DOI: https://doi.org/10.52436/1.jutif.2024.5.1.1223
p-ISSN: 2723-3863
e-ISSN: 2723-3871

SYSTEMATIC LITERATURE REVIEW ON INFORMATION SECURITY RISK MANAGEMENT IN PUBLIC SERVICE ORGANIZATIONS

Rifia Andita[1], Faizan Aditya[2]

[1]Faculty of Management, Universitas Nasional, Indonesia
[2]National Cyber and Crypto Agency, Indonesia
Email: [1]rifia.andita@gmail.com, [2]faizanaditya@gmail.com

(Article received: July 18, 2023; Revision: August 11, 2023; Published: February 31, 2024)

Abstract

For an organization, information security is a priority. Within the rapid growth of information technology, information becomes easier to access, processed, and used in organization globally. Using information systems in government will improve efficiency, effectiveness, transparency, and accountability in respect of good governance. Regarding the use of information technology sometimes it does not align with its purpose, because there is uncertainty or particular risk that must be faced in using IT. The study conducts a systematic literature review (SLR) to understand the steps and frameworks for information security risk management. Data sources such as IEEE Xplore, ScienceDirect, Proquest, and ACM from 2009 to 2023 are used to obtain literature. Sixteen papers were obtained to complete this study. This research identifies three frameworks that can be used in information security risk management: ISO 27005, NIST SP 800-30, and Cobit 5 For Risk. stages in information security risk management in general are Context Formation, Risk Identification, Risk Assessment, Risk Treatment, and Risk Monitoring.

Keywords: *risk management, public service organizations, information security*.

1. INTRODUCTION

Information and communication technology (ICT) has helped governments and other organizations to facilitate citizens and other stakeholders in ways that are possible. By deciding on ICT, it becomes very easy for government organizations to collect, filter, collect, and produce data that were previously considered the most difficult aspects of e-governance [1]. In Indonesia, e-government innovation has been started in recent years. In addition to the need, both the central and regional governments for an integrated system, the development of e-government in Indonesia begins with the issuance of the Presidential Instruction of the Republic of Indonesia Number 3 of 2003 concerning National Policies and Strategies for e-Government Development. To offset the current industry 4.0 demands, the Government of the Republic of Indonesia then issued Presidential Regulation (Perpres) Number 95 of 2018 concerning Electronic-Based Government Systems (SPBE). This regulation is a policy to create clean, effective, transparent, and accountable governance as well as quality and reliable public services.

Noting the development of ICT use and complexity in the era of globalization, a condition has been created that places information as a valuable commodity. Good information is essential for effective operations and decision making at all levels of the business [2]. According to Whitman & Mattord, information is one of the important assets to protect its security [3]. The organization needs to pay attention to the security of its information assets, information leakage and failure in the system can result in losses both in the financial and productivity side of the company.

Information security is the protection of information from various threats in to ensure the continuation of business processes, reduce business risks, and increase return on investment (ROI) and business opportunities [4]. In designing information systems security systems there are aspects of information security that need to be considered. These aspects include Confidentiality, Integrity, and Availability [5]. These three aspects are vulnerable to the threat of attacks that threaten their existence both attacks on information sources. It becomes extremely important for organizations, especially public service providers to use information security management system that manages information assets effectively [6]. From vulnerability and potential threats that produce negative impacts, can pose an information security risk to the organization's business processes in public service organizations. Therefore, we need information security risk management that is applied to public service organizations. The risk management process should be an essential function beyond a technical scope in public service organizations [7]. Information Risk Management is critical for a business to sustain growth and development. It is important to mention that risk management is a crucial part of any organization's existence, without which any incident can be devastating [8]. The risk management process in public service organizations is a continuous event, so its repeatability is very important [7].

The literature on information security risk management is replete with diverse taxonomies, frameworks, and methodologies. Countless sources present a wide array of structured categorizations, systematic frameworks, and systematic approaches that aim to address the complexities of managing risks in the realm of information security. Paz and Picon conduct research on risk management methodologies for complex organizations in industry 4.0 and 5.0 [9]. In the government sector, several studies regarding the implementation standards of risk management in e-government include information technology risk management on e-government [10], ISO 31000 for public sector organizations [11], IT project risk management [12], software lifecycle [13] [14], ISO 27000 for information security risk management [15] [16] [17], cloud computing [18], and COBIT as a tool for calculating the maturity level of e-government risk management [19].

