2022 - Risk Assessment (JATISI)

by Laqma Dica

Submission date: 05-Jul-2022 10:48AM (UTC+0700)
Submission ID: 1866766947
File name: 18._Laqma_Dica_JATISI_-_artikel.pdf (367.77K)
Word count: 6567
Character count: 35297

Risk Assessment And Development Of Access Control Information Security Governance Based On ISO/IEC 27001:2013 At XYZ University

Laqma Dica Fitrani[1]
[1]Information System Department, Faculty of Engineering and Design, Hayam Wuruk Perbanas University; Jl. Wonorejo Utara 16, Surabaya, East Java.
e-mail: [1]Laqma.fitrani@hayamwuruk.ac.id

Abstract

Perkembangan teknologi informasi yang pesat saat ini turut berimbas kepada penggunaan teknologi informasi di lingkungan universitas. Universitas XYZ sebagai universitas yang memiliki mahasiswa cukup banyak ini juga menerapkan teknologi informasi untuk mendukung pembelajaran jarak jauh yang mereka terapkan. Tentunya peran teknologi informasi ini cukup krusial dan penting. Sayangnya masalah keamanan informasi yang merupakan bagian penting dari teknologi informasi sering kali kurang mendapatkan perhatian. Tidak dapat dipungkiri bahwa munculnya ancaman ataupun kelemahan dalam teknologi informasi dapat menggangu jalannya kegiatan pelayanan yang menggunakan teknologi informasi. Oleh karena itu diperlukan pengelolaan teknologi informasi dan dokumen standart prosedur berbasis risiko yang dituangkan dalam tata kelola untuk mengelola ancaman ataupun kelemahan yang muncul. ISO/IEC 27001:2013 merupakan framework sistem manajemen keamanan informasi yang dapat dijadikan dasar dalam pengelolaan keamanan informasi. Penelitian ini mengidentifikasi asset, ancaman, kelemahan, analisa risiko, BIA, penilaian risiko, dan pemetaan risiko berdasarkan klausul sehingga menghasilkan rekomendasi dokumen kebijakan, procedure, dan intruksi kerja untuk meningkatkan control keamanan informasi berdasarkan klausul ISO 27001:2013. Dilihat dari risiko yang memiliki nilai tinggi, penelitian ini menghasilkan rekomendasi dokumen keamanan yaitu 5 dokumen kebijakan, 6 pedoman prosedur, 8 intruksi kerja, dan 12 formulir.

Kata kunci— Akses Kontrol, ISO 27001:2013, Penilaian Risiko

Abstract

The rapid development of information technology at this time also has an impact on the use of information technology in the university environment. XYZ University as a university that has quite a lot of students also applies information technology to support their distance learning. The role of information technology is quite crucial and important. Unfortunately, the issue of information security which is an important part of information technology often gets less attention. Its undeniable that the emergence of threats or weaknesses in information technology can disrupt the course of service activities using information technology. Therefore, it is necessary to manage information technology and risk-based document standard procedures as outlined in governance to manage emerging threats or weaknesses. ISO/IEC 27001:2013 is an framework of information security management system that can be used as a basis for managing information security. This study identifies assets, threats, weaknesses, risk analysis, BIA, risk assessment, and risk mapping based on clauses to produce recommendations for policy documents, procedures, and work instructions to improve information security control based on ISO 27001:2013 clauses. Considering its high risk value, this study produced several recommendations for security documents, namely 5 policy documents, 6 procedure guidelines, 8 work instructions, and 12 forms.

Keywords — Access Control, ISO 27001:2013, Risk assessment

1. INTRODUCTION

Businesses are becoming escalatingly dependent on information technology to fix the operations and serve competitive advantage [1]. Strengthening information technology is very important because most businesses cannot continue to operate successfully if their information technology services are not available [2].

In this internet era, Internet Data Center (IDC) has emerged as the main network service platform to unify internet services into one location and offer more efficient data center services for an institution or company. IDC manages servers and networks along with critical and sensitive data.

XYZ University is one of the universities that implements an open and distance learning system. This learning system has proven to be effective in increasing the coverage and equity of quality higher education opportunities for all Indonesian citizens, including those living in remote areas, both throughout the country and in various parts of the world. This wide coverage makes XYZ University has a large number of students, amounting to 292,465, so that adequate information storage is needed in the data center.

Information technology uses for support in carrying out its daily duties in an organization, information technology and systems operations become a critical matter [3]. As a data processing center, the data center stores company information including critical and sensitive information. As a result, data center needs physical and logical protection to secure information systems from attacks that threaten its security.

