Bulletin of Computer Science and Electrical Engineering
Vol. 1, No. 1, June 2020, pp. 1~11
ISSN: 2722-7324, DOI: 10.25008/bcsee.v1i1.2

Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City)

Adrian Fathurohman[1], R. Wahjoe Witjaksono[2]
[1,2]School of Industrial and System Engineering, Telkom University

Article Info

Article history:

Received May 09, 2020
Revised Jun 02, 2020
Accepted Jun 29, 2020

Keywords:

Information Security
Management System
ISMS
Clause
ISO 270001: 2013
ANNEX

ABSTRACT

The Department of Communication and Information (Diskominfo) of the Bandung City Government is an agency that has the responsibility of carrying out several parts of the Regional Government in the field of communication and informatics. Based on the composition of the regional service organization Bandung City Diskominfo has five fields and two UPTs which are part of the Bandung City Diskominfo. Bandung City Diskominfo in implementing work programs has IT as a supporter of business processes in government agencies. Based on the results of research conducted that IT management in Bandung City Government Diskominfo found several clauses that were still unfulfilled in this Diskominfo impact on the management of government information security institutions that can affect the performance of Bandung City Government. Therefore, there is a need for standardization that needs to be implemented as a guide that examines the direction in safeguarding information or assets that are considered sensitive to an organization. With the existence of these problems pushed to design information security recommendations based on ISO 27001: 2013 standards at Diskominfo. Also makes the design of IT information security systems that are focused on the control of Annex Information Security Policies, Human Resource Security, Operational Security, Communication Security and Asset Management so that business IT processes can run in accordance with the objectives of the organization. The results of this study are expected to help in securing IT information at the Bandung Diskominfo City and can also improve the goals of an organization.

Corresponding Author:

Adrian Fathurohman,
School of Industrial and System Engineering, Telkom University
Email: adrianfathu@gmail.com

1. INTRODUCTION

At present, the development of Information Technology (IT) has become a very important part of almost all fields of life. This development can support the organization in fulfilling all organizational activities which are processes to achieve goals. The latest fact is the increasing dependence of organizations on IT to achieve business strategies and needs is the main thing in the importance of success in an organization. The dependency has an impact on the growing need for IT services that continue to grow. IT services can increase the effectiveness and efficiency of organizational needs [1].

In the era of the millennial society at this time, the development of IT is not only limited to the industrial sector but has entered the government sector also has implemented IT management.

This development has an impact on the main business processes, namely in the decision-making process carried out by management. With IT, the role of each managerial in decision making can provide decisions based on accurate, reliable information and can consider the risks that will occur [2], [3]. When viewed in terms of implementation, IT has produced positive things that can build into the ongoing needs of government, but on the other hand, there are also negative things that can reduce the performance of the government. Therefore, it must pay attention to any external factors that can influence the application of IT, to reduce the negative impact. IT risk management is a process of risk identification, risk assessment, and taking steps to reduce risk to an acceptable level. negativity can give can be bad for the performance of government agencies [4]–[7].

Initially, the Bandung Office of Communication and Information (Diskominfo) was one of the regional technical institutions in the form of the Bakominfo Communication and Information Agency. Formed based on Bandung City Regulation Number 12 the Year 2007, December 4, 2007, and is a merging of the Local Government Work Unit (SKPD) Office and Office within the City Government of Bandung, namely the Information and Communication Office with the Electronic Data Processing Office (KPDE).

Based on the results of observations and interviews that have been carried out that IT management in Bandung City Government Diskominfo found several clauses that were still unfulfilled in this Diskominfo impact on the management of government information security institutions that can affect the performance of the Government of Bandung City. Therefore, there needs to be standardization that needs to be implemented as a guide that provides direction in safeguarding information or assets that are considered sensitive to an organization.

With the existence of these problems pushed to design information security recommendations based on ISO 27001: 2013 standards [8]–[10] at Diskominfo. It also makes the design of IT information security systems that are focused on the control of Annex Asset Management, Access Control, Cryptography, Physical and Environmental Security, Operational Security, Communication Security, Acquisition, Development, and Maintenance of the System [10]. so that business IT processes can run in accordance with the objectives of the organization.

2. LITERATURE STUDY

2.1. Information System Security

Information System Security is an attempt to secure information assets from various threats and vulnerabilities that exist to ensure the continuity of business, and reduce the impact that will occur due to threats and vulnerabilities that occur. The following is a model of aspects of information system security.

