Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0893
p-ISSN: 2089-3787

Information Security Analysis in PT. XYZ Using ISO/IEC 27001:2013

Rivaldo Rizky Junior[1*], Rio Guntur Utomo[2], Dita Oktaria[3]
School of Computing, Telkom University, Bandung, Indonesia
**Email Corresponding Author*: rivaldojr@student.telkomuniversity.ac.id

Abstract

As a company engaged in the field of information technology, problems with information leakage, data loss, and so on can pose detrimental threats, so a security standard is needed to prevent information security leaks from occurring. The standard raised in this research is ISO 27001:2013. The method used in this research is interviews and observations of related employees and documents at PT. XYZ, the stages in this study refer to the standards in ISO 27001:2013. Currently, the company where this research was conducted does not yet have standards in accordance with ISO/IEC 27001:2013. Furthermore, this research is expected to improve the security system and also prevent security data leaks at PT. XYZ. As well as make recommendations or suggestions from the research results.

Keywords*: ISO/IEC 27001:2013; Information Security; Data Leak*

Abstrak

Sebagai perusahaan yang bergerak pada bidang teknologi informasi, permasalahan kebocoran informasi, kehilangan data, dan lain sebagainya dapat menimbulkan ancaman yang merugikan sehingga dibutuhkanlah suatu standar keamanan untuk mencegah terjadinya kebocoran keamanan informasi. Standar yang diangkat pada penilitian ini yaitu ISO 27001:2013. Metode yang digunakan pada penelitian kali ini adalah wawancara dan observasi terhadap pegawai terkait dan dokumen pada PT. XYZ. Tahapan pada penelitian ini merujuk dengan standar yang ada pada ISO 27001:2013. Saat ini perusahaan tempat penelitian ini dilakukan belum memiliki standar yang sesuai dengan ISO/IEC 27001:2013. Selanjutnya, penelitian ini diharapkan dapat meningkatkan sistem keamanan dan juga dapat mencegah kebocoran data keamanan pada PT. XYZ. Serta membuat rekomendasi atau saran dari hasil penelitian.

Kata Kunci: *ISO/IEC 27001:2013; Keamanan Informasi; Kebocoran Data.*

1. Introduction

Information technology is one of the developments of the times that is very profitable for many people, especially for organizations that run their companies in the field of technology and information. However, on the other hand, there are also many negative impacts resulting from the development of technology and information at this time, such as data theft and loss of data which may be important data for a company.

To assure or guarantee business continuity, minimize business risks, and be able to maximize or accelerate returns on investment and commercial prospects, information security is the safeguarding of facts against all potential dangers[1].

To guide organizational information security standards and information security management practices, including the selection, implementation, and management of controls that take into account the organization's information security risk environment, ISO 27001:2013 is an international standard for information security management systems (ISMS)[2].

PT. XYZ has not implemented standardization for its Information Security issues, so it is still prone to data leaks and other information security disturbances that can disrupt the company's business continuity. For this reason, using ISO 27001:2013 provides standardization of data and system security issues that exist in companies, which are expected to reduce or prevent security risks to data and systems. The consideration of using the ISO 27001 standard in this study is that this standard has the flexibility to be developed according to the company's needs and objectives, security requirements, business processes, number of employees, and the size of the organizational structure[3]. This goal focuses on improving information security at PT. XYZ.

2. Theoritical Basis

Research entitled Information Security Management System Analysis using ISO/IEC 27001 and ISO/IEC 27002 standards at the head office of PT. Jasa Marga from the results of ISO/IEC 27001 research, it is found that there is still a lack of attention from managerial parties regarding the determination and establishment of policies on information security, while the results from ISO/IEC 27002 can be seen that operational activities are already in the planning and tracking stages[4].

Furthermore, the research entitled Identification, assessment, and mitigation of information security risks based on ISO 27001:2005 and ISO 27002:2013 standards using the FMEA method (Case study: ISNET) produced 20 risks. The results of the assessment are categorized into five levels, namely very high, high, medium, low, and very low. Where one risk enters the very high level, three risks enter the high level, one risk enters the medium level, thirteen risks enter the low level and two risks enter the very low level[5].

As a result of further investigation into the Academic Management Information System Security Audit (SIMAK) at the Faculty of Economics, University of Udayana (FE UNUD), it was discovered that SIMAK FE UNUD was at maturity level 3, or Well Defined, indicating that there were already established standards and procedures[6].