In the management of the organization, the problem of risk is often not a concern of management. Meanwhile, in the concept of sustainable management, an organization is established with the assumption that it will continue to operate in an indefinite period of time. Risk is often a limiting factor in the organization's operations to achieve goals. When an incident or disaster occurs, the organization will generally suffer losses. These losses include: inaccessible information (loss of availability), data that is damaged or has turned into wasted data (loss of integrity) and the possibility of leakage of important information that should be protected [4]. Good IT management is able to minimize these risks by providing appropriate treatment of risks that may occur so that the business can continue to operate well [5].

The current condition is that there is still a lack of information security handling so that it still creates threats and vulnerability, which results in unachieved targets and affects confidentiality, integrity, and availability which in turn will affect the business impact analysis.

ISO/IEC 27001 is one of the methods with information security standards issued by the International Standardization Organization and the International Electrotechnical Commission [6].

ISO 27001 is the most extensive used information security management standard by businesses and organizations, providing the most comprehensive specific reference for information security management in the world. ISO 27001 is an information security management standard that is widely used by businesses and organizations, providing the most comprehensive specific reference for information security management in the world. There are several studies that use ISO 27001:2013 such as in the journal "Evaluasi Keamanan Informasi Data Center Berdasarkan Standar ISO 27001:2013 (Studi Kasus PT. Pupuk Kalimantan Timur)" the purpose of this research is to evaluate the security of data center information using the FMEA assessment index. and provide recommendations for ISO 27001 and produce recommendations for improvement to update the information security policy on a regular basis [7]. In the second journal with the title "Implementation of ISO / IEC 27001: 2013 for Information Security Management Systems (SMKI) at the Faculty of Engineering Uika-Bogor" the author wants to obtain the level of security on the Faculty of Engineering hotspot network based on these standards and the results of the analysis show that users only trust security level

of 49% and the management only trusts the security level of 45%. Based on this, it is shown that the ISMS on the hotspot network at the Faculty of Engineering is less secure according to the ISO/IEC 27001:2013 Standard [8]. Further research with the title "Evaluasi Keamanan Sistem Informasi Pasdeal Berdasarkan Indeks Keamanan Informasi (Kami) ISO/IEC 27001:2013" Based on the results of the KAMI assessment, it was found that Pasdeal scored 591 points from the application of the ISO 27001 standard with a pretty good predicate [9]. From the research that has been done previously, it shows that the research carried out an assessment and produced recommendations for improvements based on the ISO 27001:2013 framework. While in this research, there are several things that the author does, namely identifying assets, threats, weaknesses, risk analysis, BIA, risk assessment, and risk mapping based on clauses so as to produce recommendations for policy documents, procedures, and work instructions to improve information security control, and produce several recommendations for security documents based on the ISO 27001:2013 clause.

ISO 27001 is also defined as Information Security Management System, commonly called as ISMS, which provides a general description of what an institution should do in their efforts to perform, assess, and preserve security of information based on "best practice" in information security [10].

Thus, the form of support in controlling the information security management system from the CIA side at the ICT Center of XYZ University is to conduct risk assessments, doing control and giving recommendations for the preparation of risk management documents related to information security and recommendations for making SOP (standard operational procedures) documents with the aim of being a work reference and standardization to regulate and improve the quality of existing information security [11]. This is selected through control objectives and information security controls by considering the results of the security risk management carried out.

2. RESEARCH METHODS

2.1 Literature Review

2. 1.1 Information Security

Stoneburner, Goguen, & Feringa (2002) from the National Institute of Standards and Technology (NIST) stated that risk management is a action that permit IT managers to equilibrium between economic costs and operational costs through preservative rate to reach profits, in accordance with the university by preserving the IT systems and data that support their organization's task [12].

Information security is an activity to protect or prevent misuse of information by people who are not responsible for the operation of a system [13].

Information security is got by executing a set of suitable control tools, in the form of policies, work guidelines (SOPs), organizational structures, and software. In information security there are various kinds of risks that will be faced which come from various sources, including internal, external and natural disasters such as floods, fires, and others.

Information security composed of defense towards the following aspects:

1. Confidentiality is the aspect that confirms the confidentiality of informations and the data, ensures that information can only be entranced by guaranteed persons and ensures the data sent confidentiality, accepted and saved.

2. Integrity is the aspect that confirms that the data is not substituted without the permission of the authorized party, maintaining the integrity accuracy of the information as well as its process method in order to ensure this aspect of integrity.
3. Availability is an aspect that confirms that data will be available, confirming that authorized users may use the information and connected assets or tools when needed.

Information security is gained by executing a set of suitable control tools, containing practices, procedures, policies, organizational structures and software [14].

