JDBIM
(Journal of Digital Business and Innovation Management)
Volume 3, No 1, Juni 2024, 36-52
ISSN (Online): **2962-3898**
DOI: 10.26740/jdbim.v3i1.59167
https://ejournal.unesa.ac.id/index.php/jdbim

Information Security Awareness Analysis of the Threat of Data Leakage in Educational Institutions with the ISO 27001 Framework

Demas Muhammad Rijal [1*], Mukhamad Fahmi Assydiqi[2], Yoel Rensisko Prasetya[3], Lidya Nurhapsari Prasetya Ningsih[4], Nisya Kayla Putri Anindra[5]

[12345]Department of Digital Business, Universitas Negeri Surabaya
Ketintang, Surabaya 60231, Indonesia

Abstract

In the rapidly evolving digital era, information security has become a major concern for various organizations, including educational institutions that are facing pressures such as "publish or perish" and performance metrics like VOS viewer. Serious threats such as cyber-attacks and data breaches require more advanced security solutions. Implementing an Information Security Management System (ISMS) based on ISO 27001 standards is crucial in safeguarding information assets. This research discusses the importance of information security awareness, identifies threats to data protection, and applies ISO 27001 standards in the context of educational institutions. The research methodology employs the PRISMA guideline to systematically evaluate related reviews and meta-analyses. Information security awareness, data protection, and ISO 27001 compliance focus on building a robust information security system within educational institutions facing performance and assessment demands.

Keywords: *Information Security Awareness; Data Protection; ISO 27001; Management System for Educational Institutions*

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

*Corresponding author
E-mail: demasmuhammad.22024@gmail.com.

INTRODUCTION

In today's rapidly developing digital era, information security is a major concern for all organizations, from multinational companies to government agencies and educational institutions. Security threats such as cyberattacks, data leaks and privacy breaches are becoming increasingly sophisticated, requiring more advanced security strategies and solutions.

Implementing an effective Information Security Management System (ISMS) becomes crucial to protect valuable information assets.

The ISO 27001 standard offers a comprehensive framework for establishing, implementing, maintaining, and improving information security in an organization. This standard helps identify and mitigate information security risks and provides guidance for establishing sustainable risk management processes, ensuring compliance with relevant regulations, and strengthening customer and stakeholder trust. Not only is it a risk management tool, but ISO 27001 also acts as a guide to establishing the policies and procedures necessary to ensure adequate information security. By focusing on continuous risk control and assessment, this standard enables organizations to adapt to changes in security threats and technology.

In this report, we will discuss the importance of information security and the compliance goals with the ISO 27001 standard. Some of the keywords that will be discussed in this paper include Information Security, which refers to the principles and practices used to protect information from unauthorized access, inappropriate use, disclosure, destruction, modification, or interference; Compliance Objectives, which is the intention to comply with established information security requirements to enhance data protection and minimize security risks; and ISO 27001, which is an international standard that establishes requirements for information security management systems, providing a framework for maintaining the confidentiality, integrity, and availability of information.

Research on information security awareness analysis of the threat of data leaks in educational institutions is a relevant and important topic in the education sector's information security context. Several previous studies have been conducted to explore this aspect. Conti, M., et al. (2018) conducted a case study on information security awareness in a higher education institution. The main focus is on the understanding and attitudes of staff and students towards information security practices, as well as the efforts made to increase this awareness. Alzahrani, A. I., (2021) evaluating information security awareness among students at universities. This research identifies the level of awareness of information security threats, knowledge of best practices in dealing with risks, and factors that influence information security awareness in higher education environments.

To cite this document:

Rijal, Demas Muhammad., Assydiqi, Mukhamad Fahmi., Prasetya, Yoel Rensisko., Ningsih, Lidya Nurhapsari Prasetya., Anindra, Nisya Kayla Putri. (2024). Information Security Awareness Analysis of the Threat of Data Leakage in Educational Institutions with the ISO 27001 Framework. *Journal of Digital Business and Innovation Management*, Vol. 3 No.1, pp. 36-52.

Nasir et al. (2019) conducted an analysis of information security awareness and practices in higher education institutions in Malaysia. The main objective is to evaluate the level of understanding of information security threats among staff and students and the effectiveness of existing training programs. Dada et al. (2021) examined information security awareness in Nigerian universities. The focus is on evaluating the understanding and implementation of information security practices in higher education institutions and the challenges faced in increasing awareness and compliance with security policies. These studies provide valuable insight into how information security awareness can be measured and improved in educational institutions and the challenges faced in the process. The findings from this research can be used as a basis for designing effective training programs. However, there has been no comprehensive research on better security policies and appropriate risk mitigation measures to prevent data leaks and secure sensitive information in educational environments, so there is a research gap in this research.