The research entitled Information security management system planning based on ISO 27001:2013 standards at KOMINFO East Java Province resulted in risk identification, risk assessment, and risk response for each information asset. In addition, it provides recommendations for SOP documents that are in accordance with organizational needs[7].

The latest research entitled Information system security audit at the Bogor District Communication and Informatics Office using ISO/IEC 27001:2005 and COBIT 5 standards produces several recommendations that can be used to prevent or anticipate the impact that will occur if one day an incident of server damage and hacking incident occurs. From these recommendations, it can also be used as a reference for fixing existing gaps in ISO/IEC 27001:2013 security controls as material for planning an ISMS according to ISO/IEC 27001:2013 standards[8].

This study differs from other ones in that it looked at a private company that provided IT solutions, PT. XYZ. Additionally, this study employs the ISO 27001 standard to quantify and evaluate information security with various control provisions and goals in accordance with the findings of determining the requirements of PT. XYZ. In this study, maturity level assessment was conducted using Capability Maturity Model Integration (CMMI)[9]. This study intends to evaluate PT. XYZ's information security in accordance with ISO 27001 standards in order to identify a number of shortcomings and weaknesses so that it can make ideas and recommendations for management to improve corporate information security. Thus, it is anticipated that the findings of this study will be used as one of the references by PT. XYZ when making decisions about the construction and upgrading of information security systems.

3. Methodology

The research method used in carrying out an information security audit can be seen in Figure 2.

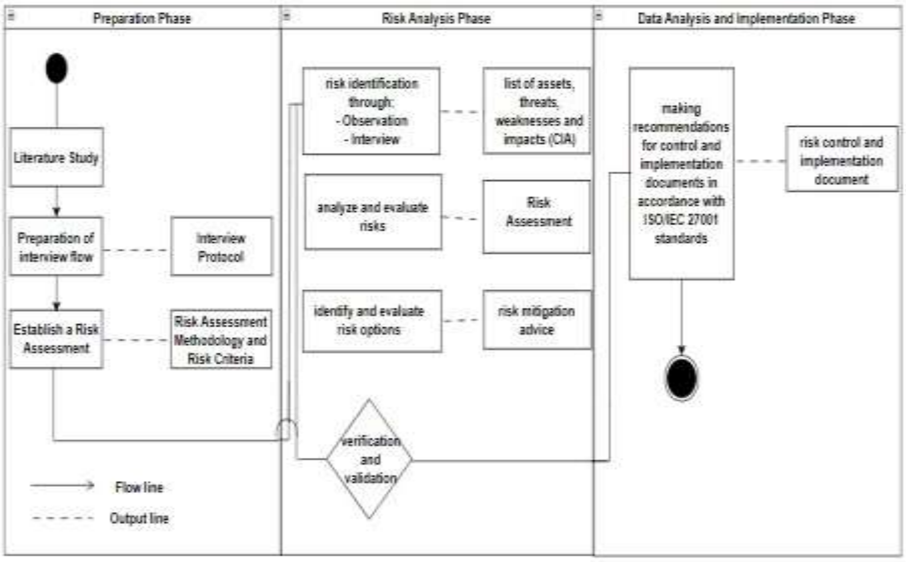

Preparation Phase
Risk Analysis Phase
Data Analysis and Implementation Phase
Literature Study
Preparation of interview flow
Interview Protocol
Establish a Risk Assessment
Risk Assessment Methodology and Risk Criteria
risk identification through:
- Observation
- Interview
list of assets, threats, weaknesses and impacts (CIA)
analyze and evaluate risks
Risk Assessment
identify and evaluate risk options
risk mitigation advice
verification and validation
making recommendations for control and implementation documents in accordance with ISO/IEC 27001 standards
risk control and implementation document
Flow line
Output line

Figure 1. Flowchart Methodology

A. Data Collection

There are several techniques or ways of collecting data used in this study, namely:

a. Interview
The interview is a process in carrying out research, especially in qualitative research[10]. Researchers conducted interviews directly with the IT staff of PT. XYZ.

b. field studies
Researchers conducted field studies in the form of observations and direct visits to PT. XYZ.

c. Literature Study
The literature study was carried out by researchers in the form of literature searches or references from books and journals related to ISO/IEC 27001:2013.

1) ISO/IEC 27001

According to Gehrmann, ISO/IEC 27001 is a standard that determines how an information security management system should be implemented[11]. The ISO/IEC 27001 standard is generally used to address information security challenges. According to Rahman, ISO 27001 can help establish and implement information security programs[12]. It can assist with various IT delivery and management procedures when used in conjunction with ITIL.