2.1.2 Risk Management of Information Technology

The definition of risk can be defined as an opportunity or possibility that can affect a goal and result in losses if not managed properly and can be categorized into several categories, i.e. Strategic Risk, Financial Risk, Compliance, Reputational Risk and Operational Risk [15].

Risk management of information technology is a process of recognize threats vulnerabilities to resource of the information that organization use and performed by information technology managers to reach business purposes, decrease the risks, and stability the cost in attaining benefits and preserving IT [16].

There are two things in this definition that need explanation. First, the risk management process which is an iterative and continuous process. This is a process that must be repeated indefinitely, due to the flexible or constantly changing business environment that causes new threats to emerge. Second, the choice of countermeasures or control used to manage risk must maintain a balance between expense, productivity, effectiveness of countermeasures, and value of information assets that must be protected.

The Function of IT Risk Management:

1. Providing directive to help the management and executives request the key of inquiries, make better and more notified risk-adapted resolves to guide their companies so the risks are organized effectively.
2. Helping to save time, money and strive with tools in addressing risk of business.
3. Integrating IT management related to risks of business into roundly enterprise risk management.
4. Helping the leader to understand the company's risks and risk tolerance.
5. Providing practical directive encouraged by the leadership requirement of companies around the world.

2.1.2 ISO/IEC 20071

ISO/IEC 27001 is a framework used to specify the needs to develop, implement, monitor and periodically improve the management of people, processes and ICT in an organization (whether in small, medium or large scale of organization).

The increasing need and use of ICT in supporting the business activities of an organization will increase the value of the risk of information security disruption. Increased risk of disruption in an organization that rely heavily on ICT services will greatly affect the achievement of the organization's goals.

An organization requires ISO/IEC 27001 management to:

- Regularly inspect information security risks from the organization, considerate into account vulnerabilities, impacts, and threats;
- Design and perform a comprehensive and coherent set of information security controls or the other establishes of risk treatment (such as risk aversion or risk transfer) to overcome risks considered inadmissible;
- Take a comprehensive management process to confirm that information security controls continue to fulfil the organization's information security requires on an ongoing basis.

What controls will be examined as part of certification to ISO27001 depends on the auditor's certification. This may contain any controls that the organization has assumed to be within the reach of the ISMS and these tests may be performed to any profundity or level evaluated by the auditor as necessary to test that the controls have been performed and are operating successfully.

Management decides the scope of the ISMS for certification goals and may confine, for example, one business location or unit. A certificate of ISO/IEC 27001 does not necessarily matter that the rest of the organization (outside of the coverage area) has an suffice approach of information security management.

2. 2 Research Stages

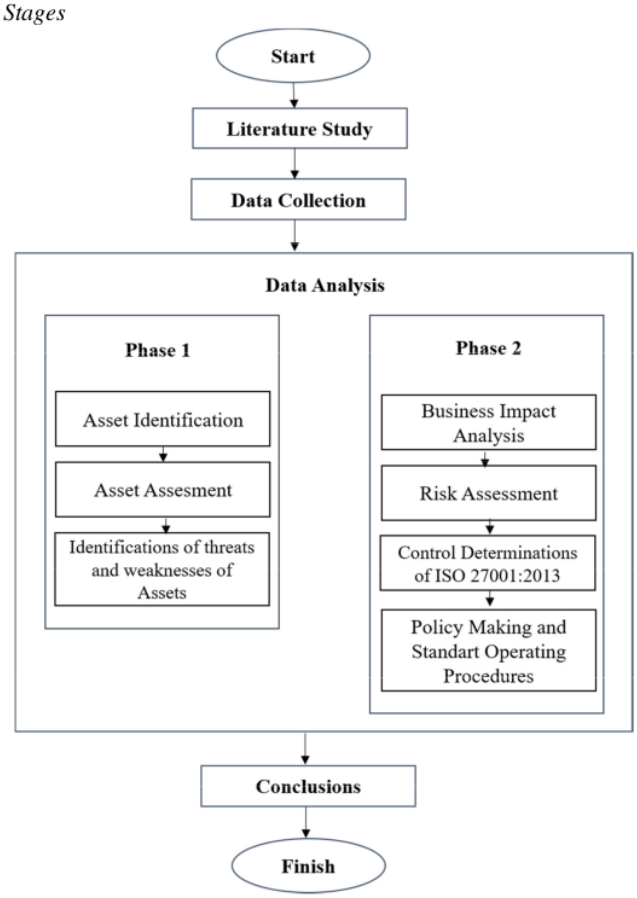

Figure 1. Research Stages

The research methodology used in this study broadly consists of four stages, including:

1. Literature Review
   The research began with reviewing related research/literatures. The related literature was literature on the asset identification process, asset value calculation. Assessing the risks

using the literature was expected to provide a fairly complete picture and framework to analyze the risks of information security.

2. Data Collection
   The data collection in this research was arranged using observations and interviews with each division head to find out the details of the problems, business processes, and management related to information technology, especially those related to information security at XYZ university.
3. Data Analysis
   At this stage, assets identification was performed, calculating the value of assets that have been collected, identifying threats and weaknesses of assets, conducting business impact analysis (BIA), identifying risk levels and finally calculating risk value to know the risk level of the assets.

Asset's identification was done by conducting interviews and observations to find out what assets are owned by this XYZ university.

After identified the assets, the next step was to count the asset value. This approach was taken by using three sides of security, namely confidentiality in the following table 1, integrity in the following table 2 and availability in the following table 3. The reference for asset valuation is as follows [17]:

Table 1. Identification Confidentiality of Registered Assets

Confidentiality Criteria	Confidentiality Value
Public	0
Internal use only	1
Private	2
Confidential	3
Secret	4

Table 2. Identification Integrity of Registered Assets

Integrity Criteria	Integrity Value
No Impact	0
Minor Incident	1
Genaral Disturbance	2
Mayor Disturbance	3
Unacceptable damage	4

Table 3. Identification Availability of Registered Assets

Availability Criteria	Availability Value
No Availability	0
Office Hour Availability	1
Strong Availability	2
High Availability	3
Very High Availability	4

The calculation was done by using the equation below (1):

$$AV = CV+IV+AV \quad (1)$$

Explanation:

AV : Asset Value
CV : Convidentiality Value
IV : Integrity Value
AV: Availability Value

The next calculation was to recognize threats and weaknesses to every asset, then determine the average value of the possibility of the emergence, weaknesses, and threats using the following value ranges:

- Low: The average possibility value is 0,0 – 0,3
- Medium: The average possibility value is 0,4 – 0,6
- High: The average probability value is 0,7 – 1,0

The next what is often called a Business Impact Analysis (BIA). The valuation criteria for business impact analysis may be observed in the following table 4:

Table 4. Assessment Criteria for BIA

Disturbance Tolerance Limit	Description	BIA Value
< 1 week	Not Critical (NC)	0
1-2 days	Minor Critical (MiC)	1
< 1 day	Mayor Critical (MaC)	2
< 12 hours	High Critical (HC)	3
< 1 hour	Very High Critical (VHC)	4

The risk level assessment used a risk matrix as shown in Table 5. The value obtained was derived from the multiplication between the probability of threat and the business impact analysis (BIA).

Table 5. The Risk Level Assessment Used A Risk Matrix

Probability of Threats	Business Impact				
	Not Critical	Low Critical	Medium Critical	High Critical	Very High Critical
Low (0,1)	Low 0	Low 0,1	Low 0,2	Low 0,3	Low 0,4
Medium (0,5)	Low 0	Medium 0,5	Medium 1	Medium 1,5	Medium 2
High (1,0)	Low 0	Medium 1	Medium 2	High 3	High 4

To determine whether a risk is accepted or a risk management is needed, it is necessary to calculate the value of the existing risk [18].

Risk value can be calculated by using the equation below (2):

$$Risk\ Value = AV + BIA + TV \quad (2)$$

Description:
AV : Asset Value
BIA: Business Impact Analysis
TV : Threat Value

After getting the risk value, the risk level was obtained by adjusting the risk value with Table 5 (Risk Level Matrix). The levels of risk of the results obtained for each asset were then identifired. The risk levels based on the table showed Low, Medium or High level. From these results, the assets were categorized as high-risk assets.

3. RESULTS AND DISCUSSION

Information Technology (IT) resources when viewed specifically have a direct impact on organizational goals. IT acts as an sustainable in the organization to support operational action which will have an impact on the mission of the agency. The value of IT supports business value through the invention of organizational abilities so that the organization is able to reach its competitive benefit and meet the set goals.

3.1 Asset Identification

An asset is anything that has a certain value to the organization. XYZ University has defined that organizational assets include hardware assets, software assets, human resource assets, and information assets.

Identifying assets in the ISMS can be done using a table of assets that have been categorized according to the type or need of the organization [16]. Asset identifications may be observed in the following table 6:

Table 6. Identification of Registered Assets

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

3.1.1 Asset Assessment

After the assets have been identified, the next step was to conduct asset assessments based on a three-aspect approach of information security, specifically confidentiality, integrity and availability. Identification Value of Registered Assets can be observed in the table 7 and can be calculated by using the equation below (3):

$$Asset\ value = Confidentiality + Integrity + Availiability \quad (3)$$

Table 7. Identification Value of Registered Assets

No	Asset	C	I	A	Asset Value
1	Server	3	3	3	9
2	Network	3	3	3	9
3	PC/Laptop	2	2	3	7
4	Router	3	3	3	9
5	Printer	2	2	2	6
6	Hardisk	2	2	2	6
7	Switch	2	2	2	6
8	Linux & Windows	2	2	2	6
9	Microsoft 365	2	2	2	6
10	Academic System	3	3	4	10
11	Teaching Material System	3	3	4	10
12	Reporting System	3	3	4	10
13	E-support	3	3	3	9
14	E-Learning	3	3	3	9
15	Employment Information System	3	3	4	10
16	Academic Data	4	3	3	10
17	Teaching Material Data	3	3	3	9
18	Employment Data	4	3	3	10
19	Report Data	3	3	4	10

3.1.2 Identification of Threats and Weaknesses of Assets

After determining the worth of the assets, the next step was to recognize weaknesses or threats against every asset, then determine the average value for the possibility of the emergence of weaknesses and threats using the values range as follows. Identification of threats and weaknesses of assets can be observed in the table 8:

Table 8. Identification of Threats and Weaknesses of Assets

Asset Category	Asset	Incident	Threat/ Weakness	Inherent Risk				Threat Value (TV)
				PO	even	Nilai PO	∑ PO	
Hardware	Server	Server down	Threat	Low	0	0	0,3	0,1
		Server configuration error	Threat	Low	2	0,2		
		Virus attack	Threat	Low	1	0,1		
	Network	Hacker attack	Threat	Low	0	0	0	0
		Network disruption	Weakness	Low	0	0		
	PC/ Laptop	PC/Laptop Theft	Threat	Low	0	0	0,1	0,05
		Damage to PC/Laptop	Weakness	Low	2	0,1		
	Router	Router malfunction	Weakness	Low	0	0	0	0
	Printer	Printer theft	Threat	Low	0	0	0	0
	Hardisk	Hard disk damage	Weakness	Low	1	0,1	0,1	0,1
	Switch	Router malfunction	Weakness	Low	0	0	0	0
Software	Linux &	Virus attack	Threat	Med	3	0,1	0,15	0,05

	Windows	Not updating linux/windows	Weakness	Low	0	0		
		Use of administrator access rights on the user's PC	Weakness	Low	2	0,05		
	Microsoft 365	Illegal access	Threat	Low	0	0	0	0
	Academic System	Virus attack	Threat	Low	0	0	0,4	0,13
		Application not updated	Weakness	Low	0	0		
		Illegal access	Weakness	Med	2	0,4		
	Teaching Material System	Virus attack	Threat	Low	0	0	0,2	0,06
		Application not updated	Weakness	Low	0	0		
		Illegal access	Weakness	Low	1	0,2		
	Reporting System	Virus attack	Threat	Low	0	0	0,2	0,06
		Illegal access	Weakness	Low	1	0,2		
		Operational failure	Weakness	Low	0	0		
	E-Support	Virus attack	Threat	Low	0	0	0,15	0,05
		Application not updated	Weakness	Low	1	0,15		
		Operational failure	Weakness	Low	0	0		
	E-Learning	Virus attack	Threat	Low	1	0,1	0,2	0,06
		Application not updated	Weakness	Low	0	0		
		Kegagalan operasional	Weakness	Low	1	0,1		
	Employement System	Virus attack	Threat	Low	0	0	0,2	0,06
		Application not updated	Weakness	Low	1	0,2		
		Operational failure	Weakness	Low	0	0		
Data information	Academic Data	Kesalahan input data	Weakness	Low	2	0,1	0,25	0,08
		Data theft	Threat	Low	0	0		
		Damaged data storage	Threat	Low	1	0,15		
	Employement Data	Data input error	Weakness	Low	0	0	0	0
		Data theft	Threat	Low	0	0		
		Damaged data storage	Threat	Low	0	0		
	Reporting Data	Data input error	Weakness	Low	0	0	0	0
		Data theft	Threat	Low	0	0		
		Damaged data storage	Threat	Low	0	0		
	Teaching material data	Data input error	Weakness	Low	0	0	0	0
		Data theft	Threat	Low	0	0		
		Damaged data storage	Threat	Low	0	0		

3.2 Risk Analysis

This risk analysis stage aimed to analyze and assess the impact on each asset, conduct a risk assessment, and determine what controls must be carried out according to the ISO 27001:2013 standard. This risk analysis process should be carried out comprehensively or thoroughly so that risks can be assessed systematically [20].

3.2.1 Business Impact Analysis (BIA)

After getting the results of the threat value from the identification process of threats and weaknesses, the next step was to analyze and assess the Business Impact Analysis (BIA) on each asset. This BIA illustrates the impact of a disruption to the business activities that support key products and services. The BIA was conducted to decide the toleration limit of existing assets against the emerging weaknesses and threats, the identification of BIA can be seen in table 9.

Table 9 Identification of Business Impact Analysis

No	Asset	BIA Value
1	Server	4
2	Network	2
3	PC/Laptop	2
4	Router	2
5	Printer	1
6	Hardisk	1
7	Switch	2
8	Linux & Windows	3
9	Microsoft 365	2
10	Academic System	3
11	Teaching Material System	3
12	Reporting System	3
13	E-support	3
14	E-Learning	3
15	Employment Information System	3
16	Academic Data	4
17	Teaching Material Data	3
18	Employment Data	4
19	Report Data	3

3.2.2 Risk Assessment

The level of risk is the level of risk that arises when associated with the impact and probability of threats that may arise. Identifying the level of risk can be seen in accordance with the asset values, threat probabilities, and business impact analysis that have been determined. Risk assessment and its level can be seen in table 10.

Table 10. Risk Assessment

No	Asset	Asset Value	Threat Value	BIA	Risk Value	Risk Level
1	Server	9	0,1	4	3,6	High
2	Network	9	0	2	0	Low

3	PC/Laptop	7	0,05	2	0,7	Low
4	Router	9	0	2	0	Low
5	Printer	6	0	1	0	Low
6	Hardisk	6	0,1	1	0,6	Low
7	Switch	6	0	2	0	Low
8	Linux & Windows	6	0,05	3	0,9	Medium
9	Microsoft 365	6	0	2	0	Low
10	Academic System	10	0,13	3	3,9	High
11	Teaching Material System	10	0,06	3	1,8	Medium
12	Reporting System	10	0,06	3	1,8	Medium
13	E-support	9	0,05	3	1,35	Medium
14	E-Learning	9	0,06	3	1,62	Medium
15	Employment Information System	10	0,06	3	1,8	Medium
16	Academic Data	10	0,08	4	3,2	High
17	Employment Data	9	0	3	0	Low
18	Report Data	10	0	4	0	Low
19	Teaching Material Data	10	0	3	0	Low

3.3 Control Determination of ISO 27001

The next step was to determine the appropriate security controls on assets that have a higher risk level. The determination of the objectives of contol and security was adjusted to the threats and weaknesses of each asset. The control objectives used were based on the objectives contained in Annex A ISO/IEC 27001:2013 which were adjusted to the threats and weaknesses of the risk in the access control clause, risk mapping using the clauses of ISO 27001:2013 can be seen in table 11.

Table 11. Risk Mapping Using The Clauses of ISO 27001:2013

Name of Asset	Existing Risk	Clause	Control Objective	Security Control	Control
Server	Server configuration error	A.11 – Physical and Environmental Security	A.11.2 – Equipments	A.11.2.4 – Equipment maintenance control	Equipment must be properly preserved to confirm its continued integrity and availability
	Virus attack	A.12 – Operation Security	A.12.2 - Protection againts Malware	A.12.2.1 - Control against malware	Discovery, precaution and restoration oversees to defend towards malware must be performed, conjoined with suitable awareness of user

		A.13 – Communication Security	A.13.1 – Network security management	A.13.1.2 – Network service security	The mechanisms of security, levels of service, and requirements of management for all services of network must be recognized and included in the network service agreement, if these services are providing that outsourced or internally.
Academic System	Ilegal Access	A.9 – Access Control	A.9.1 – Business requirements for access control	A.9.1.1 – Access control policies	Access control policies should be founded, recorded and coveraged based on information security and business needs.
			A.9. 4 – Control of application and system access	A.9.4.1 – Information access limitation	Access to the application system and information functions must be limited in suitable with access control policies
Academic Data	Data input error	A.12. – Operational Security	A.12.3 - Backup	A.12.3.1 – Information Backup	Back-up information copies, software and system images should be taken and examined systematically in accordance with the policy agreement's backup.
			A.12.4 - Logging and monitoring	A.12.4.1 - Event logging	Event logs that record user activity, exclusions, errors, and events of information security should be generated, stored, and systematically reviewed.
	Damaged data storage	A.11 – Physical and environmental security	A.11.1 – Equipments	A.11.1.2 – Equipment maintenance control	Equipment must be properly preserved to confirmed its seriated availability and integrity.