This paper analyzes information security risk management procedures in public service organizations through several literature studies concerning the framework used. This paper provides a systematic review of risk management frameworks, such as ISO/IEC 27005, NIST SP 800-30, and COBIT 5 For Risk, with a focus on their risk management methodologies.

2. RESEARCH METHODS

2.1. Literature Review

Information is an asset for the organization. Therefore, information must be secured so that it is free from threats or dangers. Information security is the safeguarding of information from all threats that may occur to ensure or guarantee business continuity, minimize business risk, and maximize or accelerate the return on investment and business opportunities [4].

United States National Information System Security defines information system security as protection of information systems against unauthorized access or modification of information, whether that occurs during storage, processing or transit, denial of service to authorized users or providing services to unauthorized users, also includes actions the actions needed to detect and fight the threat [20].

Based on ISO 27001, the goal of information security is to be consistent with information security policies, be measured, pay attention to information security requirements and the results of risk assessment and handling, communicated, and updated according to needs. [21].

Risk is a combination of impacts caused by the occurrence of an unexpected event with the likelihood of that event occurring [22]. Risk management is a process in identifying, estimating, and determining steps to reduce risk to an acceptable level [23].

The information security risk management process is regulated in ISO 27001 which is divided into four stages: Plan, Do, Check, and Act [22]. Information security risk management can support an information security management system.

2.2. Method

Systematic Literature Review (SLR) is a secondary study to map, identify, critically evaluate, consolidate, and collect the results of relevant primary studies on a certain research topic [3]. SLR becomes a standard method for getting answers by reviewing the literature based on earlier relevant studies. The purpose of conducting SLR is to summarize earlier research, identify gaps that need to be met between previous and current research, produce coherent reports / synthesis, and make a research framework.

The purpose of the literature study in this research is to further understand the methods and framework of information security risk management. To obtain comprehensive results, this study conducted studies on several literature published from the IEEE Xplore, Scopus, ScienceDirect, ProQuest, and ACM database journals from 2009 to 2023. Stages of the systematic literature review were used in this study consists of three parts, including planning, implementation, and reporting. The process applied in conducting a systematic literature review involve these steps: 1) defining the research question, 2) determine the search strategy, 3) selecting the proper studies, and 4) extracting the data and synthesis.

2.3. Research Question

Research Question (RQ) was determined to keep the focus of the literature review. In formulating the RQ, this study used the PICOC Formula (Population, Intervention, Comparison, Outcome, and Context). Table 1 shows the PICOC structure of the research questions.

Table 1. The Criteria of Research Question

Field	Description
Population	IT risk management, ICT risk management, information security risk management
Intervention	Framework used for information security risk management
Comparison	-
Outcomes	Outcomes are all frameworks that applied for information security risk management
Context	Case Studies in public

	service organizations

The research questions and motivation addressed by this literature review are shown in Table 2.

Table 2. Research Questions

Research Question	Motivation
What kind of frameworks are used for information security risk management in public service organizations?	Identify the frameworks for information security risk management in public service organizations
What are the steps involved in information security risk management?	Identify the steps in information security risk management

2.4. Search Strategy

Before starting a search, collecting the proper database must be chosen to improve finding relevant articles. The most popular literature databases in the field are searched to have the broadest set of studies possible. This study used six electronic database resources to find research articles: IEEE Xplore, ScienceDirect, Proquest, dan ACM. This study used the following search terms, derived from the major terms in the research question: (IT OR ICT OR "information technology" OR "information security") AND (risk OR "risk management" OR "risk assessment") AND (government OR "public sector" OR “public service”). Table 3 shows the results of the search.

Table 3. Results of the Search

Database Journal	Number of Articles
IEEE Xplore	1114
ScienceDirect	267
Proquest	402
ACM	594

2.5. Study Selection

To select the proper studies were relevant to the research question, this study use inclusion and exclusion criteria. These criteria are shown in Table 4.

Table 4. Criteria

Criteria	
Inclusion Criteria	I1 - Papers studies relate to information security risk management in public service organizations. I2 - Papers can be accessed in full-text. I3 - Papers written in English.
Exclusion Criteria	E1 - Similar papers from different database journal E2 - Papers in conference review or white paper

Figure 1 displays the filter stages performed following the specified criteria.