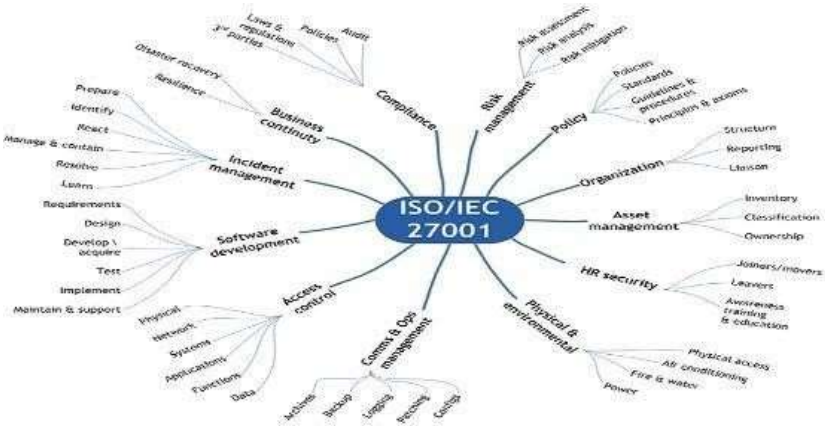


Figure 2. ISO/IEC 27001

So it can be concluded that ISO/IEC 27001 is a standard that can be used as a reference for carrying out organizational operations, so that information security is maintained and stable.

2) Capability Maturity Model Integration (CMMI)
Syafitri (2016) asserts that the CMMI evaluation process flow is divided into tiers. The evaluation was created specifically to obtain software that can promote process improvement and is based on a questionnaire. A maturity model called CMMI can be utilized in institutions to enhance procedures (process improvement). The goal of implementing CMMI within a company is to enhance the process of creating and enhancing the company's software product[13].
The following is a maturity level based on CMMI in general[14].

Table 1. Maturity Level Based on CMMI

Maturity Level	***Description***
0 – Incomplete	*There was no evidence that the company knew there are problems that need to be addressed.*
1 – Initial	*There is proof that the business is aware of issues that need to be fixed. However, there isn't a set procedure; instead, cases are handled individually or on a case-by-case basis. The process approach is generally disorganized.*
2 – Managed	*The process is developed into stages where the process has been planned, documented, and is reactive. For the same work, various parties adhere to the same procedures. Each person is left to learn procedures, standards, and duties on their own without any official training or communication. There is a high level of trust in individuals, allowing large errors to occur.*
3 – Defined	*Standardized, documented processes are then communicated through training. It then mandated that those processes should be followed. However, the storage cannot be found. Although not finished, the technique has institutionalized continuous practice.*
4 – Quantitively Managed	*Management keeps an eye on how well procedures are being followed, measures compliance, and takes corrective action when necessary. Processes are continuously being improved,*

	and good practices are offered. Automation and devices are used within certain limits
5 – Optimizing	*The process is already at the level of good practice, and the company's improvement. The business has adapted rapidly by using the results of the enhancements to increase quality and effectiveness.*

B. Defining Scope and Objectives

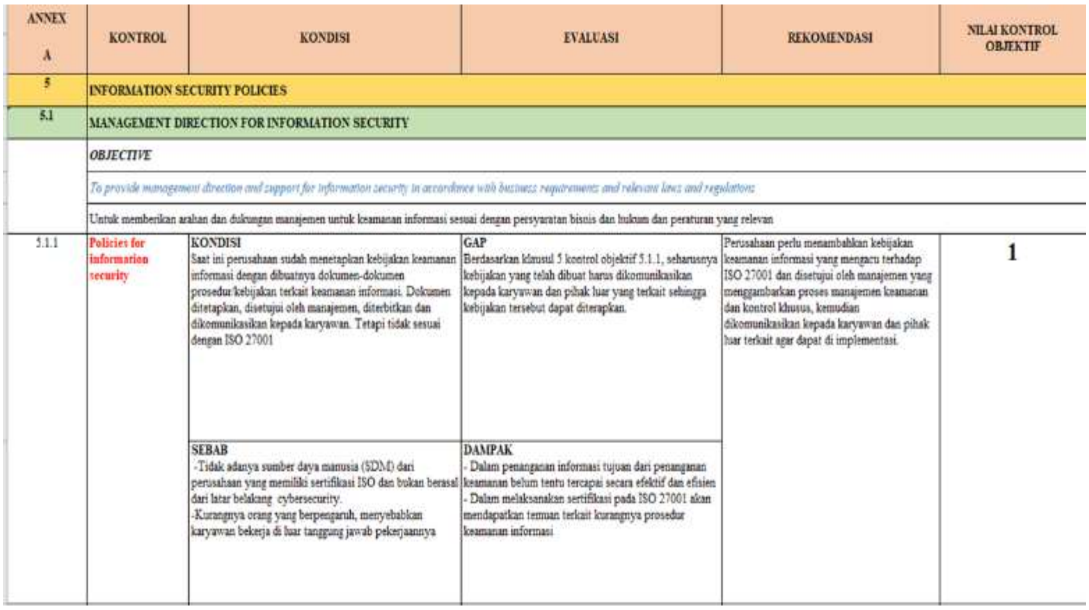
The scope of research was carried out by conducting interviews with PT. XYZ IT staff, field studies, and literature studies. The results of interviews with PT. XYZ IT staff, the clauses used in the ISO 27001: 2013 standard are determined. Table 1 is a mapping of the ISO 27001: 2013 clause based on the results of interviews with the IT staff of PT. XYZ.