METHOD

PRISMA is a guide used 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 Figure 1 as follows:

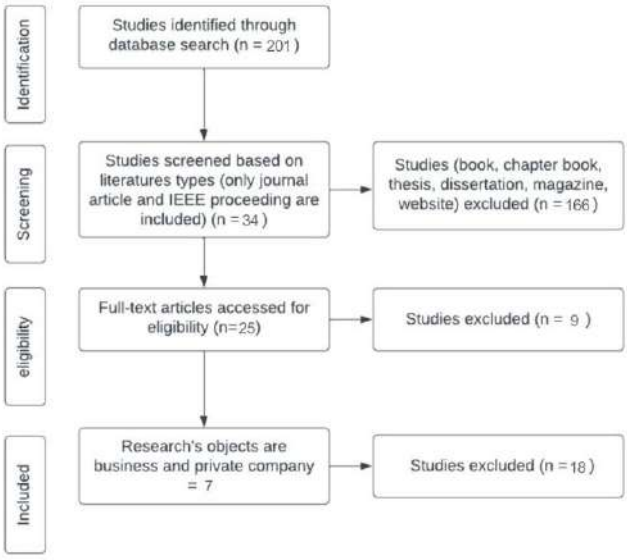

Figure 1. Research model

RESULTS AND DISCUSSION

Analyze Data with Publish or Perish

The Publish or Perish application is software that can help researchers analyze and evaluate published scientific publications. Below are search results using Publish or Perish with the keywords "information security awareness; threats to data protection; ISO 27001" for the last 10 years, namely from 2011 to 2022 and there are 200 journals with citations for applications and patents.

Data Analysis with VOS viewer

Network Visualization uses VOSviewer software to visualize the relationships between elements in a scientific network based on bibliometric analysis. The analysis we use is normalization analysis with the association strength method.

The results of our analysis show 4 colors, namely red, green, blue and yellow. Each color represents its respective cluster. such as red (cluster 1), green (cluster 2), blue (cluster 3), and yellow (cluster 4). From the results of our analysis, each cluster has different items. The results of the analysis of 200 journals in VOSviewer using the association strength method contained 19 items, 4 clusters, 149 links, and 1074 total link strengths (Table 1):

Table 1. Cluster

Cluster	Item
Cluster 1 (red)	1. gdpr 2. general data protection regulation 3. implementation 4. iso 5. risk 6. risk management 7. study
Cluster 2 (green)	1. awareness 2. employee 3. security awareness 4. threat 5. training

To cite this document:
Rijal, Demas Muhammad., Assydiqi, Mukhamad Fahmi., Prasetya, Yoel Rensisko., Ningsih, Lidya Nurhapsari Prasetya., Anindra, Nisya Kayla Putri. (2024). Information Security Awareness Analysis of the Threat of Data Leakage in Educational Institutions with the ISO 27001 Framework. *Journal of Digital Business and Innovation Management*, Vol. 3 No.1, pp. 36-52.

Cluster 3 (blue)	1. data 2. data protection 3. information 4. privacy 5. risk assessment
Cluster 4 (yellow)	1. analysis 2. control

Figure 1 is the result of connecting VOS viewers articles from network visualization w. Many studies discuss general regional data protection, implementation, ISO, risk, risk management, and study, which are marked with red clusters. Meanwhile, from the analysis we conducted, little research still discusses analysis and control, which is marked by the yellow cluster.

