JDBIM
(Journal of Digital Business and Innovation Management)

Volume 3, No.1, Juni 2024, 62-76
ISSN (Online): **2962-3898**
DOI: 10.26740/jdbim.v3i1.59163
https://ejournal.unesa.ac.id/index.php/jdbim

Information Security Behavior and Compliance with ISO 27001 in IT Companies

Mohammad Rafli[1*], Nuansa Cinta Akhwat Nusantara[2], Ella Rosediana Putri[3], Intan Pravda Sari[4], Naufal Zamzami[5], Aflahal Insan Muharroman[6]

[123456] Department of Digital Business, Universitas Negeri Surabaya
Ketintang, Surabaya 60231, Indonesia

Abstract

This article discusses the importance of information security behavior and the application of the ISO 27001 standard in the context of IT companies. Using PRISMA guidelines, we outline the important role of information security behavior in maintaining the integrity, confidentiality, and availability of necessary information within an enterprise. We introduce the ISO 27001 standard as the main framework for managing secure information systems, highlighting the main stages in its implementation: plan, do, and check. This study also identified factors that influence the implementation of information security behavior in IT companies, such as organizational culture, training, management supervision, and communication between departments. With a deep understanding and implementation of ISO 27001, companies can ensure the security of their information, which is the main goal of information security in the organizational context and information technology environment.

Keywords: *ISO 27001; information; security; behaviour*

Received: 1 April 2024; Accepted: 29 Juni 2024; Published: 30 Juni 2024

*Corresponding author
E-mail: mohammadrafli.22073@mhs.unesa.ac.id

INTRODUCTION

Information security behavior in a company is important to ensure the required security and availability of information. ISO 27001 is a standard used to regulate and manage secure information systems. This standard has three main stages: plan, do, and check. In the planning stage, the company organizes patterns, objects, processes, and procedures to

To cite this document:
Rafli, Mohammad., Nusantara, Nuansa Cinta Akhwat., Putri, Ella Rosediana., Sari, Intan Prava., Zamzami, Naufal., Moharroman, Aflahal Insan. (2024). Information Security Behavior and Implementation of ISO 27001 in IT Companies. *JDBIM (Journal of Digital Business and Innovation Management),* Vol.3 No.1, pp. 62-78.

manage risks and achieve goals by organizational goals. The "do" stage implements and operates the risk management information system, while the check stage carries out monitoring, measurement, and collection of measurements to be updated by management. Implementing ISO 27001 in companies reduces risks and increases information security. To organize and manage a secure information system, companies must carry out an ISMS audit using ISO 27001. This audit will help companies identify and reduce risks. (Kaban & Legowo, 2018)

In the era of digital technology that continues to develop and is complex, managing information security is an important and challenging task for an organization. ISO 27001 provides a structured, cost-effective, and systematic way to establish, implement, operate, monitor, review, maintain, and improve information security by implementing an Information Security Management System (ISMS). ISMS helps organizations keep their infrastructure and business safe and risk-free. ISMS includes processes, methods, procedures, policies and tools associated with specific organizational and technical steps that are continuously monitored in stages towards a controlled environment. Every environmental component, such as human resources, organization, software, hardware, etc., must be protected from danger and attacks to keep critical systems safe (Junaid, 2023).

This research aims to explore the body of knowledge regarding information security behavior, compliance, and strategies for implementing ISO 27001 in IT companies that are considered companies with a high level of maturity toward IT risks. Information security behavior is important to maintain the integrity, confidentiality, and availability of information vital to the organization. This is also closely related to security awareness, where education and organizational culture are important in encouraging safe behavior in managing information. The combination of good information security behavior and compliance with ISO 27001 is the key to effectively managing information security risks, protecting valuable information assets, and building a strong foundation for IT enterprise sustainability and growth in today's increasingly connected and complex environment.

Information Security Behavior

Information security behavior is very important in maintaining sensitive information's integrity, confidentiality, and availability. It reflects the way individuals or organizations interact with information technology and the systems they use to protect information from various threats, risks, or security breaches (Hooper & Blunt, 2020).