Table 2. Clause

Clause
A.5 – Information Security Policy
A.6 – Information Security Organization
A.7 – Human Resources Security
A.8 – Asset Management
A.9 – Access Control
A.11 – Physical and Environmental Security

C. Determine Work Paper Gap Analysis

Researchers interviewed informants (workers of PT. XYZ) by asking them questions, and the answers were subsequently incorporated into the work paper gap analysis. To assess the effectiveness of information security implemented by research objects with information security standards ISO/IEC 27001:2013, a gap analysis was conducted. Below is an example of a gap analysis work paper used in this study.

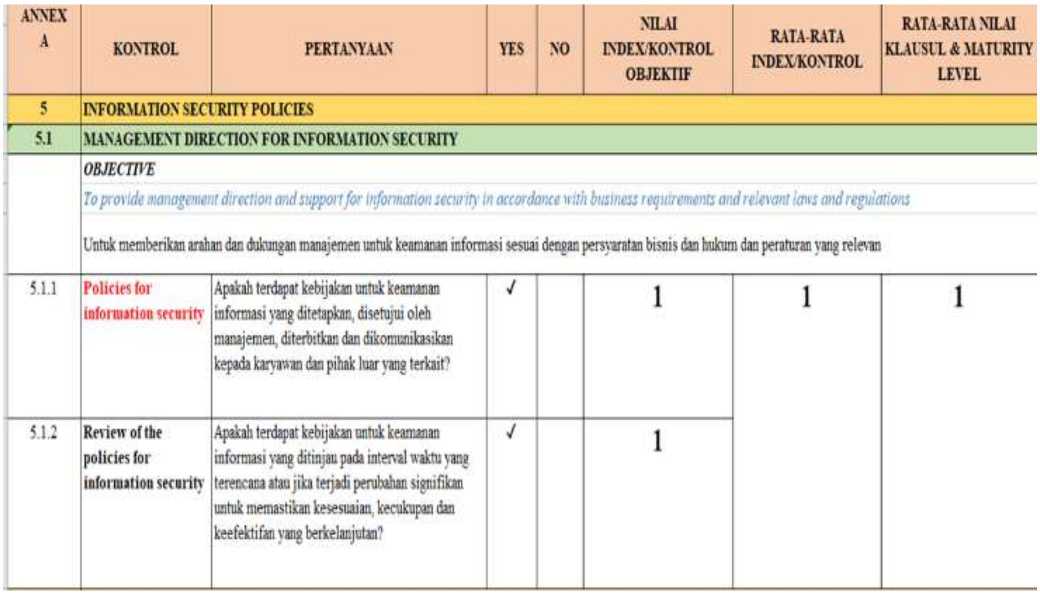


ANNEX A	KONTROL	KONDISI	EVALUASI	REKOMENDASI	NILAI KONTROL OBJEKTIF
5	INFORMATION SECURITY POLICIES				
5.1	MANAGEMENT DIRECTION FOR INFORMATION SECURITY				
	OBJECTIVE				
	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations				
	Untuk memberikan arahan dan dukungan manajemen untuk keamanan informasi sesuai dengan persyaratan bisnis dan hukum dan peraturan yang relevan				
5.1.1	Policies for information security	KONDISI Saat ini perusahaan sudah menetapkan kebijakan keamanan informasi dengan dibuatnya dokumen-dokumen prosedur kebijakan terkait keamanan informasi. Dokumen ditetapkan, disetujui oleh manajemen, diterbitkan dan dikomunikasikan kepada karyawan. Tetapi tidak sesuai dengan ISO 27001	GAP Berdasarkan klausul 5 kontrol objektif 5.1.1, seharusnya kebijakan yang telah dibuat harus dikomunikasikan kepada karyawan dan pihak luar yang terkait sehingga kebijakan tersebut dapat diterapkan.	Perusahaan perlu menambahkan kebijakan keamanan informasi yang mengacu terhadap ISO 27001 dan disetujui oleh manajemen yang menggambarkan proses manajemen keamanan dan kontrol khusus, kemudian dikomunikasikan kepada karyawan dan pihak luar terkait agar dapat di implementasi.	1
		SEBAB -Tidak adanya sumber daya manusia (SDM) dari perusahaan yang memiliki sertifikasi ISO dan bukan berasal dari latar belakang cybersecurity. -Kurangnya orang yang berpengaruh, menyebabkan karyawan bekerja di luar tanggung jawab pekerjaannya	DAMPAK - Dalam penanganan informasi tujuan dari penanganan keamanan belum tentu tercapai secara efektif dan efisien - Dalam melaksanakan sertifikasi pada ISO 27001 akan mendapatkan temuan terkait kurangnya prosedur keamanan informasi		