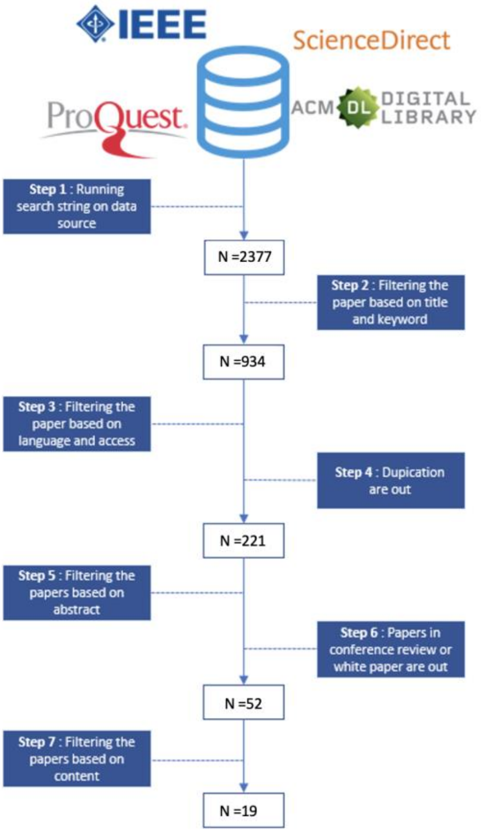
IEEE
ScienceDirect
ProQuest
ACM DL DIGITAL LIBRARY
Step 1 : Running search string on data source
N =2377
Step 2 : Filtering the paper based on title and keyword
N =934
Step 3 : Filtering the paper based on language and access
Step 4 : Dupication are out
N =221
Step 5 : Filtering the papers based on abstract
Step 6 : Papers in conference review or white paper are out
N =52
Step 7 : Filtering the papers based on content
N =19

Figure 1. Process of filtering selected studies

Papers were selected according to the title, and keywords, then obtained 85 journal papers, conference proceedings, workshops, and symposiums. Next filter followed by looking at the language of the paper. If the language of the paper is not English, the paper is not included. Duplicate papers also came out. Then continue to read the abstract of the paper, screening whether abstract has described information security risk management about their research topics. Papers with abstracts that do not meet the criteria are excluded. The paper in the conference review or white paper also came out. The last stage, we filter paper based on content. After applying the inclusion and exclusion criteria, several papers, which published in periodic journal or conference proceeding, satisfy the criteria, and can be used as the main reference for SLR. The selected paper is a paper that satisfy the goals and research questions. Finally, 19 selected papers will be reviewed.

2.6. Data Extracting and Synthesis

The goal of extracting data is to classify and save the information from selected studies accurately to answer the research questions. Data extraction must be defined to reduce the opportunity of bias [24]. Relevant information is extracted into a table from which contains information about the title, publication, year, topic, and method. The synthesized data collects and summarizes the results of data extraction to answer the research questions.

