Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849
e-ISSN: 2548-1398
Vol. 7, No. 11, November 2022

Analysis of Risk Management Information System Applications Using Iso/Iec 27001:2022

Kanka Wiemas N. G.[1], Jarot S. Suroso[2]
Bina Nusantara University, Information System Management Department, BINUS Graduate Program, Master of Information Systems Management, Jakarta, Indonesia.
Email: kanka.ghiffari@binus.ac.id[1*], jsembodo@binus.edu[2]

Abstract

The rapid development of information technology can make it easier for anyone to obtain, process, and disseminate various information systems. Information system security is an important aspect in maintaining information confidentiality. One way to maintain the security of information systems is by conducting risk management. The goal of risk management is to control and lessen the likelihood of risks that could jeopardize information system security. This research aims to carry out a risk management process in one of the government agencies in Indonesia by controlling mitigation that refers to ISO / IEC 27001: 2022. Data collection in this study was carried out by means of observation, interviews, and Forum Group Discussion (FGD). The results of this study were the discovery of 15 risks, 50 risk threats, and 15 impacts caused by the risk. This research resulted in 42% of the risks falling into a moderate impact.

Keywords: Information System; Information System Security; Risk; Risk Management; ISO/IEC 27001:2022.

Introduction

Information technology has a significant impact on every aspect of life in the 4.0 era, including government, education, health, and the economy. It is because almost every activity today relies heavily on information technology. Humans can create, process, distribute, and retrieve information more efficiently because of information technology. Information should be very easy to obtain, process, and distribute for everyone given the speed at which information technology develops. For this reason, all parties need to maintain the confidentiality of information security. The term "information security" refers to a group of policies and tools that businesses and other organizations use to protect their personal information from unauthorized access, alteration, disruption, and destruction by careless individuals.

There was malicious code and viruses infected 55.51% of computers during 2016 and are likely to be a risk for many organizations. A risk caused by human error compromising the information security of an organization can be reduced with the help of an ideal or strong information security culture, which in turn can limit incidents or data breaches. One of the most important aspects of the perfect information security culture is an informed and aware workforce that demonstrates diligent and considerate behaviour to adhere to management-directed policies.

How to cite:	Kanka Wiemas N. G., Jarot S. Suroso (2022) Analysis of Risk Management Information System Applications Using Iso/Iec 27001:2022, *(7) 11.*.
E-ISSN:	2548-1398
Published by:	Ridwan Institute

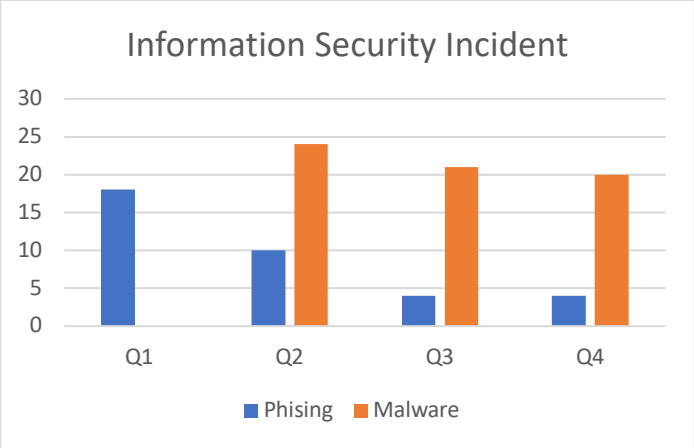


Figure 1. Information Security Incident at XYZ Directorate in 2022

Threats to an information system can threaten anyone and anywhere, including threatening government agencies in Indonesia. The ABC Ministry, especially in the XYZ directorate, is one of the government agencies in Indonesia which during 2022 had at least 65 hostnames used in their business processes indicated by malware. Malicious software (Malware) is any software that maliciously attacks other software, where an observable attack means causing behavior that is actually different from the intended behavior. Malware is constantly growing at a startling rate. Malware is constantly growing at a startling rate. Certain malwares have the ability to conceal themselves inside the system through various means.

In the same year, the XYZ directorate also identified a ransomware attack. The most dangerous cyberattack in the world is ransomware. Ransomware locks devices used by users screens or encrypts their files to prevent users from accessing their devices. Until ransomware is paid, the user's file is encrypted. Even after it is removed, the impact of this kind of cyberattack is hard to reverse without the perpetrator's assistance. A total of 36 ransomware attacks hit the XYZ directorate. The attack is the trigona variant of ransomware. Trigona is a ransomware attack that encrypts files and adds the "._locked" extension to the file name. Then, the irresponsible party also usually includes a "how_to_decrypt.hta" file that contains a ransom note.

In maintaining information security, an organization performs a process commonly referred to as risk management. The term "risk management" refers to a coordinated set of actions used to guide and govern an organization regarding risk. An organization faces risks in all its operations. To manage risks, an organization must first identify them, analyze them, and determine whether risk treatment is necessary to meet the organization's risk criteria.