Figure 3. Work Paper Gap Analysis

D. Determine Maturity Level

The information obtained from the work paper gap analysis is assessed using a maturity level. The maturity level assessment table index used in this audit activity can be seen in Figure 4, the following is an example of a table and its assessment.



ANNEX A	KONTROL	PERTANYAAN	YES	NO	NILAI INDEX/KONTROL OBJEKTIF	RATA-RATA INDEX/KONTROL	RATA-RATA NILAI KLAUSUL & MATURITY LEVEL
5	INFORMATION SECURITY POLICIES						
5.1	MANAGEMENT DIRECTION FOR INFORMATION SECURITY						
	OBJECTIVE *To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations* Untuk memberikan arahan dan dukungan manajemen untuk keamanan informasi sesuai dengan persyaratan bisnis dan hukum dan peraturan yang relevan						
5.1.1	Policies for information security	Apakah terdapat kebijakan untuk keamanan informasi yang ditetapkan, disetujui oleh manajemen, diterbitkan dan dikomunikasikan kepada karyawan dan pihak luar yang terkait?	✓		1	1	1
5.1.2	Review of the policies for information security	Apakah terdapat kebijakan untuk keamanan informasi yang ditinjau pada interval waktu yang terencana atau jika terjadi perubahan signifikan untuk memastikan kesesuaian, kecukupan dan keefektifan yang berkelanjutan?	✓		1		

Figure 4. Maturity Level

The formula for obtaining the value of the Maturity level is as follows.

$$\text{Rata - rata indeks/kontrol}(n) = \frac{\text{Total Nilai Indeks / Kontrol objektif (n)}}{\text{Total kontrol Objek (n)}}$$

After averaging the maturity level value of each clause. The following is the average formula for the maturity level value.

$$\text{Rata - rata Nilai Klausul}(n) = \frac{\text{Total Nilai Indeks / Kontrol objektif (n)}}{\text{Total kontrol Objektif (n)}}$$

The final results of the maturity level assessment can be seen in the following table.

Table 3. Maturity Level Result Index

Maturity Index	Maturity Level
0.00 - 0.49	0 *Incomplete*
0.50 - 1.49	1 *Initial*
1.50 – 2.49	2 *Managed*
2.50 – 3.49	3 *Defined*
3.50 – 4.49	4 *Quantitatively Managed*
4.50 – 5.00	5 *Optimized*

4. Result & Discussion

4.1. Audit Activity

Audit activities at PT. XYZ carried out a series of audit processes starting from submitting an audit permit to preparing the report described in Table 4.