Table 5. Summary of Papers

Year	Ref	Object	Framework Used	Stages
2009	[7]	Public Organization	-	Preparation, Risk identification and analysis, Risk control, Assessment of mitigation approaches
2010	[25]	Government Agency	-	Risk Identifying, Risk Analyzing, Risk Controlling
2012	[26]	Public Organization	ISO 27005	Context Establishment, Risk Assessment, Risk Treatment, Risk Acceptance, Risk Communication, Risk Monitoring and Review
2013	[27]	-	-	Categorize, Select, Implement, Asses, Authorize, Monitor
2014	[28]	Government Agency	ISO 27005	Context Establishment, Risk Assessment, Risk Treatment, Risk Acceptance
2014	[29]	Public Organization	-	Establish Context, Risk Identification, Risk Analysis, Risk Response, Monitoring and Review
2016	[27]	-	-	Context Establishment, Identification, Estimation, Risk Assessment, Risk Treatment, Actions/ Monitoring and Review
2017	[30]	Academic Environment	-	Identify IT security threats, Assess risks based on current situation, Determine controls, Apply controls, Monitor results
2017	[31]	Government Agency	ISO 27005 & NIST SP 800-30	Context Establishment, Risk Assessment, Risk Treatment and Acceptance
2017	[32]	University	-	Assets identification, Defining system boundaries, Vulnerability identification and assessment, Quantitative risk level measurement, Upgrade recommendations
2018	[33]	Government Agency	ISO 27005	Context Establishment, Risk Identification, Risk Estimation, Risk Evaluation
2018	[34]	Government Agency	COBIT 5 for Risk & NIST SP 800-30	Risk Identification, Risk Assessment, Risk Response
2018	[35]	Public Organization	-	Identification Asset, Identification Risk, Determining Risk Priorities, Risk Management, Risk monitoring and review
2019	[36]	Government Agency	Cobit 5 For Risk	Data Collection, Data Analysis, Risk Analysis
2019	[15]	Government Agency	ISO 27005 & NIST SP 800-30	Context Establishment, Identification of Assets, Identification of Threats, Identification of Existing Controls, Identification of Vulnerabilities, Risk Analysis, Risk Evaluation
2020	[37]	-	ISO 27005 & NIST SP 800-30	Context Establishment, Risk Assessment, Risk Analysis, Risk Evaluation, Risk Treatment and Acceptance
2021	[17]	Government Agency	ISO 27005 & NIST SP 800-30	Context Establishment, Conduct Assesment, Risk Treatment, Risk Acceptance
2022	[38]	IT Consulting Industry	ISO 27005 & NIST SP 800-30	Threat Identification, Vulnerability Identification, Control Analysis, Likelihood Determination, Impact Analysis, Risk Determination, Control Recommendation, Result Documentation
2023	[39]	Government Agency	ISO 27005 & NIST SP 800-30	Context Establishment, Risk Assessment, Risk Treatment and Acceptance

The next section explains the selected papers and analyzes them to find the framework used and steps in information security risk management in public service organizations.

3. RESULT

This section presents the results of a literature review of this study. It starts by describing of the selected papers. Next, it mentions the framework used and steps in information security risk management. A summary of the results of the reviewed paper can be seen in Table 5.

3.1. Framework for Information Security Risk Management

The number of papers selected in this study amounted to 19. Of the 19 papers, 11 papers applied an existing risk management framework. mation security risk management

Table **6** shows the list of frameworks for information security risk management

Table 6. List of Frameworks

Frameworks	Literature
ISO 27005	[15] [17] [26] [28] [31] [33] [37] [38] [39]
NIST SP 800-30	[15] [17] [31] [34] [37] [38] [39]
Cobit 5 For Risk	[34] [36]

The most widely used framework is ISO 27005. 9 papers have been reviewed, using ISO 27005 in their research [15] [17] [26] [28] [31] [33] [37] [38] [39]. ISO 27005 can be applied to all types of organizations that need to safeguard their information [31] [33]. The framework approach of ISO 27001 based on organizational environment suitability and the same way with risk management in general. The defined context is evaluated first, then a risk assessment is carried out. If enough information is provided to determine the actions needed to modify the risk to an acceptable level, then risk treatment is finally followed. If there is insufficient information, another iteration is carried out in the revised context. The effectiveness of risk treatment depends on the results of the risk assessment. It is possible that risk treatment does not immediately produce an acceptable level of residual risk. This is the case when another iteration of risk assessment is needed with changing context parameters. Risk acceptance activities must ensure that the organization’s directors explicitly approve residual risks. ISO 27005 can be combined and be equipped with other guidelines.

The second framework is NIST SP 800-30. NIST SP 800-30 is a framework to provide guidance in conducting risk assessments of information systems in an organization both public and private [34]. Risk assessment approach on NIST SP 800-39 supported by security standard and other guidance to manage information security risk. NIST SP 800-30 also can be applied to complete ISO 27005 standard in performing risk assessment [31]. Risk assessments are used to identify, estimate, and prioritize risks for the business process of organizations, assets, and use of information systems. NIST defines risk assessment synonymous with risk analysis.

COBIT 5 for Risk is one of the COBIT 5 family products that focus on IT risk. The guidelines and principles contained in COBIT 5 for Risk can be applied in various organizations. COBIT 5 for Risk provides two perspectives in the context of risk, Risk Function and Risk Management Perspective. COBIT 5 for Risk defines IT risk as business risk, specifically, the business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise.

All three frameworks can be used partially or together for risk management. From the papers collected, ISO 27005 is the most used framework.

