Chance Evaluation and Improvement of Get to Control Data Security Administration Based On ISO/IEC 27001 at Telkom University Jakarta Campus

Nurwan Reza Fachrur Rozi
School of Applied Science, Telkom University, Jakarta, Indonesia
Andri Agustav Wirabudi
School of Applied Science, Telkom University, Jakarta, Indonesia
Seandy Arandiant Rozano
School of Applied Science, Telkom University, Jakarta, Indonesia

Abstract: The digital-based smart campus system, consisting of components such as the campus application, digital presence with QR code, and campus development dashboard, is one of the services offered by Telkom University Jakarta Campus. In addition, it utilizes artificial intelligence (AI) technology, especially image recognition, to support the Green Campus concept and increase environmental protection efforts, demonstrating the university's dedication to utilizing innovative technologies for a sustainable future. Therefore, the security of information assets is very important. Issues of confidentiality, integrity, and availability can arise if the information security system is not properly managed. This research aims to improve the security information system by conducting a risk assessment using the OCTAVE method. This risk assessment aims to identify the most significant impacts when risks occur and prioritize the most important risks. According to ISO/IEC 27001:2013, safety controls and targets are established. The results of this research are purpose and security management documents, risk management documents, and operational standards of procedures (SOPs). Risk management documents related to information security include risk assessment, risk identification, risk analysis, and evaluation at the campus. Standard Operational Procedures (SOP) documentation includes policy documents, work instructions, and work records that are consistent with the selection of objective controls and security controls for risk management.

Keywords: Risk Assessment, ISO 27001, OCTAVE, Standard Operational Procedure

Correspondents Author:
Nurwan Reza Fachrur Rozi, School of Applied Science, Telkom University, Jakarta, Indonesia
Email : nurwan@telkomuniversity.ac.id

Received: May 05, 2024; Accepted: June 19, 2024; Publication: July 7, 2024

Introduction

Telkom University Jakarta Campus is a private university in Indonesia that has implemented various innovative programs to realize a smart eco-campus, with a focus on sustainability and environmental concerns (Permana & Raharjo, 2023). The university has implemented the concept of a digital-based smart campus, combining components such as the Campus Application, Digital Presence with QR Codes, and Campus Development Dashboard, as well as striving to improve areas such as the Campus Academic System, E-learning, and Job Fair. Career Systems and Centers (Maliha, Anwar, & Rodiah, 2023; Zen, Nugroho, Miraj, Yuningsih, & Sintowoko, 2023). In addition, Telkom University Jakarta Campus has been at the forefront of the use of technologies such as Artificial Intelligence (AI) to improve environmental sustainability, with a special focus on the application of AI for image recognition to support the Green Campus initiative (Qurtubi, 2022). In addition, the university has expanded its reach by offering Open Courseware Services through the Open Library, providing free learning resources to the public, and promoting easy access to information. The processes that exist in Telkom University's main business services Jakarta Campus, can be obtained by value chain analysis. The current condition is that there are many threats and weaknesses (Vulnerable) from a managerial and technical perspective, including Threats that occur from outside the organization including viruses, worms, and malware that cause damage, loss, and slow access to data needed to run one of the main services and there is no server recovery policy when experiencing a system failure (down) that causes information to be unavailable so that the service business process annoyed. Based on the Service Level Agreement (SLA), the downtime in these problems occurs for a maximum of 24 hours. There is no asset management policy related to information security, so no one is responsible for managing information assets. In addition, there is no authentication and authorization policy related to information security for users who have access rights to information related to quality determination, planning, control, and evaluation of key business processes, so that when there is a loss or error of business process information can be disrupted and the manager cannot trace the error that occurred. Thus, the form of support in controlling the information security management system from the CIA side is the preparation of the Information Security Management System document and the creation of SOP (Standard Operational Procedure) with the aim of working reference and standardization to regulate the number of people who use and make the existing business processes at Telkom University Jakarta Campus to be more structured, as well as improve the quality of existing information security. The preparation of SOP (Standard Operational Procedure) documents is selected through objective control and security control using ISO/IEC 27001:2013 which is in accordance with information security