3.4 Policy Making and Standard Operating Procedures

Based on the information security management system pyramid, the document structure of the information security consists of 3 levels. The first level is the policy structure, the second level is procedures, and at the third level is work instructions and forms. The source of this document is taken from the mapping of the ISO 27001 clause, where the document serves as a direction in carrying out work processes based on ISO 27001 information security.

The results of the recommendations for information system security documents are shown in the following table 12:

Table 12. Mapping of Policies, Procedures, Work Instructions, and Forms

Asset	Policy	Procedure Guideline	Work Instructions	Forms
Server	**KB01** – Telecommunication network and hardware management	**PP01** – Hardware management	**IK01** – hardware maintenance - Hardware crash reporting - Hardware handling - Hardware improvements	**FM01** – IT equipment maintenance **FM02** – Breakdown report **FM03** – IT equipment usage evaluation report
	KB02 – Protection against virus	**PP02** – Protection againts malware	**IK02 – Kontrol terhadap malware** - Malware detection - Prevention of malware - Recovery from malware	**FM04** – Report of detected malware **FM05** – System recovery evaluation report
Academic System	**KB03** – Control of access rights	**PP03 –** Access rights management	**IK03 -** Change of access rights - Granting of access rights - Removal of access rights - Changes of access rights	**FM06** – Access rights management **FM07** – Access rights agreement contract **FM08** – Log on access rights management
Academic Data	**KB04** – Information security and control	**PP04** – Information security	**IK04** – Information security classification	**FM09** – Monitoring of information security
			IK05 – Information security and responsibility	
	KB05 – Backup and restore	**PP05 –** Backup and restore	**IK06** – Data and file Backup	**FM10** – Data classification **FM11** - Log Backup data
			IK07 – Data Restore	**FM12** – Data restore
	KB01 – Telecommunication network and hardware management	**PP06 –** Storage maintenance and management	**IK08** – Storage maintenance: - Storage handling - Storage crash reporting - Storage improvements	**FM01** – IT equipment maintenance **FM02** – Breakdown report **FM03** – IT equipment usage evaluation report

4. CONCLUSIONS

According to the results of the analysis that has been obtained, it can be concluded that there are three assets that need risk management because they have a high risk value, i.e. servers, academic systems, and academic data. Based on the risk assessment that has a high value, it can be mapped into four clauses, i.e. A.9, A.11, A.12, and A.13. At the stage of preparing security documents, 5 policy documents, 6 procedure guidelines, 8 work instructions, and 12 forms were produced.

5. RECOMMENDATIONS

1. Research development can be done by adding the cost of the impact of losses experienced by the organization
2. This research is limited to the recommendation for making SOP documents without SOP testing and implementation in the business processes of the organization
3. This SOP documents can still be developed as seen from the rapid development of technology so that the organization can continue to compete and be able to run their business processes well

ACKNOWLEDGE

The author would like to thank the chairman and members of ICT Center of XYZ University who helped a lot and took the time so that this research could be carried out.

REFFERENCES

[1] Bhatt, G. D., Grover, V., & Grover, V. 2017. *Types of Information Technology Capabilities and Their Role in Competitive Advantage: An Empirical Study Types of Information Technology Capabilities and Their Role in Competitive Advantage*: *Journal of Management Information System*, *1222*(April), 253–277.

[2] R., Brahmasari, I. A., & Panjaitan, H. 2018. *Peran Teknologi Informasi Dalam Peningkatan Kepercayaan dan Citra Perguruan Tinggi Swasta. Jurnal Mebis (Manajemen Dan Bisnis)*, *3*(2), 78–86. https://doi.org/10.33005/mebis.v3i2.37

[3] Fitrani, L. 2021. *The Combination of Ahp and Topsis Methods In Determining The Ranking of Recommendations For Improvement of Information Technology Services*. *Pilar Nusa Mandiri: Journal of Computing and Information System*, *17*(2), 119-126. https://doi.org/10.33480/pilar.v17i2.2319

[4] Bradbury, C. (2008, April). DISASTER! Creating and Testing An Effective Recovery Plan. *Manager*.

[5] Tipton, H. F., & Krause, M. 2007. *Information Security Management Handbook, Sixth Edition*. *Information Security Management Handbook, Sixth Edition* (pp. 1–3233). CRC Press. https://doi.org/10.1201/ebk1439819029-b

[6] Mikes, A., & Kaplan, R. S. 2012. *Managing Risks: Managin Risks: A New Framework. Harvard Business Review*, (June), 48–60.