Based on the problems that exist in the background above, the researcher initiated a study on risk management on the application system used in the XYZ directorate. The goal of this study is to implement risk management procedures, starting from risk identification, risk analysis, risk evaluation, and providing recommendations for information system security controls referring to ISO/IEC 27001: 2022.

Research Methods

This study is a qualitative type of research. The data collected was done by observation and interview. Researchers conducted interviews with PICs in 5 sub-directorates under the IT team of the XYZ directorate. This research was conducted from

September 2023 - February 2024. The location of this research was carried out at the XYZ Directorate, Ministry of ABC.

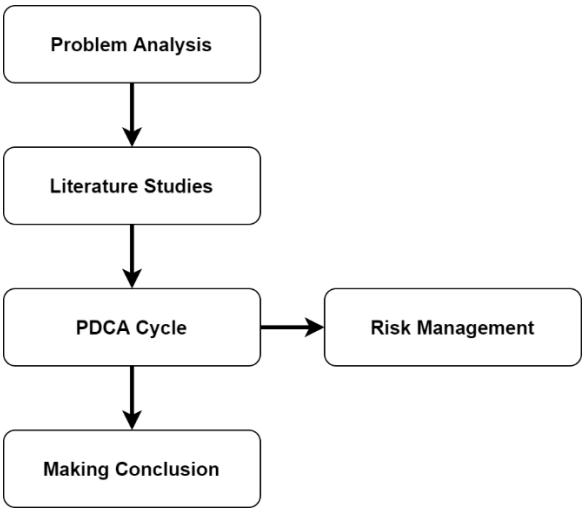


Figure 2: Research Stage

Based on figure 2, the first research stage is the problem analysis stage. At this stage, researchers conducted interviews with relevant sources regarding the problems that exist in the XYZ directorate. From the results of these interviews, it is known that at least 65 hostnames were used in the business operations of the XYZ directorate in 2022, as indicated by the malware. The XYZ directorate also encountered a ransomware attack that year. Directorate XYZ was the target of a total of 36 ransomware attacks. The ransomware used in the attacks was the trigona variant.

Then, the second research stage is a literature study. At this stage, researchers searched for theories related to this research. Then, in order to find references and learn what could be learned, researchers searched through journals and completed risk management-related works. The third stage of this research is the stage where researchers carry out PDCA cycle activities related to risk management. This PDCA cycle can be described as:

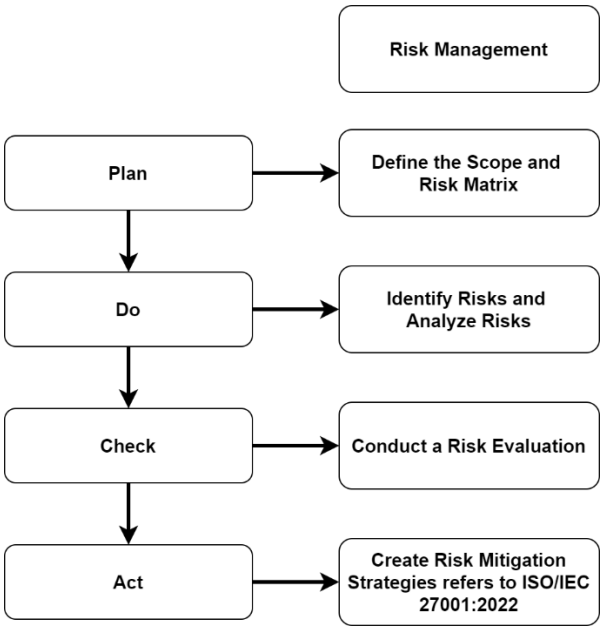


Figure 3. PDCA Cycle

Then the last stage is the stage of making conclusions. At this stage, a conclusion is made on the research that has been carried out by the researcher. The result of this research will be given to the campus and the XYZ Directorate

Results And Discussion

Define Risk Matrix

In this study, researchers used a 5x5 risk matrix that refers to previous research conducted by [25]. Based on table 2, this risk matrix has 5 levels of impact (very low, low, medium, large, and very large) resulting from the risks that arise at the XYZ Directorate. Then, this matrix also contains 5 levels of possibility (very rarely occurs, rarely occurs, occasionally, often occurs, and very often happens) of the emergence of a risk at the XYZ Directorate.

The risk likelihood level is divided into 5 levels. The Decree of the Minister of ABC of the Republic of Indonesia Number 105/KMK.01/2022 concerning Guidelines for the Implementation of Risk Management of the Ministry of ABC is the basis for these five possible outcomes. In determining the level of possibility, a qualitative and quantitative approach is used based on observational data on risk events, risk causes and involves the judgment of the head of the Risk Owner Unit (UPR) based on experience and careful consideration.

Table 1. The Criteria of Vulnerability Level

Vulnerability Level	Number of Frequency
Very Rarely Occurs 1	< 2 times in the last 12 months
Rarely Occurs 2	2 times - 5 times in the last 12 months
Occasionally 3	6 times - 9 times in the last 12 months
Often Occurs	10 times - 12 times in the last 12 months
Very Often Occurs	> 12 times in the last 12 months

Based on table 1, the level of impact of risk occurrence is divided into 5 levels. These five levels of impact are based on the Decree of the Minister of ABC of the Republic of Indonesia Number 105/KMK.01/2022 concerning Guidelines for the Implementation of Risk Management of the Ministry of ABC.