needs by considering the results of information security risk management carried out. Information technology affects the operation of systems and helps organizations perform their daily tasks. To protect information systems from security threats, data centers need physical and logical protection. In addition, Telkom University Jakarta Campus will have an open and distance learning system. Effectively, this learning system will increase access and equality of opportunities for high-quality higher education for all Indonesians, including those living in remote areas, both across the country and in various parts of the world. Risk-related issues in organizational management are often not management issues. Sustainable management, on the other hand, refers to the idea that an organization is founded with the expectation that it will continue to function for an indefinite period of time. In many cases, risk helps organizations achieve goals. Organizations usually suffer losses as a result of adverse events or disasters. These losses include information that is inaccessible (loss of access), data that is corrupted or has turned into lost data (loss of integrity), and the possibility of leakage of important information that must be protected. By protecting businesses from potential harm, good IT management can mitigate them (Awasthi, 2020; Fitrani, 2021a; Junior, Utomo, & Oktaria, 2023). The following is a comparative discussion of journals where currently the lack of information security processing continues to pose threats and vulnerabilities, resulting in unattainable goals and affecting confidentiality, integrity, and availability. As a result, the business impact analysis will be affected. ISO/IEC 27001 is an information security management standard issued by the International Organization for Standardization and the International Electrotechnical Commission. ISO 27001 is the most widely used information security management standard by companies and organizations and provides the most comprehensive dedicated reference for information security management worldwide (Engemann & Miller, 2024). ISO 27001 (Nurbojatmiko et al., 2024; Olaniyi, Omogoroye, Olaniyi, Alao, & Oladoyinbo, 2024) is a commonly used standard by businesses and organizations for information security management. It provides the most complete and specific reference on global information security management. ISO 27001:2013 is used in many studies. This journal, "Risk Assessment and Development of Access Control Information Security Governance Based on ISO/IEC 27001:2013 at XYZ University," addresses several research topics, such as identifying assets, threats, weaknesses, risk analysis, BIAs, risk assessments, and risk maps based on ISO/IEC 27001:2013 (Andry, 2024; Fitrani, 2021b). In addition, in the second journal entitled "Implementation of ISO/IEC 27001:2013 for Information Security Management System (SMKI) at the Faculty of Engineering, Uika-Bogor," the author seeks to evaluate the level of hotspot network security of the Faculty of Technology-based on standard requirements. The results show that only 49% of users trust the level of security, and 45% of managers trust it (Wijaya, 2021). The purpose of the research in the third

journal, entitled "Information Security Assessment of Data Centers Based on ISO 27001:2013," is to evaluate data center information security using the FMEA rating index. The journal also provides recommendations for ISO 27001 and offers suggestions for improvements that can be made to update information security policies consistently (Fathurohman & Witjaksono, 2020; Malekolkalami, Jabbari, & Mantegh, 2024; Nafisah, Putra, & Herlambang, 2020). Previous research has shown that this study conducts assessments and recommendations for improvement to the ISO 27001:2013 framework. The author also identifies assets, weaknesses, threats, risk assessment and analysis, as well as risk maps.

Research Method

This research was carried out in 3 stages, namely the initial stage, the development stage, and the final stage. The detailed research methodology is found in Figure 1.

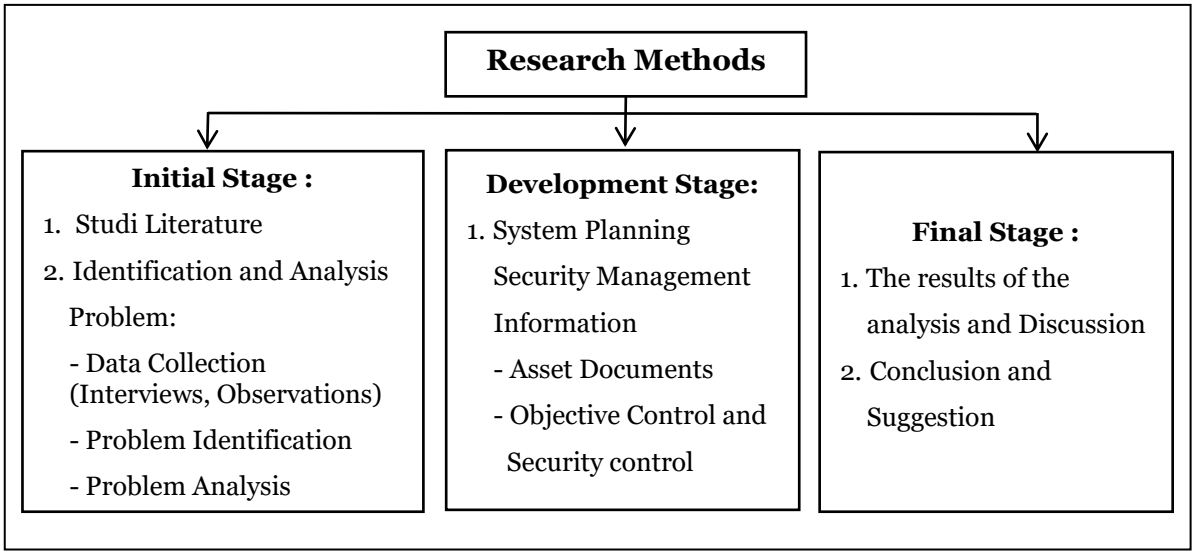

Figure 1 Research Methodology

The Research Method image outlines the three stages of the research process: the initial stage, the development stage, and the final stage.

Initial Stage :

Literature study : This involves conducting a comprehensive review of relevant literature related to information security to establish the basis for the research.

Problem identification : This involves identifying the important assets owned by the organization, organizational security needs, and problems related to the research object, namely at Telkom University Jakarta Campus, especially in the Technical Support division.

Identify assets and risks : This involves understanding the risks that the organization may face if its information is threatened or compromised in security, causing a failure to maintain information security aspects. This process includes identifying assets and classifying them, calculating the value of assets based on the aspect of information security (CIA), calculating the threat and weakness value of an asset, and identifying the impact of failure on the information security aspect (CIA).

Development Stage:

Risk assessment: This involves assessing the identified risks by applying the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) method with mathematical calculations in the risk assessment analysis.

Identify and evaluate risk management: This involves identifying or determining risk management options, which include risk mitigation by implementing appropriate security controls, accepting risk by using risk criteria that have been applied, and accepting risk by transferring risk to a third party (insurer, vendor, or specific party).

Determination of the scope of the Information Security Management System: This involves identifying problems from the external and internal sides in the ICT section to determine the scope of the Information Security Management System (SMKI).

Final Stage: *Result and discussion*: This involves presenting the results of the research and discussing the findings.

It is important to note that the specific details and steps of the research process may vary depending on the research question, the data collection methods, and the analysis techniques used.

Studi Literature

Literature studies are carried out by studying and looking for references, which is the basis for the relevance of research topics related to information security. Given the importance of information security for an organization, information security is needed to protect information from all threats that may occur, to ensure or guarantee business continuity, minimizing business risks (Amalia & Nasution, 2024; Fairuzabadi et al., 2023; Wardana & Suryani, 2023; Yuliana & Hasibuan, 2022)

Problem Identification

Problem identification was carried out by identifying important assets owned by the organization, organizational security needs, and problems related to the object in the research, namely at Telkom University Jakarta Campus, especially in the Technical Support division. Identification was carried out by the results of interviews and observations related to the current conditions in the agency.

Identify Assets and Risks

Risk identification aims to understand how big and what risks will be accepted by the organization if the organization's information is threatened or compromised in security causing a failure to maintain information security aspects (ISO, 2013). This process has four steps, namely:

- Identify assets and classify assets by using the asset table and
- Calculate the value of assets based on the aspect of information security (CIA) by providing the value of each, after this the value of the asset is calculated.
- Calculate the threat and weakness value of an asset
- Identification of the impact of failure on the information security aspect (CIA) is by creating a business impact identification table along with the level of impact that occurred.

Risk Assessment

Assessment of the identified risks by applying the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) method with mathematical calculations in the risk assessment analysis (Alsafwani, Fazea, & Alnajjar, 2024; Friman, 2024; Gerardo & Fajar, 2022). OCTAVE is an approach to risk evaluation from three aspects of information security, namely confidentiality, integrity, and availability that is comprehensive, systematic, directed, and self-conducted. (Pangestu & Wijaya, 2020; Pradana, Utomo, & Al Makky, 2023; Saputra, Ambarwati, & Setiawan, 2020)

Identify and evaluate risk management

Carrying out risk management the steps that must be taken are identifying or determining risk management options. Risk management options: risk mitigation by implementing

appropriate security controls, accepting risk by using risk criteria that have been applied, and accepting risk by transferring risk to a third party (insurer, vendor, or specific party) (Fairuzabadi et al., 2023; Hodson, 2024)

Determination of the Scope of the Information Security Management System

The determination of this scope is urgently needed with the purpose of the documents produced by the needs of information security problems in the IT Technical Support division. In determining the scope of the Information Security Management System (SMKI), it is necessary to identify problems from the external and internal sides in the ICT section.

Result and Discussion

Identify Critical Assets

The list of critical assets owned by the Technical Support division is found in Table 1 and is fully presented in the continuation of Table 1 in the appendix.

Table 1. List of Critical Assets

No	Category	Asset
1	Data Information	- Report Data, - Teaching Material Data, - Academic Data, - Employment Data
2	Software	- Microsoft 365, - Linux & Windows, - Academic System - Employment System, - Reporting System, - Teaching Material System, - E-Learning, - E-Support
3	Hardware	- Printer, - Hardisk, - Router, - Switch, - Server, - PC/Laptop, - Network

Table 1 lists the critical assets owned by the Technical Support division of Telkom University Jakarta Campus. The table has three columns: No., Category, and Asset. The category column has three categories: Data Information, Software, and Hardware. The asset column lists the specific assets that fall under each category.

- Data Information: This category includes critical data assets that are important for the Technical Support division's operations. The assets listed under this category are : Report Data, Teaching Material Data, Academic Data, Employment Data
- Software: This category includes critical software assets that are essential for the division's operations. The assets listed under this category are : Microsoft 365, Linux

& Windows, Academic System, Employment System, Reporting System, Teaching Material System, E-Learning, E-Support

- Hardware : This category includes critical hardware assets that are necessary for the division's operations. The assets listed under this category are : Printer, Hardisk, Router, Switch, Server, PC/Laptop, Network

There is no mention of decryption in Table 1. Decryption is the process of converting encrypted data back into its original, readable format. It is not relevant to the information provided in Table 1.

Identification of Threats and Weaknesses Assets

Critical assets are categorized into information data, software, and hardware in the IT Technical Support division (Marszal-Pomianowska et al., 2024). A complete list of threats and weaknesses is found in Table 2.

Table 2. Identification of Threats and Weaknesses of Assets

Asset Category	Asset	Incident	Threat / Weakness
Data Information	Employement Data	Data input error	Weakness
		Data theft	Threat
		Damaged data storage	Threat
	Reporting Data	Data input error	Weakness
		Data theft	Threat
		Damaged data storage	Threat
	Academic data	Data input error	Weakness
		Data theft	Threat
		Damaged data storage	Threat
	Teaching material data	Data input error	Weakness
		Data theft	Threat
		Damaged data storage	Threat
Software	Microsoft 365	Illegal access	Threat
	Teaching Material System	Virus attack	Threat
		Application not updated	Weakness
		Illegal access	Weakness
	Linux & Windows	Use of administrator access rights on the user'sPC	Weakness

		Not updating linux/windows	Weakness
		Virus attack	Threat
	Academic System	Illegal access	Weakness
		Application not updated	Weakness
		Virus attack	Threat
	E-Support	Application not updated	Weakness
		Virus attack	Threat
		Operational failure	Weakness
	Reporting System	Illegal access	Weakness
		Virus attack	Threat
		Operational failure	Weakness
	Employement System	Application not updated	Weakness
		Virus attack	Threat
		Operational failure	Weakness
	E-Learning	Application not updated	Weakness
		Virus attack	Threat
		Operational failures	Weakness
Hardware	Network	Network disruption	Weakness
		Hacker Attack	Threat
	Server	Server Done	Threat
		Server Configuration Error	Threat
		Virus Attack	Threat
	Switch	Router malfunction	Weakness
	Router	Router malfunction	Weakness
	PC / Laptop	PC/Laptop Theft	Threat
		Damage to PC/Laptop	Weakness
	Printer	Printer theft	Threat
	Hardisk	Hard disk damage	Weakness

Table 2 provides a detailed breakdown of potential threats and weaknesses that could compromise the security of the critical assets identified in Table 1. For each asset category, the table lists the specific threats and weaknesses that have been identified, along with an assessment of potential threats and weaknesses that could compromise the security of critical assets. the risks associated with each threat/weakness pair. Risk assessment is based on two factors: the likelihood of a threat occurring, and the impact of the threat on the asset if the threat occurs. The level of risk is then determined by combining the two factors, using a standard risk assessment matrix. The table also includes a column of recommended

countermeasures, which are actions that can be taken to mitigate the risks associated with each threat/weakness pair. These countermeasures are based on industry best practices and are intended to provide a roadmap to improve the organization's overall security posture.

Risk Assessment & Determining Probability

Risk Assessment itself is a situation faced by humans in every activity and risk is an uncertainty in the coming time about losses (Pangestu & Wijaya, 2020). The method used in risk assessment is the OCTAVE method. By using an approach to risk evaluation from three aspects of information security, namely confidentiality, integrity, and availability that is comprehensive, systematic, directed, and carried out by yourself with quantitative calculations. The objective determines the possible threats that arise according to the identification and weaknesses. Determination of probability based on the history of previous threat events or determined based on the observation of assessed conditions. It is described in table 3.

Identify and evaluate risk management

Risk identification and evaluation aims to determine the selection of risk handling that arises cannot be directly accepted but needs to be further managed using risk acceptance criteria. The risk management options in ICT are determined as follows:

- Accept risk by establishing appropriate security controls
- Accepting risk by using existing risk acceptance criteria

Table 3. Identification of Threats and Weaknesses of Assets

Asset Category	Asset	Incident	Threat / Weakness	Probability	Average Probability
Data Information	Employement Data	Data input error	Weakness	Low	0
		Data theft	Threat	Low	0
		Damaged data storage	Threat	Low	0
	Reporting Data	Data input error	Weakness	Low	0
		Data theft	Threat	Low	0
		Damaged data storage	Threat	Low	0
	Academic data	Data input error	Weakness	Low	0,1

		Data theft	Threat	Low	0
		Damaged data storage	Threat	Low	0,13
	Teaching material data	Data input error	Weakness	Low	0
		Data theft	Threat	Low	0
		Damaged data storage	Threat	Low	0
Software	Microsoft 365	Illegal access	Threat	Low	0
	Teaching Material System	Virus attack	Threat	Low	0
		Application not updated	Weakness	Low	0
		Illegal access	Weakness	Low	0,2
	Linux & Windows	Use of administrator access rights on the user's PC	Weakness	Low	0,04
		Not updating linux/windows	Weakness	Low	0
		Virus attack	Threat	Low	0,13
	Academic System	Illegal access	Weakness	With	0,3
		Application not updated	Weakness	Low	0
		Virus attack	Threat	Low	0
	E-Support	Application not updated	Weakness	Low	0,13
		Virus attack	Threat	Low	0
		Operational failure	Weakness	Low	0
	Reporting System	Illegal access	Weakness	Low	0,2
		Virus attack	Threat	Low	0
		Operational failure	Weakness	Low	0
	Employement System	Application not updated	Weakness	Low	0,2
		Virus attack	Threat	Low	0
		Operational failure	Weakness	Low	0
	E-Learning	Application not updated	Weakness	Low	0
		Virus attack	Threat	Low	0,1

		Operational failures	Weakness	Low	0
Hardware	Network	Network disruption	Weakness	Low	0
		Hacker Attack	Threat	Low	0
	Server	Server Done	Threat	Low	0
		Server Configuration Error	Threat	Low	0,2
		Virus Attack	Threat	Low	0,1
	Switch	Router malfunction	Weakness	Low	0
	Router	Router malfunction	Weakness	Low	0
	PC / Laptop	PC/Laptop Theft	Threat	Low	0
		Damage to PC/Laptop	Weakness	Low	0,1
	Printer	Printer theft	Threat	Low	0
	Hardisk	Hard disk damage	Weakness	Low	0,1

In Table 3, The process of identifying and evaluating risk management involves identifying potential risks and weaknesses in an organization's assets and then assessing the likelihood and impact of those risks. This information is used to prioritize risks and develop risk management plans to mitigate or eliminate those risks. In the context of this writing, the process of risk management identification and evaluation is described in the section "Risk management identification and evaluation". This section describes the use of the OCTAVE (Operational Critical Threat, Asset and Vulnerability Assessment) method to identify and evaluate risks. The OCTAVE method involves a series of steps, including :

- Asset identification: This step involves identifying the organization's critical assets, such as data, software, and hardware.
- Identify threats and vulnerabilities: This step involves identifying potential threats and vulnerabilities that could impact the organization's assets. This information is used to assess the likelihood and impact of such risks.
- Assess risk: This step involves assessing the likelihood and impact of any identified risks. This information is used to prioritize risks and develop risk management plans.

- Developing a risk management plan: This step involves developing a plan to mitigate or eliminate the identified risks. The plan should include specific actions to be taken, as well as a timeline for the implementation of those actions.
- Implementing a risk management plan: This step involves implementing a risk management plan. This may involve implementing new security measures, updating policies and procedures, or providing training to employees.
- Monitoring and reviewing the risk management plan: This step involves monitoring and reviewing the effectiveness of the risk management plan. This information is used to make necessary adjustments to the plan.

In the context of this writing, the OCTAVE method is used to identify and evaluate risks associated with an organization's assets. This information is used to develop a risk management plan to mitigate or eliminate such risks. However, as of this writing, there is no Table 3 that provides information on the identification of threats and weaknesses of assets.

Choosing Objective Controls and Risk Management Security Controls

The purpose of determining this objective control mapping is to adjust to the threats and weaknesses of each asset. The following is a table mapping the results of risk control recommendations with the needs of ISO 27001:2013. The risk mapping with needs is found in Table 4 and is fully presented in the continuation of Table 4 in the appendix.

Table 4. Risk Mapping Using The Clauses of ISO 27001:2013

Name of Asset	Existing Risk	Clause	Control Objective	Security Control	Control
Academic System	Ilegal Access	A.11 – Access Control	A.11.1 – Business requirements for Access control	A.11.1.1 – Access Control policies	Based on information security and business requirements, access control policies should be established, documented, & covered.
			A.11. 4 – Control of application and system access	A.11.4.1 – Information access limitation	Access control policies must be followed when limiting access to the application system and information functions.
Server	Virus attack	A.13 – Operation Security	A.13.2 - Protection againts Malware	A.13.2.1 - Control against malware	To protect against malware, it is necessary to carry out discovery, preventive, and restoration procedures while also having

					appropriate user knowledge.
		A.14 – Communication Security	A.14.1 – Network security management	A.14.1.2 – Network service security	Whether services are offered internally or through an external provider, the security protocols, service standards, and management requirements for each service on the network must be acknowledged and specified in the network service agreement.
	Server configuration error	A.15 – Physical and Environme ntal Security	A.15.2 – Equipments	A.15.2.4 – Equipment maintenance control	It is necessary to maintain equipment in good condition to ensure its availability and integrity.
Academic Data	Data input error	A.16. – Operational Security	A.16.3 -Backup	A.16.3.1 – Information Backup	Software, system images, and backup copies of information should all be captured and methodically inspected by the backup policy agreement.
			A.16.4 -Logging and monitoring	A.16.4.1 - Event logging	Event logs ought to be created, saved, and routinely examined to document user behavior, exclusions, mistakes, and information security-related incidents.
	Damaged data storage	A.17 – Physical and environmental security	A.17.1 – Equipments	A.17.1.2 – Equipment maintenance control	Maintaining equipment effectively is necessary to ensure its verified availability and integrity.

In Table 4 in the document maps the identified risks and their corresponding controls to the relevant clauses of ISO 27001:2013. The table has several columns, each with a specific meaning :

- Asset Category: This column lists the category of the asset that is associated with the risk.
- Asset Name: This column lists the specific name of the asset that is associated with the risk.
- Existing Risk: This column lists the identified risk associated with the asset.

- Clause: This column lists the relevant clause of ISO 27001:2013 that applies to the risk.
- Control Objective: This column lists the objective of the control that is intended to mitigate the risk.
- Control: This column lists the specific control that is intended to mitigate the risk.

Decryption is not explicitly mentioned in Table 4. However, one of the clauses listed in the table is A.10 - Cryptography. This clause requires the organization to implement cryptographic controls to protect the confidentiality, integrity, and authenticity of information. Cryptography involves the use of mathematical algorithms to transform plaintext (readable data) into ciphertext (encrypted data) and vice versa. Decryption is the process of converting ciphertext back into plaintext using the appropriate decryption key. Therefore, if there is a risk associated with the confidentiality, integrity, or authenticity of information, and cryptography is identified as a control to mitigate that risk, then decryption may be necessary to ensure that the information can be accessed and used by authorized parties. For example, if encrypted data needs to be decrypted for use by an authorized user, then the decryption process must be performed using the appropriate decryption key. This is to ensure that the data is not accessed by unauthorized parties and that the integrity of the data is maintained.

Table 5. Planning and structure of SOP content

Structure	Sub-Chapters	Content
Introduction	Purpose	General description of the document Information asset security procedures
	Scope of Data Security Overview	Security aspects of information assets
	Evaluation of Information Asset Security Risk Assessment	Information asset security risk priority list table
Access rights control policy	Policy details	Access rights management
		Third-party access rights
	Related Documents	Access rights management procedures
Information security policy	Purpose	General description of access rights control and Data Security
	Scope of Reference	References used in policy-making - Information system management - Log-on system management - Pegguna password - Back-up management and information restore
	Related Documents	Password management procedures
		Back-up and restore procedures
Hardware and network management policies	Purpose	General description of hardware and network management policies

The structure and content of this SOP will be adjusted to the needs of the research. Standard Operating Procedures (SOPs) are guidelines that contain standard operating procedures used by an organization to ensure that all decisions and actions, as well as the use of process facilities carried out by people involved in the organization, can run effectively, efficiently, standardized, and systematically (Nabilla, 2022; Nikmah & Pratama, 2023). The structure or content that will be included in the framework of the SOP document is in Table 5. Decryption is not explicitly mentioned in Table 5. However, if there is a risk associated with the confidentiality, integrity, or authenticity of information, and cryptography is identified as a control to mitigate that risk, then decryption may be necessary to ensure that the information can be accessed and used by authorized parties. Decryption is the process of converting ciphertext back into plaintext using the appropriate decryption key. Therefore, if there is a need for decryption in the context of the SOP, it could be included in the "Content" column of Table 5 as a sub-chapter under the "Information security policy" or "Hardware and network management policies" sections. For example, "Decryption procedures" could be added as a sub-chapter under "Information security policy" to provide guidance on how to decrypt information in a secure manner. Alternatively, "Decryption key management" could be added as a sub-chapter under "Hardware and network management policies" to provide guidance on how to securely manage decryption keys.

Resulting Documents

Discussing the process and output of this study, the explanation can be seen in Table 6.
Decryption is not explicitly mentioned in Table 6. However, if there is a risk associated with the confidentiality, integrity, or authenticity of information, and cryptography is identified as a control to mitigate that risk, then decryption may be necessary to ensure that the information can be accessed and used by authorized parties. Decryption is the process of converting ciphertext back into plaintext using the appropriate decryption key. Therefore, if there is a need for decryption in the context of the output process results, it could be included in the "Process" or "Output" columns of Table 6. For example, if the output process result is "Data restore work instructions", then decryption may be necessary if the data was encrypted prior to backup. In this case, "Decryption procedures" could be included as a step in the "Data restore work instructions" process. Alternatively, if the output process result is "Hardware maintenance work instructions", then decryption may be necessary if the hardware contains encrypted data. In this case, "Decryption procedures" could be included as a step in the "Hardware maintenance work instructions" process. It's important to note that the specific details of the decryption process will depend on the particular encryption algorithm and key management system being used. Therefore, any decryption procedures should be developed in consultation with the relevant

technical experts and in accordance with the organization's information security policies and protocols.

Table 6. Output Process Results

Process	Output
Clause mapping with objective controls	Hardware management policy
Risk mapping with security controls	Human resource security policy
Mapping clauses to security needs	Work instructions for access rights management
Risk mapping with policy documents	Password reset work instructions
Policy mapping, work instructions, & work records	Work instructions to back up data and files
	Data restore work instructions
	Hardware maintenance work instructions
	Information security work instructions
	Cable & network maintenance work instructions
	Access rights management procedures
	Password management procedures
	Backup and restore procedure
	Hardware management procedure
	Access rights management form

Conclusions

In conclusion, the document presents a research study on the risk assessment and improvement of access control information security governance based on ISO/IEC 27001:2013 at Telkom University Jakarta Campus. The study identified the critical assets, threats, and vulnerabilities of the university's information system and conducted a risk assessment using the OCTAVE Allegro method. Based on the risk assessment, appropriate security controls were identified and implemented to mitigate the risks. The resulting documents from the study include policy documents, work instructions, and work records related to the determination of objective controls and security controls from the results of risk management related to information security. The development of the final project can be done by considering the impact of the cost of losses experienced by the agency, and the SOP document can still be developed and improved due to the rapid development of technology. Therefore, it is recommended that the agency continues to compete and run their business processes better by implementing the SOP document. Overall, the study demonstrates the importance of conducting risk assessments and implementing appropriate security controls to protect critical assets and mitigate the risks associated with information security.

Based on the results of the analysis that has been obtained:

1. The results of the analysis show that three assets, namely servers, academic systems, and academic data, require risk management because they have a high-risk value. Based on a high-risk assessment, they can be arranged into four clauses, namely A.11, A.15, A.13, and A.14.
2. Objective risk management and security documents Risk management documents related to information security include risk assessment, risk identification, risk analysis, and risk evaluation.
3. Standard Operating Procedure (SOP) documents include policy documents, work instructions, and work records related to the determination of objective controls and security controls from the results of risk management related to information security.

Limitations to this study:

- Firstly, the research only covers the creation of SOP documents without the SOP testing process and the implementation of SOPs for the organization's business processes. Therefore, the effectiveness of the SOPs in mitigating the identified risks is not evaluated in this study.
- Secondly, the scope of the research is limited to a single university, which may limit the generalizability of the findings to other organizations or contexts. Future research could expand the scope to include multiple organizations and industries to validate the findings and provide more generalizable recommendations.
- Thirdly, the research relies on the OCTAVE Allegro method for risk assessment, which is a qualitative method that may be subject to bias and variation in interpretation. Future research could consider using a quantitative risk assessment method to provide more objective and accurate risk assessments.
- Lastly, the document does not discuss the potential impact of human factors on information security risks. Human errors, negligence, and malicious intent can significantly impact the security of information systems. Therefore, future research could incorporate a human factors analysis to provide a more comprehensive understanding of information security risks. In conclusion, while the research presented in the document provides valuable insights, it is essential to consider its limitations when interpreting the findings and applying them in practice. Future research could address these limitations to provide more comprehensive recommendations for improving access control information security governance based on ISO/IEC 27001:2013.

The recommendations are as follows:

a. The development of the final project can be done by considering the impact of the cost of losses experienced by the agency

b. This research only covers the creation of SOP documents without the SOP testing process and the implementation of SOPs for the organization's business processes

c. Due to the rapid development of technology, this SOP document can still be developed and developed. Thus, agencies can continue to compete and run their business processes better.

References

Alsafwani, N., Fazea, Y., & Alnajjar, F. (2024). Strategic Approaches in Network Communication and Information Security Risk Assessment. *Information, 15*(6), 353. doi:10.3390/info15060353

Amalia, P., & Nasution, M. I. P. (2024). Tantangan Terkini Dalam Keamanan Informasi Analisis Resiko Dan Upaya Perlindungan. *Jurnal Ekonomi Bisnis dan Manajemen, 2*(1), 24-37. doi:10.59024/jise.v2i1.529

Andry, J. F. K., Nadia Tannady, Hendy. (2024). Disater Recovery Planning For IT/IS Of Hospital Industry Using NIST SP 800-34 Rev. 1 Method. *Journal of Theoretical and Applied Information Technology, 102*(8). doi:10.59141/jiss.v4i09.879

Awasthi, A. (2020). Disaster Recovery-Foundation Pillars. *Int Sci Res, 9*(1), 1360-1362. doi:10.21275/ART20204296

Engemann, K. J., & Miller, H. E. (2024). Toward revealing concealed risks for agile IT service management practices. *Information Systems and e-Business Management*, 1-31. doi:10.1007/s10257-023-00666-8

Fairuzabadi, M., Pangaribuan, J. J., Moedjahedy, J. H., Sihotang, J. I., Simarmata, J., Andryanto, A., . . . Suardinata, S. (2023). *Keamanan Sistem Informasi dan Kriptografi*: Yayasan Kita Menulis.

Fathurohman, A., & Witjaksono, R. W. (2020). Analysis and design of information security management system based on ISO 27001: 2013 using Annex Control (Case Study: District of Government of Bandung City). *Bulletin of Computer Science and Electrical Engineering, 1*(1), 1-11.

Fitrani, L. D. (2021a). The Combination Of AHP And Topsis Methods In Determining The Ranking Of Recommendations For Improvement Of Information Technology Services. *Jurnal Pilar Nusa Mandiri, 17*(2), 119-126. doi:10.33480/pilar.v17i2.2319

Fitrani, L. D. (2021b). Risk Assessment And Development Of Access Control Information Security Governance Based On ISO/IEC 27001: 2013 At XYZ University. *Jurnal Teknik Informatika dan Sistem Informasi ISSN, 2407*, 4322.

Friman, O. (2024). Agile and DevSecOps Oriented Vulnerability Detection and Mitigation on Public Cloud.

Gerardo, V., & Fajar, A. N. (2022). Academic IS Risk Management using OCTAVE Allegro in Educational Institution. *Journal of Information Systems and Informatics, 4*(3), 687-708. doi:10.51519/journalisi.v4i3.319

Hodson, C. J. (2024). *Cyber risk management: Prioritize threats, identify vulnerabilities and apply controls*: Kogan Page Publishers.