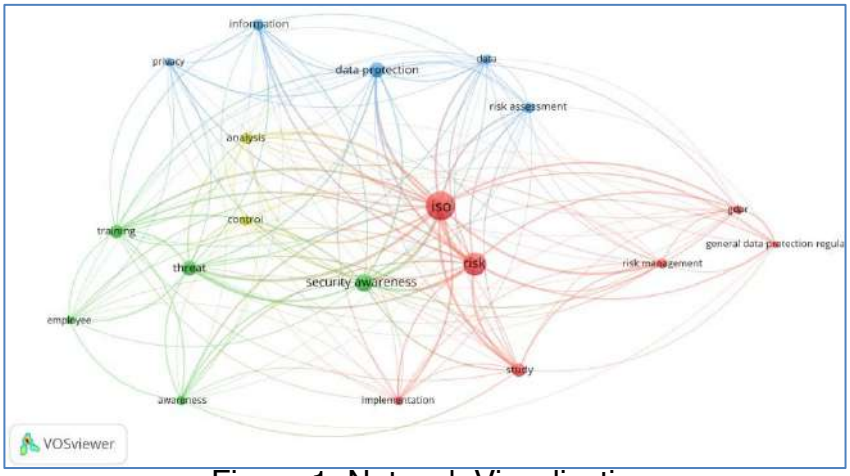

Figure 1. Network Visualization

Overlay Visualization

Overlay Visualization is a visualization technique used to display several types of information or data on one visual display according to the time span of the research that has been carried out. If the color of an item is darker (further to the left) then the publication of the research has been carried out a long time ago. Meanwhile, if the color of an item is getting brighter (going to the right), then the publication of the research has just been carried out. The results of our analysis using the overlay visualization technique state that those discussing GDPR, general data protection regulation, risk assessment, risk management, data protection were published in 2019 and above. Research discussing ISO, study, data, information, implementation, and security awareness was published in mid-2018. Meanwhile, research discussing privacy, analysis, control, training, threats, awareness, and employees was published in early 2018 (Figure 2).

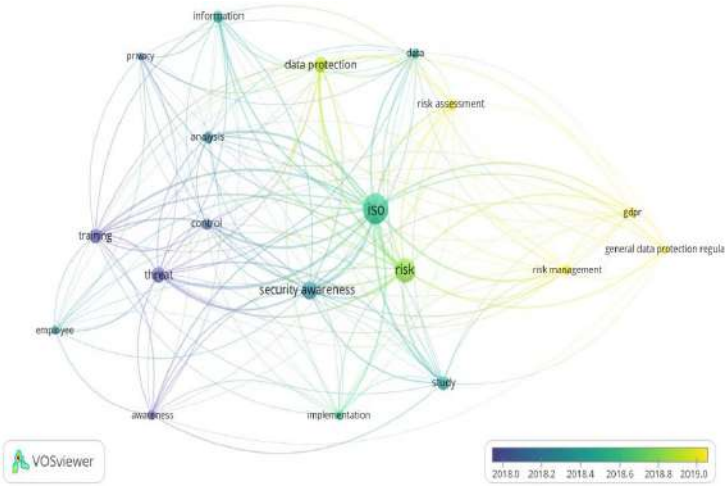

Figure 2. Overlay Visualitation

Density Visualization

Figure 3 shows the data visualization used to display the density distribution of data. Density can be affected by items. The lighter the color (yellow), the denser the data or the more often the term appears in the document. From the results of our analysis shown in the image below, it can be seen that the terms ISO, risk and security awareness have a density or that these terms often appear in a document.

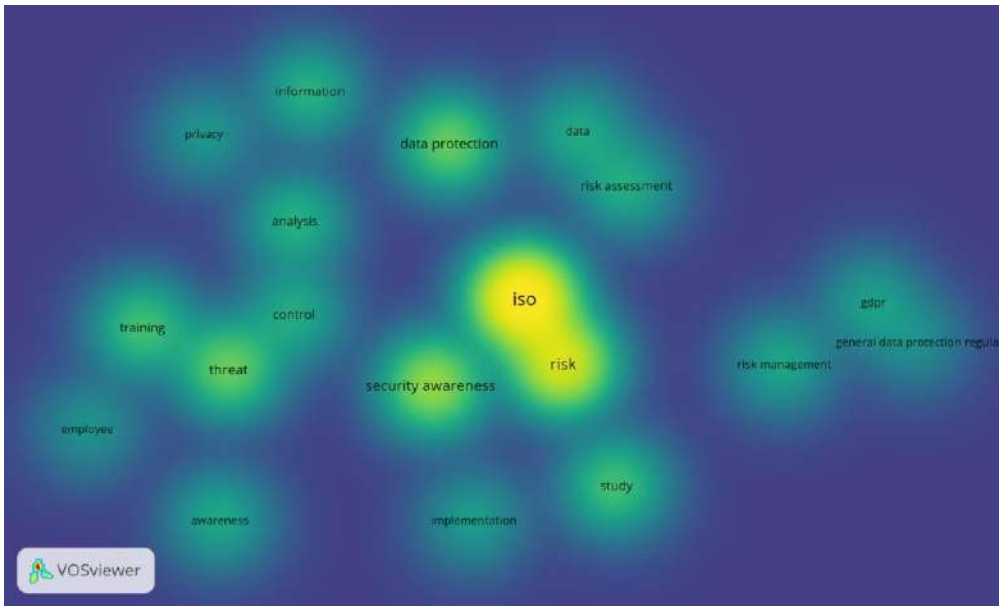

Figure 3. Density Visualization

To cite this document:

Rijal, Demas Muhammad., Assydiqi, Mukhamad Fahmi., Prasetya, Yoel Rensisko., Ningsih, Lidya Nurhapsari Prasetya., Anindra, Nisya Kayla Putri. (2024). Information Security Awareness Analysis of the Threat of Data Leakage in Educational Institutions with the ISO 27001 Framework. *Journal of Digital Business and Innovation Management*, Vol. 3 No.1, pp. 36-52.

The results of our analysis can also be seen in the image below, where each item has been grouped according to its respective cluster, such as cluster 1, consisting of 7 items: GDPR, general data protection, implementation, ISO, risk, risk management, and study, as well as clusters 2-4, as shown in Figure 4.

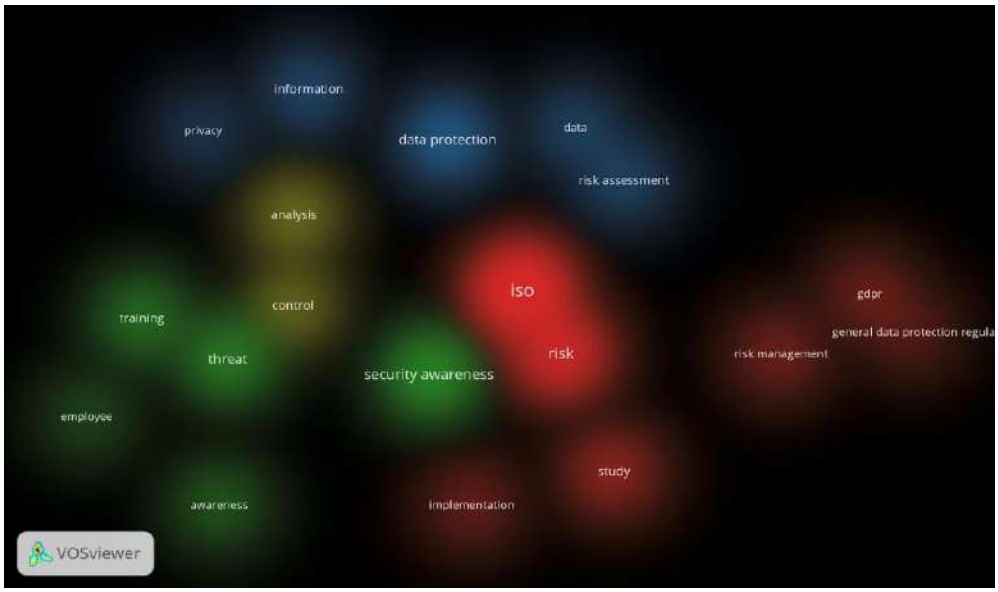

Figure 4. Cluster Visualization

Data Analysis with Excel

Search results using Publish or Perish with the keywords "information security awareness; threats to data protection; ISO 27001" in the last 10 years, namely 2011 to 2022, show 200 journals with citation records and patents. Then, from the 200 journal data, we identified 50 journal data using the PDF type by filtering the type by only selecting journals with that type. After identification, 50 journal data were obtained using the PDF type.

The second stage was screening. After obtaining 50 journal data that used the PDF type, we filtered the publishers by only selecting credible publishers. Thus, after carrying out the screening process, 25 journal data were obtained that were published by credible institutions.

The third stage is eligibility, after obtaining 25 journal data published by credible institutions, we filtered the journal titles that were appropriate and related to the business we were going to analyze so that we obtained 9 journal data that matched the topic we were going to analyze. After we analyzed the citations for each journal, we had 7 journal data included in the topics we would analyze, namely topics that were still related to the keywords "information security awareness; threats to data protection; ISO 27001 " in the last 10 years, namely 2011 to 2022. From the 7 journal data included, we analyzed publisher names and cities. The results of the analysis we carried out showed that there were 7 names of publishers, namely core.ac.uk with 83 cities or 57%, jjmie.hu.edu.jo

with 39 cities or 27%, researchoutput.csu.edu.au with 11 cities or 8%, research.mitwpu.edu.in is 8 cities or 5%, while the remaining 1% is diva-portal.org, real.mtak.hu, and irjaes.com (Table 2 and Figure 5).

Table 2. Top Publisher 2011-2022

Publisher name	Quantities
jjmie.hu.edu.jo	39
diva-portal.org	2
research.mitwpu.edu.in	8
real.mtak.hu	2
irjaes.com	1
core.ac.uk	83
researchoutput.csu.edu.au	11

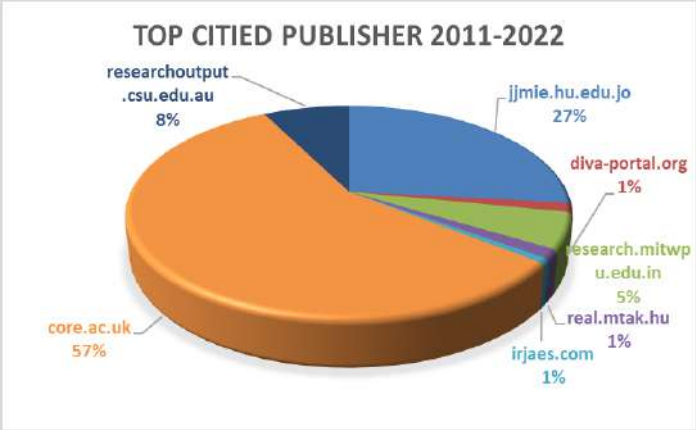

Figure 5. Pie Chart Top Publisher

Why is it important to have information security awareness, and be aware of threats to data protection, especially in educational institutions?

Understanding the importance of information security and threats to data protection has a crucial role, especially within the scope of educational institutions. Information and data stored and managed by educational institutions contain various sensitive information, including student and employee personal,

To cite this document:
Rijal, Demas Muhammad., Assydiqi, Mukhamad Fahmi., Prasetya, Yoel Rensisko., Ningsih, Lidya Nurhapsari Prasetya., Anindra, Nisya Kayla Putri. (2024). Information Security Awareness Analysis of the Threat of Data Leakage in Educational Institutions with the ISO 27001 Framework. *Journal of Digital Business and Innovation Management*, Vol. 3 No.1, pp. 36-52.

academic, and financial information. Threats to information security, such as cyber-attacks, data theft, and information leaks, can result in financial losses, damaged reputations, and even serious privacy violations.

With the increasing use of information technology in education, educational institutions are becoming increasingly vulnerable to cyber-attacks and security breaches. Therefore, it is important for all members of the educational community, from leaders to staff to students, to be highly aware of the importance of maintaining information security and protecting data. With a good understanding of existing threats and the steps that can be taken to prevent them, educational institutions can ensure the continuity of their operations and protect information assets more effectively.

Research by Awni Itradat et al., in "Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study" emphasizes the importance of information security. This includes vulnerability evaluation, penetration testing, and implementing an ISO/IEC 27001 Information Security Management System to improve information security. This study evaluates the level of information security in Jordanian universities, focusing on Hashemite University. The document also discusses vulnerabilities, threats, and risks. Vulnerabilities, threats and risks are closely related in the context of information security. Vulnerability refers to a weakness or loophole in a system that can be exploited by unauthorized parties. Meanwhile, threats are potential events that could exploit the vulnerability and cause losses or negative impacts. Risk results from a combination of vulnerabilities and threats, which describes the possibility of certain losses or negative impacts. It also provides recommendations to overcome vulnerabilities in various aspects such as hardware, software, networks, personnel, and organizations.

Vulnerability Evaluation and Penetration Testing are important tools for identifying and measuring system weaknesses to improve security controls. BackTrack is a commonly used platform for penetration testing. ISMS, based on ISO27001, is a management plan for protecting information assets. ISMS implementation steps at Hashemite University ICET include determining scope, policy, risk assessment, risk mitigation, controls, and Feasibility Statement. Risk management methodology is critical to maintaining network security. The ISO 31000 standard helps in identifying and addressing risks. The document details various policies related to risk management, awareness, performance management, asset management, physical security, operations management, access management and others to ensure the security and protection of ICET assets and information. This includes policies on risk assessment, awareness training, asset inventory, physical security controls, backup procedures, server

access management, email management, and password policies. Educational institutions like Hashemite University can effectively protect information assets by building a secure network infrastructure, conducting employee access audits, providing security awareness training, and implementing strict policies. The need for a strong security framework and the implementation of structured security measures will help reduce information security risks and maintain the sustainability of educational institutions in the face of existing threats.

What stages are required in an effective and sustainable ISO 27001 implementation process?

The steps for implementing ISO 27001, according to Phirke, A., & Ghorpade-Aher, J. (2019), contain 10 stages. The steps for implementing ISO 27001 begin with identifying organizational goals taken from the company's mission and vision. These goals may include assuring employees and clients of their understanding of information security, protecting employee and client data, increasing organizational productivity, and conducting operations ethically according to IT guidelines. Next, in stage 2, the organization needs to gain internal support to ensure the successful implementation of the ISO 27001 standard. This includes consolidating potential resources to work with the ISMS and involving appropriate delegates in ISMS training. The third step involves determining the scope of the ISMS, which must be appropriate to the organization's size and goals. This involves selecting controls from 114 available controls according to the organization's requirements to obtain certification from an external auditor.

Next, in stage 4, the appropriate risk assessment methodology will be determined after studying and analyzing the risks associated with the organization. The methodology needs to include appropriate steps to address risks, including strategies to resolve and control the risks the organization faces. This also includes identifying and separating resources that may pose risks and threaten the organization's security. After identifying the risks associated with the organization, the probability and consequences of each risk are measured or analyzed and entered into a table. Then stage 5 involves developing a risk management plan that

To cite this document:
Rijal, Demas Muhammad., Assydiqi, Mukhamad Fahmi., Prasetya, Yoel Rensisko., Ningsih, Lidya Nurhapsari Prasetya., Anindra, Nisya Kayla Putri. (2024). Information Security Awareness Analysis of the Threat of Data Leakage in Educational Institutions with the ISO 27001 Framework. *Journal of Digital Business and Innovation Management*, Vol. 3 No.1, pp. 36-52.

includes basic risk mitigation strategies that include accepting, avoiding, transferring or reducing risks to a certain level of acceptance.

In stage 4, the next step is to establish an appropriate risk assessment methodology after reviewing and analysing the risks associated with the organization. This methodology should include steps to address risks, including strategies to resolve and control them. This also includes identifying and isolating resources that may threaten the organization's security. After risk identification, the probability and consequences of each risk are analyzed and recorded in a table. In stage 5, the next step is to develop a risk treatment plan that includes basic risk mitigation strategies, such as acceptance, avoidance, transfer, or reduction of risk to a specified level of acceptance. In stage 6, organizations develop an ISMS implementation program appropriate to their objectives, by selecting relevant controls from 114 available controls. Stage 7 involves preparing documentation of the implemented controls, including creating documents such as a Statement Of Applicability (SOA) necessary to meet ISO 27001 certification requirements. After implementing controls, in stage 8, the organization periodically reviews compliance to ensure conformance with organizational objectives. It involves monitoring objectives, controls, and measurement methodologies. Next, in stage 9, an internal audit is prepared to evaluate the organization's compliance and performance and take corrective and preventive actions as needed. The final stage, stage 10, is a periodic management review carried out to ensure the policies and procedures implemented to align with the organization's objectives and to take action on detected violations of policies and procedures.

What are the leadership responsibilities in training and developing information security awareness in educational institutions?

Leadership responsibilities in training and developing information security awareness within educational institutions are critical to creating an environment that is safe and protected from cyber threats. Leaders of educational institutions, as explained by Awni Itradat et al., in "Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study", that leadership must ensure that all members of the educational community, from staff to students, have a good understanding of information security and the threats that may be encountered. Leadership needs to provide sufficient support and resources for information security awareness training programs, including providing adequate time and budget for training and development activities.

Leadership has a close relationship with ISO27001, the information security management standard. Leadership is responsible for ensuring the implementation and maintenance of information security by ISO27001 standards in educational institutions. They must ensure that required information security policies, procedures, and controls are implemented and adhered to by all educational community members. With support and commitment from leadership, educational institutions can achieve ISO27001 certification, showing the quality and reliability of their information security systems.

Additionally, leadership must ensure that information security awareness training programs are designed comprehensively and relevant to the educational institution's needs. This includes developing training materials appropriate to the educational context, arranging interactive and informative training sessions, and regularly evaluating the effectiveness of the training program. Leaders also need to set a good example in implementing good information security practices so that all educational community members can be inspired and motivated to follow in the same footsteps.

Educational institutions' leadership is responsible for ensuring that information security awareness training programs are integrated into the organizational culture. Leaders must ensure that information security values are applied in every activity and decision taken at all levels of educational institutions. In addition, leadership also needs to be actively involved in disseminating information regarding security threats, as well as actual information and mitigation strategies that can be carried out by all members of the education community. This will help increase awareness of potential information security risks. With strong commitment and support from leadership, educational institutions can create an environment safe and protected from information security threats. Through joint efforts in training, awareness development, policy implementation, and strict supervision, educational institutions can ensure that their sensitive data and information remain safe and protected from potential risks.

What are the key success factors for effective information security management?

In the study "Critical Success Factors Analysis on Effective Information Security Management: A Literature Review" by Yufei Yuan and Zhiling Tu from McMaster University, emphasis is placed on the importance of information security management within the scope of organizational management.

To cite this document:
Rijal, Demas Muhammad., Assydiqi, Mukhamad Fahmi., Prasetya, Yoel Rensisko., Ningsih, Lidya Nurhapsari Prasetya., Anindra, Nisya Kayla Putri. (2024). Information Security Awareness Analysis of the Threat of Data Leakage in Educational Institutions with the ISO 27001 Framework. *Journal of Digital Business and Innovation Management*, Vol. 3 No.1, pp. 36-52.

Information security management is a systematic process that effectively deals with information security threats and risks in an organization. Based on a review of information security standards and literature in information systems, six critical success factors (CSFs) were identified, and relationships between these factors were proposed. These factors include business alignment, organizational support, organizational awareness, IT competency, security control development, and performance evaluation.

The study results found that business alignment, organizational support, IT competency, and organizational awareness of security risks and controls are important elements in developing effective information security controls. This leads to successful management of information security. Business alignment ensures that information security goals and activities are aligned with business objectives and led by business management, while organizational support comes from the organizational structure and managerial decisions around information security. Organizational awareness includes all employees' understanding of security threats, fundamentals, and literacy.

Meanwhile, IT competency plays an important role in information security because information technology is used to maintain information security. By focusing on these key success factors, organizations can be more effective in implementing information security management. Providing sufficient resources, including staff, time, money, methods used in security work, facilities, tools, machines, and others, is crucial to supporting effective information security management. In addition, successful information security management also depends on establishing an organizational structure that supports reporting, communication, authority, and workflow. This study contributes theoretically by proposing a theoretical model of successful information security management and practically by helping organizations better implement information security management.

CONCLUSION

The results of the analysis show that information security awareness and risk management are very important in the context of information security, especially in educational institutions. The ISO 27001 standard is an effective framework for protecting an organization's information assets. This journal recommends risk management, awareness, and implementation of ISO 27001. Steps for implementing ISO 27001 include preparing documentation of implemented controls, internal audits, and periodic management reviews to ensure the policies and procedures aligned with organizational goals. A limitation of this journal is the lack of emphasis on the practical implementation of the recommendations presented. Therefore, further research could focus on the practical application of risk management methodology and implementing the ISO

27001 standard in educational settings. In addition, further research can also expand the scope to consider other aspects of information security, such as physical security, operations management, access management, and others to ensure the security and protection of assets and information.

Suggestions for further research based on this journal are to develop an appropriate risk assessment methodology after studying and analysing the risks associated with the organization. The methodology needs to include strategies for addressing, resolving and controlling the risks faced by the organization, as well as identifying and separating resources that may cause risks and threaten the organization's security. Further research could also focus on developing risk treatment plans that include basic risk mitigation strategies, such as acceptance, avoidance, transfer, or risk reduction to a certain level of acceptability.

REFERENCES

Abazi, B. (2020). A novel approach for information security risk assessment maturity framework based on ISO 27001 (Doctoral dissertation, Budapesti Corvinus Egyetem).

Alkahtani, H. K. (2018). Raising the information security awareness level in Saudi Arabian organizations through an effective, culturally aware information security framework (Doctoral dissertation, Loughborough University).

Allendevaux, S. (2021). How US State Data Protection Statutes Compare in Scope to Safeguard Information and Protect Privacy Using Iso/Iec 27001: 2013 and Iso/Iec 27701: 2019 Security and Privacy Management System Requirements as an Adequacy Baseline (Doctoral dissertation, Northeastern University).

Alzahrani, L., & Seth, K. P. (2021). The impact of organizational practices on the information security management performance. *Information*, *12*(10), 398.