Table 2. The Criteria of Impact Level

Impact Level	Impact Area		
	Fraud	Operational	Reputation
Very Low	Rp1 - Rp10 Million	< 25% of daily service operating hours	1) The number of complaints verbally (can be documented) / written to the organization amounts to 1 - 10 complaints 2) The level of stakeholder / investor trust is very good 3) The level of satisfaction of service users is 4.25 to 5 (scale 5)

Low	Rp10 Million - Rp100 Million	25% - 49% of daily service operating hours	1) The number of grievances verbally (can be documented) / written to the organization amounts to >10 grievances 2) The level of stakeholder / investor trust is good 3) Service user satisfaction level of 4 to 4.24 (scale 5)
Medium	Rp100 Million - Rp1 Billion	50% - 74% of daily service operating hours	1) Massive negative coverage on social media sourced from non-opinion leaders 2) Negative coverage in local mass media 3) Moderate level of stakeholder / investor confidence 4) Service user satisfaction level of 3.75 to 3.99 (scale 5)
High	Rp1 Billion - Rp10 Billion	75% - 89% of daily service operating hours	1) Massive negative coverage on social media sourced from opinion leaders 2) Negative coverage in national mass media 3) Low level of stakeholder / investor confidence 4) Service user satisfaction level of 3.5 to 3.74 (scale 5)
Very High	> Rp10 Billion	> 89%% of daily service operating hours	1) Negative coverage in international mass media 2) Very low level of stakeholder / investor confidence 3) Service user satisfaction level of < 3.5 (scale 5)

In determining the level of possibility, a qualitative and quantitative approach is used based on observational data on risk events, risk causes and involves the consideration of the Risk Owner Unit (UPR) leadership based on experience and careful consideration. Based on table 4, the impact area caused by the risk is divided into 3 areas. Each impact area has 5 levels of impact based on agreed criteria.

At this stage, the XYZ directorate handled the risk identification procedure. Researchers identify the risk ID, risk description, risk threat, impact that the risk will cause, and the risk's category during the risk identification stage. Researchers obtained up to 15 identified risks, 15 different types of impacts resulting from the emergence of risks, and three different types of risk categories from the results of this risk identification process.

In this process, the risk analysis is carried out at the XYZ Directorate. At the risk analysis stage, researchers analyzed the determination of the level of likelihood of a risk and its explanation. Then, researchers also analyzed the level of impact caused by the existence of a risk along with its explanation. Then, the researchers also determined the value of the risk magnitude caused by the emergence of risks at the XYZ Directorate. The risk magnitude is obtained from the results of cross-multiplication in the risk matrix between the likelihood level and the impact level.

After obtaining the results of the risk analysis, the division of the impact area category is carried out based on the risk level that has been obtained. Referring to the risk matrix, the risk level is obtained from the result of multiplying the likelihood level multiplied by the impact level. Based on the risk matrix that has been used, it can be seen that each level of risk has a category based on the impact area, such as:

Risk level 1 - 2 = very low, Risk level 3-6 = low, Risk level 8 - 12 = medium, Risk level 15 - 16 = high, Risk level 20-25 = very large

Then, after categorizing the impact area, calculations can be made to determine the percentage of the number of each impact area that has been found, namely:

Very low impact area = 0, Low impact area = 19, Medium impact area = 21, High impact area = 10, Very high impact area = 0

In calculating the percentage of the amount of each risk level, researchers used the following formula:

$$\frac{Number\ of\ risk\ level\ findings}{Total\ sum\ of\ all\ risk\ levels}\ \mathbf{x\ 100\%}$$

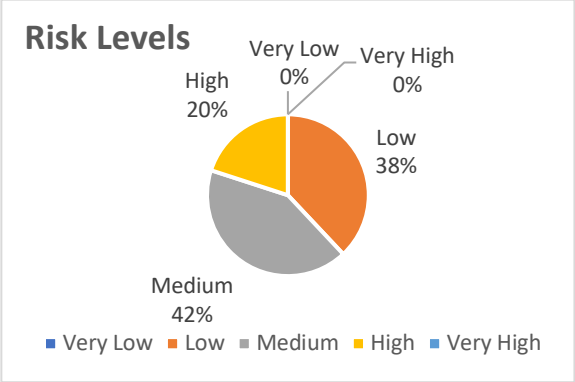


Figure 4. Percentage Total Risk Level

Based on Figure 4, the percentage of each risk level can be calculated as follows:

1. Very low risk level: 0/50 x 100% = 0%
2. Low risk level: 19/50 x 100% = 38%
3. Medium risk level: 21/50 x 100% = 42%
4. High risk level: 10/50 x 100% = 20%
5. Very high risk level: 0/50 x 100% = 0%

In the process of risk identification and risk analysis, researchers have found many risks along with threats, impacts, likelihood levels, impact levels, and the risk level itself. In this process, researchers conducted a process that aims to determine what mitigation is needed from each risk, the necessary control system, and also provide residual risk expectations. In determining risk mitigation, researchers refer to the theory from [15] which categorizes risk mitigation into:

Reduce, This mitigation reduces or mitigates the risk by utilizing various controls. Transfer, The company can transfer the risk to another party. Acceptance, The organization can take the identified risk. Avoidance, Avoiding a risk means choosing not to take it.