Junior, R. R., Utomo, R. G., & Oktaria, D. (2023). Information Security Analysis in PT. XYZ Using ISO/IEC 27001: 2013. *Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi, 12*(1). doi:10.35889/jutisi.v12i1.1118

Malekolkalami, M., Jabbari, L., & Mantegh, H. (2024). Evaluating the status of information security management in faculty libraries: a case study of Allameh Tabatabai University. *Information Security Journal: A Global Perspective*, 1-14. doi:10.1080/19393555.2024.2347255

Maliha, I., Anwar, R. K., & Rodiah, S. (2023). Penerapan Layanan Opencourseware Open Library Telkom University sebagai Media Pembelajaran Gratis. *Jurnal Pustaka Ilmiah, 9*(1), 21-34. doi:10.20961/jpi.v9i1.71725

Marszal-Pomianowska, A., Motoasca, E., Pothof, I., Felsmann, C., Heiselberg, P., Cadenbach, A., . . . Schaffer, M. (2024). Strengths, weaknesses, opportunities and threats of demand response in district heating and cooling systems. From passive customers to valuable assets. *Smart Energy, 14*, 100135. doi:10.1016/j.segy.2024.100135

Nabilla, D. R. (2022). Analisis Efektivitas Penerapan Standard Operating Procedure (SOP) pada Departemen Community & Academy RUN System (PT Global Sukses Solusi Tbk).

Nafisah, F. A., Putra, W. H. N., & Herlambang, A. D. (2020). Evaluasi Keamanan Informasi Data Center Berdasarkan Standar ISO 27001: 2013 (Studi Kasus PT. Pupuk Kalimantan Timur). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 4*(6), 1858-1865.

Nikmah, F. K., & Pratama, R. A. (2023). Pengembangan standar operasional prosedur (sop) pada bagian keuangan pt. Xyz. *Jurnal Ekonomi, Bisnis, dan Akuntansi, 25*(1), 10-18. doi:10.32424/jeba.v25i1.3508

Nurbojatmiko, N., Aini, Q., Wasiqi, N. C., Alfajri, M. F., Ulinnuha, Z., Purwati, Y. K., . . . Yasmin, N. A. (2024). Risk Assessment Maturity Level of Academic Information System Using ISO 27001 System Security Engineering-Capability Maturity Model.

Journal of Applied Engineering and Technological Science (JAETS), 5(2), 941-954. doi:10.37385/jaets.v5i2.2971

Olaniyi, O. O., Omogoroye, O. O., Olaniyi, F. G., Alao, A. I., & Oladoyinbo, T. O. (2024). Cyberfusion protocols: Strategic integration of enterprise risk management, ISO 27001, and mobile forensics for advanced digital security in the modern business ecosystem. *Journal of Engineering Research and Reports, 26*(6), 31-49. doi:10.9734/jerr/2024/v26i61160

Pangestu, R. P., & Wijaya, A. F. (2020). Analisis Manajemen Risiko Aplikasi SINTESA Pada Perpustakaan XYZ. *J. Bina Komput, 2*(2), 1-14.

Permana, A. G., & Raharjo, J. (2023). Integrated waste management system with IOT-based centralized control towards a smart eco campus-Telkom University. *International Journal of Energy Economics and Policy, 13*(2), 322-333. doi:10.32479/ijeep.14048

Pradana, R. F. W., Utomo, R. G., & Al Makky, M. (2023). Analisis Risiko Keamanan Informasi Pada Divisi Penjualan Pt Matahari Department Store Cabang Jogja City Mall Menggunakan Metode Octave Allegro. *eProceedings of Engineering, 10*(5).

Qurtubi, A. (2022). Digital-Based Smart Campus at Telkom University, Indonesia. *Education Quarterly Reviews, 5*(3). doi:10.31014/aior.1993.05.03.543

Saputra, R. R., Ambarwati, A., & Setiawan, E. (2020). Manajemen Risiko Teknologi Informasi Menggunakan Octave Allegro Pada Pt. Hd. *SITEKIN: Jurnal Sains, Teknologi Dan Industri, 17*(1), 1-10.

Wardana, A. A., & Suryani, E. (2023). Evaluation of Information Security Management in Micro, Small, and Medium Enterprises (MSMEs) using Penilaian Mandiri Keamanan Informasi (PAMAN KAMI).

Wijaya, Y. D. (2021). Evaluasi Kemananan Sistem Informasi Pasdeal Berdasarkan Indeks Keamanan Informasi (Kami) Iso/Iec 27001: 2013. *Jurnal Sistem Informasi dan Informatika (Simika), 4*(2), 115-130. doi:10.47080/simika.v4i2.1178

Yuliana, R., & Hasibuan, Z. A. (2022). Best practice framework for information technology security governance in Indonesian government. *International Journal of Electrical and Computer Engineering, 12*(6), 6522. doi:10.11591/ijece.v12i6.pp6522-6534

Zen, A., Nugroho, A., Miraj, I., Yuningsih, C., & Sintowoko, D. (2023). *The role of artificial intelligence in image recognition to support green campus in Telkom University*. Paper presented at the AIP Conference Proceedings.