p–ISSN: 2723 - 6609 e-ISSN: 2745-5254
Vol. 4, No. 9 September 2023 http://jist.publikasiindonesia.id/

ASSESSING INFORMATION SECURITY MANAGEMENT USING ISO 27001:2013

Stella Clarissa, Gunawan Wang
Bina Nusantara University Jakarta, Indonesia
Email: stella.clarissa@binus.ac.id

*Correspondence

ARTICLE INFO

Accepted : 01-09-2023
Revised : 14-09-2023
Approved : 25-09-2023

Keywords: information security; maturity level; ISO/IEC; ISO 27001:2013.

ABSTRACT

To ensure operational continuity, reduce risks to businesses, and optimize investment returns and business opportunities, information security is an essential element in ensuring the protection of information from different threats. Information protection may be facilitated by the implementation of international standard frameworks, given that a set of standards or provisions is needed to achieve and maintain an adequate level of safeguards for the use of assets. The Ministry of XYZ is handling various important, highly confidential, and sensitive data. Therefore, information protection is not only essential but also mandatory. The organization has implemented ISO 27001:2013 in Pusat Data dan Teknologi Informasi (Pusdatin) and called the security management standard Sistem Manajemen Keamanan Informasi (SMKI). However, according to the Cyber Security Maturity assessment result by a public institution in 2022, there is still a wide gap between the technical implementation and the governance itself. Therefore, to improve the good governance of information security, we need to specifically evaluate the maturity of SMKI itself. This study will use the ISO 27001:2013 Compliance Checklist.

Introduction

Information security, with its role of protecting information against various threats, is essential to ensure continued operations, minimize business risks, and optimize return on investment and business opportunities (Bawono, Soetomo, & Apriatin, 2020). The implementation of an international standard framework can enable information protection due to the urgency to achieve or maintain an appropriate level of protection for the use of assets (Disterer, 2013).

The Ministry is handling various important, highly confidential, and sensitive data such as public workers' profiles (performance evaluation, work permit, etc.), personal reports for medical insurance, and/or feasibility studies for new technology registration. It has implemented ISO 27001:2013 in Pusdatin to ensure that all resources are managed as intended and all possible risk is mitigated and controlled. They have developed standards, policies, and procedures called Sistem Manajemen Keamanan Informasi (SMKI). However, according to one Cyber Security Maturity assessment in 2022, which assessed the maturity of the governance, identification, protection, detection, and response process area, it showed that the lowest score is in the governance area (3,16) while the detection and identification area came as the first and second with the highest

score (4,34 and 3,93). There is still a wide gap between the technical implementation and the governance itself (Yasin, Arman, Edward, & Shalannanda, 2020).

Another consideration taken is regarding the number of threats that occurred in a specific period. According to (Ella et al., 2021), The primary security risks faced by public sector data centers include technical vulnerabilities, social engineering attacks, and intentional human threats. These were succeeded by risks such as spyware, phishing, and bluesnarfing. It is aligned with what happened in the Ministry for the first half year (January-June) in 2023. There are 37.945 threats detected which consisted of trojan, worm, virus, and potentially unwanted applications as shown in Table 1 below.

Table 1
List of Detection in the Ministry

Detection Type	Total
Trojan	6,571
Worm	74
Virus	2
Potentially unsafe application	990
Potentially unwanted application	29,492
Suspicious application	162
Application	654
Total	37,945

A thorough evaluation regarding SMKI implementation has never been carried out. Therefore, to improve the good governance of information security, we plan to evaluate the maturity of SMKI itself. SMKI is developed based on ISO 27001:2013. ISO 27001:2013 is an international standard used to provide, manage, and developing information security management systems to be a tool for measuring and controlling Information Security (COMPUTING, 2019).

The scope of this research is SMKI which has been implemented in the Pusdatin area of The Ministry. This research uses quantitative and qualitative research methods to discover underdeveloped components of SMKI and provides recommendations for improvement. Qualitative research is conducted by literature study on ISO 27001:2013 and by interviewing Pusdatin to obtain the expected number at the maturity level that will be used in gap analysis. Quantitative research was carried out by conducting questionnaires on research respondents (Pusdatin) and performing analysis on the questionnaire responses (Fathurohman & Witjaksono, 2020). This study is to provide an overview of the information technology (IT) security management that has been put in place, which will lead to recommendations for a broader improvement and development of IT governance.

Information Security

(Monev, 2020) defines information security as ensuring information is protected from confidentiality breaches, and maintaining integrity and availability when needed. Information security is a business enabler that is closely related to all stakeholders to gain a competitive advantage. The protection of sensitive information from unauthorized activities such as monitoring, modification, recording, and any damage or destruction shall be ensured by IT security. ISACA (2015) states that the objective of information security is to guarantee the security and confidentiality of critical information, including customer account specifics, financial data, and proprietary business knowledge. Information security can be threatened because of events that have the potential to expose to risk the company's information resources or by people and/or organizations who may feel that they have no time for it, that they are not interested in it, or that they do not care to learn about it (Zammani & Razali, 2016). The threat may arise from inside and outside the organization, but it may also be accidental or deliberate (Somepalli, Tangella, & Yalamanchili, 2020). Other types of threats to the security of IT systems may also differ, e.g. physical damage which can be caused by an earthquake, sudden events, loss of important services like power or telecommunication information and functionality compromise as well as technical failure (Aedah & Hoga, 2020).

