Indexed in Clarivate Analytics WoS, and ScienceOPEN

E-B Environment - Behaviour Proceedings Journal

ITMAHuB2023

https://kppim.uitm.edu.my/research/conferences/itmahub-2023

2nd International Conference on Information Science, Technology, Management, Humanities, and Business

Hotel UiTM, Shah Alam, Malaysia, 26-27 Sep. 2023

Organised by College of Computing, Informatics and Mathematics, UiTM, Malaysia

Implementation of Information Security Management Systems for Data Protection in Organizations: A systematic literature review

Siti Suhaida Marhad, Siti Zaleha Abd Goni, Mad Khir Johari Abdullah Sani

School of Information Science, College of Computing, Informatics, and Mathematics,
Universiti Teknologi MARA, Puncak Perdana Campus, 40150, Selangor

sitisuhaida93@gmail.com, sitizaleha.ag@gmail.com, madkhirjohari@uitm.edu.my
Tel: +6019-2437884

Abstract

This systematic literature review investigates the implementation of Information Security Management Systems (ISMS) as a pivotal strategy for safeguarding organizational information in the digital era. Focusing on key factors influencing ISMS implementation, its impact on data protection, and the methodologies employed, the review underscores the significance of awareness and training in fostering compliance. Emphasizing the ISO/IEC 27001 standard as a prevalent framework, the study reveals positive impacts on organizational performance, financial outcomes, corporate reputation, and branding. The findings advocate for a comprehensive and structured approach to information security, urging future research to explore diverse organizational contexts and industries for a nuanced understanding of ISMS practices and their impact on organizational agility.

Keywords: Information Security Management Systems, Information Security Management, ISO/IEC 27001, Data protection in organization.

DOI: https://doi.org/10.21834/e-bpj.v9iSI18.5483

1.0 Introduction

In light of today's technological advancements and digitalization initiatives, the most important asset of any individual or organization is information (Amini et al., 2021). The swift progress of countries toward the information society has resulted in the rapid rise of information systems and services, as well as the emergence of new types of organizations known as virtual organizations, which are primarily information-based (Soomro et al., 2016). In conjunction with this, information security (IS) is one of the most crucial challenges in today's business environment. The issue of information system security, and consequently, information as a critical resource in today's information society, is one that all organizations in all industries face in some way. Many organizations have implemented a continuous, structured, and systematic security approach to manage and protect an organization's information from undermining individuals by establishing security policies, processes, procedures, and IS organizational structures to ensure that information remains secure (Nurazean et al., 2019). Despite this, security threats, incidents, vulnerabilities, and risks continue to plague many organizations (Arbanas and Zajdela Hrustek, 2019), with a lack of understanding of information system security key success factors being one of the root causes (Mirtsch et al., 2021). IS, which includes system development and execution, is, therefore, a key success factor that can assist organizations in managing how to concentrate scarce resources on those factors that truly impact success, saving time and money,

eISSN: 2398-4287 © 2024. The Authors. Published for AMER and cE-Bs by e-International Publishing House, Ltd., UK. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/). Peer–review under responsibility of AMER (Association of Malaysian Environment-Behaviour Researchers and cE-Bs (Centre for Environment-Behaviour Studies), College of Built Environment, Universiti Teknologi MARA, Malaysia.
DOI: https://doi.org/10.21834/e-bpj.v9iSI18.5483

adding value, and further enabling operational business. Importantly, ensuring that organizations are resilient against internal and external threats can enhance organizational agility. This notion of IS is becoming increasingly clear and defined. Indeed, organizations are becoming more and more aware of the importance of adopting a comprehensive system and recruiting competent human resources. These studies aim, in particular, to ensure better data protection through implementing or setting up an ISMS while preserving the confidentiality, integrity, and availability of organizational information. Thus, the variables driving ISMS adoption, the impact of ISMS itself, and how ISMS is deployed must be prioritized.