Table 4. Audit Activities

No	Activity	Duration	September				October				November				December			
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Literature Study ISO/IEC 27001:2013	2 Month	■	■	■	■	■	■	■	■								
2	Create Audit Questions	1 Month					■	■	■	■								
3	Create Gap Analysis Workpapers	2 Week					■	■										
4	Workpaper Maturity Level	1 Month					■	■	■	■								
5	A.5 – Information Security Policy	1 Week									■							
6	A.6 – Information Security Organization	1 Week									■							
7	A.7 – Human Resources Security	1 Week										■						
8	A.8 – Asset Management	1 Week										■						
9	A.9 – Access Control	1 Week											■					
10	A.11 – Physical and Environmental Security	1 Week											■					
11	Analysis of Audit Results	1 Month												■	■	■	■	■
12	Research Report Writing	4 Month	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

This study effort spanned 4 months, and in September and October, investigations and inquiries were conducted to prepare for the audit. The last step of analysis and reporting of audit results is then carried out for 1 month in December after the audit operations are completed for 1 month in November.

4.2. Respondent Data

In conducting this research, the primary data obtained came from structured interviews with informants who could represent the company and have responsibilities, then observed and studied the documents available at PT. XYZ. As for some of the respondents, namely staff from PT. XYZ which helped become the source of this research is shown in the table below.

Table 5. Respondent

No	Name
1	Kevin Ahmad Nasution
2	Ridho Vivyan Adam
3	Muhammad Hilmi Faisal
4	Fariz
5	Steven C. H

4.3. Data Reduction

Based on the results of the data that has been obtained in different formats, the first analysis to be carried out is to reduce the results of interviews, direct observation, or document policies/procedures that exist in the company. The following is the result of the reduction of the data described in the table.

Table 6. Data Reduction

Clause	Summary
A.5 – Information Security Policy	Work instructions and policies have been made, but are not in line with ISO/IEC 27001; instead, they are based on the organization's internal standards. Annually, the corporation evaluates them, but review operations are handled by staff members with auditing expertise and experience in information security.
A.6 – Information Security Organization	There is no policy or process paper on the division of responsibilities, even though the organization has segregated and divided staff roles.
A.7 – Human Resources Security	Although an examination has been carried out, it is not carried out thoroughly. There is a contract between the company and its employees, but it does not contain all of the penalties that will be applied in the event of an information security breach. Information security education and training have been provided, but not yet. There is no disciplinary matrix, no definition of the level of information security violations, and only the dismissal of personnel is defined as a sanction. However, work was stopped according to safety regulations.
A.8 – Asset Management	Even though asset ownership and custody have been finalized, there is no documented policy or process governing the distribution of client assets and data obtained from customers. Even though asset returns have been made, asset lending is still not fully under control. Return documents also need to be checked again. Relevant asset management documentation will need to be updated to reflect the disposal of customer assets. Assets have been categorized and labeled, but management has not fully built on these classifications. Transfer of assets, write-off of assets, and monitoring of the use of released media are not yet fully by the norms. Documentation needs to be added regarding the assets.
A.9 – Access Control	Although access controls are in place, they are not fully adequate, and review activities are not carried out effectively. Access to the program code has not been completely blocked, and authentication selection has not been explained. Instances have been hardened and decoupled, although there are currently no reference documents.
A.11 – Physical and Environmental	Environmental protection has been outlined, documented, analyzed, and evaluated, but

Security	not yet fully put into practice. The wiring lacks instructions, and there is insufficient oversight of equipment maintenance. Not properly defined, documented, or implemented how to dispose or reuse assets. Equipment outside the company is not fully guaranteed and controlled. Employees do not fully understand and are familiar with deleting tables and layers.

4.4. Maturity Result

The ISO 27001:2013 standard used is the Security Control section which consists of 51 control objectives and 114 security controls. To find out the weak controls, the management of PT. XYZ takes action to correct those controls that need addressing.

The maturity level value is obtained from the average results of the respondents' answers contained in the ISO 27001: 2013 clause. Table 7 is the result of calculating the questionnaire to obtain the maturity level of information security.

Table 7. Maturity Level Result PT. XYZ

Clause	Level	Description
5 – Information Security Policy	1	*Initial*
6 – Information Security Organization	1,45	*Initial*
7 – Human Resources Security	2,33	*Managed*
8 – Asset Management	1,27	*Initial*
9 – Access Control	1,35	*Initial*
11 – Physical and Environmental Security	1,38	*Initial*
Average	**1,46**	***Initial***

4.5. Discussion

Figure 5, is a graph of the comparison of the current maturity level value with the expected maturity level value.