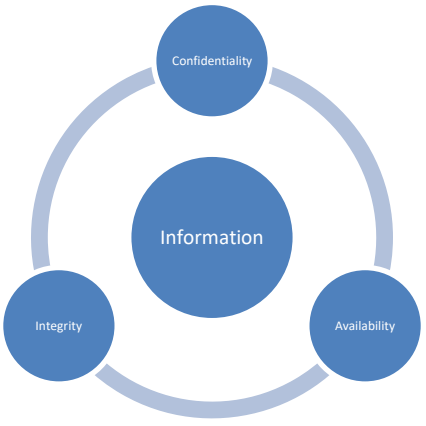

Figure 1 Aspects of Security Information Systems

The following is an explanation of the aspects of information system security [11], as follows:

1. Confidentiality

Aspects that maintain the confidentiality of information or data, to ensure that information can only be accessed by people who have the authority and guarantee the confidentiality of data.

2. Integrity

Aspects that guarantee the data will not be changed without permission from the party that has the authority (authorized), to maintain the integrity of the information and method of the process.

3. Availability

The aspect that provides that data will be available when needed, ensures that authorized users can use the information and related tools.

2.2. IT Risk Management

Risk management is a scientific approach to managing risk by anticipating possible losses, designing, and implementing procedures that can minimize the occurrence of losses or the financial impact of losses that occur [7]. Risk Management is an act of practice with risk management, using methods and tools to manage the risks of a project [4], [5]. Risk management is the total process used in identifying, controlling, and minimizing the impact of uncertain events [6].

In general, risk management will be followed by determining the priority of risks that can have an adverse impact on the organization or company, as well as priorities in handling them. The steps that can be taken by an organization or company in handling risk are as follows:

1. Accept

Top Management decides to accept the risk if the magnitude of the impact and the level of inclination is still within the organizational tolerance limits.

2. Avoid

The organization decides not to carry out an activity or choose other alternative activities that produce the same output to avoid the risk.

3. Mitigate

The organization decides to reduce the impact and the likelihood of risks to the institution.

4. Transfer

The organization decides to transfer all or part of its responsibilities to third parties

2.3. SNI ISO / IEC 27001- Information Security Management System Requirements

SNI ISO / IEC 27001 issued in 2009 and is the Indonesian version of ISO / IEC 27001: 2005, contains specifications or requirements that must be met in building an Information Security Management System (ISMS). This standard is independent of IT products, requires the use of a risk-based management approach, and is designed to ensure that selected security controls are able to protect information assets from various risks [12].

This standard was developed using a process approach as a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS. The process approach encourages users to emphasize the importance of [12]:

1. Understand the organization's information security requirements and the need for information security policies and objectives
2. Implement and operate controls to manage information security risks in the context of the organization's overall business risk
3. Monitoring the performance and effectiveness of ISMS
4. Continuous improvement is based on measuring the level of achievement of objectives

The PLAN - DO - CHECK - ACT (PDCA) method is applied to the overall structure of ISMS [5]. In the PDCA model, the whole ISMS process can be mapped as shown in Table 1.

Table 1 PLAN - DO - CHECK - ACT (PDCA) Method

No	PDCA Cycle	Explanation
1	PLAN (Establish ISMS)	Establish ISMS policies, objectives, processes and procedures that are relevant for managing risk and improving information security.

2	DO (Implement and operate ISMS)	Implement and operate ISMS policies, controls, processes and procedures that apply.
3	CHECK (monitor and retake ISMS)	Assess and measure the performance of the process against policies, targets, practices in implementing ISMS and report the results to management for review.
4	ACT (Maintaining and improving ISMS)	Take corrective and preventive actions, based on evaluation results, internal audits and management reviews of ISMS

2.4. Control of ANNEX

Annex controls are controls that have been designed to ensure that selected information security controls are able to protect information assets from a variety of risks and provide a level of security for stakeholders. The following is an explanation of the controls used in related research:

1. A.8 Asset Management

A guideline in providing appropriate protection of organizational assets and identifying these assets properly.

2. A.9 Access Control

Is control in which there is a way to limit user access to information by regulating the authority of its access rights, including control in networking or in mobile-computing.

3. A.10 Cryptography

It is a sure use of cryptographic appropriate effective guidelines to protect the integrity of confidential information

4. A.11 Physical and Environmental Safeguards

Is a guideline in preventing data loss / damage arising from the physical environment, including natural disasters and theft of data stored in storage media.