3.1. Steps in Risk Management

To classify steps to carry out information security risk management, a framework used at ISO, namely PDCA (Plan, Do, Check, Act). However, this grouping only reaches the Check stage. Steps to be taken for information security risk management can be seen in Table 7.

Table 7. Steps of Information Security Risk Management

Stages	Steps	Literature
Plan	Preparation	[7]
	Context Establishment	[15] [26] [28] [29] [31] [32] [33] [37] [39]
Do	Risk Identification	[7] [25] [29] [32] [33] [34] [35] [38]
	Risk Analyzing	[7] [15] [25] [29] [37]
	Risk Estimation	[33] [35]
	Risk Assessment	[7] [26] [27] [28] [31] [32] [34] [37] [40] [39]
Check	Risk Control	[7] [38]
	Risk Communication	[26]
	Risk Monitoring and Review	[26] [27] [35] [29]
	Risk Evaluation	[33]
	Recommendation	[32] [38]
Act	Risk Acceptance	[26] [28] [31]
	Risk Treatment	[26] [28] [31] [37] [38]
	Risk Response	[29] [34]
	Implement	[27]

The Plan stage supposes the establishment of the context, assessment of the risk, development of a risk treatment plan and risk acceptance. In the Do stage there are implemented the security actions and controls necessary for risk reduction, according to a risk treatment plan. In the Check stage the managers will establish the necessities for reviewing the risk assessment and treatment procedure considering the incidents that were produced from the last review and on the context change [26].

The context of information security risk management should be established which involves the determination of the basic criteria necessary for information security risk management, defining scope and boundaries and establish an appropriate organization of information security risk management activities [31] [34]. Risks need to be identified. Risks identification supposes the identification of the vulnerabilities and threats to all assets or groups of assets, of risk sources, security events or incidents that may occur. The already existent security controls must be identified, as well as their efficiency, the consequences (loss of confidentiality, integrity, availability) and the impact on the interested parties, loss of business or market position, damage of reputation, etc. Risk identification consists of several activities: Identification of assets, Appraisal of critical assets, Identification of threats, Identification of controls, and Identification of Vulnerabilities. After identifying assets, threats, vulnerabilities, and flow control, followed by estimating the existing risk.

After identifying the risks, the next step is to conduct an analysis for each risk. Risk analysis is conducted by looking at the risk likelihood and risk impact. Risk analysis can also provide an input into making decisions where choices must be made, and the options involve different types and levels of risk [29]. Risk assessment is a process of risk management during which there must be identified, estimated, and established the risk level and the priority degree in terms of the risk criteria adopted by the organization, which runs repetitively by utilizing iterations. NIST SP 800-30 framework can be used as tool for assessing risk [31].

Risk acceptance is the decision to accept the risk and responsibility for the decisions taken in managing these risks [28]. Risk control is to choose and use some risk controlling methods to guarantee that the risk can be reduced to an acceptable level. Risk control is the most important step in the risk management. It is the key factor to determine whether the risk management is successful or not. Risk is not static. Threats, vulnerabilities, likelihood, or consequences can change suddenly without any sign. Monitor and review that lead to the results of the risk management system undertaken as well as to identify the changes that need to be done.

Okonofua and Shawon mention that factors help to sustain risk management plan in organizations depend almost entirely on the key elements of i) people: Management commitment to organizational needs ii) process: Repeatable Approach to Risk Management, and iii) technology: Sustainable Data Quality and Integrity [8].

4. DISCUSSION

Risk management plays a vital role in upholding information security within every organization. Numerous methodologies exist for executing risk management, each presenting distinct approaches and qualities. The purpose of this section is to emphasize the differences among three frameworks: ISO/IEC 27005, NIST SP 800-30, and COBIT 5 for Risk. Moreover, it aims to offer guidance on selecting an appropriate strategy tailored to specific circumstances.

ISO/IEC 27005 is part of the ISO/IEC 27000 series and provides guidelines for information security risk management. It emphasizes a systematic and comprehensive approach to identifying, assessing, and treating information security risks. The framework is aligned with the ISO 31000 standard for risk management.

NIST Special Publication 800-30 offers guidance on risk assessment and risk management for federal information systems. It provides a structured approach to risk assessment, including threat identification, vulnerability assessment, impact analysis, and risk determination. NIST SP 800-30 is widely used in government and industry.