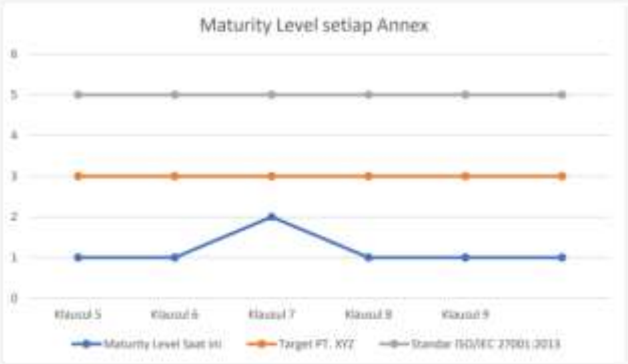


Figure 5. Comparison Maturity Level Graph

Based on the results of the calculation of the information security maturity level, the level of information security as a guide is at Level 3 (Defined Process). Based on the results of the maturity level calculation that has been done, the information security maturity level at PT. XYZ on average is at Level 1 (Initial Process). Means that information security at PT. XYZ needs improvement and needs to be developed at a better next stage because it is still at Level 1 (Initial Process).

A more detailed explanation of the graph in Figure 5, namely:

1. Information security of PT. XYZ regarding Information Security Policy is at level 1 (initial). Due to the policies made by PT. XYZ has not been distributed to workers and other related parties, the policy has not been enforced. As a result, problems that arise are usually handled individually or on a case-by-case basis and are disorganized. To increase it can be done:
   - Policy is communicated to staff members and relevant external parties for implementation.
   - The proposed ISMS implementation will need to schedule regular reviews at least once a year or more frequently if there are substantial changes in the environment or technology.
2. Information security PT. XYZ related to Information Security Organization is at level 1 (initial). To manage the risks associated with the use of mobile devices, supporting security policies and procedures, as well as information security roles and responsibilities, have not been established and defined. However, there is no standard process. In general, the process approach is not organized. To increase it can be done:
   - To control the risks associated with the use of mobile devices, information security responsibilities are defined and defined, and appropriate security policies and measures must be developed.
   - Procedures that must exist in PT. XYZ determines when and by whom authorities (law enforcement, regulatory agencies, supervisory authorities, POLRI's cybercrime unit, and others) should be contacted, as well as how identified information security incidents must be reported promptly (eg. when there is a suspicion that a breach has occurred law).
   - PT. XYZ should actively foster positive relationships with security-related trade communities, forums, and organizations such as ISACA, CISO Forum, and others.
3. Information security PT. XYZ regarding Human Resources Security is at level 2 (Managed). Procedures and policies of PT. XYZ is standardized and documented, but does not yet fully reflect ongoing practice. To increase it can be done:
   - Personnel assigned to work on information security duties must undergo further screening to ensure they have the required competence.
   - PT. XYZ shall develop written policies for employee and contractor contractual obligations that reflect the organization's policies regarding information security, confidentiality, data protection, ethics, and the proper use of organizational facilities and equipment, as well as the good practices expected of the organization.
4. Information security PT. XYZ regarding Asset Management is at level 1 (initial). Because of PT. XYZ does not yet have rules and procedures governing asset management, assets related to information and information processing facilities have not been identified, and an inventory of assets owned has not been properly recorded and maintained. To increase it can be done:
   - It is important to identify information-related assets and facilities for information processing, and to document and maintain an accurate inventory of the assets held.
   - PT. XYZ needs to implement procedures that can quickly identify who is responsible for each asset developed or transferred to the company and who is responsible for the people responsible for each asset.
   - PT. XYZ must establish legal procedures that mandate that after the termination of employment, contracts, and employment agreements, all staff, employees, and external users must return all company assets that they own.
5. Information security PT. XYZ regarding Access Control is at level 1 (Initial). Most of the restrictions necessary to enforce access control have already been implemented, whether through the operating system, database, or application system. However, the use of these restrictions is still not based on formal policies and methods, and so they are not always consistent, efficient, or ideal. To increase it can be done:
   - With various specificities and tight controls reflecting related information security threats, PT. XYZ must define appropriate access control rules, access rights, and restrictions for specific user roles on assets.

- By the established access control policy, PT. XYZ must establish explicit policies for network usage and network services.

6. Information security PT. XYZ regarding Physical and Environmental Security is at level 1 (Initial). PT. XYZ, but methods are standardized, and activities are completed individually or on a case-by-case basis, so the process is disorganized. Concerns and knowledge of information security for the environment are still lacking. To increase it can be done:
    - Improve physical entry controls, such as registration of guests to enter and exit facilities and implementation of RFID-based access control devices for key areas.

The company has not implemented and documented information security in line with ISO/IEC 27001:2013, according to the aforementioned rationale and maturity results. In order to increase information security to a higher degree, businesses must add and build procedures. They also need to hire and train workers who understand information security. The outcomes of the recommendations should be taken into account and used as a guide in order to keep PT. XYZ's information security compliant with ISO/IEC 27001:2013 standard.

5. Conclusion

The following conclusions are reached as a consequence of research conducted at PT. XYZ utilizing ISO 27001:2013: The information security measures put in place by PT. XYZ does not adhere to ISO/IEC 27001:2013. The average annex value is still below the standard of ISO/IEC 27001:2013 because of PT. XYZ only implemented 51 of the 114 objective controls, its application of ISO/IEC 27001:2013 was 44.73% with an Initial maturity level or its implementation of ISO/IEC 27001:2013 was not organized.

Based on the conclusions obtained, the suggestions that can be given by researchers are as follows:

All control objectives in ISO/IEC 27001:2013 must be implemented by PT. XYZ, including developing policies and procedures related to information security, assessing and improving documented policies and procedures, and exercising control over policies and procedures that have been documented but not yet practiced and all information security measures of PT. XYZ needs improvement. Employee training is needed to standardize, document, and communicate the process so that it can be used to implement and implement the requirements of ISO/IEC 27001:2013.

Reference

[1] “International Standard ISO/lEe FDIS 27002 Information technology-Security techniques-Code of practice for information security controls Technologies de l’information-Techniques de securite-Code de bonne pratique pour Ie management de la securite de l’information(E) Copyright Protected Document” 2013. [Online]. Available: www.iso.org

[2] “Information technology-Security techniques-Information security management systems-Requirements ISO/IEC 27001 International Standard (E) ii Copyright Protected Document”

[3] R. Sarno dan I. Iffano. Sistem Manajemen Keamanan Informasi, Surabaya: ITS Press, 2009.

[4] N. F. Octariza, “Analisis Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO/IEC 27001 dan ISO/IEC 27002 Pada Kantor Pusat PT. Jasa Marga,” 2019.

[5] D. Pembimbing, B. Cahyo, S. Si, M. K. Hanim, M. Astuti, and S. Kom, “Menggunakan Metode FMEA (Studi Kasus: ISNET) Krisna Harinda Dewantara NRP 5211 100 148.”

[6] Y. C. N. Bless, G. M. A. Sasmita, dan A. A. K. A. Cahyawan, “Audit Keamanan SIMAK Berdasarkan ISO 27002 (Studi Kasus: FE UNUD)”, Menara Penelitian Akademika Teknologi Informasi, vol. 2, no. 2, pp. 162-166, 2014.

[7] P. Studi, “Pada KOMINFO Provinsi Jawa Timur Tugas Akhir,” 2019.

[8] Maulana MM, “Audit Keamanan Sistem Informasi pada Dinas Komunikasi dan Informatika Kabupaten Bogor Menggunakan Standar ISO/IEC 27001:2005 dan COBIT 5,” 2019.

[9] A. Deswadi dan B. Hudaya, “Audit Pengembangan Perangkat Lunak Menggunakan Metode Capability Maturity Model Integration Level 3”, Jurnal Informatika, vol. 7, no. 2, pp. 148-155, September 2020.

[10] M. Rosaliza, “Wawancara, Sebuah interaksi komunikasi dalam penelitian kualitatif,” Jurnal Ilmu Budaya, vol. 11, no. 2, pp. 71–79, 2015.

[11] Maico Gehrmann, “Combining ITIL, COBIT And ISO/IEC 27002 For Structuring Comprehensive Information Technology For Management In Organizations,” Revista de Gestão e Tecnologia, vol. 2, 2012.

[12] A. N. Rahman, H. Tanuwijaya, and E. Sutomo, “Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Berdasarkan ISO 27002:2005 Pada Rumah Sakit Islam Jemursari,” 2016.

[13] P. D. Syafitri, “Penilaian kualitas pengembangan sistem informasi pada perusahaan distributor,” IQRA: Jurnal Ilmu Perpustakaan dan Informasi (e-Journal), vol. 10, no. 1, pp. 15–27, 2016.

[14] E. Elue, “Effective Capability and Maturity Assessment Using COBIT 2019,” COBIT Focus, 2020.

[15] M. Rosaliza, “Wawancara, Sebuah interaksi komunikasi dalam penelitian kualitatif,” Jurnal Ilmu Budaya, vol. 11, no. 2, pp. 71–79, 2015.