5. A.12 Operation Safety

Is a maintenance of information security at large, in maintaining and maintaining the integrity of the information system against external parties. The aim is to prevent loss, damage, theft or compromise of assets and disruption to the organization's operations.

6. A.13 Communication Security

Ensuring that communication security has provided more security, both communication technology and its contents. The aim is to ensure the protection of information in the network and supporting information processing facilities.

7. A.14 System Acquisition, Development and Maintenance

Ensuring that information systems and applications that have just been implemented are able to be integrated through the validation of data / information.

3. RESEARCH METHODOLOGY

3.1. Conceptual Model

In this research, we need a conceptual model that provides a framework for thinking by describing methods in solving problems in a structured manner [13]. Based on the conceptual models that have been made, three elements describe the flow of research in the design and modeling of Information Security Management Systems in Bandung City Communication and Information.

1. The first element is related to the problem and the environment. Where the problem in Bandung City Diskominfo is the lack of human resources who understand the importance of information security, the absence of Company Operational Standards related to Information Security and the absence of management in securing information in the scope of service.
2. The second element contains Information Systems Research that illustrates some of the implementations needed to provide solutions to problems that exist in Diskominfo. Some of these stages started from the Initiation of the ISMS Project to the Design of the ISMS

3. The third element is a knowledge base consisting of concepts and methods. The concept will be applied in this study, while the method is a way to collect data conducted in this study consisting of interviews, observations, and literature studies.

3.2. Systematic Research

The problems contained in this study require regular problem-solving. Systematic problem solving will help the research carried out by having the stages to be passed in the research process. The following explanation of the research system can be seen in Figure 2.

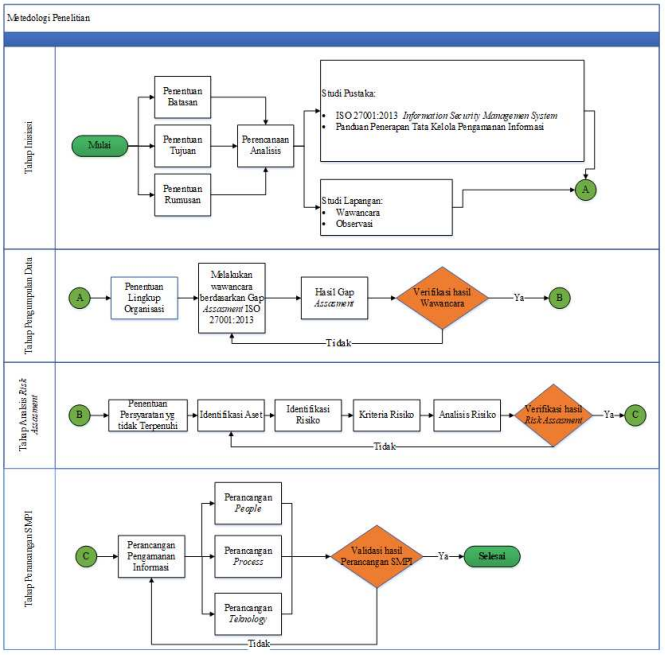

Figure 2 Systematic Research

4. RESULTS AND ANALYSIS

4.1. GAP Assessment

Gap assessment is an assessment process carried out divided into two parts, namely those that will conduct an assessment of the current conditions with ideal conditions in accordance with ISO 27001: 2013 guidelines which will help to know the extent of achieving the objectives at Diskominfo. This gap assessment is obtained by conducting research on each annex control contained at ISO 27001: 2013.

1. Assessment Results

The results of the gap assessment are the results of the requirements derived from the ISO 27001: 2013 gap assessment. This result represents the number of requirements that are met and not met from the total presentation of each annex control. The following are the results of the gap assessment. The following are the results of the gap assessment which can be seen in Table 2.

Table 2 Results of the ISO 27001: 2013 Gap Assessment

No	Standard Inside Area	Standard Inside Area	Standard Inside Area	Standard Inside Area
1	A.8 Asset Management	10	10	100%
2	A.9 Access Control	14	11	79%
3	A.10 Cryptography (Cryptography)	2	2	100%
4	A.11 Physical and Environmental Security	14	12	86%

5	A.12 Operational Security	14	10	71%
6	A.13 Communications Security	7	7	100%
7	A.14 System Acquisition, Development and Maintenance	13	11	85%
	Total	**74**	**63**	

2. Identification of Findings that are not in accordance with the Terms
The purpose of risk identification is to find out the list of clauses that are not fulfilled in accordance with the controls in ISO 27001: 2013. The following are the results of risk identification based on the assessment of information security gaps which can be seen in Table 3.