Mapping ISO/IEC 27001:2022 Control

After the researchers conducted a risk evaluation, in this process the researchers determined or mapped the risk controls used against the risk control system strategy. The controls used are controls in ISO / IEC 27001: 2022 with the following description:

Table 3. Mapping ISO/IEC 27001:2022

Risk ID	Risk	Mitigation Decisions	ISO 27001:2022 Control

1.1	Low knowledge of information security among employees	Reduce	5.1 The information security policy 5.2 Aspects of information security roles and duties 5.3 Division of labour 5.4 Accountability for management 5.24 Information security incident management planning and preparation 6.8 Information security incident reporting 8.7 Malware protection 8.12 Preventing information leaks 8.19 Software installation on operating systems
1.2	Low knowledge of information security among employees	Reduce	5.1 The information security policy 5.2 Aspects of information security roles and duties 5.3 Division of labour 5.4 Accountability for management 5.24 Information security incident management planning and preparation 6.8 Information security incident reporting 8.7 Malware protection 8.12 Preventing information leaks 8.19 Software installation on operating systems
1.3	Low knowledge of information security among employees	Reduce	5.1 The information security policy 5.2 Aspects of information security roles and duties 5.3 Division of labour 5.4 Accountability for management 5.24 Information security incident management planning and preparation 6.8 Information security incident reporting 8.7 Malware protection 8.12 Preventing information leaks 8.19 Software installation on operating systems
2.1	Internal Compliance Task Implementation Evaluation Score Below Target	Reduce	5.1 Policy for Information Security 5.2 Positions and duties in information security 5.3 Distinctive Task Assignment 5.4 The duty of management 5.21 Information and communication technology (ICT) supply chain management of information security 5.24. Information security incident preparation and management 5.30 Business continuity through ICT preparedness 6.3 Awareness, instruction, and training related to information security

2.2	Internal Compliance Task Implementation Evaluation Score Below Target	Reduce	5.1 Policy for Information Security 5.2 Positions and duties in information security 5.3 Distinctive Task Assignment 5.4 The duty of management 5.21 Information and communication technology (ICT) supply chain management of information security 5.24. Information security incident preparation and management 5.30 Business continuity through ICT preparedness 6.3 Awareness, instruction, and training related to information security
2.3	Internal Compliance Task Implementation Evaluation Score Below Target	Reduce	5.1 Policy for Information Security 5.2 Positions and duties in information security 5.3 Distinctive Task Assignment 5.4 The duty of management 5.21 Information and communication technology (ICT) supply chain management of information security 5.24. Information security incident preparation and management 5.30 Business continuity through ICT preparedness 6.3 Awareness, instruction, and training related to information security
3.1	Digitalization of State Financial Management Not on Target	Reduce	5.1 The policy regarding information security 5.2 Positions and duties in information security 5.4 Accountabilities in management 5.8 Data protection in project administration
3.2	Digitalization of State Financial Management Not on Target	Reduce	5.1 The policy regarding information security 5.2 Positions and duties in information security 5.4 Accountabilities in management 5.8 Data protection in project administration
4.1	Directorate XYZ's Open Data Implementation Not Implemented	Acceptance	5.2: Aspects of information security roles and duties 5.4: Accountabilities in management 5.5: Interaction with the government 5.21: Information security management in the supply chain for information and communication technology (ICT)
4.2	Directorate XYZ's Open Data Implementation Not Implemented	Acceptance	5.2: Aspects of information security roles and duties 5.4: Accountabilities in management 5.5: Interaction with the government 5.21: Information security management in the supply chain for information and communication technology (ICT)

4.3	Directorate XYZ's Open Data Implementation Not Implemented	Acceptance	5.2: Aspects of information security roles and duties 5.4: Accountabilities in management 5.5: Interaction with the government 5.21: Information security management in the supply chain for information and communication technology (ICT)
5.1	Treasury Main System Service Application cannot be accessed	Acceptance	5.5 Interactions with law enforcement 5.6 Interactions with interest-based organizations 5.9 List of pertinent data and resources 5.24 Planning and preparation for information security incident management 5.29 Data protection in the face of interruptions 5.30 IT preparedness for ongoing business operations 7. 13 Upkeep of equipment 8.19 Software installation on live systems 8.20 Security of networks
5.2	Treasury Main System Service Application cannot be accessed	Acceptance	5.5 Interactions with law enforcement 5.6 Interactions with interest-based organizations 5.9 List of pertinent data and resources 5.24 Planning and preparation for information security incident management 5.29 Data protection in the face of interruptions 5.30 IT preparedness for ongoing business operations 7. 13 Upkeep of equipment 8.19 Software installation on live systems 8.20 Security of networks
5.3	Treasury Main System Service Application cannot be accessed	Acceptance	5.5 Interactions with law enforcement 5.6 Interactions with interest-based organizations 5.9 List of pertinent data and resources 5.24 Planning and preparation for information security incident management 5.29 Data protection in the face of interruptions 5.30 IT preparedness for ongoing business operations 7. 13 Upkeep of equipment 8.19 Software installation on live systems 8.20 Security of networks