Anwar, M. J., & Gill, A. (2021, January). Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model. In Australasian Conference on Information Systems 2020.

To cite this document:

Rijal, Demas Muhammad., Assydiqi, Mukhamad Fahmi., Prasetya, Yoel Rensisko., Ningsih, Lidya Nurhapsari Prasetya., Anindra, Nisya Kayla Putri. (2024). Information Security Awareness Analysis of the Threat of Data Leakage in Educational Institutions with the ISO 27001 Framework. *Journal of Digital Business and Innovation Management*, Vol. 3 No.1, pp. 36-52.

Banciu, D., Radoi, M., & Belloiu, S. (2020). Information security awareness in Romanian public administration: an exploratory case study. *Studies in Informatics and Control*, 29(1), 121-129.

Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of bitcoin. *IEEE communications surveys & tutorials*, *20*(4), 3416-3452.

Dada, M. S., Atobauka, I. S., & Ogunode, N. J. (2021). Deployment of Information Communication Technology for universities administration in Nigerian public universities: challenges and way forward. *Middle European Scientific Bulletin*, *19*, 163-175.

Dhakal, R. (2018). Measuring the effectiveness of an information security training and awareness program. *Doctoral Thesis*, Charles Sturt University.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, 4(2).

Dombora, S. (2016). Characteristics of information security implementation methods. *Book Chapter*, Institute of Communication Engineering OBUDA, Hungary.

Faris, S., Ghazouani, M., Medromi, H., & Sayouti, A. (2014). Information security risk assessment—A practical approach with a mathematical formulation of risk. *International Journal of Computer Applications*, 103(8), 36-42.

HONG, H. L. (2013). Feasibility Study on Incorporating IEC/ISO27001 Information Security Management System (ISMS) Standard in it Services Environment, *Doctoral dissertation*, Universiti Teknologi Malaysia).

Itradat, A., Sultan, S., Al-Junaidi, M., Qaffaf, R., Mashal, F., & Daas, F. (2014). Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study. *Jordan Journal of Mechanical & Industrial Engineering*, 8(2).

Kárász, B. and Kollár, C. (2021). Leadership Responsibilities in Information Security Awareness Development", *AARMS – Academic and Applied Research in Military and Public Management Science*. Budapest, 19(2), pp. 79–91. doi: 10.32565/aarms.2020.2.6.

Kurii, Y., & Opirskyy, I. (2022). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001: 2013. NIST Spec. Publ, 800(53), 10.

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.

Nasir, A., Abdullah Arshah, R., & Ab Hamid, M. R. (2019). A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher

educational institutions. *Information Security Journal: A Global Perspective*, *28*(3), 55-80.

Phirke, A., & Ghorpade-Aher, J. (2019). Best practices of auditing in an organization using ISO 27001 standard. *Int. J. Recent Technol. Eng*, 8(2), 691-695.

Ramadhan, N., & Rose, U. (2022). Adapting ISO/IEC 27001 Information Security Management Standard to SMEs.

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.

Stanciu, V., & Tinca, A. (2016). Students' awareness on information security between own perception and reality–an empirical study. *Accounting and Management Information Systems*, 15(1), 112-130.

Stefaniuk, T. (2020). Training in shaping employee information security awareness. *Entrepreneurship and Sustainability Issues*, 7(3), 1832.

Syifaurachman, A. W. (2023). Risk Assessment Related To Privacy Information On Electronic Money Server- Based Using Iso 27001 Iso 27005, Iso 27701. *Journal of Theoretical and Applied Information Technology*, 101(3).

Tu, Z., & Yuan, Y. (2014). Critical success factors analysis on effective information security management: A literature review. *Twentieth Americas Conference on Information Systems*, Savannah, pp. 1-15.

Zec, M. (2015). Cyber security Measures in SME's: a study of IT professionals' organizational cyber security awareness. Linnaeus University, Kalmar. Zugriff unter http://www. divaportal. org/smash/get/diva2, 849211.

To cite this document:

Rijal, Demas Muhammad., Assydiqi, Mukhamad Fahmi., Prasetya, Yoel Rensisko., Ningsih, Lidya Nurhapsari Prasetya., Anindra, Nisya Kayla Putri. (2024). Information Security Awareness Analysis of the Threat of Data Leakage in Educational Institutions with the ISO 27001 Framework. *Journal of Digital Business and Innovation Management*, Vol. 3 No.1, pp. 36-52.