[7] Nafisah, F. A., Putra, W. H .N., & Herlambang, A. D. 2020. *Evaluasi Keamanan Informasi Data Center Berdasarkan Standar ISO 27001:2013 (Studi Kasus PT. Pupuk Kalimantan Timur).* Jurnal Teknologi Informasi dan Ilmu Komputer, Vol. 4, No, 6.

[8] Goeritno, A., & Hendrawan, A. H. 2016. *Implementasi ISO / IEC 27001 : 2013 Untuk Sistem Manajemen Keamanan Informasi (SMKI) pada Fakultas Teknik UIKA-Bogor. Seminar Nasional Sains dan Teknologi Fakultas Teknik Universitas Muhammadiyah Jakarta*, *8*(November), 1–5. Retrieved from https://media.neliti.com/media/publications/174077-ID-none.pdf

[9] Wijaya, Y. D. 2021. *Evaluasi Kemananan Sistem Informasi Pasdeal Berdasarkan Indeks Keamanan Informasi (Kami) ISO/IEC 27001:2013. Jurnal Sistem Informasi dan Informatika (Simika)*, *4*(2), 115–130. https://doi.org/10.47080/simika.v4i2.1178

[10] Februari, P., & Fitria, F. 2019. *Audit Sistem Keamanan Informasi Menggunakan ISO 27001 pada SMKN 1 Pugung, Lampung. POSITIF: Jurnal Sistem Dan Teknologi Informasi*, *5*(2), 97. https://doi.org/10.31961/positif.v5i2.833

[11] Musyarofah1, S.R., & Bisma, R. 2020. *Pembuatan Standard Operating Procedure (SOP) Keamanan Informasi Berdasarkan Framework ISO/IEC 27001:2013 dan ISO/IEC 27002:2013 pada Dinas Komunikasi dan Informatika Pemerintah Kota Madiun. (*Journal of Emerging Information Systems and Business Intelligence), Volume 01 Nomor 01.

[12] G. Stoneburner, Goguen, a., & Feringa, a. 2002. *Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology, Special Publication 800 -30*, *800–30*, 55.

[13] Pradipta, Y. C., Rahardja, Y., & Sitokdana, M. N. N. 2019. *Audit Sistem Manajemen Keamanan Informasi Pusat Teknologi Informasi dan Komunikasi Penerbangan dan Antariksa (Pustikpan) Menggunakan Sni Iso/Iec 27001:2013. Sebatik*, *23*(2), 352–358. https://doi.org/10.46984/sebatik.v23i2.782.

[14] Santosa, I., & Kuswanto, D. 2016. *Analisa Manajemen Resiko Keamanan Informasi pada Kantor Pelayanan Pajak Pratama XYZ. Rekayasa*, *9*(2), 108. https://doi.org/10.21107/rekayasa.v9i2.3347

[15] Husein, Gilang M., 2015. *Analisis Manajemen Resiko Teknologi Informasi Penerapan pada Document Management System di PT. Jabar Telematika (JATEL),* Jurnal Teknik Informatika dan Sistem Informasi Vol. 1 No. 2 hal. 77.

[16] Jakaria, D. A., Dirgahayu, R. T., & Hendrik. 2013. *Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro*. Fakultas Hukum UII, 37–42.

[17] Utomo, M., Utomo, M., Ali, A. H. N., & Affandi, I. 2012. *Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 pada Kantor*

Pelayanan Perbendaharaan Surabaya I. *Jurnal Teknik ITS*, *1*(1), A288–A293. Retrieved from http://ejurnal.its.ac.id/index.php/teknik/article/view/900 https://ejurnal.its.ac.id.

[18] Setiawan, I., Sekarini, A. R., Waluyo, R., & Afiana, F. N. 2021. *Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto*. *MATRIK: Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *20*(2), 389–396. https://doi.org/10.30812/matrik.v20i2.1093

[19] Setiawan, I., Sutopo, M., & Azis, A. 2020. *Manajamen Risiko SIMRS Menggunakan Metode OCTAVE-S dan Standar Pengendalian ISO/EIC 27001.* Jurnal Teknik Informatika dan Sistem Informasi, Vol. 7, No. 3.

[20] Nurfadilah, D.R., Putra, W.H.N, & Rachmadi, A. *Analisis Manajemen Risiko Keamanan Sistem Informasi pada BKPSDM Kota Batu Menggunakan Kerangka Kerja OCTAVE-S dan ISO 27001:2013 (Studi Kasus: Aplikasi E-Kinerja).* Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer. Vol. 4, No. 9,

2022 - Risk Assessment (JATISI)

ORIGINALITY REPORT

13%	13%	4%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

4%

★ worldwidescience.org

Internet Source

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

2022 - Risk Assessment (JATISI)

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17