5.4	Treasury Main System Service Application cannot be accessed	Acceptance	5.5 Interactions with law enforcement 5.6 Interactions with interest-based organizations 5.9 List of pertinent data and resources 5.24 Planning and preparation for information security incident management 5.29 Data protection in the face of interruptions 5.30 IT preparedness for ongoing business operations 7. 13 Upkeep of equipment 8.19 Software installation on live systems 8.20 Security of networks
5.5	Treasury Main System Service Application cannot be accessed	Acceptance	5.5 Interactions with law enforcement 5.6 Interactions with interest-based organizations 5.9 List of pertinent data and resources 5.24 Planning and preparation for information security incident management 5.29 Data protection in the face of interruptions 5.30 IT preparedness for ongoing business operations 7. 13 Upkeep of equipment 8.19 Software installation on live systems 8.20 Security of networks
6.1	Operationalization and development of an obstructed Finance Application System	Acceptance	5.2 Aspects of information security roles and duties 5.4 Accountabilities for management 5.5 Interaction with law enforcement 5.6 Interaction with interest-based organizations 5.21 Information security management in the supply chain for information and communication technology (ICT) 5.30 IT preparedness for ongoing business operations 6.3 Knowledge, instruction, and training in information security 6.7 Functioning from a distance 7.1 The perimeter of physical security
6.2	Operationalization and development of an obstructed Finance Application System	Acceptance	5.2 Aspects of information security roles and duties 5.4 Accountabilities for management 5.5 Interaction with law enforcement 5.6 Interaction with interest-based organizations 5.21 Information security management in the supply chain for information and communication technology (ICT) 5.30 IT preparedness for ongoing business operations 6.3 Knowledge, instruction, and training in information security 6.7 Functioning from a distance 7.1 The perimeter of physical security

6.3	Operationalization and development of an obstructed Finance Application System	Acceptance	5.2 Aspects of information security roles and duties 5.4 Accountabilities for management 5.5 Interaction with law enforcement 5.6 Interaction with interest-based organizations 5.21 Information security management in the supply chain for information and communication technology (ICT) 5.30 IT preparedness for ongoing business operations 6.3 Knowledge, instruction, and training in information security 6.7 Functioning from a distance 7.1 The perimeter of physical security
6.4	Operationalization and development of an obstructed Finance Application System	Acceptance	5.2 Aspects of information security roles and duties 5.4 Accountabilities for management 5.5 Interaction with law enforcement 5.6 Interaction with interest-based organizations 5.21 Information security management in the supply chain for information and communication technology (ICT) 5.30 IT preparedness for ongoing business operations 6.3 Knowledge, instruction, and training in information security 6.7 Functioning from a distance 7.1 The perimeter of physical security
6.5	Operationalization and development of an obstructed Finance Application System	Acceptance	5.2 Aspects of information security roles and duties 5.4 Accountabilities for management 5.5 Interaction with law enforcement 5.6 Interaction with interest-based organizations 5.21 Information security management in the supply chain for information and communication technology (ICT) 5.30 IT preparedness for ongoing business operations 6.3 Knowledge, instruction, and training in information security 6.7 Functioning from a distance 7.1 The perimeter of physical security
7.1	Directorate XYZ ICT Blueprint Update Failed	Acceptance	5.1 The policy regarding information security 5.2 Aspects of information security roles and duties 5.4 Accountabilities in management 5.21 Information and communication technology (ICT) supply chain management of information security 5.36 Compliance to guidelines, policies, and standards for information security

7.2	Directorate XYZ ICT Blueprint Update Failed	Acceptance	5.1 The policy regarding information security 5.2 Aspects of information security roles and duties 5.4 Accountabilities in management 5.21 Information and communication technology (ICT) supply chain management of information security 5.36 Respect for rules, regulations, and information security standards
7.3	Directorate XYZ ICT Blueprint Update Failed	Acceptance	5.1 The policy regarding information security 5.2 Aspects of information security roles and duties 5.4 Accountabilities in management 5.21 Information and communication technology (ICT) supply chain management of information security 5.36 Respect for rules, regulations, and information security standards
8.1	Preparation of Treasury and Budget System Development Study Not on Target	Acceptance	5.1 The policy regarding information security 5.2 Aspects of information security roles and duties 5.4 Accountabilities in management 5.21 Information and communication technology (ICT) supply chain management of information security 5.36 Respect for rules, regulations, and information security standards
8.2	Preparation of Treasury and Budget System Development Study Not on Target	Acceptance	5.1 The policy regarding information security 5.2 Aspects of information security roles and duties 5.4 Accountabilities in management 5.21 Information and communication technology (ICT) supply chain management of information security 5.36 Respect for rules, regulations, and information security standards
8.3	Preparation of Treasury and Budget System Development Study Not on Target	Acceptance	5.1 The policy regarding information security 5.2 Aspects of information security roles and duties 5.4 Accountabilities in management 5.21 Information and communication technology (ICT) supply chain management of information security 5.36 Respect for rules, regulations, and information security standards