Information security behavior includes several actions taken by individuals or organizations, such as using strong passwords, using security software such as antivirus and firewalls, compliance with established security policies, and the level of awareness of security threats that may arise. It also involves individual or organizational attitudes, habits, and knowledge about good security practices in information management (Kaitazi & Bulgurcy, 2013)

The empirical study conducted aims to identify factors that influence information security behavior. These factors may include psychological, social, organizational, and technical aspects that influence an individual's or organization's decision to adopt information security practices. For example, the awareness of security threats, perception of the need for information security, knowledge of effective security practices, and organizational support for information security policies (Nævestad et al., 2023). A deeper understanding of information security behavior and its influencing factors can help organizations develop more effective strategies to increase security awareness, strengthen security policies and procedures, and engage users more actively to maintain information security. Thus, empirical studies such as those conducted in the journal can provide valuable insights into understanding and improving information security in various organizational contexts and information technology environments.

Implementation of Information Security Behavior in IT Companies

Analyse factors in implementing information security behavior in information technology (IT) companies. One of the main findings is that organizational culture plays a very significant role in shaping employee attitudes and behavior regarding information security. A culture that supports information security tends to encourage employees to be more proactive in complying with security policies and protecting company information assets.

Information security training is also considered important in increasing employee awareness and skills in dealing with ever-growing security threats. Regular and relevant training can help employees understand the importance of information security and best practices for reducing security risks). Management oversight is also an important factor in driving compliance with security policies. By monitoring and supervising employee compliance levels, management can identify areas that require improvement and take appropriate actions to strengthen information security (Kajtazi et al., 2013).

Additionally, increased awareness of security risks was also a significant factor. Employees who better understand security threats tend to be more alert and proactive in protecting company information from attacks or security breaches. Lastly, cooperation and open communication between departments and individuals within an IT company are also considered important. By sharing information about security threats and best practices, companies can improve their readiness to deal with complex and evolving security threats. By understanding and paying attention to these factors, IT companies can develop holistic and sustainable strategies to improve their information security, reduce security risks, and maintain customer trust and company reputation (Hooper & Blunt, 2020).

Compliance with ISO 27001

ISO 27001 is an information system security standard that companies can use to implement information system security (Information Security Management System/SKMI). ISO 27001 has eleven controls that can be applied to an organization or company, which can be seen as existing controls to maximize the security of the company's existing information systems. ISO 27001 has four life cycles that must be carried out in a company to analyze things that can be used as a reference for maximizing SKMI. The four life cycles are plans (establishing appropriate ISMS policies, objectives, processes, and procedures in managing risks and results following overall organizational policies and objectives). The next stage is implementing and operating ISMS policies, controls, processes, and procedures. Next is checking (monitoring and assessing the ISMS), assessing and, if possible, measuring process performance against policies, objectives, and practical experience, and reporting the results to management for assessment. Action (Improvement and maintenance of ISMS), namely carrying out corrective and preventive actions based on the results of internal audits and management reviews or other relevant information, to achieve continuous improvement in SKMI (Fagade & Tryfonas, 2017).

The methodology of an ISO 27001-compliant IT company involves establishing appropriate policies, objectives, processes, and procedures to manage risks in alignment with organizational goals. The company collects data from related parties, such as IT companies, to analyze compliance with the ISO/IEC 27001:2009 standard, focusing on asset management, communications, operational management, and access control. The company then implements information system security controls and objectives to improve and maintain the security of existing

information systems. ISO 27001 guarantees confidentiality, integrity, and availability, which are the primary security and protective objectives of this standard. Confidentiality ensures that authorized persons can only access information by implementing encryption and access control mechanisms (Kajtazi et al., 2013).

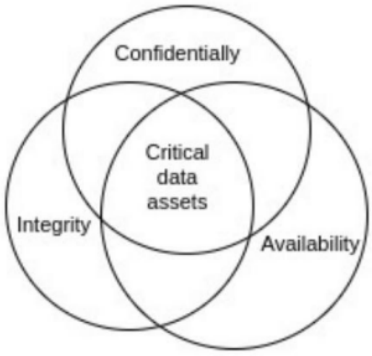

Figure 1. ISO 27001 Framework

Integrity ensures that data is only changed in a legitimate manner, protecting the organization from attackers trying to change the information and protecting against unintentional technical errors. Availability ensures that information is available to authorized systems or persons whenever needed. For critical assets, organizations need protection on all three security objectives, as shown above, which can be achieved with the help of ISO 27001.

METHODS

PRISMA is a guide to assess a systematic review and/or meta-analysis. PRISMA helps writers and researchers in compiling a quality systematic review and meta-analysis with the steps shown in the following chart:

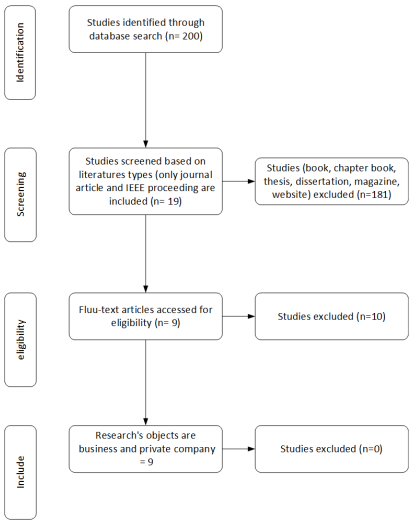

Figure 2. Research Method Framework with PRISMA

RESULT AND DISCUSSION

Analyze Data with Publish or Perish

The Publish or Perish application is software that can help researchers analyze and evaluate scientific publications. The following are search results using Publish or Perish with the keywords "data security; intention to comply; ISO 27001" in the last 10 years, namely 2012 to 2023. There are 200 journals that have citation records and patents.

Data Analysis with VOS viewer

a. Network Visualization

Network Visualization is a network visualization of data analysis. The analysis we carried out used normalization analysis with the association strength method. From the analysis we carried out, there are 3 colors: red, green and blue. Each color represents each cluster, such as red (cluster 1), green (cluster 2), and blue (cluster 3). From the analysis we conducted, no items fell into 2 clusters simultaneously. The analysis results of 200 journals in VOSviewer contained 13 items, 3 clusters, 62 links, and a total link strength of 446.

Table 1. Clustering article keywords

Cluster	Item
Cluster 1 (6 items)	1. Analysis 2. Information Security 3. ISO 4. Paper 5. Research 6. Standard
Cluster 2 (4 items)	1. Employee 2. Information Security Behaviour 3. Information Security Policy 4. Risk
Cluster 3 (3 items)	1. Certification 2. Information Security Management System 3. ISMS

The following is the result of connecting VOSviewers articles from network visualization, where there is a lot of research discussing cobit, compliance, security, and governance. From the analysis we conducted, little research still discusses information security policy, risk, paper, research, certification, and ISM (Figure 1).

Figure 1. Network Visualisation

a. *Overlay Visualization*

Overlay Visualization is a visualization of the time span of research that has been carried out. From the results of the analysis that we carried out, if the color of the item is further to the left or the color is getting darker (closer to purple) then the publication of the research was carried out a long time ago, and if the color of the item is further to the right or the color is brighter than the publication of the research has just been carried out. In the picture below, research discussing information security policy, risk, and research was published in 2018 and above, then research discussing analysis was published in 2018, while research discussing information security behavior, paper, ISO, standards, isms, information security management, information security, certification, and employee were published in 2015 (Figure 2).

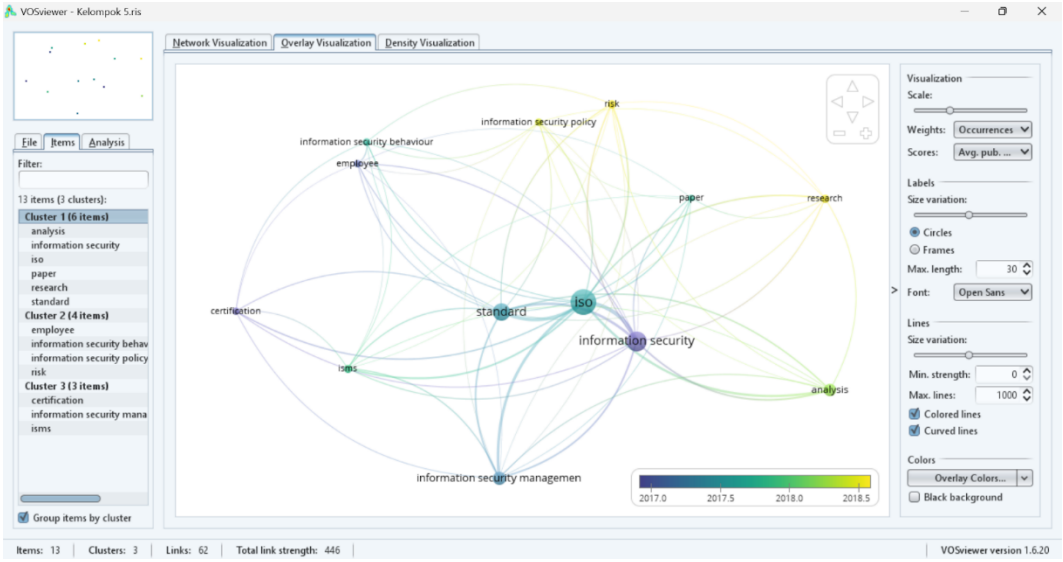

Figure 2. Overlay Visualisation

b. Density Visualization

Density Visualization is a visualization of density related to the number of occurrences. Density can be affected by items. The brighter the color (yellow), the denser the data or the more often the term appears in a document. From the results of our analysis, it can be seen in Figure 3 that the terms ISO, standard, and information security have a density or that these terms often appear in a document.

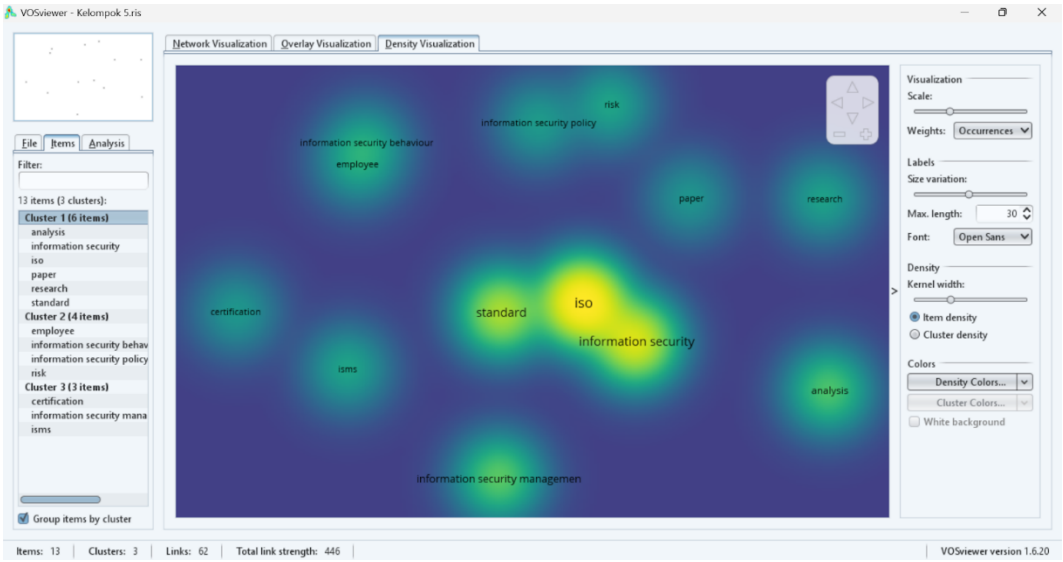

Figure 3. Density Visualisation

Density can be influenced by clusters. From the results of our analysis, it can be seen in the image below that each item has been grouped based on its cluster. Cluster 1 consists of analysis, information security, ISO, paper, research, and standards, then Cluster 2 consists of employees, information security behavior, information security policy, and risk, while Cluster 3 consists of certification, information security management system, and IMS.

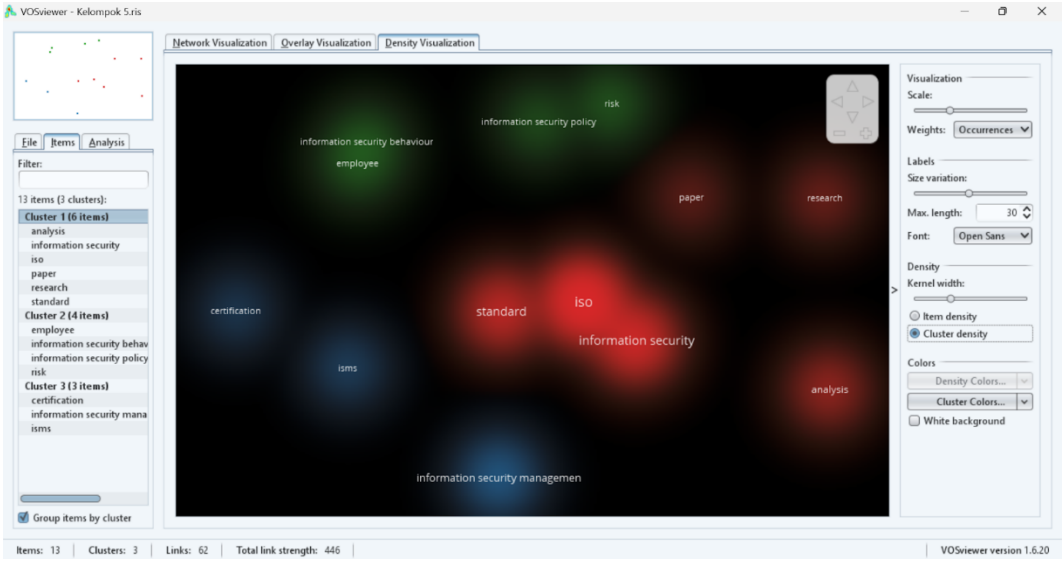

Figure 4. Visualization Clusterization

Data Analysis with Excel

In this research, we searched the Publish or Perish tool using the keyword "information security behavior; ISO 27001" for the last 10-year period, from 2013 to 2023. The results of this search produced 200 journals that have citation and patent records. Next, we identified the 200 journals by filtering by type, only selecting journals with the PDF type. After the identification process, we identified 19 journals that use the PDF type.

The next stage is screening. Of the 19 journals that use the PDF type, we filtered by publisher, selecting only credible publishers. The results of this screening process produced 9 journals published by credible institutions. The next stage is eligibility. After getting 9 journals published by credible institutions, we filtered them based on journal titles that were appropriate and relevant to the keywords we would analyze. Thus, we identified 9 journals relevant to the topic we will analyze. Of the 9 journals included, we analyzed publisher names and cities. The results of our analysis are presented in the form of a bar chart.

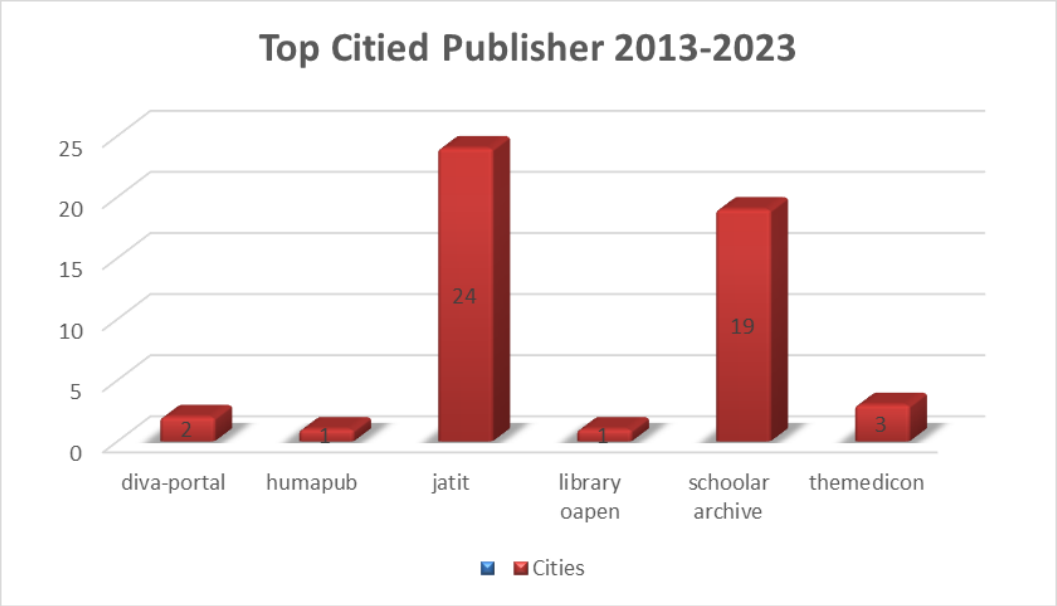

Figure 5. Top Cited Publishers

Based on the results of the analysis we conducted, there are 6 names of publishers, namely diva-portal in 2 cities, humapub in 1 city, jatit in 24 cities, library oapen in 1 city, schoolar archive in 19 cities, and the medicon in 3 cities.

DISCUSSION

Information security is still in the early stages of development. This condition occurs because of threats from malicious parties on the network who are always looking for loopholes in the system, potentially harming the organization with their unscrupulous activities. Therefore, developing an information security policy is of utmost importance, as it forms the basis for significant standards and procedures to reduce the risks associated with an organization or its networks. In an organization, especially in Small and Medium Enterprises (SMEs), implementing information security standards is crucial. This implementation's success will affect SMEs' ability to manage Information Security Systems (ISMS) effectively. However, challenges arise because most standards, including ISO 27001, provide requirements for what is required without providing guidance on how to implement it. To overcome these challenges, there is a need for a deep understanding of the information security management standards domain, as well as highlighting the importance of examinations focused on ISO-27001, this article aims to provide useful guidance for various types of SMEs during the implementation of ISO 27001.

In an era of rapidly developing digital technology and increasing complexity, managing information security is a critical and challenging task

for an organization. Fortunately, the ISO 27001 standard provides a structured, cost-effective and systematic way to establish, implement, operate, monitor, review, maintain and improve information security by adopting an Information Security Management System (ISMS). ISO 27001 is part of ISO 27000 which has around 63 published standards, but only ISO 27001 provides ISMS certification. It's a complete framework for ISMS where other standards offer a very prescriptive view of how you implement controls to manage information security, but what it doesn't do is provide a way to actually apply the existing framework to then implement the controls. ISO 27001 is a technology-agnostic and vendor-independent framework for ISMS that is suitable for organizations of all sizes and types and can be adapted to every sector. This paper provides detailed insight into ISO 27001 so that an organization will successfully comply with the standard to achieve ISO 27001 certification.

Utility organizations have implemented several security and compliance frameworks in their data centers to keep valuable information safe. However, implementing this framework still raises several problems, such as imperfections in access control management. Many previous studies aim to develop information security compliance frameworks in enterprise data centers. Using qualitative methods through semi-structured interviews to collect data. The hope is that it will provide an important contribution to organizational security professionals and management in improving the physical protection of information in the context of an information security compliance framework.

Modern organizations rely heavily on information to carry out activities effectively, making it important to protect information from threats from both inside and outside the company. Employee behavior in an organization greatly influences information protection, which is why it is crucial to build a strong culture for information security. Several previous studies proposed using a control framework to address gaps in assessing information security culture and focused on assessing that culture and identifying relevant components. By using a qualitative approach and various data collection techniques, such as literature reviews and qualitative content analysis, it is hoped that we will be able to produce a control framework that is useful for developing information security in organizations.

CONCLUSION

Information security behavior plays a vital role in maintaining the integrity, confidentiality and availability of information in the company.

Empirical studies of these behaviors provide valuable insights into improving information security across various organizational contexts and information technology environments. Factors such as awareness of security threats, perception of the need for information security, and organizational support for security policies contribute to shaping this behavior. Implementing information security behavior in IT companies is influenced by organizational culture, information security training, management supervision, and open communication between departments. These factors help strengthen information security in companies and increase awareness of security risks. With a deep understanding and implementation of ISO 27001, organizations can ensure the security of their information, thereby ensuring the confidentiality, integrity and availability of information which is the main goal of information security. The limitation of this research is that it does not explore the factors that influence information security behavior using surveys or interview methods, which would explore more personally the compliance motivation of IT company employees amidst the increasingly high risk of IT security threats. Hence, the future research is expected to use participatory research methods that actively involve participants or communities in the entire research process, from planning, implementation, to interpretation of results. This increases the opportunity to deeply understand their perspectives and experiences in complying with ISO 27001.

REFERENCES

Abazi, B. (2020). A Novel Approach for Information Security Risk Assessment Maturity Framework Based on ISO 27001 (Doctoral Dissertation, Budapesti Corvinus Egyetem).