Table 3 Identification of Findings that are not in accordance with the Terms

No	Categories in ISO 27001	Categories in ISO 27001
1	A.9.4.2 Secure log-on procedure	The absence of procedures related to secure log-on application that is used
2	A.9.4.3 Password Management System	Do not have procedures related to password management
3	A.9.4.5 Control access to source code	There are no restrictions on the source code in the application
4	A.11.2.3 Cable security	Internal cable security is still inadequate
5	A.11.2.6 Security of equipment and assets outside the office/site	There is still a lack of specific security related to equipment outside the office
6	A.11.2.9 Clear desk and clear screen policy	The absence of a clear desk and clear screen
7	A.12.1.1 Documented operating procedures	Operational procedures have not been documented
8	A.12.2.1 Control of malware	Don't have Anti-Malware-related Policies
9	A.12.5.1 Software installation on operational systems	The absence of procedures regarding software installation controls in operational systems that have been implemented
10	A.12.6.2 Restrictions on software installation	There are no restrictions on the installation of software
11	A.14.2.4 Limitation of changes to the software package	There are no restrictions on the software package
12	A.14.2.5 Principles of safe engineering systems	The absence of safe engineering principles

4.2. Risk Assessment

The process of risk assessment or assessment of risk is an assessment of the risks that have been and are happening in Bandung City Diskominfo. This process is expected to bring up the priority process of the agency according to the assets seen from various kinds of risks that have occurred and are taking place in Bandung's Diskominfo. In conducting this risk assessment researchers conducted several stages including searching for identification of risks, vulnerabilities, threats to make risk criteria, risk analysis that led to the determination of the ISO 27001 process that must be prioritized relating to solutions of risk resolution.

1. Identification of Assets
Asset identification is useful for determining assets associated with access control in Bandung City Diskominfo. Based on the results of observations made, the assets identified can be seen in Table 4.

Table 4 Asset Identification

Asset Category	Asset Category	Asset Category
Information	Operation	Operational documentation Operational procedure
	Audit and Compliance	Risk assessment documentation Internal audit report

		Documentation Procedure
	Leader	Leadership Plan
	Employee	Employee Data
		Training Records
	Policy	Policy Documents
Organization		Organization
Hardware	Regular Equipment	PC
		Server
Software	Service, Maintenance, Administration Software	The website
	Network Devices	Intranet
		LAN cable (Local Area Network)
		Router

2. Identification of Threats and Vulnerabilities

The threat identification stage is the stage of combining the information obtained when direct observation, interviews, or literature studies have been carried out by looking for any threats that will appear in the gap assessment that is not met can be seen from Table 5.

Table 5 Identification of Vulnerabilities and Threats

No	Findings	Risk Description		
		Asset	Vulnerability	Threat
1	The absence of procedures related to secure log-on application that is used	The website	There is no direction in making secure log-on	Spambot
2	Do not have procedures related to password management	Network Devices	There is no guide to good password management	Easily accessed by others
3	There are no restrictions on the source code in the application	The website	There are no restrictions on the source code of applications	Staff make modifications to the Application
4	Internal cable security is still inadequate	LAN cable	Random laying of cables and lack of cable protection	LAN cable is bitten by a mouse
5	There is still a lack of specific security related to equipment outside the office	Network Devices	Natural disasters and unexpected events	ICT infrastructure has been damaged
6	The absence of clear desk and clear screen	Employee Data	Lack of security training	Misuse of access rights on the PC Password is known to others
7	Operational procedures have not been documented	The website	Lack of guidance in conducting a good system operation	a system error occurred while documenting
8	Don't have Anti-Malware-related Policies	Employee Data	Staff do not understand the importance of Antivirus	The PC used is attacked by a virus
9	The absence of procedures regarding software installation controls in operational systems that have been implemented	The website	There is no procedure regarding software installation	Error during software installation
10	There are no restrictions on the installation of software	The website	There are no restrictions on access rights on software installation	Local IT device employees can access the software
11	There are no restrictions on the software package	The website	There are no restrictions on access rights to the software	Local IT device employees can access the software

			package	package
12	The absence of safe engineering principles	Documentation Procedure	Security awareness is still lacking	Error in network infrastructure

4.3. Risk Analysis

Risk analysis is the activity of analyzing risks to the likelihood and impact that has been determined and determining the level of risk based on the specified risk appetite.

1. Identification of Risk Levels

Risk criteria are a standard measure of how likely an impact or consequence will occur and how likely it is or the frequency of risk will occur. In making risk criteria, researchers use a 5 x 5 probability and impact table consisting of 5 probability levels and 5 impact levels can be seen in Figure 3. To find out the standards and criteria of probability and impact arising from each risk assessment researchers propose criteria the probability and impact after being verified by Diskominfo Kota Bandung can be seen in Table 6.

Figure 3 Risk Criteria Based on Likelihood and Impact

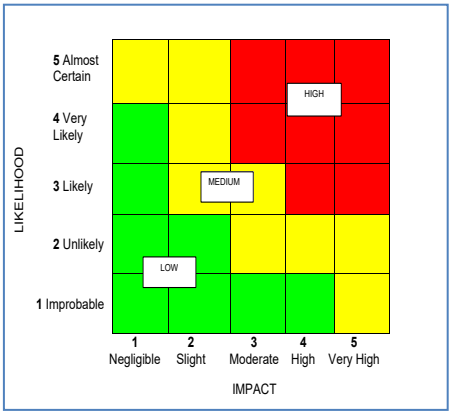

Table 6 Risk Criteria Results

No	Finding	Risk Level
1	The absence of procedures related to secure log-on application that is used	MEDIUM
2	Do not have procedures related to password management	HIGH
3	There are no restrictions on the source code in the application	HIGH
4	Internal cable security is still inadequate	HIGH
5	There is still a lack of specific security related to equipment outside the office	HIGH
6	The absence of clear desk and clear screen	MEDIUM
7	Operational procedures have not been documented	MEDIUM
8	Don't have anti-malware related policies	MEDIUM
9	The absence of procedures regarding software installation controls in operational systems that have been implemented	LOW
10	There are no restrictions on the installation of software	MEDIUM
11	There are no restrictions on the software package	HIGH
12	The absence of safe engineering principles	MEDIUM

4.4. Designing People

People design is the result of design obtained based on risk assessment that discusses controls about the organization, competencies and abilities. The design of people carried out will produce recommendations for new organizational structures on competencies and abilities will produce recommendations for competency resources that must be possessed by each organizational structure based on the needs of the implementation process

1. Organizational Structure Design
The design of the organizational structure is the result of recommendations given from the gaps that occur in the organizational structure contained in Bandung City Government Diskominfo. This recommendation will be carried out in the design process of the organizational structure that manages the strategy, manages the budget, secures information and manages relationships between third parties, then an additional description will be made.
a. Head of Department
1) Plan and establish programs related to information security management systems for the Bandung City Government Diskominfo
2) Coordinate the implementation of information security management system implementation in each field
b. Secretary
1) Coordinate related to the preparation of materials needed in the implementation of information security
c. Head of Sub. General and Staffing Section
1) Carry out monitoring and evaluation related to asset management and staffing at Diskominfo
2) Conduct staffing training on information security management to increase awareness of every employee of the importance of ISMS
d. Head of Sub. Financial department
1) Carry out monitoring and evaluation related to the budget in the implementation of ISMS in Bandung City Government Diskominfo
e. Head of Sub. Program Section
1) Arranging plans and programs for the implementation of ISMS in Bandung City Government Diskominfo
2) Conduct an evaluation related to the implementation of ISMS Diskominfo Bandung City Government
f. All Division Heads
1) Arrange ISMS plans and programs based on the scope of the Diskominfo
2) Conduct reporting, evaluation, and monitoring for the implementation of ISMS.
g. Head of ICT Infrastructure
1) Carry out planning and documentation of the operational activities of the system and infrastructure at the Diskominfo.
2) Perform adequate security for all hardware in Diskominfo
h. Fields of Encoding and Information Application
1) Carry out coordination related to IT Risk Assessment and preparation of follow-up plans every year
2) Carry out plans related to ISO 27001 certification in order to support the business activities of an organization that will increase the value of the risk of information security disruption
i. Application Management Section
1) Arrange management of application access rights so that the Regional Apparatus cannot make application modifications
j. Head of Information System Encryption and Security Section
1) Conduct staffing training on information security management to increase awareness of every employee of the importance of ISMS
2) Implementing ISMS management practices in the scope of Diskominfo.

4.5. Design Process

The process design is the result of design obtained based on the risk assessment that discusses the control of the regulations and documentation that has been owned by Diskominfo. The process design that is carried out will produce recommendations in the form of documentation such as policies, SOP (Standard Operational Procedure), as well as work instructions that can later make Diskominfo even better.

1. Policy Design

Policies are general guidelines or guidelines for carrying out a process that is in the organization and in carrying out a job. The design of the policy that becomes a recommendation is the application of an information security management system. Policy on the application of ISMS is a policy that contains arrangements for obligations for Electronic System Operators in the application of information security management based on the principle of risk.
a. Hardware Management Policy
b. Password Management Policy
c. Information System Access Rights Policy
d. Application Information System Management Policy

2. Draft SOP (Standard Operational Procedure)
The design procedure is a design that is designed from a risk assessment that requires documentation related to guidance or direction that can later help Diskominfo become better.
a. Application Information System Management Procedure
b. Password Management Procedure
c. Hardware Management Procedure
d. Cable Security Procedure

4.6. Technology Design

The design of technology is the result of design obtained based on the design of the risk assessment that has been analyzed. The design of technology carried out at risk assessment will produce recommendations for tools and applications used to support the needs of the implementation process.

1. Recommended Tools
The design of tools is carried out based on recommendations from risk assessments which are based on high risk categories carried out in Bandung City Diskominfo. On the results of the risk assessment, it can be concluded that in Bandung City Diskominfo there are no adequate supporting tools in conducting ISMS.
Based on the research results, it is recommended to use the McAfee application because these tools are the cheapest in cost and available in free applications for use with features that can support maintaining forms to secure, detect, and remove computer viruses from computer systems.

5. CONCLUSION

Based on the results of gap analysis and risk assessment results that have been carried out in the study, it can be concluded that the solution that will be made is the design of people based on the design of the organizational structure and competence of human resources, while the process will be made policies and standard operational procedures to improve government agency documentation and the last solution technology that will support information security in terms of antivirus. This research resulted in the design of information security in the form of a description of the current security conditions as well as the proposed improvement of security in the future that can be used as a reference in making ISMS planning strategies to improve performance and support the achievement of business strategies in Bandung City Government Communication and Information.

REFERENCES

[1] K. C. Laudon and J. P. Laudon, “Management information systems: new approaches to organization and technology,” *Up. Saddle River, NJ*, 1998.
[2] R. K. Rainer Jr, C. A. Snyder, and H. H. Carr, “Risk analysis for information technology,” *J. Manag. Inf. Syst.*, vol. 8, no. 1, pp. 129–147, 1991.
[3] A. Behnia, R. A. Rashid, and J. A. Chaudhry, “A survey of information security risk analysis methods,” *SmartCR*, vol. 2, no. 1, pp. 79–94, 2012.
[4] G. Stoneburner, A. Goguen, and A. Feringa, “Risk management guide for information technology systems,” *Nist Spec. Publ.*, vol. 800, no. 30, pp. 800–830, 2002.

[5] P. Hopkin, *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*. Kogan Page Publishers, 2018.
[6] T. R. Peltier, *Information security risk analysis*. CRC press, 2005.
[7] E. J. Vaughan and T. Vaughan, *Fundamentals of risk and insurance*. John Wiley \& Sons, 2007.
[8] T. Humphreys, "State-of-the-art information security management systems with ISO/IEC 27001: 2005," *ISO Manag. Syst.*, vol. 6, no. 1, 2006.
[9] W. Boehmer, "Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001," in *2008 Second International Conference on Emerging Security Information, Systems and Technologies*, 2008, pp. 224–231.
[10] B. Shojaie, H. Federrath, and I. Saberi, "Evaluating the effectiveness of ISO 27001: 2013 based on Annex A," in *2014 Ninth International Conference on Availability, Reliability and Security*, 2014, pp. 259–264.
[11] M. Syafrizal and S. Kom, "Information Security Management System (ISMS) MenggunakanStandar ISO/IEC 27001: 2005," *J. DASI*, vol. 10, no. 1, pp. 92–117, 2009.
[12] T. D. K. Informasi, "Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik," *Republik Indones. Kementeri. Komun. dan Inform.*, 2011.
[13] A. Hevner and S. Chatterjee, "Design science research in information systems," in *Design research in information systems*, Springer, 2010, pp. 9–22.