papers (high citations per paper).<br>Keywords show emphasis on network security, intrusion detection, IoT security, federated learning, etc., indicating trending research topics. | Calls for future research in federated learning and privacy-preserving AI to secure IoT/IoMT systems.<br>Notes the need to address emerging threats (e.g., adversarial attacks on AI) and to integrate AI with privacy/security by design.<br>Suggests strengthening international collaborations and interdisciplinary approaches (combining AI with domain knowledge) to tackle complex cyber threats. |

| Study (Reference)                                                          | Focus/Scope                                                                                                                    | Bibliometric Methods/Tools                                                                                                                                                                | Data Source                                                                      | Key Findings / Trends                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Research Gaps / Future Directions                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Judijanto et al. 2024 [24]<br><i>Global Cybersecurity Research Mapping</i> | Global landscape of cybersecurity research (2010–2024); evolution of research themes and international collaboration patterns. | VOS viewer used for network visualization (co-authorship, co-word, co-citation networks). Analysed publication counts, collaborative networks and topic clusters over time.               | Scopus (2010–2024): cybersecurity-related publications worldwide.                | Dramatic growth in cybersecurity publications over the period, reflecting rising importance of security R&D. Shift in focus from basic IT security to advanced tech integration: recent literature heavily features AI, IoT, blockchain in cybersecurity context. Global collaboration network is mapped: USA, China, India, Germany, UK are key hubs driving research and cooperating internationally. Highlights the field's increasingly interdisciplinary nature (technical, human, policy angles) to address complex cyber challenges.                                                                                               | Stresses the need for continuous innovation and broad collaboration to keep pace with evolving threats. Recommends interdisciplinary approaches in future research – integrating fields (technical and human factors) and expanding analytical frameworks. Suggests using more diverse data sources (beyond just one index, and including real-time threat data) in bibliometric analyses to fully capture the fast-changing cybersecurity landscape. |
| Erdoğan & Akmeşe 2025 [25]<br><i>Cybercrime Research Trends</i>            | Cybercrime studies (2000–2023); literature on illegal cyber activities (hacking, cyber fraud, etc.) and countermeasures.       | Bibliometric (R) and Excel for bibliometric analysis. Examined publication trends, prolific authors, top journals, citation counts; visualized author and country collaboration networks. | Web of Science (2000–2023): 2,566 publications on “cybercrime” related keywords. | Steady long-term growth in cybercrime research output as cyber threats proliferate. Top author: K. Jaishankar (21 papers) – a leading scholar in cyber criminology. Leading journal: <i>IEEE Access</i> (151 papers on cybercrime); indicates a tech-oriented approach to cybercrime issues is common. Most-cited work on Stuxnet (cyber warfare), showing crossover between cybercrime and national security topics. Major contributing institutions and countries identified (e.g., strong output from certain universities and cross-country collaborations visualized); reflects an international research effort against cybercrime. | Provides a baseline for future cybercrime research, helping identify less-explored topics. Implies need for further study in emerging crime areas (e.g., AI-enabled crimes, crypto crimes) as well as underrepresented regions, though specific future directions are general. Emphasizes using these findings to guide policy and research focus, given the dynamic nature of cybercrime (“moving target” requiring ongoing study).                  |

### 3 Methodology

Bibliometrics is a specialized field within library and information sciences that applies quantitative techniques to bibliographic data, such as publication and citation metrics, by utilizing sophisticated statistical methodologies [26 – 27]. This approach plays a crucial role in providing an objective, data-driven overview of a collection of bibliographic documents, facilitating the analysis of research patterns and trends. The application of bibliometric analysis is invaluable for understanding various research components, such as authorship dynamics, institutional contributions, geographic patterns, journal performance and emerging research topics. It also allows for the exploration of collaboration networks and the intellectual structure of scientific disciplines [28 – 29].

This study employs bibliometric analysis to investigate the current state of research in managing information security risks. Bibliometric methods are increasingly gaining recognition for their capacity to unravel complex data and uncover meaningful insights from large sets of scholarly works, which

would be difficult to achieve through traditional qualitative approaches. By systematically evaluating a vast array of publications, citation patterns and collaborative relationships, this study provides a detailed mapping of the research landscape. Such an approach not only identifies emerging trends and knowledge gaps but also offers valuable guidance to researchers, practitioners and policymakers seeking to make informed decisions in this field.

The study specifically adopts a five-step literature review process, widely utilized by prominent scholars in the domain, to ensure a comprehensive and structured analysis of the selected articles [30 – 31]. This method is essential for selecting relevant studies, synthesizing findings and offering a robust framework for future investigations. The systematic nature of this approach guarantees that the bibliometric analysis is rigorous and that the insights derived are both reliable and actionable, thereby enhancing the impact and significance of this research.

The five-steps in the analysis of the article are as follows:

#### *Step 1: Rationale for selection of time period*

The articles included in this review span a period of two decades, from 2000 to 2025. This time frame was selected due to the significance and evolving nature of the topic under investigation. While the initial search covered the period from 2000, the analysis focuses specifically on publications from 2015 onward. This decision is based on the observation that a substantial body of research on risk management and information security has emerged since 2015. A preliminary search of the Web of Science (WoS) database revealed a limited number of relevant publications for the selected keywords between 2000 and 2004. Therefore, the final timeframe for this bibliometric analysis was determined by the research question, the study objectives, and the availability of a sufficient and robust dataset.

#### *Step 2: Rationale for selection of database*

The WoS database was selected for this study due to its comprehensive and high-quality collection of academic literature, making it an ideal resource for conducting bibliometric analysis. WoS provides access to a wide range of scholarly sources, including journals, conference proceedings and books, across various disciplines, ensuring that the analysis covers an extensive pool of research in the domain of information security risk management. The database's rigorous selection criteria for indexing publications guarantee the inclusion of reputable and impactful research, which enhances the reliability of the findings.

One of the primary reasons for choosing WoS is its robust citation tracking capabilities. The ability to track citations and identify citation relationships between articles enables a deeper understanding of the influence and interconnectedness of research across different studies. This is particularly important for mapping the intellectual structure of the field, identifying seminal works and recognizing key authors and research clusters (Zhu & Liu, 2020). WoS also provides advanced search functionalities, allowing for precise filtering of research articles based on keywords, publication years, authorship and other relevant criteria. This ensures that only the most pertinent literature is selected for analysis, thus increasing the quality and relevance of the bibliometric review.

Furthermore, WoS supports citation and co-citation analysis, which is crucial for identifying trends in the evolution of the field and understanding collaboration patterns across institutions, countries and research network. This capability not only enables a systematic exploration of how research topic have developed over time but also allows researcher to track the emerging trends and themes within specific areas of study. By selecting WoS, this study ensures a comprehensive, high-quality and methodologically sound approach to bibliometric analysis, strengthening the credibility and significance of the results.

