JIKO (Jurnal Informatika dan Komputer)
Vol. 6, No. 2, Agustus 2023, hlm. 88-96
DOI: 10.33387/jiko.v6i2.6182

Accredited KEMENDIKBUD RISTEK, No.105/E/KPT/2022
p-ISSN: 2614-8897
e-ISSN: 2656-1948

CAUSES OF INEFFECTIVE IMPLEMENTATION OF IT GOVERNANCE IN RISK MANAGEMENT: A SYSTEMATIC LITERATURE REVIEW

Ananda E S Setyadji[1], Arief R Putrananda[2], Daffa H Permadi[3], Rais I Nustara[4], Reyhan B Pratama[5], Tegar A Masyhuda[6], Eva Hariyanti[7]

[123456]Undergraduate of Information Systems, Airlangga University, Indonesia
[7]Airlangga University, Indonesia
[*]Email: [1]ananda.elang.satriatama-2020@fst.unair.ac.id, [2]arief.rizqie.putrananda-2020@fst.unair.ac.id, [3]daffa.hafiizh.permadi-2020@fst.unair.ac.id, [4]rais.ilham.nustara-2020@fst.unair.ac.id, [5]reyhan.bayu.pratama-2020@fst.unair.ac.id, [6]tegar.alwinata.masyhuda-2020@fst.unair.ac.id, [7]eva.hariyanti@fst.unair.ac.id

(Received: 28 May 2023, Revised: 20 June 2023, Accepted: 27 June 2023)

Abstract

Information Technology Governance is currently widely implemented in companies. One of the domains that can be of concern is risk management. The application of TKTI in this domain can help companies identify, evaluate, reduce, and manage risks related to their business to achieve company goals better. In this case, three frameworks can be considered, including NIST, ISO 27001, and Octave, but implementing these frameworks only sometimes goes as planned. This study aims to identify the factors that cause the ineffectiveness of implementing Information Technology Governance (ITG) in the risk management domain using the NIST, ISO 27001, and Octave frameworks. Through an analysis of existing literature and data processing, this study found that factors such as lack of understanding of the framework, lack of adequate resources, and implementation challenges play an essential role in ineffectiveness. This study concludes by providing valuable insights for organizations seeking to strengthen their risk management capabilities.

Keywords: *risk management, it governance, nist, iso, octave*

**Corresponding Author: Ananda E S Setyadji*

1. INTRODUCTION

Risk management has become one of the most researched topics along with the increasing importance of information in everyday life. Information managed by the organization must be protected to prevent the risk of data theft or misuse [5]. Risk management is critical in a complex and changing business environment to maintain operational sustainability and achieve organizational goals. Many organizations use well-established and globally recognized frameworks to effectively manage risk.

In previous studies, there was a comparison of several frameworks in risk management. Most of them suggest ISO 27001 [12, 13], NIST [14, 15], and Octave [16]. In accordance with these recommendations, we chose the three frameworks to be discussed in this study.

However, the implementation of risk management standards and frameworks such as the NIST Cyber Security Framework (NIST CSF), ISO 27001, and OCTAVE often face various obstacles [8]. These obstacles can be in the form of a lack of resources, a lack of top management support, the complexity of standards implemented, and a limited understanding of the standards and frameworks applied [6].

Implementation of risk management standards requires significant changes to the organization's business processes and information technology. This change requires a large investment so that it becomes a consideration for organizations, especially small and medium organizations (SMEs). In addition, the integration of risk management standards into the organization's business processes can take years so the organization requires patience and determination in its implementation [10].

The active participation and support of top management is critical to the successful implementation of risk management standards. [9]. Unfortunately, top management involvement is not

always easy to obtain due to different priorities and a lack of understanding of the importance of information risk management [10].

In addition to internal organizational factors, the implementation of risk management standards is also faced with external challenges. The rapid development of information technology has made information security threats increasingly complex and diverse [7]. To deal with new threats, organizations must constantly update their procedures and controls. This makes it difficult for organizations, especially small and medium-sized organizations (SMEs), to comply with information security and privacy standards. In addition, the costs incurred for security and privacy devices that comply with international standards are quite expensive for many organizations [4].