9.1	Finishing the ICT Information System Not the intended target	Reduce	5.1 The policy on information security 5.2 Aspects of information security roles and duties 5.3 Division of labour 5.4 Accountability for management 5.21 Information security management in the supply chain for information and communications technology (ICT) 5.36 Adherence to information security guidelines, regulations, and guidelines
9.2	Finishing the ICT Information System Not the intended target	Reduce	5.1 The policy on information security 5.2 Aspects of information security roles and duties 5.3 Division of labour 5.4 Accountability for management 5.21 Information security management in the supply chain for information and communications technology (ICT) 5.36 Adherence to information security guidelines, regulations, and guidelines
9.3	Finishing the ICT Information System Not the intended target	Reduce	5.1 The policy on information security 5.2 Aspects of information security roles and duties 5.3 Division of labour 5.4 Accountability for management 5.21 Information security management in the supply chain for information and communications technology (ICT) 5.36 Adherence to information security guidelines, regulations, and guidelines
9.4	Finishing the ICT Information System Not the intended target	Reduce	5.1 The policy on information security 5.2 Aspects of information security roles and duties 5.3 Division of labour 5.4 Accountability for management 5.21 Information security management in the supply chain for information and communications technology (ICT) 5.36 Adherence to information security guidelines, regulations, and guidelines
10.1	Public Satisfaction Index score for IT team services below target	Reduce	5.4 Accountabilities for management 5.21 Information security management in the supply chain for information and communications technology (ICT) 5.36 Adherence to information security guidelines, regulations, and guidelines
10.2	Public Satisfaction Index score for IT team services below target	Reduce	5.4 Accountabilities for management 5.21 Information security management in the supply chain for information and communications technology (ICT) 5.36 Adherence to information security guidelines, regulations, and guidelines

10.3	Public Satisfaction Index score for IT team services below target	Reduce	5.4 Accountabilities for management 5.21 Information security management in the supply chain for information and communications technology (ICT) 5.36 Adherence to information security guidelines, regulations, and guidelines
11.1	Disruption of Critical Information System Backup and Recovery process	Acceptance	5.1 Policies for information security 5.4 Accountabilities for information security 5.29 Data protection in the face of interruptions 5.30 IT preparedness for ongoing business operations 7.10 Media for storage 8.19 Software installation on live systems
11.2	Disruption of Critical Information System Backup and Recovery process	Acceptance	5.1 Policies for information security 5.4 Accountabilities for information security 5.29 Data protection in the face of interruptions 5.30 IT preparedness for ongoing business operations 7.10 Media for storage 8.19 Software installation on live systems
11.3	Disruption of Critical Information System Backup and Recovery process	Acceptance	5.1 Policies for information security 5.4 Accountabilities for information security 5.29 Data protection in the face of interruptions 5.30 IT preparedness for ongoing business operations 7.10 Media for storage 8.19 Software installation on live systems
11.4	Disruption of Critical Information System Backup and Recovery process	Acceptance	5.1 Policies for information security 5.4 Accountabilities for information security 5.29 Data protection in the face of interruptions 5.30 IT preparedness for ongoing business operations 7.10 Media for storage 8.19 Software installation on live systems
11.5	Disruption of Critical Information System Backup and Recovery process	Acceptance	5.1 Policies for information security 5.4 Accountabilities for information security 5.29 Data protection in the face of interruptions 5.30 IT preparedness for ongoing business operations 7.10 Media for storage 8.19 Software installation on live systems

12.1	Information leakage caused by illegal access to Information System devices	Reduce	5.1 The policy on information security 5.2 Aspects of information security roles and duties 5.3 Division of labour 5.4 Accountability for management 5.8 Security of information in project management 5.19 Security of information in supplier relationships 5.20 Managing security of information in supplier contracts 5.21 Information security management in the technology supply chain and information technology 5.24 Planning and preparation for information security incident management 5.25 Evaluation and determination of information security events 5.26 Reaction to incidents involving information security 5.27 Acquiring knowledge from cyber security events 5.35 An unbiased assessment of information security 5.37 Operating Procedures Documented 8.12 Preventing data leaks 8.26 Requirements for application security
12.2	Information leakage caused by illegal access to Information System devices	Reduce	5.1 The policy on information security 5.2 Aspects of information security roles and duties 5.3 Division of labour 5.4 Accountability for management 5.8 Security of information in project management 5.19 Security of information in supplier relationships 5.20 Managing security of information in supplier contracts 5.21 Information security management in the technology supply chain and information technology 5.24 Planning and preparation for information security incident management 5.25 Evaluation and determination of information security events 5.26 Reaction to incidents involving information security 5.27 Acquiring knowledge from cyber security events 5.35 An unbiased assessment of information security 5.37 Operating Procedures Documented 8.12 Preventing data leaks 8.26 Requirements for application security