#### *Step 3: Rationale for paper selection*

The WoS Core Collection database was utilized with the keywords ALL = ("Risk management" AND "Information security") to retrieve all scientific documents pertinent to these topics. A search using these keywords yielded over 889 documents published between 2000 and 2025. After refining the results to include only articles published in English, a total of 418 papers were selected for this study.

The use of English-language articles in this study was primarily due to the authors' proficiency in English, which allowed for a comprehensive and accurate analysis of the retrieved documents. While the WoS Core Collection database includes publications in multiple languages, limiting the search to English articles ensures that the authors can fully understand and assess the content of each paper. Given that English is the predominant language of academic publishing in the field of information security risk management, focusing on English-language articles provides a more reliable and consistent dataset for the analysis. Additionally, the authors' expertise in English ensures that key themes, methodologies, and findings in the selected papers are accurately interpreted and integrated into the study.

*Step 4: Review using VOS viewer and Power BI analysis*

Any scientific field requiring investigation must employ an appropriate science mapping technique [32]. While numerous programs are available for this purpose, the most widely recognized include VOS viewer, Gephi, Citespace, HistCite, and Sci2. For this bibliometric analysis, VOS viewer was utilized as per Table 1. This software generates two-dimensional maps based on mathematical techniques, making it a valuable tool in many bibliometric studies. It provides insightful graphical representations of network data and can display the structure and interconnections among various categories of data, including authors, references, keywords, journals, organizations, and countries. Additionally, it illustrates diverse relationships such as co-authorship, co-occurrence, citation, bibliographic coupling, and co-citation [33].

A co-occurrence analysis of author keywords was conducted using VOS viewer to identify prevalent terms and their interrelationships, focusing on keywords that appeared together within the same publications. Following data cleaning, both VOS viewer and Power BI were employed to analyse the literature corpus on information security risk management from 2000 to 2025. Power BI, leveraging its flexibility in handling data from databases like WoS, was used for descriptive analysis, including institutional, national, and disciplinary trends. VOS viewer was used to construct a co-occurrence network of all keywords extracted from the dataset. This network visualization facilitated a deeper understanding of the conceptual links and research foci within the field.

A detailed citation and co-citation analysis was conducted on the 418 articles retrieved from the WoS database. In addition to analysing definitions for conceptual clarification, a fundamental analysis was performed on various categories, including the number of publications, journals, countries, authors, universities, sectors, and the different research tools employed. Tables summarizing these findings were generated using Power BI desktop software. The data were subsequently exported to VOS viewer Software (version 1.6.20), where visual representations were created to facilitate inferences regarding interrelationships. Distance-based maps were constructed in VOS viewer, with the distance between two nodes reflecting the strength of the relationship between them [34].

*Step 5. Research gaps identified*

Through a comprehensive review and rigorous bibliometric analysis, several key research gaps were identified in the field of information security risk management. These gaps highlight areas where existing research is limited, and they provide valuable insights into where future research efforts should be focused to advance the field. The identification of these gaps not only deepens our understanding of the current landscape but also reveals critical opportunities for further exploration.

## 4 Results

Following the methodological framework suggested by Qudah et al. [32], the results are presented in three subsections: (1) Publication Analysis, (2) Co-occurrence Analysis, and (3) Cluster Analysis.

### 4.1 Exploring Information Security Risk Management: A Publication Analysis

Evaluating publishing activity involves counting the number of articles published by a specific unit (journals, publisher, countries and etc.) within a given period of time. Indicators of publication activity enable us to identify the most representative journals, publishers, countries, area of research categories, as well as a picture of the quantitative evolution and structure of the topic under examination. Power BI desktop software was used to evaluate the publishing activity based on their frequency calculation. Meanwhile, VOS viewer software was used to visualise the network connection between countries and authors from different institutions and companies.

A total of 418 journal articles related to information security risk management, published between 2000 and early 2025, were retrieved from the Web of Science (WoS) database. The findings indicate exponential growth in the literature on this topic in recent years. As illustrated in Figure 1, publication activity was relatively low from 2000 to 2007, averaging 3 to 4 publications annually. A notable increase occurred in 2008 ( $n = 19$ ), followed by a slight decrease in 2009 ( $n = 11$ ). However, since 2015, publication numbers have steadily risen: 2016 ( $n = 20$ ), 2017 ( $n = 25$ ), and 2018 ( $n = 30$ ). A minor dip occurred in 2019 ( $n = 20$ ), followed by substantial growth, peaking in 2020 ( $n = 26$ ), 2021 ( $n = 29$ ), 2022 ( $n = 35$ ), and 2023 ( $n = 40$ ). In 2024, the number of publications slightly decreased ( $n = 37$ ). Only one publication was found in January 2025. The increased publication activity from 2020 to 2025 likely reflects the growing importance of information security risk management as businesses increasingly rely on digital platforms. This publication trend is summarized in Figure 1.



**Figure 1.** Total of Publications Activity from 2000 until 2025

The retrieved articles were published in 233 different scholarly sources. This analysis identifies the most significant and productive institutions and explores their interrelationships. Table 4 presents the top 10 journals based on the total number of publications related to information security risk management. Computers & Security leads with 28 publications, followed by the Information Security Journal (n = 16), the Handbook of System Safety and Security (n = 11), IEEE Access (n = 11), and Information and Computer Security (n = 11). The remaining five journals each contributed fewer than 10 publications. Most of these articles were indexed in the Web of Science under the Science Citation Index Expanded (SCIE), Emerging Sources Citation Index (ESCI), and Social Sciences Citation Index (SSCI).

**Table 4.** Top Ten Journals with Highest Total of Publication Activities (2000 – 2025)

| Top Ten Journals                                                                                                                                                         | Total of Publication |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| Computers & Security                                                                                                                                                     | 28                   |
| Information Security Journal                                                                                                                                             | 16                   |
| Handbook of System Safety and Security: Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems | 11                   |
| IEEE Access                                                                                                                                                              | 11                   |
| Information and Computer Security                                                                                                                                        | 11                   |
| International Journal of Information Security                                                                                                                            | 9                    |
| Journal of Information Security And Applications                                                                                                                         | 8                    |
| International Journal of Advanced Computer Science and Applications                                                                                                      | 7                    |
| International Journal of Computer Science and Network Security                                                                                                           | 6                    |
| IET Information Security                                                                                                                                                 | 5                    |
| International Journal of Information Management                                                                                                                          | 5                    |

Table 5 shows the Top 10 journals with the highest citation on information security risk management. Computers & Security journal has highest total citations (n = 882) compared to other journals. This journal also has highest total of publications related to information security risk management. This indicated that many of the articles published in Computer & Security journals will get many citations of their works.

**Table 5.** Top Ten Journals with Highest Citation (2000 – 2025)

| Top 10 Journal       | Times Cited, WoS Core |
|----------------------|-----------------------|
| Computers & Security | 882                   |
| MIS Quarterly        | 391                   |

| Top 10 Journal                                              | Times Cited, WoS Core |
|-------------------------------------------------------------|-----------------------|
| International Journal of Information Management             | 327                   |
| Information & Management                                    | 191                   |
| International Journal of Critical Infrastructure Protection | 170                   |
| Journal of Management Information Systems                   | 167                   |
| Information Systems Research                                | 156                   |
| Decision Support Systems                                    | 141                   |
| International Journal of Information Security               | 111                   |
| Journal of Information Security and Applications            | 90                    |

Figure 2 presents the most productive research areas in information security risk management, as categorized by Web of Science. Computer Science and Information Systems is the leading category, with 187 publications, followed by Management with 61. Other prominent categories include Computer Science, Theory & Methods (n = 46); Information Science & Library Science (n = 45); Computer Science, Software Engineering (n = 41); and Computer Science, Interdisciplinary Applications (n = 31). Several categories have fewer than 30 publications each: Engineering (n = 26), Telecommunications (n = 26), Business & Finance (n = 19), and Computer Science, Artificial Intelligence (n = 19).



**Figure 2.** The most important area research on Information Security Risk Management (*Source: WoS Research Category Analysis*)

Most of these journals published by Emerald Group Publishing (n = 32), followed by Springer (n = 29) and Elsevier Advanced Technology (n = 28). The summaries of the Top 10 Publisher were shown in Table 6.

**Table 6.** Top 10 Publisher With Highest Total of Publications

| Top Ten Publisher                              | Total Publication |
|------------------------------------------------|-------------------|
| Emerald Group Publishing Ltd                   | 32                |
| Springer                                       | 29                |
| Elsevier Advanced Technology                   | 28                |
| Elsevier                                       | 25                |
| MDPI                                           | 25                |
| Taylor & Francis Inc                           | 22                |
| IEEE-Inst Electrical Electronics Engineers Inc | 15                |
| IGI Global                                     | 12                |
| Syngress                                       | 11                |
| Elsevier Sci Ltd                               | 9                 |

Total of 101 publications were from USA, followed by China (n = 24), England (n = 18), Australia and India (n = 14), South Korea (n = 13), Spain and Taiwan (n = 12). Other countries has less than 10 publications. Table 7 and Figure 3 summarises this information.

**Table 7.** Top 10 Most Productive Countries Publishing on Information Security Risk Management

| Top 10 Country | Total of Publications |
|----------------|-----------------------|
| USA            | 101                   |
| China          | 24                    |
| England        | 18                    |
| Australia      | 14                    |
| India          | 14                    |
| South Korea    | 13                    |
| Spain          | 12                    |
| Taiwan         | 12                    |
| Canada         | 10                    |
| Norway         | 10                    |

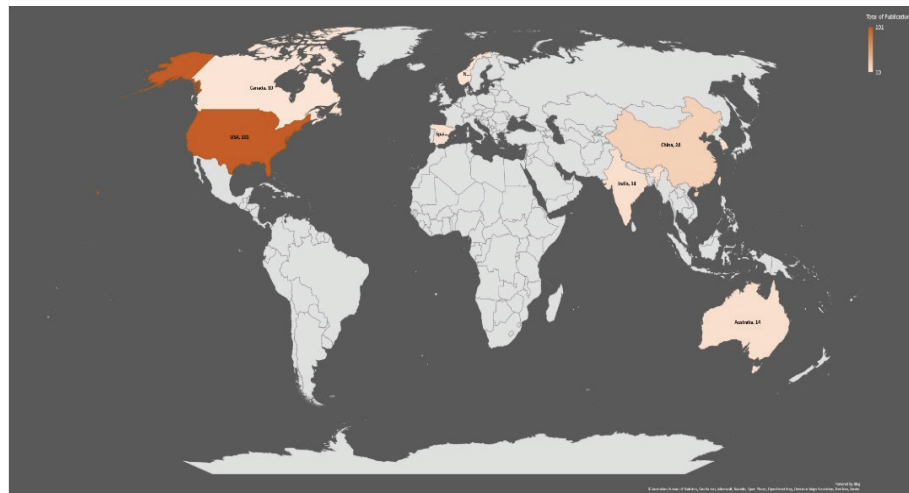


**Figure 3.** Top 10 Most Productive Countries Publishing on Information Security Risk Management

Figure 4 illustrates the network of international collaboration among contributing countries. This visualization includes countries with at least one publication, displaying the 100 most prominent bibliographic connections. Nodes, represented by labels and circles, vary in size to reflect their relative importance, with larger nodes indicating greater research output. Connecting lines represent collaborative links between countries, while the spatial proximity of nodes indicates the strength of their relationships. A key benefit of this visualization is its ability to identify clusters of countries with shared research interests. The analysis reveals five distinct clusters, often comprising countries from the same continent.

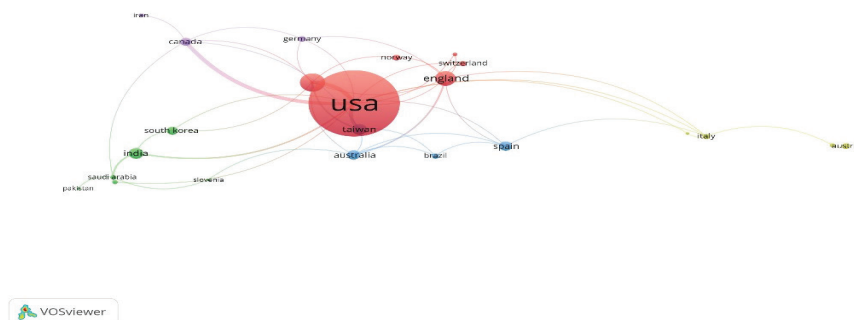


**Figure 4.** Cooperation Network Between Countries in Information Security Risk Management

The 10 most significant authors are listed in Table 8, ranked according to the total number of publications they wrote as first author and the number of their papers being cited in WoS database. Throughout the review period, each of the top authors at least produced one journal article related to information security risk management. The two (2) authors who has the most citations impact were Schuett J., n = 332 and Massimino B., n = 238.