Therefore, this literature review aims to analyze the inhibiting factors in the implementation of international standard risk management frameworks such as NIST, ISO 27001, and OCTAVE. This implementation is often faced with obstacles and challenges that can affect its success and effectiveness. This literature review can be used to help identify inhibiting factors that may arise. By understanding these inhibiting factors, organizations can develop appropriate strategies to overcome obstacles during implementation. By overcoming the inhibiting factors, the organization can ensure that the implementation of risk management standards runs more effectively and efficiently. This can contribute to higher levels of information security, protection of critical assets, and compliance with regulatory and supervisory agency standards.

2. RESEARCH METHOD

The research method used in this study is a Systematic Literature Review, which is a term used to refer to a particular research or research methodology and development carried out to collect and evaluate related research on a particular topic [11].

2.1 Research Question

At this stage it is done by making questions that can answer the objectives of this research. The questions in this study, namely:

RQ: What are the factors that cause a company or agency to experience ineffectiveness in managing risks in the Information Technology Governance domain when implementing the NIST framework, ISO 27001, and Octave?

2.2 Article Search

The journal sources used in this study came from Google Scholar, IEEE, Springer, Semantic Scholar, ResearchGate, Trans Tech Publication, Procedia Computer Science, Iopscience, and IGI. In addition, article searches are also carried out by identifying keywords and their categories, which are as follows :

Table 1. Categories and Keywords

Category	Keyword
Information Technology Governance Framework in the domain of risk management in companies	NIST, ISO 27001, Octave
The results of testing the value of the application of the Information Technology Governance framework in the risk management domain within the company	TKTI framework test results, Information Technology Governance framework test results, NIST effectiveness, ISO 27001 effectiveness, ISO 27001
Factors causing the ineffective implementation of Information Technology Governance in the risk management domain within the company	Lack of framework implementation, Framework implementation failure, Incompatibility of framework implementation, Octave fail, NIST fail, ISO 27001 fail, Octave implementation, NIST failure

In searching for articles that are relevant to the category "Information Technology Governance Framework in the domain of risk management in companies" and the keywords "NIST, ISO 27001, Octave", categories and keywords are combined by linking categories with keywords. Based on this, an article search was performed by combining the following categories and keywords: Information Technology Governance Framework in the risk management domain in companies AND "NIST" OR "ISO 27001" OR "Octave". Furthermore, searches can be performed with categories and keywords in English format such as IT Governance Framework in Risk Management Domain for Company AND "NIST" OR "ISO 27001" OR "Octave".

In the category "Results of testing the value of applying the Information Technology Governance framework in the domain of risk management within the company" with the keywords "Results of testing the TKTI framework, Testing results of the Information Technology Governance framework, NIST effectiveness, ISO effectiveness", an article search is performed by combining categories and the following keywords: Test results of the Information Technology Governance framework in the risk management domain in companies AND "NIST effectiveness" OR "ISO effectiveness". Combining these categories and keywords can also be done in an English format such as Results of Information Technology Governance Framework Testing in Risk Management Domain for Companies AND "NIST effectiveness" OR "ISO effectiveness".

The criteria and limitations of the article sources used in this study are as follows:

Table 2. Criteria and Limitations

Electronic article sources	Searched Items	Language	Publication Period

Google Scholar IEEE Springer Sematic Scholar ResearchGate Trans Tech Publication Procedia Computer Science Iopscience IGI	Article	English Indonesian	2013-2023

2.3 Literature Selection

In this study, inclusion and exclusion criteria were used to find articles that were relevant to the research objectives. The inclusion criteria include : (I1) articles in Indonesian and English, (I2) articles related to the application of Information Security Technology in the risk management domain, (I3) using the NIST framework, ISO 27001, or Octave, and (I4) articles reviewing deficiencies, failure, ineffectiveness, or implementation incompatibility in implementing TKTI.

Exclusion criteria included: (E1) articles published in predatory journals or conferences listed on BEALL'S LIST, and (E2) articles that were not fully accessible.

In the process of searching for articles that met the inclusion criteria and were not included in the exclusion criteria, an analysis was carried out using keywords, titles, and abstracts of the articles. After that, it was followed by downloading and analyzing the complete article to re-evaluate the inclusion and exclusion criteria. Articles that meet the predetermined criteria are called primary studies. Next, we filtered the primary studies that had been analyzed according to the inclusion and exclusion criteria to obtain results that were more relevant to the research objectives.

2.4 Quality Assessment

Assessment of the quality of the primary study was carried out with the aim of assessing the credibility and reliability of the sources of information used. In order to achieve this goal, standardized quality assessment criteria were adopted taken from previously published studies. These quality assessment criteria are then used to evaluate the selected primary studies, so as to ensure the validity and quality of the information produced. Overall, the use of standardized quality assessment criteria can provide significant benefits in ensuring the credibility and reliability of the sources of information used. The following are the criteria for assessing the quality of the selection of studies.

Table 3. Quality Assessment

Item	Assessment Criteria	Score	Description
KP1	Has the research purpose been clearly stated	-1	No, the purpose is not explained
		0	Objectives are partially but not clearly explained
		1	Yes, the purpose is well explained and clear
KP2	Does the study provide an elaborate explanation of the proposed resolution or methodology?	-1	No, the specifics are not provided.
		0	Some, In order to utilize a particular approach or solution, it is necessary to consult relevant references.
		1	Yes, the presented details allow for the implementation of the approach.
KP3	Is the suggested solution or approach deemed legitimate and effective?	-1	No, the approach is not validated.
		0	Part of it has been validated in the laboratory or only part of the proposal has been validated
		1	Yes, validated with case studies.
KP4	Does the research put forth a perspective or viewpoint?	-1	Yes, present an opinion or point of view.
		0	In part, because the appropriate work has been described and the article has been set in a particular context.
		1	No, scholarly articles are founded on empirical research.
KP5	Has this research been referenced in a scientific publication?	-1	No instances of studies being cited have been observed.
		0	To some extent, approximately 20% of scientific papers reference the mentioned study.
		1	Indeed, the research is referenced in more than five

scientific papers.

2.5 Backward and Forward Snowballing Techniques

Snowballing is a technique used in the literature search process to find articles that are relevant to the research topic. This technique involves using found articles as a starting point for finding new articles that are still relevant to the research topic. In this way, the researcher can identify related articles that might not appear in the initial search and obtain a complete list of references to support the research. Snowballing can be done forward (forward) or backward (backward) depending on the starting point of the selected search.

Forward snowballing is a methodology in which researchers start by exploring previously identified relevant articles, then move on to discover additional articles referenced within those initial articles. Tracing these citation trails allows researchers to find the most recent articles that are still relevant to the research topic.

Meanwhile, Backward Snowballing is a technique where researchers start searching for articles that are very relevant to the research topic and then look for articles that cite the article. By checking the list of references listed in these highly relevant articles, researchers can find other related articles that may not appear in the initial search.

In order to evaluate risk management, we conducted Forward and Backward Snowballing searches and found two journals that could be useful references. These journals discuss various aspects related to risk management, including risk identification, risk assessment, and risk management.

2.6 Data Extraction and Synthesis

In order to obtain information that was relevant to the research questions, the authors carried out a data extraction process. They used a predefined extraction form, which allowed them to record all the necessary details of the primary study. This form helped them to accurately capture all the relevant information that was related to the research question.

3. RESULT AND DISCUSSION

The results obtained will be selected based on inclusion and exclusion which have been included at the Planning Review stage. After that, a final filter will be carried out based on the Research Question in this study.

3.1 Result

The results obtained according to the keywords that have been included and the selection obtained are 26 relevant articles with the following article titles:

Table 4. Article Collection

No.	Article Title	Publication Year	Article Source
1.	Evaluation Of IS Risk Management Using Octave Allegro In Education Division	2018	IEEE
2	Sistem Pemeriksa Keamanan Informasi Menggunakan National Institute Of Standards And Technology (Nist) Cybersecurity Framework	2019	Google Scholar
3	Effectiveness and Adoption of NIST Managerial Practices for Cyber Resilience in Italy	2021	Springer
4	Studi Komparasi Framework Nist Dan ISO 27001 Sebagai Standar Audit Dengan Metode Deskriptif Studi Pustaka	2021	Google Scholar
5	Evaluasi Risiko Keamanan Informasi Menggunakan Octave-S	2018	Google Scholar
6	Security Information and Risk Management Assessment	2015	Trans Tech Publications Ltd.
7	Identifikasi, Penilaian, Dan Mitigasi Risiko Keamanan Informasi Pada Sistem Electronic Medical Record (Studi Kasus : Aplikasi Healthy Plus Modul Rekam Medis Di RSU Haji Surabaya)	2014	Google Scholar
8	Efisiensi ISO 27001, ISO 9001, dan Standar LPSE pada Data Center dan e-Procurement Pemerintahan	2021	Google Scholar
9	Review of Cyber Security on Oil and Gas Industry in United Arab Emirates: Analysis on the Effectiveness of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework	2021	Google Scholar
10	Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A	2014	IEEE
11	Research on the Impact of Information Security Certification and Concealment on Financial Performance: Impact of ISO 27001 and Concealment on Performance	2022	Google Scholar
12	Evaluation of ISO 27001 implementation towards information security of cloud service customers in	2018	Iopscience

	PT. IndoDev Niaga Internet		
13	Maturity Framework Analysis ISO 27001: 2013 on Indonesian Higher Education	2020	Google Scholar
14	Analisis, Evaluasi, Dan Mitigasi Risiko Aset Teknologi Informasi Menggunakan Framework Octave Dan Fmea (Studi Kasus: Unit Pengelola Teknis Teknologi Informasi Dan Komunikasi Universitas Xyz)	2021	Google Scholar
15	Manajemen Risiko Infrastruktur Cloud Pemerintah Menggunakan Nist Framework Studi Kasus Lembaga Ilmu Pengetahuan Indonesia (LIPI)	2017	Google Scholar
16	Risk Management Analysis on Organizational Website using Octave Allegro Method	2020	IEEE
17	Analisis Manajemen Risiko Infrastruktur Dengan Metode NIST (National Institute of Standards and Technology) SP 800-30 (Studi Kasus: STMIK Rosma)	2021	Google Scholar
18	Audit Information System Risk Management Using Iso 27001 Framework at Private Bank.	2018	Google Scholar
19	Risk Management Analysison Administration System using OCTAVE Allegro Framework	2021	Google Scholar
20	Security Controls for Monitored Use of USB Devices Based on the NIST Risk Management Framework	2016	IEEE
21	Information Security Risk Management Models For Cloud Hosted Systems: A Comparative Study	2022	Procedia Computer Science
22	Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro	2013	Google Scholar
23	Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study	2014	Google Scholar
24	Manajemen Keamanan Informasi Di Perpustakaan Menggunakan Framework SNI ISO/IEC 27001	2018	Google Scholar
25	Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia	2014	IEEE
26	NIST CyberSecurity Framework Compliance A Generic Model for Dynamic Assessment and Predictive Requirements	2015	IEEE

The selection of these articles was conducted with meticulous attention to their alignment with the study's objectives and research questions. By employing specific keywords, a focused search was performed to ensure that the identified articles closely matched the intended scope and emphasis of the investigation.

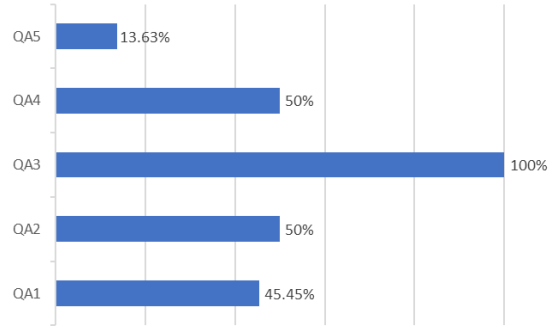

Figure 2. Assessment Score Visualization

The first criterion (QA1) evaluates the research objectives of each study, with 45.45% of studies meeting this criterion. The second criterion (QA2) evaluates whether the study provides a detailed description of the method or solution, with 50% of studies satisfying this criterion.

The third criterion (QA3) assesses the method used to validate the study results, finding that 100% of studies used an appropriate validation method, namely case studies. The fourth criterion (QA4) evaluates whether the study adopts a particular perspective or opinion, with 50% of studies meeting this criterion.

The fifth criterion (QA5) examines the number of citations that each study received, finding that 13.63% of studies were cited five or more times by other studies.

In summary, while nearly half of the studies met the first two criteria (QA1 and QA2) by stating clear research objectives and describing their methods/solutions in detail, and all studies used suitable validation methods (QA3), only about half adopted a clear perspective (QA4) and few were frequently cited (QA5). Overall, there is room for improvement in articulating perspectives and increasing impact based on citation frequency. The

following is the score of the research that has been done in Figure 2.

Table 5. Data Extraction

No.	Study Data	Description	Relevant RQ
1	Identifier		Study Overview
2	Title		Study Overview
3	Authors		Study Overview
4	Year		Study Overview
5	Article Source		Study Overview
6	Domain	What is the domain being measured?	RQ1
7	Research Goal	What is the aim of the research?	RQ1
8	Research Method	What method that they use?	RQ1
9	Research Problem	What are the problems with the framework used?	RQ1
10	Research Goal Category	What framework is being used?	RQ1

The authors conducted a review of 65 articles as part of this study. The articles were selected through the steps of determining research questions and predetermined research objectives. To find articles, a search is carried out using relevant keywords through various sources that are considered credible, such as Google Scholar, ResearchGate, IEEE, and other sources. After that, the articles were filtered using inclusion and exclusion criteria, and evaluated for quality. The articles reviewed included articles that had been published both nationally and internationally in the period between 2013 and 2023. The contents of these articles discussed deficiencies, failures, ineffectiveness, and inappropriate implementation of the NIST framework, ISO 27001, and Octave. After going through the screening and assessment process, there were finally 26 articles that met the predetermined criteria.

The results of the primary study are based on the factors that cause ineffectiveness in the management of information technology in the risk management domain when implementing the ISO 27001 framework, Octave and NIST (National Institute of Standards and Technology) indicate that there are several factors that play an important role. In this context, these factors can be attributed to a lack of understanding and a lack of resources. These factors were obtained from reviewing twenty-six papers which were divided into seven main sources in references. The following table presents information related to primary studies by category.

Table 6 explains that ineffectiveness in managing information technology risks in the field of governance occurs when implementing the ISO 27001, Octave, and NIST frameworks. The main factors that lead to this ineffectiveness can be grouped into two categories.

The first category, lack of understanding, encompasses the critical issues of awareness and knowledge. In terms of awareness, one of the main challenges lies in the management's insufficient understanding and recognition of the importance of information security within the organization. This lack of awareness can lead to a lack of prioritization and allocation of resources towards information security measures. Furthermore, employees may also lack awareness of the potential risks and the significance of their role in maintaining information security. The knowledge-related aspect of this category involves the deficiency in skills and expertise required for effective management of information technology risks. Organizations often struggle with a lack of proficiency in managing devices and systems, which hampers their ability to implement the chosen frameworks accurately. Additionally, there may be limited understanding of the intricacies and nuances of the ISO 27001, Octave, and NIST frameworks, resulting in their suboptimal utilization.

The second category pertains to resource constraints, encompassing various dimensions such as human resources, financial resources, IT resources, and methods/procedures. In terms of human resources, organizations may face challenges due to high turnover rates and a scarcity of experts in the field of information security. The loss of knowledgeable personnel and the difficulty of finding suitable replacements can severely impede effective risk management practices. Moreover, financial constraints pose a significant hurdle, as the implementation of robust information security measures often necessitates substantial investments. Limited budgets and inadequate financial resources can compromise the organization's ability to employ advanced technologies, conduct thorough risk assessments, and implement necessary security controls. Furthermore, the scarcity of backup devices for critical systems and the absence of standardized procedures in business processes contribute to the inefficiency of information technology governance. This lack of redundancy and standardized practices increases the vulnerability of the organization to potential risks and reduces its ability to respond effectively to security incidents. Additionally, the complexity of adapting and aligning with standard practices within the chosen frameworks can hinder successful implementation and subsequent risk management efforts. The impacts of these factors are far-reaching. Ineffectiveness in managing information technology risks can lead to compromised data security, increased susceptibility to cyber threats, and potential breaches that may result in reputational damage, financial losses, and legal repercussions for the organization. Moreover, inadequate risk management practices can hinder regulatory compliance efforts and jeopardize the organization's

ability to meet industry-specific standards and guidelines.

The factors contributing to the ineffectiveness of information technology governance must be properly addressed by organizations. If these factors are not adequately addressed, organizations may face serious consequences. The impacts include financial losses due to data theft, a decrease in trust from customers and business partners, irreparable damage to reputation, as well as regulatory violations and potential penalties. Additionally, organizations may experience non-compliance with security standards and industry regulations, which can jeopardize business relationships and diminish growth opportunities. Therefore, it is crucial for organizations to take appropriate measures to achieve important goals such as strengthening risk management practices, enhancing security posture, and reducing potential risks and vulnerabilities associated with information technology.

Table 6. End Result

No.	Category	Sub-Category	Factor	Relevant Article
1	Lack of understanding	Awareness	1. Lack of commitment from management. 2. A culture that is not aware of the importance of information security, and has embedded it in daily activities. 3. There is no disciplinary action when something goes wrong which results in a security breach	[3], [7], [12], [24]
		Knowledge	1. Lack of skills in managing devices 2. Lack of understanding of the framework	[1], [12], [5], [19]
2	Lack of Resources	Human Resources	1. High employee turnover 2. Lack of experts in the field of information security	[7], [10], [25]
		Financial Resources	1. Insufficient funding for activities. 2. Implementation involves high costs (high costs for IT security services and support)	[1], [5], [25]
		IT Device Resources	1. Some devices that are critical to running business processes do not have backup devices.	[13], [22] [26],
		Methods and Procedures	1. There is no clear line of relationship or mapping between NIST's CSF activities and outcomes and the organization's cybersecurity (CS) strategy. 2. Implementation takes a long time 3. The complexity of adapting standard practices to the organizational environment 4. Lack of standard procedures in every existing business process 5. Framework functions that are not fully implemented.	[2], [8], [13], [14], [17], [22], [26]

3.2 Discussion

This study highlights the ineffectiveness of information technology governance in risk management using the ISO 27001, Octave, and NIST frameworks. The main cause is a lack of understanding and lack of adequate resources.

Lack of understanding is subdivided into two categories: lack of awareness and lack of knowledge. To overcome this, organizations need to increase awareness of security risks and develop a culture that is aware of the importance of information security through training and outreach. Training, certification, and knowledge exchange between teams are also required to improve skills in managing tools and understanding of frameworks.

The second category is a lack of resources, including human resources, financial resources, IT tools, and methods and procedures. Organizations must reduce employee turnover by increasing employee satisfaction and well-being, as well as forming training partnerships with educational institutions. A sufficient budget and finding alternative financial resources are required. Adequate backup policies and budgets should be developed. A clear mapping between framework activities and results, as well as a structured implementation approach, including the establishment of documented standard procedures, are required.

By addressing these factors, organizations can improve understanding, resource allocation, and effectiveness in managing information technology risks using the ISO 27001, Octave, and NIST frameworks.

4. CONCLUSION

This paper examines the factors that can influence ineffectiveness in Information Technology Governance, especially in the Risk Management domain. Lack of understanding in implementing the framework and lack of resources are problems that need attention by organizations. This research provides a basis for taking appropriate action to increase understanding, awareness, and allocation of adequate resources to achieve effectiveness in risk management.

Acknowledgment

We would like to express our deepest gratitude to our lecturer, Ms. Eva Hariyanti, as the

corresponding author in this study. Their contributions and assistance in carrying out research and writing this manuscript were very meaningful and helped us in completing this research.

5. REFERENCE

[1] Abdullah, Kholiq, Ika Nurlaili Isnainiyah, and Mochamad Isnin Faried. "Risk Management Analysis on Organizational Website using Octave Allegro Method." 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS). IEEE, 2020.

[2] Aedah, Abd Rahman, and Saragih Hoga. "Maturity framework analysis ISO 27001: 2013 on indonesian higher education." International Journal of Engineering & Technology 9.2 (2020): 429-436.

[3] ALDhanhani, Mohamed Jumah. "Review of Cyber Security on Oil and Gas Industry in United Arab Emirates: Analysis on the Effectiveness of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12.11 (2021): 714-720.

[4] Alshitri, Khalid I., and Abdulmohsen N. Abanumy. "Exploring the reasons behind the low ISO 27001 adoption in public organizations in Saudi Arabia." 2014 International Conference on Information Science & Applications (ICISA). IEEE, 2014.

[5] Annarelli, Alessandro, et al. "Effectiveness and adoption of NIST managerial practices for cyber resilience in Italy." Intelligent Computing: Proceedings of the 2021 Computing Conference, Volume 3. Springer International Publishing, 2021.

[6] Anjani, Dea, et al. "IDENTIFIKASI, PENILAIAN, DAN MITIGASI RISIKO KEAMANAN INFORMASI PADA SISTEM ELECTRONIC MEDICAL RECORD (STUDI KASUS: APLIKASI HEALTHY PLUS MODUL REKAM MEDIS DI RSU HAJI SURABAYA)."

[7] Anton, Nicolae, and Anişor Nedelcu. "Security Information and Risk Management Assessment." Applied Mechanics and Materials. Vol. 809. Trans Tech Publications Ltd, 2015.

[8] A. Jeffry et al., "Audit Fingerprint pada PT X dengan Framework COBIT 4.1," J. Informatika dan Sistem Informasi, vol. 4, no. 1, pp. 34-43, 2018.

[9] Bahrudin, Muhammad, and Firmansyah Firmansyah. "Manajemen keamanan informasi di perpustakaan menggunakan Framework SNI ISO/IEC 27001." Media Pustakawan 25.1 (2018): 43-50.

[10] Bhakte, Rajbhooshan, Pavol Zavarsky, and Sergey Butakov. "Security Controls for Monitored Use of USB Devices Based on the NIST Risk Management Framework." 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC). Vol. 2. IEEE, 2016.

[11] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," Int. J. Crit. Infrastruct. Prot., vol. 8, pp. 53-66, 2015.

[12] C. Kuligowski, "Comparison of IT Security Standards," Masters of Science Information Security and Assurance, 65, 2009. [Online]. Available: http://www.federalcybersecurity.org/CourseFiles/WhitePapers/ISOvNIST.pdf.

[13] D. Ashenden, "Information Security management: A human challenge?" Inf. Secur. Tech. Rep., 2008.

[14] E. Triandini et al., "Metode Systematic Literature Review untuk Identifikasi Platform dan Metode Pengembangan Sistem Informasi di Indonesia," Indonesian J. Inf. Syst., 2019.

[15] Elanda, Anggi, and Robby Lintang Buana. "Analisis Manajemen Risiko Infrastruktur Dengan Metode NIST (National Institute of Standards and Technology) SP 800-30 (Studi Kasus: STMIK Rosma)." Elkom: Jurnal Elektronika dan Komputer 14.1 (2021): 141-151.

[16] Fajar, Ahmad Nurul, Hendy Christian, and Abba Suganda Girsang. "Evaluation of ISO 27001 implementation towards information security of cloud service customer in PT. IndoDev Niaga Internet." Journal of Physics: Conference Series. Vol. 1090. No. 1. IOP Publishing, 2018.

[17] Gagas, Rut Juniati, Ilham Syah, and Ferdy Febryanto. "ANALISIS, EVALUASI, DAN MITIGASI RISIKO ASET TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK OCTAVE DAN FMEA (STUDI KASUS: UNIT PENGELOLA TEKNIS TEKNOLOGI INFORMASI DAN KOMUNIKASI UNIVERSITAS XYZ)." Jurnal Khatulistiwa Informatika 9.2 (2021).

[18] H. Susanto, M. Almunawar, and Y. Tuan, "Information security management system standards: A comparative study of the big five," Int. J. Electr. Comput. Sci. IJECS-IJENS, vol. 11, no. 5, pp. 23-29, 2011.

[19] Harumi, Faradina, Lukito Edi Nugroho, and Sri Suning Kusumawardani. "Efisiensi ISO 27001, ISO 9001, dan Standar LPSE pada Data Center dan e-Procurement Pemerintahan." JISKA (Jurnal Informatika Sunan Kalijaga) 6.1 (2021): 50-58.

[20] Irsheid, Anas, et al. "Information security risk management models for cloud hosted systems: A comparative study." Procedia Computer Science 204 (2022): 205-217.

[21] Itradat, Awni, et al. "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 (2014).

[22] J. F. Courtney, "Cybersecurity Issues and Challenges: In Brief," Report, Congressional Research Service, 2020.

[23] Jakaria, Deni Ahmad, and R. Teduh Dirgahayu.

"Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro." Seminar Nasional Aplikasi Teknologi Informasi (SNATI). 2013.

[24] KABAN, EKIN, and NILO LEGOWO. "AUDIT INFORMATION SYSTEM RISK MANAGEMENT USING ISO 27001 FRAMEWORK AT PRIVATE BANK." Journal of Theoretical & Applied Information Technology 96.1 (2018).

[25] M. Alshaikh et al., "Requirements Engineering for Cybersecurity: Issues and Challenges," in 5th IEEE International Conference on Cyber Security and Cloud Computing (IEEE CSCloud), 2017, pp. 15-20.

[26] M. Bartnes, N. Moe, and P. Heegaard, "The future of information security incident management training: A case study of electrical power companies," Computers & Security, vol. 61, pp. 10.1016/j.cose.2016.05.004, 2016.

[27] M. Iorga and A. Karmel, "Managing Risk in a Cloud Ecosystem," IEEE Cloud Comput., vol. 2, pp. 51-57, 2015.

[28] N. Gushelmi, M. Neldi, and Y. Septiadi, "Analisa Kualitas Sistem Informasi Manajemen Menggunakan Framework Cobit 5 (Studi Kasus Pada Kantor Dprd Kabupaten Sijunjung)," J. Teknologi Dan Sistem Informasi Bisnis, vol. 4, no. 1, pp. 89-96, 2022.

[29] Prabowo, Wahyu Setyo, et al. "Manajemen Risiko Infrastruktur Cloud Pemerintah Menggunakan Nist Framework Studi Kasus Lembaga Ilmu Pengetahuan Indonesia (LIPI)." Jurnal Penelitian Pos dan Informatika 7.1 (2017): 17-36.

[30] Pratama, Rinaldi, Dedy Syamsuar, and Yesi Novaria Kunang. "Evaluasi Risiko Keamanan Informasi Menggunakan Octave-S." Seminar Nasional Teknologi Informasi dan Komunikasi (SEMNASTIK). Vol. 1. No. 1. 2018.

[31] R. A. Caralli, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," Pittsburgh: Carnegie Mellon University, 2007.

[32] R. Sabillon et al., "Cybersecurity Challenges and the Small and Medium Enterprise," in Proceedings of the 10th International Conference on Security of Information and Networks, ACM, New York, NY, 2016, pp. 501-504.

[33] S. Posthumus, "A framework for the governance of information security," Computers & Security, vol. 23, pp. 638-646, 2004.

[34] S. Rizvi et al., "Security Risks, Challenges, and Their Management in Cloud Computing," in Proceedings of the 11th International Conference on Security of Information and Networks, Athens, Greece, 2018, pp. 305-312.

[35] Sama, Hendi, et al. "Studi Komparasi Framework NIST dan ISO 27001 sebagai Standar Audit dengan Metode Deskriptif Studi Pustaka." Rabit: Jurnal Teknologi Dan Sistem Informasi Univrab 6.2 (2021): 116-121.

[36] Shojaie, Bahareh, Hannes Federrath, and Iman Saberi. "Evaluating the effectiveness of ISO 27001: 2013 based on Annex A." 2014 Ninth International Conference on Availability, Reliability and Security. IEEE, 2014.

[37] Sugara, Victor Ilyas, Hadi Syahrial, and Muhammad Syafrullah. "Sistem Pemeriksa Keamanan Informasi Menggunakan National Institute of Standards and Technology (Nist) Cybersecurity Framework." Komputasi: Jurnal Ilmiah Ilmu Komputer dan Matematika 16.1 (2019): 203-212.

[38] Sukri, Muh, and Imam Riadi. "Risk Management Analysison Administration System Using Octave Allegro Framework." International Journal Of Computer Applications 975 (2021): 8887.

[39] Suroso, Jarot S., and Sri Mumpuni Ngesti Rahaju. "Evaluation Of IS Risk Management Using Octave Allegro In Education Division." 2018 International Conference on Orange Technologies (ICOT). IEEE, 2018.

[40] Teodoro, Nuno, Luís Gonçalves, and Carlos Serrão. "Nist cybersecurity framework compliance: A generic model for dynamic assessment and predictive requirements." 2015 IEEE Trustcom/BigDataSE/ISPA. Vol. 1. IEEE, 2015.

[41] V. Kundra, "Federal Cloud Computing Strategy," Washington: U.S. Chief Information Officer, 2011.

[42] Wu, Wenqing, et al. "Research on the Impact of Information Security Certification and Concealment on Financial Performance: Impact of ISO 27001 and Concealment on Performance." Journal of Global Information Management (JGIM) 30.3 (2021): 1-16.

[43] Z. D. K. Washilatul Arba'ah, E. Utami, and A. H. Muhammad, "Information & Technology Audit of E-Government Using COBIT: A Literature Review," Jurnal Informatika dan Komputer, vol. 6, no. 1, 2023. [Online]. Available: http://dx.doi.org/10.33387/jiko.v6i1.5606.