13.1	Treasury Big Data Development Fails	Acceptance	5.4 Accountability for management 5.5 Interaction with law enforcement 5.6 Interaction with interest-based organizations 8. Two rights to privileged access 8.3 Information access limitations
13.2	Treasury Big Data Development Fails	Acceptance	5.4 Accountability for management 5.5 Interaction with law enforcement 5.6 Interaction with interest-based organizations 8. Two rights to privileged access 8.3 Information access limitations
13.3	Treasury Big Data Development Fails	Acceptance	5.4 Accountability for management 5.5 Interaction with law enforcement 5.6 Interaction with interest-based organizations 8. Two rights to privileged access 8.3 Information access limitations
14.1	Information Security Incidents Happen Often	Acceptance	5.1 The policy on information security 5.2 Aspects of information security roles and duties 5.3 Division of labour 5.4 Accountability for management 5.8 Information security in project management 5.24 Planning and preparing for information security incidents 5.25 Evaluation and determination of information security events 5.26 Reaction to incidents involving information security 5.27 Acquiring knowledge from cyber security events 5.35 An unbiased assessment of information security 5.37 Operating Procedures Documented 8.12 Preventing data leaks 8.26 Requirements for application security
14.2	Information Security Incidents Happen Often	Acceptance	5.1 The policy on information security 5.2 Aspects of information security roles and duties 5.3 Division of labour 5.4 Accountability for management 5.8 Information security in project management 5.24 Planning and preparing for information security incidents 5.25 Evaluation and determination of information security events 5.26 Reaction to incidents involving information security 5.27 Acquiring knowledge from cyber security events 5.35 An unbiased assessment of information security 5.37 Operating Procedures Documented 8.12 Preventing data leaks

			8.26 Requirements for application security
14.3	Information Security Incidents Happen Often	Acceptance	5.1 The policy on information security 5.2 Aspects of information security roles and duties 5.3 Division of labour 5.4 Accountability for management 5.8 Information security in project management 5.24 Planning and preparing for information security incidents 5.25 Evaluation and determination of information security events 5.26 Reaction to incidents involving information security 5.27 Acquiring knowledge from cyber security events 5.35 An unbiased assessment of information security 5.37 Operating Procedures Documented 8.12 Preventing data leaks 8.26 Requirements for application security
14.4	Information Security Incidents Happen Often	Acceptance	5.1 The policy on information security 5.2 Aspects of information security roles and duties 5.3 Division of labour 5.4 Accountability for management 5.8 Information security in project management 5.24 Planning and preparing for information security incidents 5.25 Evaluation and determination of information security events 5.26 Reaction to incidents involving information security 5.27 Acquiring knowledge from cyber security events 5.35 An unbiased assessment of information security 5.37 Operating Procedures Documented 8.12 Preventing data leaks

			8.26 Requirements for application security
15.1	Lack of Competent Human Resources to Manage the Main System	Reduce	5.1 The policy on information security 5.2 Aspects of information security roles and duties 5.4 Accountabilities for management 5.14 Transmission of information 6.5 Responsibilities following a job change or termination
15.2	Lack of Competent Human Resources to Manage the Main System	Reduce	5.1 The policy on information security 5.2 Roles and responsibilities in information security 5.4 Accountabilities for management 5.14 Transmission of information 6.5 Responsibilities following a job change or termination

Conclusion

Based on the findings of studies conducted at Directorate XYZ, Ministry of ABC, it can be summarized that the scope of risk management for information systems and technology at the XYZ Directorate encompasses 15 risks, 50 risk threats, 15 types of impacts, and 3 risk categories. The risk analysis indicates that a significant portion of identified risks, 21 out of 50, or 42% of the total, have a moderate impact. To address these risks effectively, the utilization of international standards such as ISO/IEC 27001:2022 is recommended, as it offers appropriate guidelines for risk reduction and management within this domain.

BIBLIOGRAPHY

M. Andriana, “Jenis-jenis Information Security,” School of Information Systems BINUS University, 2023. https://sis.binus.ac.id/2023/01/06/jenis-jenis-information-security/

Angraini, Megawati, and L. Haris, “Risk Assessment on Information Asset an academic Application Using ISO 27001,” in The 6th International Conference on Cyber and IT Service Management, CITSM 2018, 2018, pp. 1–4. doi: 10.1109/CITSM.2018.8674294.

A. da Veiga, L. V Astakhova, A. Botha, and M. Herselman, “Defining organisational information security culture—Perspectives from academia and industry,” Comput.