ISO 27001:2013

ISO is an international standard for management systems that provides models related to regulation and operations management systems. The initial release of the standard occurred in 2005 through a collaborative effort between the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It underwent revisions in 2013 and, more recently, in 2022. ISO / IEC 27001 stands as the foremost acknowledged standard within its category, outlining prerequisites for information system management (Bawono et al., 2020). ISO/IEC 27001 outlines criteria to guarantee the selection of suitable and balanced safeguards for safeguarding information assets. It also aims to instill confidence in stakeholders by facilitating the effective planning and establishment of an information system management within any entity (Shammugam et al., 2021).

ISO 27001:2013 presents a set of obligatory stipulations regarding the establishment and functioning of IT security. This encompasses risk management, control measures, and actions to alleviate risks linked to information assets that an organization intends to protect according to its Information Security Process (ISO/IEC, 2016). ISO 27001: 2013 contains 2 major parts:

1. Clause, is the prerequisite that an organization needs to be fulfilled by ISO 27001:2013
2. Annex A, is a reference document that can be utilized as guidance in control selection. There are 14 group domains, 35 target controls, and 114 controls defined in Annex A ISO 27001:2014

Table 2
Group Domain ISO 27001:2013

Annex	Group Domain
A.5	Information security policies
A.6	Organization of information security
A.7	Human resource security
A.8	Asset management
A.9	Access control
A.10	Cryptography
A.11	Physical and environmental security
A.12	Operation security
A.13	Communications security
A.14	System acquisition, development, and maintenance
A.15	Supplier relationships
A.16	Information security incident management
A.17	Information security aspects of business continuity management
A.18	Compliance

Process Capability Model

Using the maturity model, it is possible to measure the maturity level of information security implementation. The maturity model functions as a technique for gauging the stages of advancement in process management, consequently evaluating the proficiency of IT security skills held by managers. Process maturity levels provide a means of categorizing organizations according to their effectiveness in managing their diverse processes (Aedah & Hoga, 2020).

Process capability is used to define if a deliverable satisfies indicated item quality, service quality, and process performance objectives (Butzer, Schötz, & Steinhilper, 2017). A capable process always gives results that meet the required standards. This means that the process can be relied upon to consistently produce predictable outcomes. Process capability levels categorize the performances of relevant processes within a certain process area in an organization. The Process Capability Model is an assessment model based on ISO/IEC 15504 which underlines the framework with best practices and standards acceptable on a global scale (Walker, McBride, Basson, & Oakley, 2012).

Table 3
Capability Scale of Process Capability Model

Capability Scale (Index)	Capability Value	Capability Level
0,00 – 0,50	Level 0	Incomplete Process
0,51 – 1,50	Level 1	Performed Process
1,51 – 2,50	Level 2	Managed Process
2,51 – 3,50	Level 3	Established Process
3,51 – 4,50	Level 4	Predictable Process
4,51 – 5,00	Level 5	Optimizing Process

Research Methods

This research studies the application of information security that has been implemented by the Ministry and evaluates the level of maturity by adopting the process assessment model from ISO 15504-6:2003 to identify information security readiness by Annex A of ISO 27001:2013. In this research, the authors used different methods to find areas in information security that are not fully developed yet. The quantitative and qualitative research methods are used to provide recommendations for developing organizational conditions based on these findings. Qualitative research was carried out by observing and studying literature on ISO 27001:2013 so that the results obtained would be the mapping between ISO 27001:2013, then through an interview process with the IT Department, the expected maturity level was obtained. which then becomes the basis of assessment in the gap analysis. Quantitative research was conducted using a questionnaire given to research respondents (Pusdatin) and an analysis of the results of the questionnaire was carried out to obtain the level of maturity and gap analysis of ISO 27001:2013.

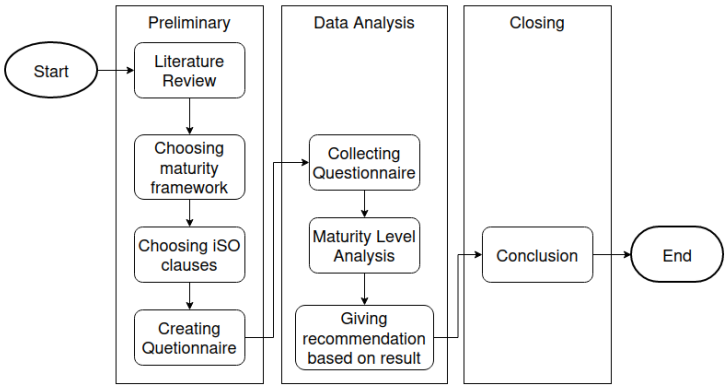

Figure 1 Research method

Data Collection

This study uses questionnaires as an instrument for collecting information, which can be seen in Figure 2. This survey shall include questions that are part of the compliance check carried out by Integrated Assessment Services and IAS. The analysis is conducted using a Microsoft Excel tool. Data analysis is carried out based on 34 valid responses from a total of 36 respondents for this study.