**Table 8.** The Top 10 Most Essential Authors of Publications Related to Information Security Risk Management from 2000 to 2025 in the WoS Database Core Collection

| First Author Full Name | Total of Publication | Total of Citation | Article Title and Doi                                                                                                                                                                                                                                                 |
|------------------------|----------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Schuett, Jonas         | 1                    | 332               | Risk Management in the Artificial Intelligence Act<br><b>DOI:</b> 10.1111/risa.17665<br><b>Summary:</b> Analyzes Article 9 of the EU AI Act, focusing on its risk management provisions.                                                                              |
| Massimino, Brett       | 1                    | 238               | On the Inattention to Digital Confidentiality in Operations and Supply Chain Research<br><b>DOI:</b> 10.1111/poms.12983<br><b>Summary:</b> Discusses the lack of focus on digital confidentiality in operations and supply chain management literature.               |
| Knowles, William       | 1                    | 229               | A Survey of Cyber Security Management in Industrial Control Systems<br><b>DOI:</b> 10.1016/j.ijcip.2015.02.002<br><b>Summary:</b> Explores cybersecurity management practices in industrial control systems.                                                          |
| Uddin, Md. Hamid       | 1                    | 214               | Cybersecurity Hazards and Financial System Vulnerability: A Synthesis of Literature<br><b>DOI:</b> 10.1016/j.ijcip.2015.02.002<br><b>Summary:</b> Reviews literature on cybersecurity risks affecting financial systems.                                              |
| Tarei, Pradeep Kumar   | 2                    | 202               | Benchmarking the Relationship Between Supply Chain Risk Mitigation Strategies and Practices: An Integrated Approach<br><b>DOI:</b> 10.1108/BIJ-12-2019-0523<br><b>Summary:</b> Proposes a framework linking risk mitigation strategies to practices in supply chains. |
| Etemadi, Nilofar       | 1                    | 198               | An ISM Modelling of Barriers for Blockchain/Distributed Ledger Technology Adoption in Supply Chains Towards Cybersecurity<br><b>DOI:</b> 10.1145/3450588.3450600<br><b>Summary:</b> Identifies barriers to adopting blockchain for cybersecurity in supply chains.    |
| Shiau, Wen -Lung       | 1                    | 196               | What Are the Trend and Core Knowledge of Information Security? A Citation and Co-Citation Analysis<br><b>DOI:</b> 10.1016/j.im.2023.103774<br><b>Summary:</b> Analyzes trends and core knowledge areas in information security research.                              |
| Culot, Giovanna        | 1                    | 189               | The ISO/IEC 27001 Information Security Management Standard: Literature Review and Theory-Based Research Agenda<br><b>DOI:</b> 10.1108/TQM-09-2020-0202<br><b>Summary:</b> Provides a literature review and research agenda for the ISO/IEC 27001 standard.            |
| Fenz, Stefan           | 5                    | 166               | Information Security Risk Management: In Which Security Solutions Is It Worth Investing?<br><b>DOI:</b> 10.28963/ais.2011.022<br><b>Summary:</b> Evaluates the effectiveness of various security solutions in risk management.                                        |
| Di Lernia, Cary        | 1                    | 165               | Cyber-Related Risk Disclosure in Australia: Evidence from the ASX200<br><b>DOI:</b> 10.3316/agispt.20200324027433<br><b>Summary:</b> Investigates the disclosure of cyber-related risks among Australian companies.                                                   |

Source: Author

## 4.2 Trends and Future Research on Information Security Risk Management

### 4.2.1. Co-occurrence of Keyword Analysis

This analysis was performed to outline the significant developments in risk management within the information security disciplines and to identify potential research avenues. Specifically, it explored the interconnections between research topics and the emergence of new sub-fields. Employing the text mining capabilities of VOS viewer, keywords were extracted from titles, abstracts, and citation contexts [34]. This software constructs a comprehensive network map of phrase co-occurrences (adjective-noun pairs) [32], where frequently co-occurring terms are positioned closer together. VOS viewer's clustering function then groups keywords based on their co-occurrence patterns.

For this analysis, a keyword frequency threshold of 10 occurrences was applied to balance comprehensiveness and noise reduction, resulting in 65 keywords meeting this criterion from an initial pool of 1670. The study also re-ran the clustering with thresholds of 8 and 12. The core clusters and their thematic labels remained stable (variation less than 5%). From these, 18 keywords were selected based on total link strength (Table 9). The keyword co-occurrence analysis revealed four distinct clusters, differentiated by color-coding (Table 9 and Figure 5). The first cluster (red) centres on risk management frameworks, encompassing terms such as "Governance" and "Performance." The second cluster (green) focuses on risk management processes within information security. The third cluster (blue) addresses security risks and system vulnerabilities. Finally, the fourth cluster (yellow) explores issues related to information security and privacy.

**Table 9.** Keywords Analysis Results

| Keywords                                                                             | Links | Total Links Strength | Occurrences |
|--------------------------------------------------------------------------------------|-------|----------------------|-------------|
| <b>Cluster 1 (Red Coding) : Information System Risk Governance &amp; Performance</b> |       |                      |             |
| Framework                                                                            | 17    | 55                   | 28          |
| Governance                                                                           | 11    | 22                   | 11          |
| Impact                                                                               | 14    | 47                   | 21          |
| Management                                                                           | 15    | 62                   | 38          |
| Performance                                                                          | 12    | 32                   | 17          |
| Technology                                                                           | 10    | 23                   | 13          |
| Information Security Management                                                      | 11    | 21                   | 19          |
| <b>Cluster 2 (Green Coding): Integrated Risk Assessment &amp; Analysis</b>           |       |                      |             |
| Computer Security                                                                    | 9     | 21                   | 10          |
| Cybersecurity                                                                        | 16    | 71                   | 47          |
| Risk Analysis                                                                        | 10    | 23                   | 14          |
| Risk Assessment                                                                      | 12    | 48                   | 35          |
| <b>Cluster 3 (Blue Coding): Risks &amp; Vulnerability</b>                            |       |                      |             |
| Risks                                                                                | 13    | 60                   | 30          |
| Security                                                                             | 16    | 87                   | 57          |
| Systems                                                                              | 12    | 46                   | 27          |
| Vulnerability                                                                        | 11    | 26                   | 14          |
| <b>Cluster 4 (Yellow Coding): Information Security &amp; Privacy</b>                 |       |                      |             |
| Cloud Computing                                                                      | 6     | 11                   | 11          |
| Information Security                                                                 | 17    | 185                  | 159         |
| Privacy                                                                              | 12    | 26                   | 16          |

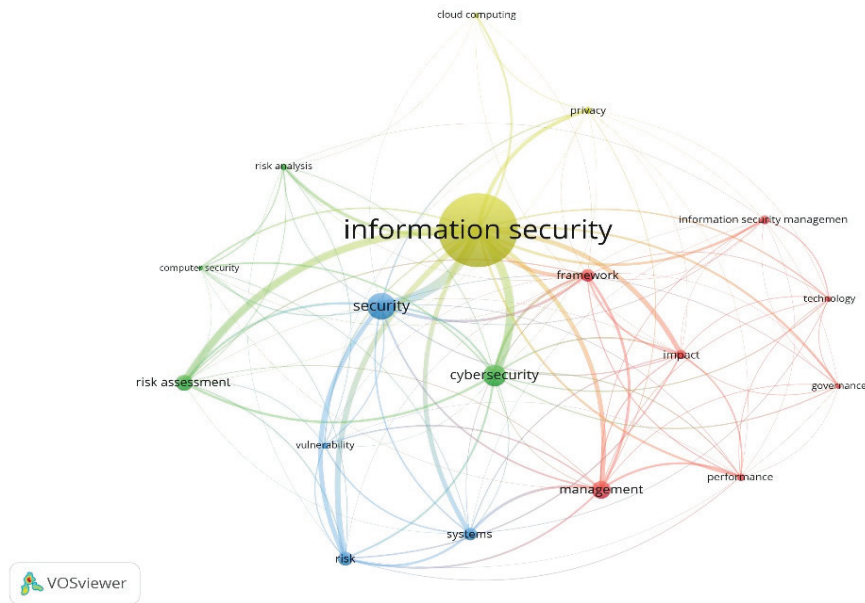


**Figure 5.** Keyword Analysis Results

**Notes (Figure 5):**

*High Connectivity:* Terms like “Information Security” and “Security” are highly linked, indicating their foundational roles across multiple clusters.

*Cross-Cluster Relevance:* Keywords such as “Risk” and “Management” connect multiple themes, reflecting their broad applicability in the field.

*Cluster Differentiation:* Each cluster represents a specific aspect of cybersecurity, from high-level frameworks to specific vulnerabilities and emerging technologies.

### 4.3 Unresolved and Emerging Issues

The trends indicate two main categories affecting information security: unresolved and emerging issues. Unresolved issues are challenges and problems from the past that persist, preventing management from fully resolving them. Emerging issues, on the other hand, represent the latest concerns in the field.

Issues related to information security risk are critical. Historically, information was recorded manually, but with the advent of computers, the internet, and now AI, the need to share and store information on hard drives or in the cloud has become essential. Consequently, the safety and integrity of information have always been, and continue to be, top priorities.

Nevertheless, in Malaysia, information security threats, such as ransomware and data breaches, can be highlighted as significant concerns in this area.

## 5 Cluster Analysis Discussion

The VOS viewer analysis has identified four distinct clusters, each representing a thematic area related to information security risk management. Each cluster groups keywords based on their co-occurrence patterns, total link strength, and connections with other keywords. These clusters highlight the interconnectedness of frameworks, processes, vulnerabilities, and privacy concerns, suggesting that an integrated approach is essential for addressing the challenges in managing information security risk in today's business environments. The discussion of each cluster was provided.

### *Cluster 1: Information System Risk Governance & Performance*

Table 9 summarizes the seven keywords in Cluster 1: “Framework,” “Governance,” and “Performance” emerge as central themes, which along with their frequencies and link strengths. This cluster captures the essential components of a comprehensive risk management framework, which guides organizations in planning, implementing, and continuously improving their risk treatment processes [18].

In established information-security standards such as ISO 27005 and the NIST Risk Management Framework (RMF), risk management is structured around context establishment, risk assessment, risk treatment and ongoing monitoring. For example, ISO 27005 emphasizes the systematic identification, analysis and evaluation of risks to support informed decision-making, while NIST RMF prescribes integrating security controls and continuous authorization to maintain an acceptable risk posture. The bibliometric prominence of terms like “Governance” and “Performance” reflects this alignment: effective governance structures (e.g., defined roles and policies) ensure that risk treatment activities adhere to organizational objectives, and performance metrics (e.g., key risk indicators) track the efficacy of controls over time [35].

A clear understanding of potential risk consequences underpins this framework, as organizations that identify, analyse and mitigate threats while also exploiting opportunities safeguard their assets and enhance business performance [18, 35]. Moreover, embedding governance mechanisms (such as risk committees or steering groups) fosters accountability and strengthens alignment between risk appetite and strategic goals.

Building on ISO 27005’s emphasis on iterative risk assessment and NIST’s focus on automation, future research should look at how data analytics, AI, and automation tools can be integrated into each stage of the risk management lifecycle. This will help to improve real-time risk identification through AI-driven threat-intelligence platforms and streamline control implementation and monitoring with automated workflows across heterogeneous IT environments. Future study should also look into how well these technology-enhanced frameworks perform in a variety of contexts, such as manufacturing, healthcare, and financial services, by evaluating factors like organizational size, regulatory requirements, and threat landscape to tailor ISO 27005 and NIST RMF principles to the needs of each industry. Finally, new governance models, like risk orchestration platforms, should be explored, along with the creation of advanced performance metrics that use predictive analytics to foresee control failures before they occur.

#### *Cluster 2: Integrated Risk Assessment and Analysis*

Table 9 presents the four keywords in Cluster 2: “Risk Assessment,” “Risk Analysis,” “Computer Security” and “Cybersecurity” among its most prominent along with their frequencies and link strengths. This cluster reflects the end-to-end process by which organizations identify, evaluate and prioritize information-security risks, drawing direct parallels to ISO 27005’s distinction between risk assessment (risk identification and evaluation) and risk analysis (in-depth examination of root causes, interdependencies and cascading effects), as well as to NIST SP 800-37’s RMF steps of “Categorize”—“Assess”—“Authorize” and “Monitor.”

In ISO 27005, risk assessment begins with context establishment and identification of assets, threats and vulnerabilities, then evaluates each risk’s likelihood and impact to determine its priority. Risk analysis follows, using qualitative or quantitative techniques to uncover underlying factors and potential knock-on effects. NIST’s RMF similarly embeds these activities in its “Assess” phase, where security control effectiveness is evaluated, and in its “Monitor” phase, which continuously feeds back new threat intelligence into the assessment/analysis loop. The inclusion of “Cybersecurity” as a core keyword underscores how digital-platform reliance makes cyber-specific scenarios, such as malware intrusion or distributed-denial-of-service attacks as a critical sub-process within the broader risk lifecycle.

For future studies, building on ISO 27005’s iterative assessment model and NIST RMF’s continuous monitoring, future studies should investigate dynamic cybersecurity-risk simulation models that integrate real-time threat intelligence feeds to re-prioritize risks on the fly. Research might also explore how emerging techniques, such as adversarial-machine-learning testing or blockchain-based audit trails, which can enhance the fidelity of risk analysis, while evaluating their interoperability with established risk-management processes across different regulatory environments. Previous study had highlighted the lack of standardized method for conducting risk analysis during incidents, therefore a new model should be proposed for incident risk analysis, which provides a structured approach to identify, assess and manage risks in diverse incident scenarios [36].

#### *Cluster 3: Risks and Vulnerabilities*

There are four keywords listed under Cluster 3: “Risks”, “Security”, “Systems” and “Vulnerability”. The information security landscape has become increasingly complex, with the proliferation of advanced technologies, such as cloud computing, Internet of Things (IoT), and 5G, as well as the growing interconnectedness of digital systems across organizations. The information’s security risks and vulnerability clusters focus on the critical threats and vulnerabilities that organization face in safeguarding their digital assets, including Information technology (IT) systems, operational technology used in industrial control systems, and the wider digital infrastructure and services utilized by the organization [37].

Under ISO 27005, vulnerability management is part of the risk identification phase, in which organizations catalogue and assess weaknesses in people, processes and technology. Similarly, NIST SP 800-30, the Guide for Conducting Risk Assessments, and NIST SP 800-40, the Vulnerability Management Guide, recommend continuous scanning, prioritization of vulnerabilities according to likelihood and impact, and timely remediation to maintain an acceptable risk posture.

As organizations increasingly interconnect IT systems with operational technology in industrial control environments and cloud-delivered services, a vulnerability in one domain can cascade through the enterprise. This cluster therefore underscores the need for integrated risk and vulnerability management processes that combine ISO 27005's structured risk assessment lifecycle with NIST's guidance on automated threat-intelligence integration and patch-management workflows [38].

Future studies should examine how vulnerabilities propagate in converged IT and OT environments, evaluating mitigation strategies that draw on ISO 27005's controls-selection guidance and NIST's vulnerability-prioritization metrics. Research on cross-sector vulnerability patterns will help map common exploit chains in industries such as finance, healthcare and manufacturing, revealing shared best practices and informing sector-specific adaptations of ISO and NIST frameworks. Finally, scholars should explore adaptive vulnerability management techniques, such as artificial-intelligence-driven discovery tools and blockchain-based patch-audit trails. This will help to enhance the speed and effectiveness of vulnerability remediation within established ISO 27005 and NIST processes.

#### *Cluster 4: Information Security and Privacy*

Table 9 presents the three key terms in Cluster 3: "Cloud Computing," "Information Security" and "Privacy". The modern digital landscape has brought about unprecedented levels of connectivity and convenience, but it has also introduced a range of challenges related to information security and user privacy. Central to this cluster is the pressing need to protect sensitive data and ensure the privacy of individuals, especially in the context of emerging technologies such as cloud computing. ISO/IEC 27701 builds on this framework by focusing on privacy information management, offering guidelines for consent management, data minimization and transparency. In contrast, ISO/IEC 27001 emphasizes a systematic approach to information security management, requiring organizations to identify and address security threats effectively.

The use of cloud computing services has undoubtedly brought about significant social and economic benefits, but it has also introduced potential privacy and security concerns for individuals and businesses [39]. The shared computing environments, ubiquitous data storage, and internet-based access inherent to cloud computing have made information more vulnerable to misuse, making privacy a major concern for organizations adopting cloud services [40]. To safeguard the confidentiality, integrity, and availability of data stored or processed in shared infrastructure, NIST SP 800-53 offers controls for cloud-based deployments, including stringent access control, encryption, and ongoing monitoring. By connecting organizational practices to privacy outcomes and governance frameworks, the NIST Privacy Framework simultaneously provides a methodology for managing privacy risks. When combined, these standards help practitioners create policies that guarantee data is properly classified, encrypted both in transit and at rest, and only available to authorized users.

One of the key issues that cloud computing faces is the threat of insider malicious attacks, where employees of the cloud provider may potentially compromise the security and privacy of the stored data, even without the provider's knowledge [41]. Additionally, the lack of transparency in the agreements between cloud providers and consumers can exacerbate these concerns, as users may not fully understand the extent of their data's protection.

Future research should address the privacy risks posed by cloud computing, focusing on insider threat mitigation strategies and data transparency in cloud contracts. A promising area for investigation could be the development of privacy-preserving techniques, such as differential privacy and secure multi-party computation, that safeguard user data in cloud environments. Furthermore, research on user behaviour and its impact on privacy risks could provide valuable insights into how individuals and organizations perceive and mitigate privacy-related threats.

## **6 Implication**

The integrity of information is paramount for any organization, underscoring the need for robust risk management planning across all industries. While the financial industry in Malaysia has historically led the way in prioritizing data protection, other sectors that manage sensitive personal information, such as healthcare, education and retail, must also recognize the critical importance of safeguarding

their data assets. As cyber threats grow in sophistication and frequency, the implications of effectively managing information security risks extend beyond mere compliance, impacting organizational resilience, stakeholder trust, and long-term sustainability [20, 42].

### *6.1 Implications for industry*

For industries, managing information security risks fosters a culture of proactive preparedness, ensuring organizations can identify and mitigate threats before they escalate. Effective risk management enhances operational continuity by preventing disruptions caused by cyber incidents, such as data breaches or ransomware attacks [16, 42]. Additionally, industries that prioritize robust information security frameworks are better positioned to meet regulatory requirements, avoid legal penalties, and maintain a competitive advantage in the marketplace.

In sectors handling sensitive data, such as healthcare and education, failure to implement comprehensive risk management measures can result in significant reputational damage and financial loss. Conversely, organizations with strong risk management practices demonstrate accountability and trustworthiness, which can enhance their market reputation and attract more customers, partners, and investors [19]. Moreover, as digital transformation accelerates across industries, managing information security risks ensures smoother adoption of new technologies without exposing organizations to heightened vulnerabilities.

### *6.2 Implications for Academia*

In academia, managing information security risks plays a critical role in fostering research integrity and protecting institutional data. Universities and research institutions often handle highly sensitive information, including intellectual property, personal student and staff data, and collaborative research findings. A robust risk management framework safeguards these assets from unauthorized access, ensuring the confidentiality and integrity of academic records and research outputs.

From an academic research perspective, the study and development of effective information security risk management strategies contribute to the broader body of knowledge, driving innovation in cybersecurity practices. Furthermore, integrating information security risk management into academic curricula equips future professionals with the knowledge and skills required to address evolving cybersecurity challenges, bridging the gap between academic theory and practical application.

### *6.3 Bridging academia and industry*

The implications of managing information security risks extend beyond individual domains, fostering collaboration between academia and industry. Academic research can inform industry practices, enabling organizations to adopt cutting-edge security solutions tailored to emerging threats. Similarly, industry partnerships provide real-world data and case studies for academia, enriching research and education in cybersecurity risk management.

This synergy supports the development of innovative tools and frameworks that benefit both sectors, ensuring they remain resilient against increasingly complex cyber threats. As a result, managing information security risks not only protects organizational assets but also drives progress and innovation in the broader cybersecurity landscape.

## **7 Conclusion**

Based on the findings from the VOS viewer and Power BI analysis, the following suggestions for future studies can be made to address the gaps and to explore the underdeveloped areas within the themes identified.

Future studies should concentrate on creating and evaluating flexible frameworks for information system risk governance and performance that can adapt to changing organizational needs and quickly changing cyberthreats. These frameworks should be based on the continuous monitoring procedures of NIST RMF and the governance principles of ISO 27005. Scholars can investigate how integrating emerging technologies, such as artificial intelligence for predictive risk analytics and automated control orchestration, enhances framework effectiveness and resilience. Furthermore, studying the governance mechanisms that promote cross-industry adoption will provide important insights into how performance metrics and collaborative governance models enhance business continuity and security outcomes, especially in high-risk industries like finance and healthcare.

Research in Cluster 2 should focus on improving risk assessment and analysis. Future studies should evaluate the role of advanced technologies and analytics in enhancing the precision of risk assessment and analysis. Longitudinal studies are recommended to measure the long-term effectiveness of specific risk management practices in mitigating cybersecurity threats. Emphasis should be placed on tailoring these processes for small and medium enterprises (SMEs), which often face resource constraints in implementing sophisticated cybersecurity measures. Moreover, exploring human factors, such as the impact of Security Education Awareness Training Programs (SETA) and organizational culture, is crucial to enhancing risk management practices.

Cluster 3 highlights the critical nature of security risks and system vulnerabilities, particularly within the financial sector. Future research should prioritize industry-specific security solutions, such as healthcare cybersecurity strategies and fraud prevention measures for international transactions. Furthermore, the integration of emerging technologies and the complex interdependencies between systems should be carefully studied to minimize potential risks.

Focused on information security and privacy, Cluster 4 emphasizes the relevance of Malaysia's Personal Data Protection Act (PDPA) in safeguarding personal information. While cloud computing offers numerous benefits, it introduces risks such as data breaches, which future research should address by examining privacy regulations and exploring privacy-preserving technologies like homomorphic encryption. Additionally, user awareness and attitudes toward privacy policies and educational programs should be assessed to enhance privacy practices.

Future research should adopt a multidisciplinary approach that combines technical, organizational, and human factors to develop holistic cybersecurity strategies. Emerging threats, such as deepfake technologies and quantum computing, should be prioritized, with benchmarking metrics employed to assess these risks effectively. Research should address the needs of both large corporations and SMEs, ensuring that solutions are scalable and adaptable.

In a conclusion, future studies should integrate multidisciplinary perspectives to develop comprehensive cybersecurity solutions. By addressing existing knowledge gaps and proactively anticipating future challenges, these studies can contribute significantly to advancing the field of cybersecurity as threats and technologies evolve.

## Acknowledgement

We would like to express our heartfelt gratitude to the Faculty of Business and Management, Universiti Teknologi MARA (UiTM) Selangor, Malaysia for their unwavering support in enabling the researchers to carry out this research. The provision of invaluable resources and facilities played a crucial role in the successful completion of this study.

## References

- [1] World Economic Forum. (2024, October 22). *Why strong cybersecurity means we must reduce complexity*. <https://www.weforum.org/stories/2024/10/strong-cybersecurity-reduce-complexity-risk-cyber/>
- [2] Selangor Journal. (2023, July 10). *Rise of cybersecurity threats a significant concern — PM*. <https://selangorjournal.my/2023/07/rise-of-cybersecurity-threats-a-significant-concern-pm/>
- [3] Syed, B., & Shahid, M. (2022). Impact of information security management system on firm financial performance: Perspective of corporate reputation and branding. *American Journal of Industrial and Business Management*, 12(5), 934-954. doi:10.4236/ajibm.2022.125048.
- [4] Xie, X., Wu, Y., Palacios-Marqués, D., & Ribeiro-Navarrete, S. (2022). Business networks and organizational resilience capacity in the digital age during COVID-19: A perspective utilizing organizational information processing theory. *Technological Forecasting and Social Change*, 177, 121548. <https://doi.org/10.1016/j.techfore.2022.121548>
- [5] Mavani, C., Patel, R., Mistry, H., & Goswami, A. (2024). The role of cybersecurity in protecting intellectual property. *International Journal on Recent and Innovation Trends in Computing and Communication*, 12(2), 529-538.
- [6] Jacqueline, J., Luky, P. W., & Anastasia, F. I. (2024). The impact of intangible asset and research and development on firm value. *Journal of Accounting, Entrepreneurship and Financial Technology (JAEF)*, 5(2). <https://doi.org/10.37715/jaef.v5i2.4553>

- [7] Norris, B. (2024, May 8). *Intangible asset value higher than tangible but protection gap persists*. Commercial Risk. <https://www.commercialriskonline.com/intangible-asset-value-higher-than-tangible-but-protection-gap-persists/>
- [8] Ikrissi, G., & Mazri, T. (2021). IOT-based smart environments: State of the art, security threats and solutions. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, XLVI-4/W5-2021*(4), 279–286. <https://doi.org/10.5194/isprs-archives-xlvi-4-w5-2021-279-2021>
- [9] Pawel, K. (2021). Human factor aspects in information security management in the traditional IT and cloud computing models. *Operations Research and Decisions, 1*, 62–76. <https://doi.org/10.37190/ord210104>
- [10] Meiser, L. C., Nguyen, B. H., Chen, Y.-J., Nivala, J., Strauss, K., Ceze, L., & Grass, R. N. (2022). Synthetic DNA applications in information technology. *Nature Communications, 13*(1), 352. <https://doi.org/10.1038/s41467-021-27846-9>
- [11] Alzoubi, N. (2024). Using information technology management with artificial intelligence techniques. *Journal of Lifestyle and SDGs Review, 5*(2), e03013. <https://doi.org/10.47172/2965-730x.sdgsreview.v5.n02.pe03013>
- [12] Metin, B., Duran, S., Telli, E., Mutluturk, M., Wynn, M. (2024). IT risk management: Towards a system for enhancing objectivity in asset valuation that engenders a security culture. *Information, 15*(55), 1-27. <https://doi.org/10.3390/info15010055>
- [13] Pretorius, R., & Blaauw, D. (2022). Digital risk management: Investigating human-factor security with a Behaviorist Approach. *International Conference on Cyber Warfare and Security, 17*(1), 513–521. <https://doi.org/10.34190/icws.17.1.64>
- [14] Birchwood University. (2024). Zero trust vs. traditional network security: What's the difference? *Birchwood University*. Retrieved from <https://www.birchwoodu.org/zero-trust-vs-traditional-network-security/>
- [15] Security Info Watch. (2024). Traditional IT security vs. cloud security: Which approach is right for your business? *Security Info Watch*. Retrieved from <https://www.securityinfowatch.com/cybersecurity/information-security/article/21089929/traditional-it-security-vs-cloud-security-which-approach-is-right-for-your-business>
- [16] Al-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMEs): A Meta-Analysis Approach. *Electronics, 12*(17), 3629. <https://doi.org/10.3390/electronics12173629>
- [17] Brunner, M., Sauerwein, C., Felderer, M., & Breu, R. (2020). Risk management practices in information security: Exploring the status quo in the DACH region. *Computers & Security, 92*, 101776. <https://doi.org/10.1016/j.cose.2020.101776>
- [18] Whitman, M., & Mattord, H. (2021). *A Model Curriculum for Programs of Study in Information Security/ Cybersecurity March 2021*. <https://www.kennesaw.edu/coles/centers/cyber-center/resources/docs/model-curriculum-2021>
- [19] Alsafwani, N., Fazea, Y., & Alnajjar, F. (2024). Strategic approaches in network communication and information security risk assessment. *Information, 15*(6), 353. <https://doi.org/10.3390/info15060353>
- [20] Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2022). Developing a risk analysis strategy framework for impact assessment in information security management systems: A case study in IT consulting industry. *Sustainability, 14*(3), 1269. <https://doi.org/10.3390/su14031269>
- [21] Sharma, D., Mittal, R., Sekhar, R., Shah, P., & Renz, M. (2023). A bibliometric analysis of cyber security and cyber forensics research. *Results in Control and Optimization, 10*, 100204. <https://doi.org/10.1016/j.rico.2023.100204>
- [22] Arroyabe, M. F., Arranz, C. F., De Arroyabe, J. C. F., & Fernandez, I. (2024). Digitalization and Cybersecurity in SMEs: A Bibliometric analysis. *Procedia Computer Science, 237*, 80–87. <https://doi.org/10.1016/j.procs.2024.05.082>
- [23] Guembe, B., Misra, S., Azeta, A., & Lopez-Baldominos, I. (2025). Bibliometric analysis of artificial intelligence cyberattack detection models. *Artificial Intelligence Review, 58*(6). <https://doi.org/10.1007/s10462-025-11167-0>
- [24] Judijanto, L., Endrianto, E., & Vandika, A. Y. (2024). Mapping the Cybersecurity Research through Bibliometric Analysis. *West Science Information System and Technology, 2*(03), 374–382. <https://doi.org/10.58812/wsist.v2i03.1534>
- [25] Erdoğan, M., & Akmeşe, Ö. F. (2025). Bibliometric analysis of studies on cyber crimes between 2000-2023. *ADBA Computer Science, 2*(1), 19-29. <https://doi.org/10.69882/adba.cs.2025014>

- [26] Broadus, R. N. (1987). Toward a definition of ‘bibliometrics.’ *Scientometrics*, 12(5–6), 373–379. <https://doi.org/10.1007/BF02016680>
- [27] Pritchard, A. (1969). Statistical bibliography or bibliometrics? *Journal of Documentation*, 25, 348–349.
- [28] Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, 133, 285–296. <https://doi.org/10.1016/j.jbusres.2021.04.070>
- [29] Merigó, J. M., Pedrycz, W., Weber, R., & de la Sotta, C. (2018). Fifty years of *Information Sciences*: A bibliometric overview. *Information Sciences*, 432, 245–268. <https://doi.org/10.1016/j.ins.2017.11.054>
- [30] Seuring, S., Müller, M., Westhaus, M., & Morana, R. (2005). Conducting a literature review—the example of sustainability in supply chains. In *Research Methodologies in Supply Chain Management*, 91–106.
- [31] Dohale, V., Gunasekaran, A., Akarte, M. M., & Verma, P. (2020). Twenty-five years’ contribution of “Benchmarking: an International Journal” to manufacturing strategy: a scientometric review. *Benchmarking: An International Journal*, 27(10), 2887–2908. <https://doi.org/10.1108/BIJ-05-2019-0208>
- [32] Qudah, S. M. A. A., Fuentes-Bargues, J. L., & Ferrer-Gisbert, P. S. (2024). Bibliometric analysis of the literature on risk management in the construction sector: Exploring current and future trends. *Ain Shams Engineering Journal*, 15(8), 102843. <https://doi.org/10.1016/j.asej.2024.102843>
- [33] Li, J., Goerlandt, F., & Reniers, G. (2021). An overview of scientometric mapping for the safety science community: Methods, tools, and framework. *Safety Science*, 134, 105093. <https://doi.org/10.1016/j.ssci.2020.105093>
- [34] Van Eck, N. J., & Waltman, L. (2010). Software survey: VOS viewer, a computer program for bibliometric mapping. *Scientometrics*, 84(2), 523–538. <https://doi.org/10.1007/s11192-009-0146-3>
- [35] Domański, Jarosław, “Risk categories and risk management processes in nonprofit organizations.” *Foundations of Management*, vol. 8, no. 1, pp. 227–42, Jan., 2016. <https://doi.org/10.1515/fman-2016-0018>.
- [36] Couce-Vieira, Aitor, et al., (2017). GIRA: A General Model for Incident Risk Analysis. *Journal of Risk Research*, 22(2), 191–208. <https://doi.org/10.1080/13669877.2017.1372509>.
- [37] Yaacoub, J. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, 21(1), 115–158. <https://doi.org/10.1007/s10207-021-00545-8>
- [38] Dube, D. P., & Mohanty, R. (2018). Towards development of a Cyber Security Capability Maturity Model (CSCMM). *International Journal of Business Information Systems*, 34(1). <https://doi.org/10.1504/ijbis.2020.10014790>
- [39] Porwal, S., Nair, S. K., & Dimitrakos, T. (2011). Regulatory Impact of Data Protection and Privacy in the Cloud. In S. Porwal, S. K. Nair, & T. Dimitrakos, *IFIP advances in information and communication technology* (p. 290). Springer Science+Business Media. [https://doi.org/10.1007/978-3-642-22200-9\\_23](https://doi.org/10.1007/978-3-642-22200-9_23)
- [40] Chawki, M. (2024). An effective cloud computing model enhancing privacy in cloud computing. *Information Security Journal a Global Perspective*, 1–24. <https://doi.org/10.1080/19393555.2024.2307637>
- [41] Asiri, N. (2024). Security and privacy issues in Cloud Storage. In N. Asiri, arXiv (Cornell University). Cornell University. <https://doi.org/10.48550/arxiv.2401.04076>
- [42] Chen, H., & Hai, Y. (2024). Exploring the critical success factors of information security management: a mixed-method approach. *Information and Computer Security*, 32(5), 545–572. <https://doi.org/10.1108/ics-03-2023-0034>