Secur., vol. 92, no. May, 2020, 2020, doi: https://doi.org/10.1016/j.cose.2020.101713.
S. Kramer and J. C. Bradfield, "A general definition of malware," J. Comput. Virol., vol. 6, no. 2, pp. 105–114, 2009, doi: 10.1007/s11416-009-0137-1.
O. Aslan and R. Samet, "A Comprehensive Review on Malware Detection Approaches," IEEE Access, vol. 8, pp. 1–23, 2020, doi: 10.1109/ACCESS.2019.2963724.
Ekta and U. Bansal, "A Review on Ransomware Attack," ICSCCC 2021 - Int. Conf. Secur. Cyber Comput. Commun., pp. 221–226, 2021, doi: 10.1109/ICSCCC51823.2021.9478148.
I. Akkiyat and N. Souissi, "Modelling risk management process according to ISO standard," Int. J. Recent Technol. Eng., vol. 8, no. 2, pp. 1–6, 2019, doi: 10.35940/ijrte.B3751.078219.
I. 31000:2009, "ISO 31000:2009(en) Risk management — Principles and guidelines," 2009. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en
S. K. Boell and D. Cecez-Kecmanovic, "What is an information system?," Proc. Annu. Hawaii Int. Conf. Syst. Sci., vol. 2015-March, no. March, pp. 4959–4968, 2015, doi: 10.1109/HICSS.2015.587.
A. P. Putra, "MANAJEMEN RISIKO KEAMANAN INFORMASI PADA APLIKASI DATA KORPORASI DENGAN MENGGUNAKAN ISO/IEC 27005:2018 DAN NIST SP 800-30 REV.1 (STUDI KASUS: PT. XYZ)," UNIVERSITAS BINA NUSANTARA, 2023. [Online]. Available: http://library.binus.ac.id/Collections/ethesis_detail/OS2-KG-MTI-2023-0003
Y. P. Surwade and H. J. Patil, "Information Security," Knowl. Resour. Centre, Dr. Babasaheb Ambedkar Marathwada Univ., vol. 101v1.1, no. February, p. 10, 2019, doi: 2394-2479.
I. D. Gurpreet Dhillon, Kane Smith, "Information systems security research agenda: Exploring the gap between research and practice," J. Strateg. Inf. Syst., vol. 30, no. 4, 2021, [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0963868721000408
N. I. Goncharov, I. V. Goncharov, P. A. Parinov, A. V. Dushkin, and M. Maximova, "Modeling of Information Processes for Modern Information System Security Assessment," Proc. 2019 IEEE Conf. Russ. Young Res. Electr. Electron. Eng. ElConRus 2019, pp. 1758–1763, 2019, doi: 10.1109/EIConRus.2019.8656828.
A. Fathurohman and R. W. Witjaksono, "Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City)," Bull. Comput. Sci. Electr. Eng., vol. 1, no. 1, pp. 1–11, 2020, doi: 10.25008/bcsee.v1i1.2.
D. Kim and M. G. Solomon, Fundamentals of Information Systems Security, 3rd Editio. Burlington: Jones & Bartlett Learning, LLC, an Ascend Learning Company, 2018.
J. S. Suroso and M. A. Fakhrozi, "Assessment of Information System Risk Management with Octave Allegro at Education Institution," Procedia Comput. Sci., vol. 135, pp. 202–213, 2018, doi: 10.1016/j.procs.2018.08.167.
ISO31000:18, "Risk Management - Guidelines," British Standards Istitution Limited 2018, Switzerland, 2018.
E. Wheeler, Security Risk Management: Building an Information Security Risk Management Program from the Ground Up. 2011. doi: 10.1016/C2010-0-64926-1.
C. Yuliana, "Manajemen Risiko Kontrak Untuk Proyek Konstruksi," Rekayasa Sipil, vol. 11, no. 1, pp. 1–8, 2017, doi: 10.21776/ub.rekayasasipil.2017.011.01.2.

British Standards Institution, “ISO/IEC 27001 Information Security Management System: Keep your confidential information safe,” BSIGroup.com, 2022. https://www.bsigroup.com/en-ID/ISO-IEC-27001/

M. Malatji, “Management of enterprise cyber security: A review of ISO/IEC 27001:2022,” in 2023 International Conference On Cyber Management And Engineering (CyMaEn), 2023. doi: 10.1109/CyMaEn57228.2023.10051114.

I. B. Kaja Prislan, “Risk Management with ISO 27000 Standards in Information Security,” Fac. Crim. Justice Secur. Univ. Maribor, pp. 1–6, 2010.

E. Kaban and N. Legowo, “Audit Information System Risk Management Using ISO 27001 Framework at Private Bank,” J. Theor. Appl. Inf. Technol., vol. 96, no. 1, pp. 1–10, 2018.

N. Legowo and Y. Juhartoyo, “Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001,” J. Syst. Manag. Sci., vol. 12, no. 3, pp. 181–199, 2022, doi: 10.33168/JSMS.2022.0310.

B. GÜR, Ş. YAVUZ, A. D. ÇAKIR, and D. A. KÖSE, “Determination Of Hazards And Risks In A Solar Power Plant Using The Matrix Risk Analysis,” Eur. J. Sci. Technol., no. 23, pp. 497–511, 2021, doi: 10.31590/ejosat.881614.

Copyright holder:
Kanka Wiemas N. G., Jarot S. Suroso (2022)

First publication right:
Syntax Literate: Jurnal Ilmiah Indonesia

This article is licensed under:

