Journal of Information Technology and Cyber Security 2(2) July 2024: 58-75 EISSN 2987-386X | PISSN 2987-3878
DOI: 10.30996/jitcs.12099

Risk Management Analysis of Information Security in an Academic Information System at a Public University in Indonesia: Implementation of ISO/IEC 27005:2018 and ISO/IEC 27001:2013 Security Controls

Sonya Meitarice [1,*], Lidya Febyana [2], Aidil Fitriansyah [3], Rahmad Kurniawan [4], and Riki Ario Nugroho [5]

[1,2,4,5] Department of Information Systems, Universitas Riau, Indonesia
[3] Department of Informatics Management, Universitas Riau, Indonesia
* Corresponding author: sonya@lecturer.unri.ac.id

Received: 27 October 2024
Accepted: 14 November 2024
Revised: 12 November 2024
Available online: 20 November 2024

To cite this article: Meitarice, S., Febyana, L., Fitriansyah, A., Kurniawan, R., & Nugroho, R. A. (2024). Risk Management Analysis of Information Security in an Academic Information System at a Public University in Indonesia: Implementation of ISO/IEC 27005:2018 and ISO/IEC 27001:2013 Security Controls. *Journal of Information Technology and Cyber Security*. *2*(2), 58-75. https://doi.org/10.30996/jitcs.12099

Abstract

An online academic information system is potentially exposed to various threats from internal and external sources, which may compromise the institution's objectives if not managed effectively and appropriately. Academic portals often experience issues such as server downtime and unauthorised access attempts. However, there is no specific documentation dedicated to managing these issues. This study aims to analyze risk management in information security for the academic portal of Universitas Riau, Indonesia. The study employs the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27005:2018 standard and ISO/IEC 27001:2013 security controls, following four key stages: context establishment, risk assessment, risk treatment, and recommendations. The findings identify eight categories of information system assets, 30 identified threats, and 43 vulnerabilities, including two high-risk categories, 19 medium-risk categories, and 22 low-risk categories. Of the 43 vulnerabilities, 21 risks required risk modification, four required risk avoidance, and four required risk sharing. Fourteen risks, which can be managed through risk retention (acceptance of risk), fall under the category of risk acceptance. Furthermore, ISO/IEC 27001 suggests that implementing control recommendations can minimize and effectively address these risks. Nevertheless, this study focuses primarily on information security risks and does not extensively cover related areas such as data privacy, regulatory compliance, or operational risks. Future research can explore the effectiveness of training programs and awareness campaigns in reducing human-related risks, such as phishing and social engineering attacks.

Keywords: risk management, ISO/IEC 27005, ISO/IEC 27001, academic information system.

1. Introduction

The fourth industrial revolution has brought rapid and disruptive advancements in information and communication technology (ICT), significantly enhancing the growth of IT services (Ibrahim, Mohamad, & Shah, 2020). ICT plays a crucial role in a country's development by facilitating knowledge dissemination and fostering innovation, particularly in both developed and developing nations (Appiah-Otoo & Song, 2021). Nearly all businesses rely on ICT for faster, more precise, and accurate information processing and data management (Jorgenson & Vu, 2016). However, the widespread use of the Internet has introduced numerous internal and external threats. Globally, cyberattacks are increasing at an alarming rate, resulting in substantial financial losses (Sharif & Mohammed, 2022). This can threaten the continuity of business activities in the organization, including the academic sector.

Universitas Riau (Unri) is a public educational institution located in Riau Province, Indonesia, which has adopted information technology to manage academic data through a web-based Academic Portal. The Academic Portal includes several features such as course registration and printing, viewing academic transcripts, accessing lecture materials, and viewing announcements related to student affairs and academic activities. The purpose of implementing the Academic Portal is to facilitate academic processes for lecturers and students, as well as to assist staff in managing course registrations, academic transcripts, and other student-related information.

With the increasing use of information technology in academics, particularly the information systems at Unri, the information technology risks that Unri must face also increase. The reason is challenges in security and resource management. Potential threats can come from within the system itself or from external elements. For instance, there could be student data loss during course registration. This aligns with previous research by Leasa & Prassida (2024), which revealed similar findings that the Academic Portal system at Unri has security vulnerabilities. There have been incidents of account hijacking, leading to alterations in student data, including changes to student names.

To address the risks associated with the Academic Portal at Unri, a technique called risk management is required. Risk management involves a series of processes, such as identifying, assessing, and planning actions to mitigate risks, allowing the organization to achieve an acceptable level of risk (Amirinnisa & Bisma, 2023). Many standards are used in the implementation of risk management, including ISO 27005, which is widely applied in profit and non-profit organizations in other countries (Rambe, Gandhi, & Sabariah, 2023). Based on recommendations from another study, ISO 27005 is one of the international standards that is easy to implement in providing guidelines for information security risk management (Fahrurozi, Tarigan, Tanjung, & Mutijarsa, 2020).

This study aims to conduct an information security risk assessment using ISO/IEC 27005:2018 as a risk management framework. Following the ISO/IEC 27001:2013 framework, the recommended controls include risk treatment and acceptance. This guideline is used to determine and implement information security risk management controls inside an information security management system (ISMS) based on ISO/IEC 27001 (International Organization for Standardization, 2013).

2. Literature Review

2.1. Risk Management

Risk is the likelihood of an event occurring that disrupts business processes or impacts the organization, potentially leading to the failure of its business objectives (Isnaini, Sari, & Kuncoro, 2023). Effective risk management, particularly in information security, involves identifying, evaluating, and mitigating risks to an acceptable level (Whitman & Mattord, 2018). Information security risk management is a practical approach to managing the risks associated with an organization's information security, aiming to protect its information and (Klipper, 2011). The key processes in risk management include risk identification, risk assessment, and risk control. Implementing risk management in non-profit organizations offers several advantages, such as planning essential information technology resources, supporting leaders in decision-making, and enhancing operational performance by advancing the maturity level of the risk management process (Sahira, Fauzi, & Santosa, 2020).

2.2. Information Security

Information processing and security are intricately linked, particularly concerning the facilities involved such as documents, hardware, software, infrastructure, and buildings that safeguard it. The capability of organizations to accurately access and deliver valuable information is crucial, impacting their reputation. Thus, ensuring information protection involves addressing security aspects detailed in Fig. 1, as explained below:

- Confidentiality states that information security can only be accessed by those who have the right to access certain information.
- Integrity states that information must not undergo any data changes other than obtaining permission from the entitled. Information security has complete information and is protected from corruption, damage, and other threats that can cause changes in the content of source information.
- Availability relates to the availability of certain information that can be accessed by users when needed, without interruption, and not in a format that cannot be used. Attacks on information systems cause barriers to information access.

2.3. ISO 27005:2018

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical

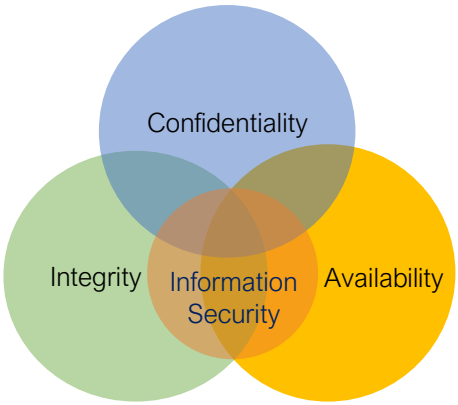

Fig. 1. Information security aspects (Kaur, Gupta, & Singh, 2017)

Commission) have established a specialized system for standardization worldwide. In 2005, ISO collaborated with IEC to release standards for Information Security Management Systems (ISMS), categorized under the ISO/IEC 27000 series. ISO 27005 provides comprehensive guidance on holistically managing information security risks. The process begins with identifying potential risks to information security, including assessing critical information assets, potential threats, and vulnerabilities within the information system. Following identification, these risks are evaluated based on their potential impact and the likelihood of occurrence (International Organization for Standardization, 2018). The risk management process framework of ISO 27005:2018 is illustrated in Fig. 2.

1. Context establishment
   Establishing the context for information security risk management involves defining risk assessment criteria, determining scope and boundaries, and setting up the organizational structure for risk management.
2. Risk identification
   This process involves identifying, describing, and understanding potential risks that could impact a project, organization, or other activities. The aim is to recognize possible risks early on to enable the implementation of appropriate preventive or mitigation actions.
3. Risk analysis
   Risk analysis is the process of understanding and evaluating the potential impact of identified risks on a project, business activity, or organization. The goal is to measure the level of risk involved and support decision-making on mitigation strategies or risk management responses.
4. Risk evaluation
   Risk evaluation is a crucial stage in risk management, where the identified and analyzed risks are further assessed to determine how successfully a project, business activity, or other objectives can withstand these risks.
5. Risk treatment
   Risk treatment focuses on developing strategies to manage the identified and assessed risks from the previous stages. This step involves selecting appropriate actions to address or mitigate risks, aiming to reduce their potential impact effectively.

2.4. ISO 27001:2013

ISO/IEC 27001 is an information security standard, with the latest version published in 2013. This standard was issued by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the ISO and IEC subcommittee, ISO/IEC Joint Technical Committee (JTC)3. ISO/IEC 27001 outlines the framework for establishing a management system related to information security, ensuring it meets specific requirements and passes an audit conducted by a certified auditing body. ISO/IEC 27001:2013 includes 14 clauses, 35 control objectives, and 144 security controls. ISO/IEC 27001 and ISO/IEC 27005 provide guidelines for establishing and managing information security within an organization. The standards have been implemented in various sectors, including education, where they support data protection and compliance efforts. Studies demonstrate that educational institutions benefit from adopting these standards by enhancing data security, streamlining risk management, and increasing resilience to cyber threats (Yustanti, Qoiriah, Bisma, & Prihanto, 2019).

Implementing ISO/IEC 27001 and 27005 in educational institutions has been documented in several recent studies. For example, Dioubate, Daud, & Norhayate (2022) in Malaysia highlighted improvements in

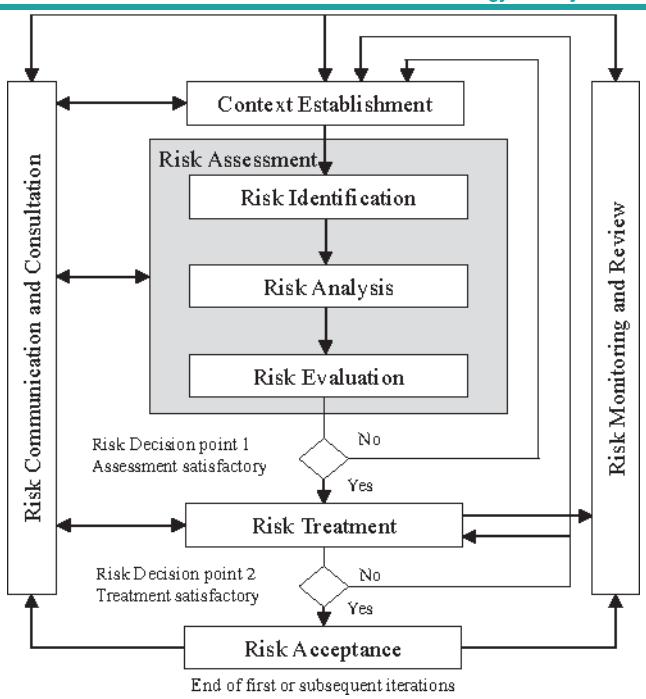

Fig. 2. Illustration of the process ISO 27005: 2018 (International Organization for Standardization, 2018)

handling student data, with a structured approach to risk assessment and management. Most public universities use the ISO 27001: 2013 international standard as a specification for ISMS. In Indonesia, Leasa & Prassida (2024) demonstrated that while institutions can face challenges such as limited technical resources and awareness, the implementation of these standards ultimately leads to a more robust information security posture.

The complementary nature of ISO 27001 and 27005 allows educational institutions to adopt a comprehensive approach to information security. While ISO 27001 focuses on establishing and maintaining an information security management system (ISMS), ISO 27005 provides a detailed risk management framework to identify, assess, and mitigate risks within the ISMS (International Organization for Standardization, 2018).

3. Methods

This research uses a case study of Unri Portal Academic. The proposed method used is the ISO/IEC 27005:2018 framework as the main risk management framework can be seen in Fig. 3. Recommendations for control used are the ISO/IEC 27001:2013 framework.

The research begins by identifying the problems that arose in the Unri Academic Portal, followed by determining the standards to measure these risks. The research objectives are also established at this stage. Next, data collection is conducted. During this phase, a literature study is carried out to facilitate the analysis, requiring the identification of several types of data such as:

a. Theories related to information system risk management and information system security,
b. Theories on ISO 27005:2018 methodology and ISO 27001:2013 controls,
c. Determining the needs for primary and secondary data. Secondary data is obtained from literature studies and analysis of supporting documents, while primary data is gathered through interviews and questionnaires. The interview was conducted with the Head of the IT Division. Additionally, questionnaires were completed by three respondents, each representing the IT Infrastructure Division, the Administration Division, and the Systems Division.

The next stage is the risk management analysis of the Unri Academic Portal using the ISO 27005:2018 method. The risk management analysis begins with Context Establishment. Context establishment involves defining the basic risk research criteria, and setting the scope, objectives, and limitations of risk management. This research establishes the context of information security risk management in the form of the Academic Information System data and IT assets at UPT TIK Unri.

After risk context establishment, this study performed a Risk Assessment. Risk assessment determines the value of information assets, identifies threats and vulnerabilities, identifies existing controls

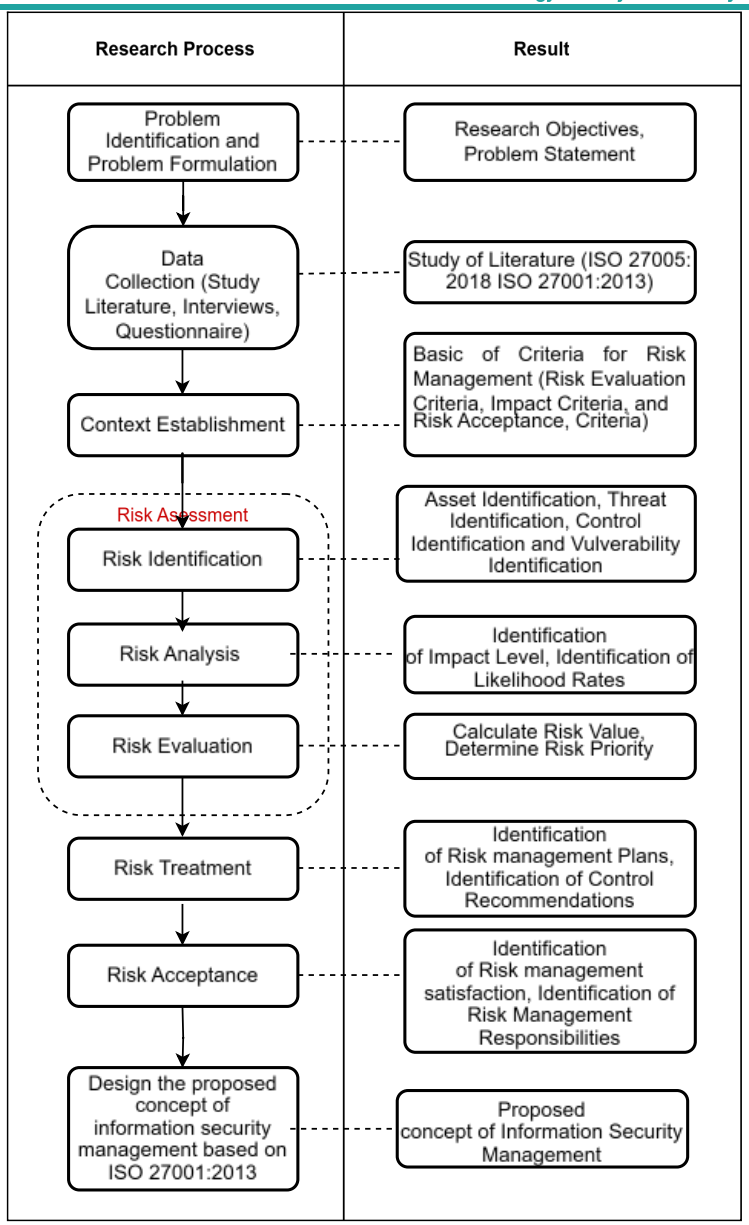

Fig. 3. Research method.

and their effects on identified risks, determines potential consequences, and prioritizes the obtained risks. The risks are then classified against the risk evaluation criteria set in the context establishment. The risk assessment process includes three sub-stages, such as risk identification, analysis, and evaluation.

In identifying risks, this study collected data or information regarding assets, threat identification, existing control identification, vulnerabilities identification, and the potential consequences and impacts of information technology (IT) risks at UPT TIK Unri.

The second sub-stage is risk analysis. In this stage, risk assessments were conducted for risks that may have been previously identified. The determination of this value will be based on the likelihood of threats and the impact categories of the risks occurring. The likelihood categories of threats range from very unlikely (1), unlikely (2), possible (3), likely (4), to frequent (5). The impact categories of risk occurrence range from insignificant impact to very significant impact that disrupts the Academic Portal. The impact categories range from very low (1), low (2), medium (3), high (4), to very high (5). Identified risks were assigned the likelihood and the impact values, which were determined through questionnaires.

The third sub-phase was risk evaluation. In this phase, the assessed risks were evaluated based on the risk level. The determination of the risk level is guided by risk criteria, namely the likelihood value and the impact value from the questionnaires filled out by the respondents. The risk levels are divided into three categories: low, medium, and high.

Table 1
Risk criteria.

Likelihood		Description
Value	Scale	
1	Very Unlikely	The likelihood of occurrence is low, with an expected frequency of once per year under certain abnormal conditions or no occurrence at all under some conditions. The probability of occurrence is less than 10%.
2	Unlikely	The likelihood of occurrence is low, with an expected frequency of 1 to 2 times per year under various conditions. The probability of occurrence ranges from greater than 13% to less than 25% annually.
3	Possible	Under all conditions, the likelihood of occurrence is 4 to 8 times per year, with a probability ranging from greater than 25% to less than 35% annually.
4	Likely	There is a likelihood of occurrence greater than 15 times per year under all conditions or various circumstances. The probability of occurrence ranges from greater than 35% to less than 65% annually.
5	Frequent	The likelihood of occurrence is consecutive under various conditions or circumstances, with a probability of greater than 65% annually.

Table 2
Impact criteria.

Likelihood		Description
Value	Scale	
1	Very Low	A non-significant impact means that it does not cause any major disruption to activities, with a resolution tolerance of up to 7 days.
2	Unlikely	A minor impact on the Academic Portal services, not affecting the main program, has a resolution tolerance of 1-2 days.
3	Medium	A moderate impact on the supporting services of the Academic Portal.
4	High	A major impact on the primary services of the Academic Portal.
5	Very High	A critical impact on both the primary and supporting services of the Academic Portal.

After the risk assessment was conducted, the next process was risk treatment. Risk treatment is a stage in information security risk management where the organization takes concrete actions to reduce the impact or likelihood of identified risks, using appropriate risk mitigation processes to minimize or eliminate the likelihood and impact of these risks. Four options are available for risk treatment based on ISO 27005:2018 standards, namely risk modification, risk avoidance, risk sharing, and risk retention.

During the risk treatment phase, risk scenarios that exceed the organization's risk appetite were mitigated and prioritized for risk treatment. This involves implementing information security control recommendations and setting information security targets based on ISO/IEC 27001:2013. The outcomes of the risk management design process were then communicated to top management for validation and approval.

4. Results and Discussion

4.1. Context Establishment

The scope of this research focuses on the data and assets possessed by Unri, particularly those related to the Academic Portal, such as hardware, software, networks, and other relevant data. The outcome of defining the scope is a focus on the IT infrastructure sub-division within the UPT TIK at Unri. In addition to defining the scope, criteria for risk assessment had also been established. These criteria were based on a literature review conducted earlier. The purpose of this process is to establish guidelines for the risk assessment phase. These guidelines include criteria for the likelihood of threats as shown in Table 1, impact criteria as shown in Table 2, risk level criteria as shown in Fig. 4, and risk treatment criteria as shown in Fig. 5.

The risk criteria were used to assess the probability of occurring risks and employ a predefined frequency scale. The impact criteria are used to evaluate the extent of a risk's effect on achieving the organization's business process goals, utilizing a scale that relates values to impact criteria. Risk Level Crite-

Impact \ Likelihood	Very unlikely (1)	Unlikely (2)	Possible (3)	Likely (4)	Frequent (5)
Very low (1)	1/L	2/L	3/L	4/M	5/M
Low (2)	2/L	4/L	6/M	8/M	10/M
Medium (3)	3/L	6/M	9/M	12/M	15/H
High (4)	4/M	8/M	12/M	16/H	20/H
Very high (5)	5/M	10/M	15/H	20/H	25/H

Fig. 4. Risk level criteria.

Impact \ Likelihood	Low	Medium	High
Low	Accept	Accept	Modification
Medium	Accept	Modification	Modification
High	Modification	Modification	Modification

Fig. 5. Risk treatment criteria.

Table 3
IT Assets.

Information System Components	IT Assets of Portal Academic
Hardware	Server, Personal Computer (PC), Uninterruptible Power Supply (UPS), Printer, Modem, Stabilizer, Air Conditioner (AC), Hard Disk, Random Access Memory (RAM), Closed-Circuit Television (CCTV).
Software	Academic portal, operating system, MySql (Database management system).
Network	LAN (Local Area Network) dan WLAN (Wireless Local Area Network), Router, Hub, Switch, and Access Point, Fiber optic, RJ 45 dan Kabel Twisted Pair (UTP).
Data and Information	Student, course and Lecturer Data.
Personel	UPT TIK Staff.

ria, often referred to as the risk assessment matrix, were used in the risk assessment sub-phase of risk evaluation. To determine the risk level, a mapping of likelihood and impact was conducted.

4.2. Risk Asessment

Risk assessment involves determining the value of information assets, identifying applicable threats and existing (or potential) vulnerabilities, identifying existing controls and their effects on the identified risks, determining potential consequences, and ultimately prioritizing the identified risks. These risks were then categorized according to the risk evaluation criteria established during the context setting.

4.2.1. Risk identification

a. Asset identification
The identification of IT assets was conducted through document analysis and interviews. The focus of information security implementation is on protecting the IT Infrastructure Division, which possesses technology assets. The assets to be identified include components of the information system, such as hardware, software, networks, data or information assets, and personnel assets as in Table 3.
In addition to identifying IT assets related to the Academic Portal, critical asset requirements were also identified to protect against various threats, with the goals of ensuring business continuity, reducing risk, and optimizing information system security. The fundamental principles commonly used in information security management are known as CIA (Confidentiality, Integrity, and Availability), which serve as guidelines for maintaining information security. In this study, the results of critical asset identification will be used as the research focus, with the CIA principles employed as categories for identifying security needs for critical assets, as presented in Table 4.

b. Threat identification
The second stage was the identification of potential threats to the information system assets of the Unri Academic Portal. Threat identification was conducted through a literature review, specifically of scho-

Table 4
Information security management.

Critical Assets	Asset Code	Information Security Management	Description
Server	A-001	Confidentiality	Access is available to authorized personnel who have permission to access it.
		Integrity	The server must not be accessed by unauthorized machines or individuals who could alter the system.
		Availability	"Access must be available 24 hours a day."
PC, UPS, Hardisk	A-002	Confidentiality	Access is available to authorized personnel.
		Integrity	Conduct monitoring to ensure performance.
		Availability	Access must be available 24 hours a day.
Portal Akademik	A-003	Confidentiality	Accessible only by UPT TIK staff and authorized personnel.
		Integrity	The information must be complete and accurate.
		Availability	Access must be available 24 hours, and the data must be frequently updated.
MySql (Database management system)	A-004	Confidentiality	Access is available to authorized personnel.
		Integrity	The information must be complete and accurate.
	A-005	Availability	Access must be available 24 hours, and the data must be frequently updated.
Operating System		Confidentiality	Access to sensitive information is restricted to authorized users only.
		Integrity	The information must be complete and accurate.
		Availability	Access must be available 24 hours, and the data must be frequently updated.
Router Hub Switch Access Point LAN, WLAN Fiber optic RJ 45	A-006	Confidentiality	A firewall should be in place to filter access and ensure that no violations occur that could lead to serious issues.
		Integrity	Conduct network monitoring to ensure the integrity of the data.
		Availability	Sensors should be installed to monitor network equipment, ensuring continuous usability.
Academic Data	A-007	Confidentiality	Access is available to authorized personnel.
		Integrity	The information must be complete and accurate.
		Availability	Access must be available 24 hours, and the data must be frequently updated.
Staf UPT TIK UR	A-008	Confidentiality	The division head must ensure that employees do not disclose important information to unauthorized parties.
		Integrity	Staff must ensure that all information is complete and accurate, and they must also participate in training related to information technology.
		Availability	A shortage of IT staff in the field of information and communication technology.

larly journals that discuss information security threats, followed by interviews. The sources of threats include natural disasters, environmental/technical failures, unintentional human actions, and intentional human actions. The results of the threat risk identification for assets such as hardware, software, networks, data or information, and personnel/human resources can be found in Table 5.

Based on Table 5, 30 types of threats have been identified that could potentially disrupt the management and security of the Academic Portal information system at Unri. The threat identification process revealed four main sources contributing to these security threats. These sources include (1)

Table 5
Threat iIdentification.

Assets	Threat Code	Typical Threats	Threat Sources
Hardware	AN1	Fire	Physical damage
	AN2	Pollution	Physical damage
	AN3	Climatic phenomenon	Natural events
	AN4	Equipment failure	Technical failures
	AN5	Theft of equipment	Compromise of information
	AN6	Configuration error and server maintenance	Technical failures
	AN7	Server down	Technical failures
	AN8	Overheating	Technical failures
	AN9	Loss of power supply	Technical failures
Software	AN10	SQL injection	Unauthorized actions
	AN11	System crash	Technical failures
	AN12	Sniffing	Unauthorized actions
	AN13	Bruteforce login	Unauthorized actions
	AN14	Error in use	Technical failures
Network	AN15	Failure of telecommunication equipment	Loss of essential services
	AN16	There is disturbance on the gateway	Loss of essential services
	AN17	Remote spying	Unauthorized actions
	AN18	Worm, malware, and virus	Unauthorized actions
	AN19	DdoS Attack	Unauthorized actions
	AN20	Saturation of the information system	Technical failures
Data and Information	AN21	Data corrupt	Unauthorized actions
	AN22	Lost of document	Compromise of information
	AN23	Data from untrustworthy sources	Compromise of information
	AN24	Data Modification	Compromise of information
Personnel and Organization	AN25	Human eror	Compromise of functions
	AN26	Illegal of access	Compromise of functions
	AN27	Data entry error	Compromise of functions
	AN28	Breach of personnel availability	Compromise of functions
	AN29	Illegal processing of data	Compromise of functions
	AN30	Undertrained personel	Compromise of functions

natural disasters, with 2 identified threats; (2) environmental/technical failures, with 11 threats; (3) unintentional human actions, with 4 threats; and (4) intentional human actions, with 13 threats.

c. Control identification
After identifying the threats, the next step was to identify the security controls or mechanisms that have been implemented by the Information and Communication Technology Unit (UPT TIK) of Unri to protect assets from various threats. Based on the results of interviews with the head of the IT infrastructure division and a review of documents, the findings are presented in Table 6.
Table 6 presents security controls for addressing potential threats associated with various activities and operations involving the assets managed by the UPT TIK Unri. Control identification is based on information system components, covering hardware, software, network, information, and personnel aspects. One of the controls implemented by UPT TIK is the use of multiple layers of access control, including firewalls and Virtual Private Networks (VPN), to prevent the risk of unauthorized data management. Each component was analyzed to identify potential vulnerabilities and threats it may face, with codes assigned following the threat identification from the previous stage.

d. Vulnerability identification
Following the identification of assets, threats, and security controls, the next step was the identification of vulnerabilities in information security that may be exploited by threats. Vulnerability identification highlights the potential weaknesses that may exist in the organization's assets. Based on document reviews and interviews, the results of the vulnerability identification can be found in Table 7.
Table 7 shows that there were 43 (forty-three) vulnerabilities affecting various assets, with some assets experiencing more than one type of vulnerability. To facilitate the analysis, each vulnerability was assigned a code. There are five assets, including the server, supporting hardware, academic portal application, MySQL (Database Management System), and the operating system, each with five vulnerabilities. Meanwhile, other assets such as the network, data, and human resources have six vul-

Table 6
Existing control identification.

Threat Code	Typical Threats	Existing Controls
AN1	Fire.	Repairs were made, and the server room was relocated to another building.
AN2	Pollution.	Regular cleaning is performed at least once a year.
AN3	Climatic phenomenon.	Installation of grounding and lightning protection system.
AN4	Equipment failure.	Repair or replacement of damaged equipment.
AN5	Theft of equipment.	Placing servers and hardware in a securely locked room.
AN6	Configuration error and server maintenance.	Monitoring is conducted on the server.
AN7	Server down.	Checking and repairing downed servers, as well as rebooting or restarting them.
AN8	Overheating.	Rotation of the server room's air conditioning system is conducted (on/off schedule).
AN9	Loss of power supply.	Utilizing backup power sources such as diesel generators.
AN10	SQL injection.	Data verification is performed against the backup data.
AN11	System crash.	Conducting improvements by revitalizing.
AN12	Sniffing.	The web service already uses Secure Socket Layer (SSL), making it more secure.
AN13	Bruteforce login.	With the presence of a firewall, an attacker's IP will be dropped.
AN14	Error in use.	If an error occurs, the database will be repaired.
AN15	Failure of telecommunication equipment.	A check will be performed on the device or the disconnected network.
AN16	There is disturbance on the gateway.	An investigation into the cause of the disruption will be conducted, followed by corrective action.
AN17	Remote spying.	The attacker's IP address will be checked, followed by network blocking.
AN18	Worm, malware, and virus.	Perform an antivirus scan.
AN19	DdoS attack.	Block the attacker's IP address.
AN20	Saturation of the information system.	Resources are limited, and the technology in use is still patchwork. The procurement of devices or infrastructure upgrades is carried out gradually.
AN21	Data corrupt.	Perform repairs or restore the database.
AN22	Lost of document.	Restore from data backup.
AN23	Data from untrustworthy sources.	Data Recovery.
AN24	Data Modification.	Actively monitor user activities to detect patterns or behaviors that may be suspicious.
AN25	Human eror.	Provide appropriate training to the UPT TIK staff.
AN26	Illegal of access.	Restrict access from external networks or through VPN connections.
AN27	Data entry error.	rovide appropriate training to the UPT TIK staff.
AN28	Breach of personnel availability.	Propose the addition of human resources to the Rectorate of Universitas Riau.
AN1	Fire.	Repairs were made, and the server room was relocated to another building.
AN2	Pollution.	Regular cleaning is performed at least once a year.

nerabilities.

4.2.2. Risk analysis

In the risk analysis process, the likelihood of the identified risks will be assessed by respondents using a questionnaire evaluation.

a. Likelihood
   Likelihood refers to the probability of a risk occurring. The respondents who provided the assessment were the heads of divisions at the IT Service Center (UPT TIK) of Unri, responsible for IT assets and information system security. There were three respondents, such as (1) Head of the IT Infrastructure Division, coded as Res1; (2) Head of the Website & Email Division, coded as Res2; and (2) Head of the IT Products Division, coded as Res3. The results of the questionnaire assessment are shown in Table 8.
b. Impact

Table 7
Vulnerability identification.

Asset Code	Threat Code	Vulnerabilities	ID
A-001	AN 1	Damaged electrical cables and electronic devices.	R1
	AN 3	Inadequate grounding and lightning protection.	R2
	AN 6	Inefficient configuration change control.	R3
	AN 7	Heavy traffic and insufficient server equipment, both in terms of quantity and capacity.	R4
	AN 9	Vulnerability to voltage fluctuations.	R5
A-002	AN 2	Lack of regular hardware maintenance.	R6
	AN 4	Lack of a periodic replacement schedule.	R7
	AN 5	Unprotected storage.	R8
	AN 8	Insufficient attention to room cooling.	R9
	AN25	Lack of knowledge in system usage.	R10
A 003	AN 7	Heavy traffic and inadequate server equipment, both in terms of quantity and capacity.	R11
	AN12	Lack of or absence of encryption on data traffic transmitted over the network.	R12
	AN13	No access restrictions, making it easily accessible to unauthorized parties.	R13
	AN14	Outdated or non-updated software.	R14
	AN 18	Uninstalled or outdated security applications on the server computers.	R15
AN 004	AN 10	User input that is not properly validated or protected.	R16
	AN 12	Lack of or absence of encryption on data traffic transmitted over the network.	R17
	AN 24	Insufficient identification and authentication of the sender and receiver.	R18
	AN 21	Applying application programs to data at incorrect times.	R19
	AN 29	Unnecessary services being activated.	R20
AN 005	AN 11	Poor interoperability between various software components.	R21
	AN 18	The server's security application is not installed.	R22
	AN 19	The server's security application is not updated.	R23
	AN 20	Lack of active monitoring of network traffic.	R24
	AN 25	Insufficient knowledge in system usage.	R25
AN 006	AN 15	Poor network quality.	R26
	AN 16	Unprotected network traffic.	R27
	AN 17	Insecure network architecture.	R28
	AN 18	The server's security application is either not installed or not updated.	R29
	AN 19	Lack of active monitoring of network traffic.	R30
	AN 20	Inadequate network management (routing resilience).	R31
A 007	AN 21	Applying the application program to data with incorrect timing.	R32
	AN 22	Lack of backup copies.	R33
	AN 23	Inability to recover data.	R34
	AN 24	Insufficient identification and authentication of senders and receivers.	R35
	AN 27	Lack of procedures for handling confidential information.	R36
	AN 29	Unnecessary services being activated.	R37
AN 008	AN 25	Insufficient knowledge in system usage.	R38
	AN 26	Lack of formal processes for reviewing access rights (supervision).	R39
	AN 27	Lack of procedures for handling confidential information.	R40
	AN 28	Excessive workload.	R41
	AN 29	Inadequate or absent provisions regarding information security in contracts with employees or staff.	R42
	AN 30	Insufficient training related to information technology.	R43

Impact refers to the degree of consequence if a risk occurs. The results of the distributed questionnaire assessment can be seen in Table 9. The next step was the combination of likelihood and impact values for each potential risk threat, which can be seen in Table 10.

4.2.3. Risk evaluation

Risk evaluation was the final stage in the risk assessment process. The identified and assessed risks were evaluated based on their risk levels using a risk criteria matrix. The results of the risk level mapping using the risk criteria matrix can be seen in Fig. 6. Based on the risk level mapping in Fig. 6, the identified risks were classified according to the obtained risk levels.

The classifications were arranged from the highest to the lowest levels: high, medium, and low, as shown in Table 11. Based on Table 11, the results of the risk evaluation indicate the risk levels associated

Table 8
Likelihood.

Risk ID	Threat Code	Asset Code	Likelihood			Average	Rounding Number
			Res1	Res2	Res3		
R1	A-001	AN1	1	1	1	1.00	1
R2	A-001	AN3	4	3	3	3.33	3
R3	A-001	AN6	3	3	3	3.00	3
R4	A-001	AN7	4	3	4	3.67	4
R5	A-001	AN9	3	3	4	3.33	3
R6	A-002	AN2	2	3	3	2.67	3
R7	A-002	AN4	1	2	1	1.33	1
R8	A-002	AN5	1	1	1	1.00	1
R9	A-002	AN8	1	2	2	1.67	2
…							
…							
R41	A-008	AN28	3	4	4	3.67	4
R42	A-008	AN29	1	1	1	1.00	1
R43	A-008	AN30	2	3	3	2.67	3

Table 9
Impact.

Risk ID	Threat Code	Asset Code	Impact			Average	Rounding Number
			Res1	Res2	Res3		
R1	A-001	AN1	5	5	5	5.00	5
R2	A-001	AN3	3	4	3	3.33	3
R3	A-001	AN6	2	2	3	2.33	2
R4	A-001	AN7	4	4	5	4.33	4
R5	A-001	AN9	4	4	4	4.00	4
R6	A-002	AN2	1	1	1	1.00	1
R7	A-002	AN4	2	3	2	2.33	2
R8	A-002	AN5	2	2	2	2.00	2
R9	A-002	AN8	1	2	2	1.67	2
…							
…							
R41	A-008	AN28	2	2	2	2.00	2
R42	A-008	AN29	2	2	2	2.00	2
R43	A-008	AN30	2	1	1	1.33	1

with each threat and vulnerability for each asset category. The evaluation identified 43 potential risks, with 2 risks classified as high-level, 19 as medium-level, and 22 as low-level. The high-risk category includes two assets and one threat, specifically the server and the academic portal system, with the threat of server downtime.

The medium-risk category encompasses seven assets and fifteen threats, which include risks such as power supply failure, brute-force login attempts, database and application portal errors/bugs, unbacked-up data, lightning strikes, system crashes, information system fatigue, gateway interruptions, data input/deletion errors, data misuse and modification, insufficient human resources, server configuration and maintenance errors, data corruption, document loss, and fire hazards.

Finally, the low-risk category comprises eight assets and fourteen threats, including risks such as overheating, operational errors (human error), DDoS attacks, unauthorized access misuse, dust and debris on hardware, undertrained employees, connectivity issues, eavesdropping (sniffing), SQL injection, worms, malware, and viruses, hardware failure/damage, equipment theft, remote spying, and illegal data processing.

4.3. Risk Treatment

At this stage, actions were selected to address the previously identified, analyzed, and evaluated risks. The risk management process for the UPT TIK Unri Academic Portal was conducted based on the risk assessment results, taking into account recovery costs, risk level, and risk transfer costs (Asriyanik & Prajoko, 2018). The selection of risk management actions includes four treatment options: modifying the

Table 10
Combination of likelihood and impact.

Risk ID	Threat Code	Asset Code	Likelihood	Impact
R1	A-001	AN1	1	5
R2	A-001	AN3	3	3
R3	A-001	AN6	3	2
R4	A-001	AN7	4	4
R5	A-001	AN9	3	4
R6	A-002	AN2	3	1
R7	A-002	AN4	1	2
R8	A-002	AN5	1	2
R9	A-002	AN8	2	2
…				
…				
R41	A-008	AN28	4	2
R42	A-008	AN29	1	2
R43	A-008	AN30	3	1

Impact \ Likelihood	Very unlikely (1)	Unlikely (2)	Possible (3)	Likely (4)	Frequent (5)
Very low (1)			R6, R43		
Low (2)	R7, R20, R28, R37, R42	R9, R10, R23, R25, R26, R30, R38, R39	R3	R41	
Medium (3)	R12, R15, R16, R17, R22, R29	R18, R19, R32, R33, R35	R2, R21, R24, R27, R31, R36, R40		
High (4)			R5, R13, R14, R34	R4, R11	
Very high (5)	R1				

Fig. 6. Risk criteria matrix.

risk (Risk Modification), retaining the risk (Risk Retention), avoiding the risk (Risk Avoidance), and sharing the risk (Risk Sharing). The results of the risk management actions were presented in Table 12.

Based on Table 12, risk management was prioritized according to the level of risk at UPT TIK Unri. Out of the 43 identified vulnerability risks, 21 risks were addressed through risk modification, 4 risks were managed by risk avoidance—including threats like fire and illegal data processing—and 4 risks were addressed by risk sharing, such as DDoS attacks and server downtime, by hiring third-party experts to manage DDoS protection on the server. Fourteen risks were managed through risk retention (accepting the risk), which involves acknowledging the risk without further mitigation. For the 21 risks that undergo risk modification, recommendations for information system security controls were provided in alignment with SNI ISO/IEC 27001:2013.

4.4. Recommendation

At this stage, controls based on ISO/IEC 27001:2013 were provided, referring to a series of recommended actions or steps for UPT TIK Unri to implement to manage information security risks according to the ISO 27001:2013 standard. Several risk recommendations mapped to selected security control domains to address each specific risk are presented in Table 13.

5. Conclusions

Based on the research findings, several key conclusions can be drawn regarding the Unri Academic Portal's information security. First, the risk identification process, utilizing ISO 27005:2018, revealed eight critical information security assets, which include five components of the information system: hardware, software, network, data/information, and personnel. In addition, thirty types of threats were identified that could potentially impact these assets. Second, the vulnerability assessment categorized the information system assets into three levels of risk: low, medium, and high. It was found that each asset could have multiple vulnerabilities, and a single vulnerability type could affect one or more assets. The risk assessment

Table 11
Risk clasification.

Risk ID	Asset Code	Threat Code	Likelihood	Impact	Risk Level
R4	A-001	AN7	4	4	High
R11	A-003	AN7	4	4	High
R5	A-001	AN9	3	4	Medium
R13	A-003	AN13	3	4	Medium
R14	A-003	AN14	3	4	Medium
R34	A-006	A23	3	4	Medium
R2	A-001	AN3	3	3	Medium
R21	A-005	AN11	3	3	Medium
R24	A-005	AN20	3	3	Medium
R27	A-006	AN16	3	3	Medium
R31	A-006	AN20	3	3	Medium
R36	A-007	AN27	3	3	Medium
R40	A-008	AN27	3	3	Medium
R41	A-008	AN28	4	2	Medium
R3	A-001	AN6	3	2	Medium
R18	A-004	AN24	2	3	Medium
R19	A-004	AN21	2	3	Medium
R32	A-007	AN21	2	3	Medium
R33	A-007	AN22	2	3	Medium
R35	A-007	AN24	2	3	Medium
R1	A-001	AN1	1	5	Medium
R9	A-002	AN8	2	2	Low
R10	A-002	AN25	2	2	Low
R23	A-005	AN19	2	2	Low
R25	A-005	AN25	2	2	Low
R26	A-006	AN15	2	2	Low
R30	A-006	AN19	2	2	Low
R38	A-008	AN25	2	2	Low
R39	A-008	AN26	2	2	Low
R6	A-001	AN2	3	1	Low
R43	A-008	AN30	3	1	Low
R12	A-003	AN12	1	3	Low
R15	A-003	AN18	1	3	Low
R16	A-004	AN10	1	3	Low
R17	A-004	AN12	1	3	Low
R22	A-005	AN18	1	3	Low
R29	A-006	AN18	1	3	Low
R7	A-001	AN4	1	2	Low
R8	A-001	AN5	1	2	Low
R20	A-004	AN29	1	2	Low
R28	A-006	AN17	1	2	Low
R37	A-007	AN29	1	2	Low
R42	A-008	AN29	1	2	Low

revealed a total of 43 potential risks, with 2 classified as high-level, 19 as medium-level, and 22 as low-level. This suggests that the infrastructure assets at UPT TIK Unri are generally at a lower risk of vulnerability. Lastly, the analysis of these risks resulted in specific risk management strategies: 21 risks were mitigated through risk modification, 4 through risk avoidance, and 4 through risk sharing. Recommendations for managing risks through risk modification are based on ISO/IEC 27001:2013 security control guidelines. These recommendations cover areas such as information security management, human resource security, asset management, access control, physical and environmental security, and operational security.

6. CRediT Authorship Contribution Statement

Sonya Meitarice: Conceptualization, Supervision, Data curation, Methodologhy, Formal Analysis, and Writing–review & editing. **Lydia Febyana:** Writing–original draft, Resources **Aidil Fitriansyah:** Visualization, Project administration. **Riki Ario Nugroho:** Funding acquisition, Investigation. **Rahmad Kurniawan:** Validation.

Table 12
Risk treatment.

Risk ID	Threat Code	Risk Level	Recovery Cost	Risk Treatment
R4	AN7	High	High	Risk Sharing
R11	AN7	High	High	Risk Sharing
R5	AN9	Medium	Medium	Risk Modification
R13	AN13	Medium	Low	Risk Modification
R14	AN14	Medium	Medium	Risk Modification
R34	A23	Medium	Medium	Risk Modification
R2	AN3	Medium	Medium	Risk Modification
R21	AN11	Medium	Low	Risk Modification
R24	AN20	Medium	Low	Risk Modification
R27	AN16	Medium	Low	Risk Modification
R31	AN20	Medium	Low	Risk Modification
R36	AN27	Medium	Low	Risk Modification
R40	AN27	Medium	Low	Risk Modification
R41	AN28	Medium	Medium	Risk Modification
R3	AN6	Medium	Low	Risk Modification
R18	AN24	Medium	Medium	Risk Modification
R19	AN21	Medium	Medium	Risk Modification
R32	AN21	Medium	Medium	Risk Modification
R33	AN22	Medium	Medium	Risk Modification
R35	AN24	Medium	Medium	Risk Modification
R1	AN1	Medium	High	Risk Avoidance
R9	AN8	Low	Low	Risk Retention
R10	AN25	Low	Low	Risk Retention
R23	AN19	Low	High	Risk Sharing
R25	AN25	Low	Low	Risk Retention
R26	AN15	Low	Low	Risk Retention
R30	AN19	Low	High	Risk Sharing
R38	AN25	Low	Low	Risk Retention
R39	AN26	Low	Low	Risk Retention
R6	AN2	Low	Low	Risk Retention
R43	AN30	Low	Low	Risk Retention
R12	AN12	Low	Low	Risk Retention
R15	AN18	Low	Medium	Risk Modification
R16	AN10	Low	Low	Risk Retention
R17	AN12	Low	Low	Risk Retention
R22	AN18	Low	Medium	Risk Modification
R29	AN18	Low	Medium	Risk Modification
R7	AN4	Low	Low	Risk Retention
R8	AN5	Low	Low	Risk Retention
R20	AN29	Low	High	Risk Avoidance
R28	AN17	Low	Low	Risk Retention
R37	AN29	Low	High	Risk Avoidance
R42	AN29	Low	High	Risk Avoidance

Table 13
Recommendation.

Risk	Risk Control	Control Code
Server Down	**Operational Security**	A.12
	Change Management: Changes in organizational structure, business processes, information processing facilities, and systems impacting information security must be controlled.	A.12.1.2
	Capacity Management: Resource utilization must be monitored, managed, and projected to ensure system performance meets future demands.	A.12.1.3
	Technical Vulnerability Management	A.12.6
	Technical Vulnerability Management: Information regarding the technical vulnerabilities of the information system must be obtained in a timely manner, the organization's exposure to these vulnerabilities assessed, and appropriate actions taken to address associated risks.	A.12.6.1

(continued on next page)

Table 13. *(continued)*

Risk	Risk Control	Control Code
Power Supply Failure	Equipment Security	A.11.2
	Supporting Utilities: Equipment must be protected from power supply failures and other disruptions due to utility failures.	A.11.2.2
Brute-force Login	User Responsibilities	A.9.3
	Use of Secret Authentication Information: Users must adhere to organizational practices in using secret authentication information.	A.9.3.1
	System and Application Access Control	A.9.4
	Secure Log-on Procedures: Access to systems and applications must be controlled by secure log-on procedures, as required by the access control policy.	A.9.4.2
	Password Management System: The password management system must be interactive and ensure password quality.	A.9.4.3
Application Errors	Technical Vulnerability Management	A.12.6
	Technical Vulnerability Management: Timely information regarding technical vulnerabilities of the information system must be acquired, organizational exposure evaluated, and appropriate actions taken to mitigate associated risks.	A.12.6.1
Unbacked-up Data	Backup (Data)	A.12.3
	Information Backup: Backups of information, software, and system images must be taken and regularly tested in accordance with approved backup policies.	A.12.3.1
Lightning	Physical and Environmental Security	A.11
	Physical Perimeter Security: Physical security perimeters must be established to protect sensitive or critical information processing facilities.	A.11.1.2
	Placement and Protection of Equipment: Equipment must be placed and protected to reduce risks from environmental threats and unauthorized access.	A.11.2.1
	Cable Security: Power and telecommunication cables carrying data or supporting information services must be protected from interception, interference, or damage.	A.11.2.3
System Crash	Operational Security	A.12
	Change Management: Changes to organizational structures, business processes, information processing facilities, and systems affecting information security must be controlled.	A.12.1.2
	Security in Development and Support Process	A.14.2
	System Change Control Procedures: Changes to systems within the development lifecycle must be controlled using standardized change control procedures.	A.14.2.2
Information System Fatigue	Security in Development and Support Process	A.14.2
	Secure Development Policy: Rules for software and system development within the organization must be established and implemented.	A.14.2.1
Gateway Disruption	Network Security Management	A.13.1
	Network Controls: Networks must be managed and controlled to safeguard information in systems and applications.	A.13.1.1
	Information Transfer Procedures and Policies: Policies, procedures, and formal controls must be in place to protect information transfer across all communication channels.	A.13.2.1
Data Input/Deletion Errors	Human Resource Security	A.7
	Management Responsibility: Management must require all employees and contractors to implement information security based on established organizational policies and procedures.	A.7.2.1
Insufficient HR	Information Security Organization	A.6
	Roles and Responsibilities in Information Security: All information security responsibilities must be defined and allocated.	A.6.1.1
	Human Resource Security	A.7
	Employment Terms and Conditions: Written agreements with employees and contractors must state their information security responsibilities and organizational expectations.	A.7.1.2
	Awareness, Education, and Training: All employees and contractors (where applicable) should receive regular awareness, education, and training on organizational policies and procedures relevant to their job functions.	A.7.2.2
Server	During Employment	A.7.2

(continued on next page)

Table 13. *(continued)*

Risk	Risk Control	Control Code
Configuration and Maintenance Errors	**Management Responsibility:** Management must require all employees and contractors to implement information security following established organizational policies and procedures.	A.7.2.1
Data Corrupt, Document Loss	**Physical and Environmental Security**	A.11
	Placement and Protection of Equipment: Equipment must be placed and protected to reduce risks from environmental threats and unauthorized access.	A.11.2.1
Worms, Malware, Viruses	**Protection from Malware**	A.12.2
	Malware Control: Detection, prevention, and recovery controls must be implemented to protect against malware, combined with appropriate user awareness.	A.12.2.1
Hardware Failure/Damage	**Physical and Environmental Security**	A.11
	Equipment Maintenance: Equipment must be properly maintained to ensure continuous availability and integrity.	A.11.2.4
	Asset Management	A.8
	Asset Inventory: Assets associated with information and information processing facilities must be identified, and an inventory of these assets must be recorded and maintained.	A.8.1.1
	Asset Handling Procedures: Procedures must be developed and implemented to manage assets according to the organization's adopted information classification scheme.	A.8.2.3
Data Misuse and Modification	**Access Control**	A.9
	Access Control Policy: An access control policy must be established, documented, and reviewed based on business and information security requirements.	A.9.1.1
	Privileged Access Rights Management: Allocation and use of privileged access rights must be restricted and controlled.	A.9.2.3
	Secret Authentication Information Management: Allocation of secret authentication information must be controlled through a formal management process.	A.9.2.4
	Use of Secret Authentication Information: Users must adhere to organizational practices in using secret authentication information.	A.9.3.1
	Information Access Restriction: Access to information and system application functions must be limited according to access control policies.	A.9.4.1

7. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

8. Funding

This research is funded by Universitas Riau, Faculty of Mathematics and Natural Sciences (FMIPA), Indonesia, through Non-Tax State Revenue (PNBP) FMIPA Universitas Riau 2024, Grant Number 1563/UN19.5.1.1.3/AL.04/2024.

9. References

Amirinnisa, M., & Bisma, R. (2023). Analysis of Information Security Risk Assessment Based on Iso 27005 for Preparation for Iso 27001 Certification in The Government of Madiun City. *Journal of Emerging Information Systems and Business Intelligence, 4*(4), 47-58. Retrieved from https://ejournal.unesa.ac.id/index.php/JEISBI/article/view/56250

Appiah-Otoo, I., & Song, N. (2021). The impact of ICT on economic growth-Comparing rich and poor countries. *Telecommunications Policy, 45*(2). doi:https://doi.org/10.1016/j.telpol.2020.102082

Asriyanik, A., & Prajoko, P. (2018). Manajemen Risiko Keamanan Informasi Menggunakan ISO 27005:2011 pada Sistem Informasi Akademik (SIAK) Universitas Muhammadiyah Sukabumi (UMMI). *JuTISI (Jurnal Teknik Informatika dan Sistem Informasi), 4*(2), 319 – 329. Retrieved from https://journal.maranatha.edu/index.php/jutisi/article/view/1499

Dioubate, B. M., Daud, W., & Norhayate, W. (2022). Cyber Security Risk Management Frameworks Implementation in Malaysian Higher Education Institutions. *International journal of academic research in business and social sciences, 12*(4), 1356–1371. doi:https://doi.org/10.6007/IJARBSS/v12-i4/12300

Fahrurozi, M., Tarigan, S. A., Tanjung, M. A., & Mutijarsa, K. (2020). The Use of ISO/IEC 27005: 2018 for Strengthening Information Security Management (A Case Study at Data and Information Center of Ministry of Defence). *2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE). 12.* Yogyakarta, Indonesia: IEEE. doi:https://doi.org/10.1109/ICITEE49829.2020.9271748

Ibrahim, H. I., Mohamad, W. M., & Shah, K. A. (2020). Investigating Information and Communication Technology (ICT) Usage, Knowledge Sharing and Innovative Behavior among Engineers in Electrical and Electronic MNCs in Malaysia. *Jurnal pengurusan, 58*, 133 – 143. Retrieved from https://www.ukm.my/jurnalpengurusan/wp-content/uploads/2022/10/jp_58-11.pdf

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.* Retrieved from ISO - International Organization for Standardization: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1

International Organization for Standardization. (2018). *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management.* Retrieved from ISO - International Organization for Standardization: https://www.iso.org/standard/75281.html

Isnaini, K., Sari, G. J., & Kuncoro, A. P. (2023). Analisis Risiko Keamanan Informasi Menggunakan ISO 27005:2019 pada Aplikasi Sistem Pelayanan Desa. *Jurnal Eksplora Informatika, 13*(1), 37-45. doi:https://doi.org/10.30864/eksplora.v13i1.696

Jorgenson, D. W., & Vu, K. M. (2016). The ICT revolution, world economic growth, and policy issues. *Telecommunications Policy, 40*(5), 383-397. doi:https://doi.org/10.1016/j.telpol.2016.01.002

Kaur, K., Gupta, I., & Singh, A. K. (2017). Data Leakage Prevention: E-Mail Protection via Gateway. *Journal of Physics: Conference Series, 933*. doi:https://doi.org/10.1088/1742-6596/933/1/012013

Klipper, S. (2011). *Information Security Risk Management: Risikomanagement mit ISO/IEC 27001, 27005 und 31010.* Wiesbaden, Germany: Vieweg+Teubner Verlag. doi:https://doi.org/10.1007/978-3-8348-9870-8_3

Leasa, Z. V., & Prassida, G. F. (2024). Manajemen Risiko pada Sistem Informasi Akademik Universitas XYZ menggunakan ISO 27005:2018. *Jurnal Teknologi Dan Sistem Informasi Bisnis, 6*(4), 649-656. doi:https://doi.org/10.47233/jteksis.v6i4.1459

Rambe, R., Gandhi, A., & Sabariah, M. K. (2023). Implementasi Manajemen Risiko pada Aplikasi XYZ dengan Pendekatan SNI ISO/IEC 27005:2018. *Proceedings of Engineering. 10*, pp. 3903-3909. Bandung, Indonesia: Universitas Telkom. Retrieved from https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/20846

Sahira, S., Fauzi, R., & Santosa, I. (2020). Analysis of Risk Management in E-Office Application Managed by PT. Telkom Indonesia Using ISO/IEC 27005:2018 Standard. *Proceedings of Engineering. 7*, pp. 6897-6909. Bandung, Indonesia: Universitas Telkom. Retrieved from https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/12642

Sharif, M. H., & Mohammed, M. A. (2022). A literature review of financial losses statistics for cyber security and future trend. *World Journal Of Advanced Research and Reviews, 15*(1), 138–156. doi:https://doi.org/10.30574/wjarr.2022.15.1.0573

Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security.* Cengage Learning. Retrieved from https://www.cengageasia.com/title/default/detail?isbn=9781337102063

Yustanti, W., Qoiriah, A., Bisma, R., & Prihanto, A. (2019). Strategi Identifikasi Resiko Keamanan Informasi Dengan Kerangka Kerja ISO 27005:2018. *JIEET (Journal of Information Engineering and Educational Technology), 3*(2), 51-56. doi:https://doi.org/10.26740/jieet.v3n2.p51-56