2.0 Literature Review

2.1 Information Security Management Systems

A recent study by Nurazean et al. (2021) demonstrates the deployment of ISMS in an organization that necessitates a significant amount of people, time, and monetary resources. There are several definitions of information security management systems (ISMS), but the common basis of these definitions is trust and confidence in the secure and accurate operation of systems and processes. ISMS is defined by Fonseca-Herrera et al. (2021) as a tool for managing and controlling security information that consists of a systematic, documented process that is known by the entire organization. Similarly, Bouziani et al. (2022) concluded that the ISMS is a collection of tools, documents, and procedures aimed at developing and implementing an IS policy tailored to an organization's needs and specifications. Furthermore, ISMS is described as a problematic topic not just in IS but also in information management by Bokhari and Manzoor (2022). Likewise, their research revealed that by using ISMS, organizations can benefit financially, which helps corporate reputation and branding. According to Safonova and Kotelnikov (2020), the prior version of ISMS emphasized the Plan-Do-Check-Act (PDCA) management approach; however, the recent version of ISMS does not. Additionally, Nurazean et al. (2021) discovered several benefits of ISMS, including the ability to focus on proactive measures, reducing client audit requirements, resulting in fewer incidents and service disruption, less resource spent on finding new customers and investors, greater productivity, increasing the effectiveness of incident response management, resulting in less time and money spent on damage limitation measures, a better understanding of business information processes, and reassuring customers. As so, assessing the elements that influence the effectiveness of ISMS deployment is critical to ensuring the achievement of the organization's goals and mission. The ISMS must be integrated into the organization's operations and structure for complete information management, with IS factored into the design of processes, information systems, and controls.

2.2 Data Protection in Organization

The ISMS standard, as previously stated, defines IS as the preservation of information against various risks, vulnerabilities, and threats to preserve the confidentiality, integrity, and availability of organizational data (Bouziani et al., 2022). Moreover, in technological communication, IS systems are used to protect crucial data from dangerous users via electronic means (Bokhari and Manzoor, 2022). Despite the widespread deployment of information security technologies in organizations, various information security researchers have emphasized the importance for executives to secure information resources from cyber-attacks and security breaches. Hallová et al. (2019) highlighted organizational security policies and noted that compliance with security standards is a necessary and crucial activity leading to the protection of sensitive corporate data of clients and the overall IS of the business itself. Existing research also acknowledges a defined risk assessment and management approach to ensure the security of organizational information assets against internal and external threats (Singh and Gupta, 2017). In this regard, without integrating security and safety system properties, total protection of organizational data, where key data assets are stored, processed, and sent, is impossible (Kharchenko et al., 2019). Above all, information must be protected during its creation, processing, storage, transfer, and disposal using logical, technical, physical, and organizational safeguards to prevent the loss of confidentiality, integrity, and availability of these critical business values. Implementing IS is thus becoming increasingly vital for organizations and is one of the fundamental determinants of their competitiveness and economic viability.

2.3 ISO-IEC 27001

The International Organization of Standardization (ISO) and the International Electrotechnical Commission (IEC) first issued ISO/IEC 27001 at the end of 2005 (Mirtsch et al., 2020) and technically revised it at the same time with the second version of ISO/IEC 27001:2013. This version remained current after being examined and confirmed in 2019 as an internationally recognized IS methodology (Bouziani et al., 2022). This ISMS standard is regarded as the common language for organizations since it helps them manage their IS while simultaneously protecting their competitive information advantages. Alzahrani and Seth (2021) provide a framework for IS management based on the NTC-ISO/IEC 27001:2013 standard to secure data from outsiders, hackers, and unauthorized personnel. According to the model's results, information assets and technological vulnerabilities are significant for IS management. Mirtsch et al. (2020), citing Van Wessel and de Vries (2013), emphasized that organizations adopt ISO/IEC 27001 and ISO/IEC 27002 for both internal reasons (quality enhancement, cost reduction, and increased risk profile) and external reasons (meeting legal or customer requirements and improving image). P.N. (2021) discovered that firms, particularly small and medium-sized ones, frequently fail to implement IS standards because of high costs and a lack of proof that the advantages outweigh the disadvantages. Previous research by Safonova and Kotelnikov (2020) established that modern ISMS practices are based on the international standard ISO/IEC 27001, which is supported by Fonseca-Herrera et al. (2021), who state that the international standard ISO/IEC 27001 is the leading standard of the ISO 27000 series and contains the ISMS requirements. Another study by Muhamad Khairulnizam et al. (2020) determined ISO/IEC 27001 (2005, 2013) and ISO.org (2013)