COBIT 5 is an IT governance and management framework. The "Evaluate, Direct, and Monitor" (EDM) domain of COBIT 5 includes guidance on managing IT-related risks. COBIT 5 for Risk focuses on integrating risk management into overall IT governance processes.

To ensure information security and business continuity, organizations should assess their requirements for a risk assessment approach that matches their objectives. Selecting an approach and performing a risk assessment is imperative for all organizations to protect their information assets and ensure business continuity.

5. CONCLUSION

This literature review aims to identify and analyze steps and frameworks used in information security risk management between 2009 and 2023. Based on the inclusion and exclusion criteria designed, finally studied 16 studies of information security risk management. This literature review has been carried out as a systematic literature review.

The results of this study also identified three frameworks that can be used in information security risk management: ISO 27005, NIST SP 800-30, and Cobit 5 For Risk. stages in information security risk management in general are Context Establishment, Risk Identification, Risk Assessment, Risk Treatment, and Risk Monitoring.

Despite having some similarities, each standard has its own unique strengths and weaknesses, and choosing any of them can enhance an organization's information security. However, it is crucial to carefully consider which standard is most suitable for an organization's security needs and requirements.

For future research endeavors pertaining to information security risk management, the frameworks identified in this study can serve as valuable resources for exploration and analysis. These frameworks can provide a solid foundation for investigating various aspects of risk management within the realm of information security. Utilizing these frameworks can help researchers delve deeper into topics such as risk assessment methodologies, implementation challenges, best practices, and the effectiveness of these frameworks in different organizational contexts. By leveraging the insights gained from these frameworks, researchers can contribute to the advancement of knowledge in the field of information security risk management.

REFERENCE

[1] H. Malhotra, R. Bhargava and M. Dave, "Challenges related to information security and its implications for evolving e-government structures: A comparative study between India and African countries," in *International Conference on Inventive Computing and Informatics (ICICI)*, Coimbatore, 2017.

[2] D. Kaye, "The importance of information," *Management Decision, Vol. 33 Issue: 5,* pp. 5-12, 1995.

[3] M. E. Whitman and H. J. Mattord, "Principles of information security," in *Principles of Information Security*, Cengage, 2011.

[4] R. Sarno and I. Iffano, Sistem manajemen keamanan informasi (Berbasis ISO 27001), Surabaya: ITS Press, 2009.

[5] M. Ciampa, Security awareness : Applying practical security in your world, 3rd ed, Boston: Couse Technology, 2010.

[6] Kautsarina and H. Gautama, "Information security readiness of government institution in Indonesia," in *International Conference on Information and Communication Technology (ICoICT)*, 2014.

[7] Y. Y. L. Helgesson, "Managing risks on critical IT systems in public service organizations," in *International Conference on Computational Science and Engineering*, 2009.

[8] H. Okonofua and S. Rahman, "Evaluating the risk management plan and addressing factors for successes in government agencies," in *International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering*, 2018.

[9] J. V. B. d. l. Paz and L. A. R. Picon, A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0, Chihuahua: Systems, Infrastructure, and Industry 5.0, 2023.

[10] A. Kurniati, L. E. Nugroho and M. N. Rizal, Information Technology Risk Management on e-Government: Systematic Literature Review, Yogyakarta: Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi, 2020.

[11] A. Alijoyo and A. F. M. S. Fisabilillah, Risk

Management Implementation in Public Sector Organizations: A Case Study of Indonesia, Common Ground Research Networks, 2021.

[12] A. Olechowski, J. Oehmen, W. Seering and M. Ben-Daya, The Professionalization of Risk Management: What Role Can the ISO 31000 Risk Management Principles Play?, Cambridge: International Journal of Project Management34 (8): 1568–78, 2016.

[13] J. Masso, F. J. Pino, C. Pardo, F. García and M. Piattini, Risk Management in the Software Life Cycle: A Systematic Literature Review, Ciudad Real: Computer Standards and Interfaces71 (March 2019): 103431, 2020.

[14] L. Y. Banowosari and B. A. Gifari, System Analysis and Design Using Secure Software Development Life Cycle Based On ISO 31000 and STRIDE. Case Study Mutiara Ban Workshop, Depok: IEEE, 2020.

[15] M. A. Fikri, F. A. Putra, Y. Suryanto and K. Ramli, sk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency, Jakarta: Procedia Computer Science161: 1206–15, 2019.

[16] M. Brunner, C. Sauerwein, M. Felderer and R. Breu, Risk Management Practices in Information Security: Exploring the Status Quo in the DACH Region, Innsbruck: Computers and Security, 2020.

[17] I. M. M. Putra and K. Mutijarsa, Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005, Bandung: IEEE, 2021.

[18] O. Ali, A. Shrestha, A. Chatfield and MurrayPeter, Assessing Information Security Risks in the Cloud: A Case Study of Australian Local Government Authorities, Egaila: Government Information Quarterly, 2020.

[19] A. Joshi, L. Bollen, H. Hassink, S. De Haes and W. V. Grembergen, Explaining IT Governance Disclosure through the Constructs of IT Governance Maturity and IT Strategic Role, Maastricht: Information & Management, 2018.

[20] J. D. White, Managing information in the public sector, Routledge, 2007.

[21] ISO/IEC, "International Standard ISO/IEC 27001: 2013," International Organization for Standardization, London, 2013.

[22] ISO/IEC, "International Standard ISO/IEC 27005: 2011," International Organization for Standardization, London, 2011.

[23] NIST, "NIST SP 800-30: Risk management guide for information technology systems," National Institute of Standards and Technology , Gaithersburg, 2002.

[24] B. Kitchenham and S. M. Charters, "Guidelines for performing systematic literature reviews in software engineering," Keele University and Durham University Joint Report, 2007.

[25] L. Zhao, "Study on security risk management in E-government," in *International Conference on E-Product E-Service and E-Entertainment, ICEEE*, 2010.

[26] F. Baicu and A. M. Baicu, "Risks management relating to information systems security evaluation of IT assets," in *Acces la Success*, 2012.

[27] L. Liang, W. Ren, J. Song, H. Hu, Q. He and S. Fang, "The state of the art of risk assessment and management for information systems," in *9th International Conference on Information Assurance and Security, IAS*, 2014.

[28] S. Prasetyo and Y. G. Sucahyo, "Information security risk management planning: A case study at application module of state asset directorate general of state asset ministry of finance," in *International Conference on Advanced Computer Science and Information Systems*, 2014.

[29] H. Wijanarka, "IT risk management to support the realization of IT value in public organizations," in *International Conference on ICT for Smart Society: "Smart System Platform Development for City and Society, GoeSmart 2014*, 2014.

[30] U. McUbe, M. Gerber and R. Von Solms, "Scenario-based IT risk assessment in local government," in *ST-Africa Conference*, 2016.

[31] F. A. Putra and H. Setiawan, "Design of information security risk management using ISO/IEC 27005 and NIST SP 800-30 revision 1: A case study at communication data applications of XYZ institute," in *International Conference on Information Technology Systems and Innovation (ICITSI)*, 2017.

[32] C. Joshi and U. K. Singh, "Information security risks management framework – A step towards mitigating security risks in university network," in *Journal of Information Security and Applications*, 2017.

[33] S. Patino, E. F. Solis, S. G. Yoo and R. Arroyo, "ICT risk management methodology proposal for governmental entities based on ISO/IEC 27005," in *5th International Conference on eDemocracy and eGovernment, ICEDEG*, 2018.

[34] Y. Supriyadi and C. W. Hardani, "Information system risk scenario using COBIT 5 for risk and NIST SP 800-30 Rev. 1 a case study," in *International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE*, 2018.

[35] H. F. Yoseviano and A. Retnowardhani, "The use of ISO/IEC 27001: 2009 to analyze the risk and security of information system assets: case study in xyz, ltd," in *nternational Conference on Information Management and Technology, ICIMTech 2018*, 2018.

[36] S. A. Wulandari, A. P. Dewi, M. R. Pohan, D. I. Sensuse, M. Mishbah and Syamsudin, Risk Assessment and Recommendation Strategy Based on COBIT 5 for Risk: Case Study SIKN JIKN Helpdesk Service, Jakarta: Procedia Computer Science, 2019.

[37] T. Weil, "Risk Assessment Methods for Cloud Computing Platforms," in *IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, Milwaukee, 2019.

[38] F. Kitsios, E. Chatzidimitriou and M. Kamariotou, "Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry," *Sustainability*, vol. 14, 2022.

[39] A. P. Putra and B. Soewito, "Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 4, pp. 625-633, 2023.