Afacan, O. (2019). Encouraging Employees On Compliant Behaviours About Information Security Measures In Workplaces. *Journal Of Current Researches On Social Sciences*, *9*(1), 87-102.

Computing, C. O. P. C. (2019). Measuring Information Security And Cybersecurity on Private Cloud Computing. *Journal Of Theoretical And Applied Information Technology*, *96*(1).

Fagade, T., & Tryfonas, T. (2017). Hacking A Bridge: An Exploratory Study Of Compliance-Based Information Security Management In Banking Organization. In *Proceedings Of The 21st World Multi-Conference On Systemics, Cybernetics And Informatics (Wmsci 2017)* (Vol. 2, Pp. 94-99).

Hai, H. L., & Wang, K. M. (2014). The Critical Success Factors Assessment of ISO 27001 Certification In Computer Organization By Test-Retest Reliability. *African Journal of Business Management*, *8*(17), 1.

Henttinen, H. (2018). Improvement Of Information Security Management System In Media X Corporation. *Master Thesis*, JAMK University of Applied Sciences.

Hong, H. L. (2013). Feasibility Study On Incorporating IEC/ISO 27001 Information Security Management System (Isms) Standard In It Services Environment, *Doctoral Dissertation*, Universiti Teknologi Malaysia).

Hooper, V., & Blunt, C. (2020). Factors Influencing The Information Security Behaviour of IT Employees. *Behaviour & Information Technology*, 39(8), 862-874.

Junaid, T. S. (2023). ISO 27001: Information Security Management Systems *Doctoral Dissertation, Ph. D. Thesis*, Unspecified Institution. Https://Doi. Org/10.13140/Rg. 2.2. 36267.52005).

Kaban, E., & Legowo, N. (2018). Audit Information System Risk Management Using ISO 27001 Framework at Private Bank. *Journal Of Theoretical & Applied Information Technology*, *96*(1).

Kajtazi, Miranda and Bulgurcu, Burcu. (2013). Information Security Policy Compliance: An Empirical Study on Escalation of Commitment. *AMCIS 2013 Proceedings*. 6. https://aisel.aisnet.org/amcis2013/ISSecurity/GeneralPresentations/6.

Koza, E. (2022). Semantic Analysis of ISO/IEC 27000 Standard Series and Nist Cybersecurity Framework to Outline Differences and Consistencies in The Context of Operational and Strategic Information Security. *Med. Eng. Themes*, *2*, 26-39.

Legowo, N., & Juhartoyo, Y. (2022). Risk Management; Risk Assessment Of Information Technology Security System at Bank Using ISO 27001. *Journal Of System and Management Sciences*, *12*(3), 181-199.

Maingak, A. Z., Candiwan, C., & Harsono, L. D. (2018). Information Security Assessment Using ISO/IEC 27001: 2013 Standard on Government Institution. Trikonomika, 17(1), 28-37.

Nævestad, T. O., Honerud, J. H., & Meyer, S. F. (2023). Information Security Behaviour In An Organisation Providing Critical Infrastructure: A Pre-Post Study of Efforts to Improve Information Security Culture. In *Safety In The Digital Age: Sociotechnical Perspectives On*

Algorithms And Machine Learning (Pp. 103-117). Cham: Springer Nature Switzerland.

Okere, I. O. (2013). *A Control Framework For The Assessment Of Information Security Culture* (Doctoral Dissertation, Nelson Mandela Metropolitan University).

Ramadhan, N., & Rose, U. (2022). Adapting ISO/IEC 27001 Information Security Management Standard To SMEs. *Master Degree Project*. Lulea University of Technology

Ristov, S., Gushev, M., & Kostoska, M. (2012). Information Security Management System For Cloud Computing. *ICT Innovations 2011, Web Proceedings Issn 1857*, *7288*, 49.

Saadat, M., & Abbasi, M. U. (2021). Information Security Policy Development: The Mechanism To Ensure Security Over Information Technology Systems. *Global International Relations Review, Iv*, 22-30.

Velayutham, Y., Samy, G. N., Maarop, N., Hassan, N. H., Hassan, W. H., Pertheban, S., & Perumal, S. (2020). Information Security Compliance Framework For Data Center In Utility Company. *Myjict-Malaysian Journal Of Information And Communication Technology*, *5*(2), 62-71.