to be the most complete and widely accepted ISM standards. In essence, the ISO/IEC 27001 international management system standard aids organizations in developing and maintaining ISMS on an organizational level, and it remains one of the most effective risk management tools for combating the billions of attacks that occur each year (Mirtsch et al. 2021). As a result, the ISO-IEC 27001 international standard has been given as a model for the design, establishment, implementation, operation, monitoring, control, maintenance, and continuous improvement of ISMS information in any type of organization. To this end, it is vital to be adept with and comprehend the subject of ISO 27001-compliant ISMS implementation, which attempts to secure any institution or organization against potential data loss, theft, or manipulation.

3.0 Methodology

This study used the systematic literature review approach, which is defined as a well-defined method for identifying, evaluating, and interpreting all relevant papers on a specific research question or topic area (Okoli and Schabram, 2010). The process began with the review's planning, conduct, and reporting, as outlined by Okoli and Schabram (2010) and shown in Figure 2. The review process included the research questions as well as the methods to be used. The research question was the determination of the ISMS that are implemented for data protection in organizations. The search technique was developed after careful consideration of the databases and search criteria. The year and kind of publication were used to determine inclusion and exclusion criteria. A systematic literature review of academic and non-academic sources, including peer-reviewed journals and conference papers. To obtain additional detailed knowledge about the broader use of ISMS in data protection, a systematic literature review is a well-suited research question. An accurate description of what will be done to answer the research question according to the guidelines by Okoli and Schabram (2010) is shown in Figure 1. These procedures are helpful for any form of literature review, but they must all be followed for a review to be considered scientifically rigorous (Okoli and Schabram, 2010).

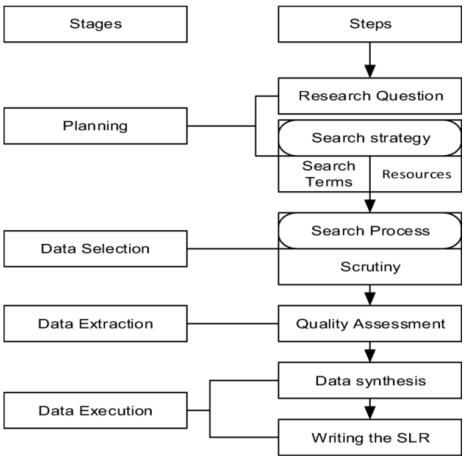


Figure 1: Review protocol based on stages and steps.
(Source: Okoli and Schabram, 2010)

Figure 2: Stages and steps of review process.

3.1 Formulation Research Questions

The research questions for this work are structured using the PICOC criteria (population, intervention, comparison, outcomes, and context) during the planning stage. Table 1 organizes the scope identification, ensuring a clear focus on the implementation of ISMS in organizations for data protection.:

Table 1: Identify the scope of structured questions

Scope	Criteria
Population	Implementation of ISMS in organizations, data protection in organizations, information security practice
Intervention	Information security management intervention
Comparison	Comparison not applied
Outcomes	ISMS implementation in organization, ISMS compliance
Context	Review of all literature related to ISMS

(Source: Research Data, 2022)

The research questions addressed in this study include the following:
RQ1: What factors influence ISMS implementation for data protection in organizations?
RQ2: What is the impact of ISMS implementation on data protection in organizations?
RQ3: How is ISMS implemented for data protection in organizations?

3.2 Search criteria

The amount of data on the internet is tremendous, and a large amount of data was generated by utilizing Google Search. The reviewed research was obtained from Google Scholar, ACM digital library, Emerald Insight, Science Direct, Taylor & Francis, and IEEE Xplore databases. The retrieval involves the usage of the ISMS implementation that affects organizational data protection as the search criterion in all databases. White papers, conference papers, journals, books, and book chapters were among the documents generated. The relevancy of the title, abstract, and entire article was used to select the work. The documents chosen were those released between 2017 and 2023. Table 2 displays the documents retrieved from each database, including those discarded and those included.

Table 2: List of databases

Database	**Number of documents retrieved**	**Discarded duplicates and/or older than 2018**	**Considered for inclusion**
ACM digital library	1		1
Emerald Insight	9	2	7
Google Scholar	22	3	19
IEEE Xplore	3	1	3
Science Direct	4	1	4
Taylor & Francis	1		1
Snowballing			3
	40	7	38

3.3 Information Sources

The implementation of ISMS in organizational data protection was utilized as the search criteria. The search query produced tens of thousands of documents because every document containing the term all over was retrieved. The first few pages of each database were searched, and all duplicate copies generated were removed. A document was eliminated if its digital object identifier (DOI) coincided with the DOI of another document. All materials released up to 2023 were included in the search. Whenever feasible, the search terms were found in the publication's title, abstract, and complete article. Before narrowing the selection, a snowball search was performed on some of the references in the selected publications and added to the list.

3.4 Inclusion and Exclusion Criteria

Publications from 2017 through 2023 were included and evaluated based on the existence of the search term. Relevant papers were selected after reading titles, abstracts, introductions, and full articles. Unpublished work, documents from other domains, and those published in other databases were excluded. Snowballing was employed to gather documents cited in relevant articles.

3.5 Data Extraction and Synthesis

The data was gathered using spreadsheets, with each row containing papers published in each of the listed databases between 2017 and 2023. Relevant bibliographic information (e.g., title, author, database, page numbers) was saved, as well as a hyperlink to the article for reading. The inclusion of an article in the final review was based on the title, keywords, and abstract. The abstract was read first, followed by the article, which was coded as relevant or not relevant based on the search context. The second phase entailed reading the entire article and contextualizing it as containing pertinent information about the compliance or implementation of ISMS in organizational data protection.

4.0 Results and Discussion

This section presents a summary of the results and the discussions.

4.1 RQ1: What factors influence ISMS implementation for data protection in organizations?

When analyzing 40 articles, it was possible to code 6 categories regarding the factors that influence the ISMS implementation (Table 3). The primary factor was awareness and training, with multiple studies emphasizing the necessity of ISMS awareness to protect organizations from various risks. It was measured in a variety of ways, including:

the necessity of ISMS awareness to protect organizations from various risks. It was measured in a variety of ways, including:

- Alshaikh (2018), the awareness of ISMS practices protecting organizations from a wide range of IS risks;
- Muhamad Khairulnizam (2020) ISMS knowledge enhancing organizational agility;
- Mohamad Noorman (2018) significant investigation of IS training;
- Njuki (2022) and Culot et al. (2021) ISMS's skill guarantees for business continuity;
- Hallová et al. (2019), Farid et al. (2023) and Mirtsch et al. (2020) discuss the confidentiality, integrity, and availability of organization assets (information) by ISMS compliance.

Interestingly, a great deal of research focuses on the factor impacting ISMS deployment for data protection in organizations, and this factor has been studied in a variety of methods, providing a more robust foundation for understanding how ISMS may enhance data protection in businesses.

Table 3: Factors that influence ISMS implementation for data protection in organizations

Category	Description
Awareness and training	Provided training to employees to create awareness and increase their knowledge, skills, and competencies on IS. Encourage awareness to ensure the compliance of IS policies.
Policy and procedure	IS Policy effectiveness being understandable, practical, and successfully communicated. IS directives are clear on the protection of IS assets from IS incidents such as unauthorized information security breaches.
Top management support	Full support and commitment and show their involvement towards an organizational initiative on IS. Provide preferences to IS as compared to any other activities.
Technology	Information technology capability fulfills technical security requirements and assists organizations in fulfilling IS policy requirements. Software and hardware work together to adhere to common technology standards.
Budget	IS investment, allocation, expenses, and budgets for IS activities.
Compliance	Monitoring IS compliance and disciplinary action about IS practices.

4.2 RQ2: What is the impact of ISMS implementation on data protection in organizations?

The impact of ISMS implementation on data protection is substantial (Table 4). Results from various studies indicate positive influences on firm performance, financial performance, corporate reputation, and branding. ISMS adoption contributes to enhanced security posture, reduced risks, increased customer trust, and improved overall firm performance. Bokhari and Manzoor (2022) hold the view that ISMS has a significant impact on corporate reputation; Gwebu et al. (2018) affirm brand and branding, and firm profitability in organizations that protect IS through a risk assessment. The findings of ISMS implementation by Menon and Siponen (2020) are data protection in organizations, such as preventing security threats and the optimal solution. An ISMS requires firms to do risk assessments regularly to identify potential threats and vulnerabilities to their data. Organizations can establish suitable controls to limit risks and secure their data from unauthorized access, disclosure, or loss if they understand the risks

Table 4: The impact of ISMS implementation on data protection in organizations

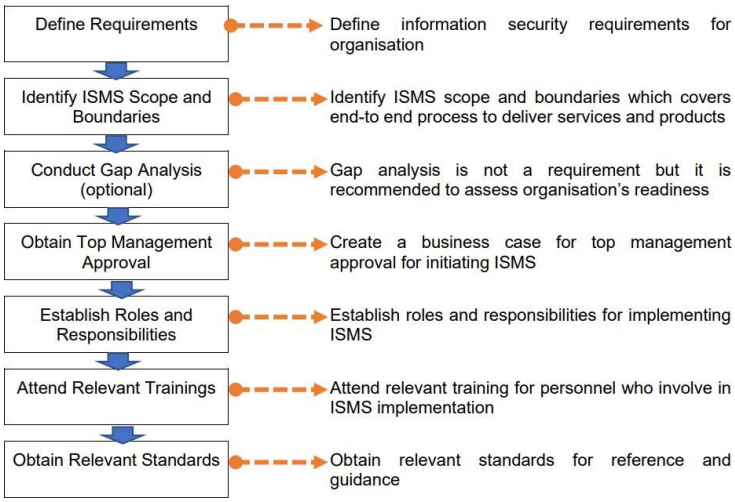
Category	Description
Firm performance	The sector, the state of the market, and the organization's aims and strategies all influence the company's performance. The organizations can improve their entire security posture, reduce risks, increase customer trust, and ultimately lead to greater firm performance by prioritizing data protection and putting an effective ISMS in place.
Financial performance	The financial performance impact of ISMS adoption, such as the industry, market conditions, and the organization's specific financial goals and strategy. Organizations, on the other hand, can reduce financial risks, maintain customer trust, gain a competitive advantage, and contribute to improved financial performance by prioritizing data protection through ISMS deployment.
Corporate reputation performance	Impact of ISMS implementation on corporate reputation based on industry, market conditions, and organization-specific factors. By implementing an ISMS and protecting data effectively, organizations can improve their corporate reputation by demonstrating a proactive and responsible approach to data protection, fostering customer trust, differentiating themselves from competitors, and positively influencing public perception.
Branding performance	Depending on the industry, the state of the market, and the unique strategies and values of the brand, the adoption of an ISMS will have a different effect on branding performance. However, organizations can boost brand trust, credibility, reputation, and distinction by putting data safety first through the implementation of ISMS, ultimately leading to greater branding performance.

4.3 RQ3: How is ISMS implemented for data protection in organizations?

The research findings indicate that ISMS implementation, following the PDCA management approach, assures comprehensive and effective data protection. Safonova and Kotelnikov (2020) emphasize the importance of policy management and ISMS execution. Additionally, Fonseca-Herrera et al. (2021) assert that incorporating the ISO/IEC 27001 standard into ISMS-implemented data protection

strategies serves as a global reference for IS. As illustrated in Figure 3, organizations can carry out ISMS deployment in a way that best suits their needs.

Figure 3: The ISMS implementation on data protection in organizations



5.0 Conclusions

In conclusion, this systematic literature review has shed light on key factors influencing the implementation of ISMS for data protection in organizations. The findings emphasize the crucial role of awareness and training, effective policy and procedures, top management support, technological capabilities, budget considerations, and compliance monitoring in the successful deployment of ISMS. Furthermore, the impact of ISMS implementation on data protection is substantial, positively influencing firm performance, financial performance, corporate reputation, and branding. The review highlights the significance of prioritizing data protection through ISMS adoption, ultimately contributing to improved organizational security posture, reduced risks, enhanced customer trust, and increased competitiveness. However, this study is not without its limitations. The research is based on a systematic literature review, and while efforts were made to encompass a variety of sources, it may not capture every relevant study in the field. Likewise, most of the material examined covers the years 2017 to 2023; new advancements not included in this analysis may arise due to the rapid evolution of technology and security standards. A retrospective evaluation of the research process reveals the reliance on selected databases and search criteria, which might introduce some bias in the studies included. Despite these limitations, this review contributes valuable insights into the multifaceted aspects of ISMS implementation for data protection. Moving forward, recommendations for improving the situation involve encouraging further empirical studies that delve into the practical applications of ISMS in diverse organizational settings. Examining the actual obstacles encountered during ISMS adoption and how businesses overcome them is needed. Hence, researchers and practitioners should collaborate to develop standardized frameworks for evaluating the effectiveness of ISMS in real-world scenarios. Identifying new directions for further research could involve investigating emerging technologies' impact on ISMS, assessing the effective of newer versions of ISO/IEC 27001, and exploring the role of cultural factors in shaping organizations' approaches to information security. By addressing these recommendations, future research can contribute to a deeper understanding of ISMS and its evolving role in safeguarding organizational data.

Acknowledgments

We wish to extend our heartfelt appreciation to the School of Information Science, College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, for their support and assistance. We greatly appreciate their dedication to promoting scholarly research.

References

Alshaikh, M. (2018), "Information security management practices in organisations (unpublished",doctoral dissertation). University of Melbourne, Melbourne.

Alzahrani, L., & Seth, K. P. (2021). The impact of organisational practices on the informationsecurity management performance. *Information*, *12* (10), 398. https://doi.org/10.3390/info12100398

Amini, M., Vakilimofrad, H., & Saberi, M. K. (2021). Human factors affecting informationsecurity in libraries. *The Bottom Line*, *34*(1), 45-67. https://doi.org/10.1108/bl-04-2020-0029

Arbanas, K., & Žajdela Hrustek, N. (2019). Key success factors of information systems security. *Journal of information and organisational sciences*, *43*(2), 131-144.https://doi.org/10.31341/jios.43.2.1

Bokhari, S. A. A., & Manzoor, S. (2022). Impact of Information Security Management System onFirm Financial Performance: Perspective of Corporate Reputation and Branding. American Journal of Industrial and Business Management, 12, 934-954. https://doi.org/10.4236/ajibm.2022.125048

Bouziani, M. M., Merbah, M. M., Tiskar, M. M., ET-Tahir, M. A., & Chaouch, M. A. (2022). When can we talk about implementing an Information Security Management System,according to ISO 27001? *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *13*(2), 394-401.

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

Farid, G., Warraich, N. F., & Iftikhar, S. (2023). Digital information security management policyin academic libraries: A systematic review (2010–2022). *Journal of Information Science*, 016555152311600. https://doi.org/10.1177/01655515231160026

Fonseca-Herrera, O. A., Rojas, A. E., & Florez, H. (2021). A model of an information security management system based on NTC-ISO/IEC 27001 standard. *IAENG Int. J. Comput. Sci*, *48*(2), 213-222.

Gwebu, K. L., Wang, J., & Wang, L. (2018). The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management. Journal of Management Information Systems, 35, 683-714. https://doi.org/10.1080/07421222.2018.1451962

Hallová, M., Polakovič, P., Šilerová, E., & Slováková, I. (2019). Data protection and security in SMEs under enterprise infrastructure. *AGRIS on-line Papers in Economics and Informatics*,*11*(665-2019-3992).

Kharchenko, V., Dotsenko, S., Illiashenko, O., & Kamenskyi, S. (2019). Integrated cyber safety & Security management system: Industry 4.0 issue. *2019 10th International Conference onDependable Systems, Services and Technologies (DESSERT)*.https://doi.org/10.1109/dessert.2019.8770010

Menon, N. M., & Siponen, M. T. (2020). Executives' Commitment to Information Security: Interaction between the Preferred Subordinate Influence Approach (PSIA) and Proposal Characteristics. ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 51, 36-53. https://doi.org/10.1145/3400043.3400047

Mirtsch, M., Kinne, J., & Blind, K. (2021). Exploring the adoption of the international informationsecurity management system standard ISO/IEC 27001: A web mining-based analysis. *IEEETransactions on Engineering Management*, *68*(1), 87-100. https://doi.org/10.1109/tem.2020.2977815

Mirtsch, M., Pohlisch, J., & Blind, K. (2020). International diffusion of the information security management system standard ISO/IEC 27001: exploring the role of culture. Mohamad Noorman Masrek, Qamarul Nazrin Harun & Muhamad Khairulnizam Zaini. (2018). The development of an information security culture scale for the Malaysian public organisation. *International Journal of Mechanical Engineering and Technology (IJMET)*, *9*(7), 1255-1267.

Muhamad Khairulnizam Zaini, Mohamad Noorman Masrek, & Mad Khir Johari Abdullah Sani. (2020). The impact of information security management practices on organisational agility.*Information & Computer Security*, *28*(5), 681-700. https://doi.org/10.1108/ics-02-2020-0020

Njuki, J. W., Muketha, G. M., & Ndia, J. G. (2022). A systematic literature review on security indicators for open-source Enterprise resource planning software. *International Journal of Software Engineering & Applications*, *13*(3), 27-38. https://doi.org/10.5121/ijsea.2022.13303

Nurazean Maarop, Witarsyah, D., Surya Sumarni Hussein, Samy, G. N., Noor Hafizah Hassan, Ten, D. W. H., Roslina Mohammad, Norziha Megat Mohd (2021). Information Security Management System Success Measurement Indicator. *International Journal of Scientific & Technology Research*, *10*(02). https://doi.org/10.3403/30134765u

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1954824

P.N., S. (2021). The impact of information security initiatives on supply chain robustness and performance: An empirical study. *Information & Computer Security*, *29*(2), 365-391. https://doi.org/10.1108/ics-07-2020-0128

Safonova, O. M., & Kotelnikov, N. V. (2020). Modeling the information security management system (ISMS) of a medical organisation. In *E3S Web of Conferences* (Vol. 224, p. 01035).EDP Sciences.

Singh, A. N., & Gupta, M. (2017). Information security management practices: Case studies from India. *Global Business Review*, *20*(1), 253-271. https://doi.org/10.1177/0972150917721836

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009