Organization Profile

Ministry of XYZ is one of the public sector in the Indonesian government which holds a strategic important role. Since 2020, it has implemented ISO 27001:2013 to ensure that all resources are managed as intended and all possible risk is mitigated and controlled. They have developed standards, policies, and procedures called Sistem Manajemen Keamanan Informasi (SMKI). As part of continuous improvement, the Ministry of XYZ wants to evaluate the maturity of SMKI which has been implemented.

Organization Structure

As mentioned in the scope of this research, Pusdatin which is one of the sections in the ministry of XYZ, consists of several work teams to handle different tasks such as

database management, public information and communication, planning, and development of information systems, information technology & infrastructure management, information security, and development and innovation of health technology.

Maturity Level Analysis

In conducting the maturity level analysis, the data obtained from the questionnaire is processed using the calculation formula for the Total Maturity Level (TML) for ISO 27001:2013 which can be seen below.

$$\frac{\frac{\sum A501}{n_{A501}} + \cdots + \frac{\sum A5n}{n_{A5n}} + \frac{\sum A601}{n_{A601}} + \cdots + \frac{\sum A6n}{n_{A6n}} + \cdots + \frac{\sum A1801}{n_{A1801}} + \cdots + \frac{\sum A18n}{n_{A18n}}}{n}$$

Legends

n = Number of processes in ISO 27001:2013

$nA.x.x$ = Number of response feedback from the questionnaire for each (Annex) control in ISO 27001:2013

After conducting a maturity level analysis and knowing the expected score of the information security maturity level in the Ministry, a gap analysis is carried out by calculating the gaps for each Annex A in ISO 27001: 2013 with the formula:

$$Gap = Expected\ Score - Current\ Maturity\ Score$$

Results and Discussion

Maturity Level of ISO 27001:2013

Based on the processed questionnaire, the existing maturity level and the expected maturity level are shown in Table 4

Table 4
ISO 27001:2013 Maturity Level

Annex A	Description	Score	Maturity Level
A.5	Information security policies	3.42	3 – Established
A.6.	Organization of information security	3.02	3 – Established
A.7	Human resource security	3.38	3 – Established
A.8.	Asset management	3.33	3 – Established
A.9.	Access control	3.36	3 – Established
A.10	Cryptography	2.43	2 – Managed
A.11.	Physical and environmental security	3.02	3 – Established

A.12	Operation security	3.08	3 – Established
A.13	Communications security	3.20	3 – Established
A.14	System acquisition, development, and maintenance	2.94	3 – Established
A.15	Supplier relationships	2.88	3 – Established
A.16	Information security incident management	2.87	3 – Established
A.17	Information security aspects of business continuity management	3.06	3 – Established
A.18	Compliance	2.66	3 – Established
Average		**3.05**	**3 – Established**

In the analysis of the survey data, it was found that there is a value of 3.05 for Pusdatin's IT security control within the Ministry. This value is an indication of the maturity being on 3rd level, i.e. established. A graph of maturity values is presented in Figure 2, taking into account the results shown in Table 3 for all ISO 27001:2013 clauses.

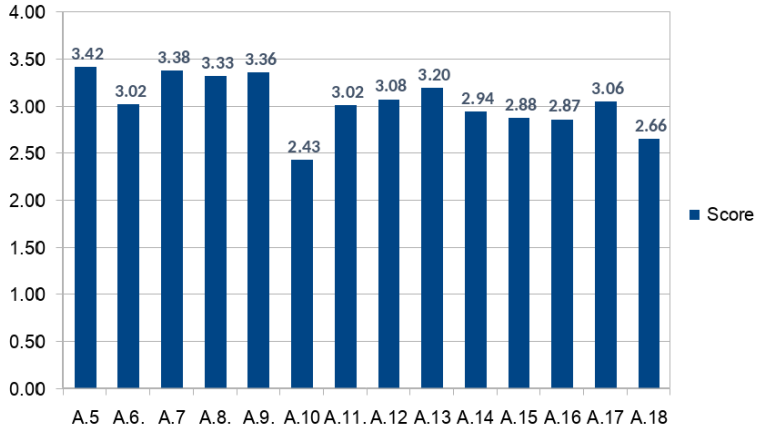

Figure 2 ISO 27001:2013 Maturity Level Graph

Gap Analysis

The maturity level according to ISO 27001:2013 is at 3.05 (Managed) and the expected value of maturity level is 5 (Optimized). Table 6 provides an analysis of the divergence between maturity levels.

Table 5
Gap Analysis ISO 27001:2013

ISO 27001:2013

Annex A	Description	Current Score	Expected Score	GAP
A.5	Information security policies	3.42	5	1.58
A.6.	Organization of information security	3.02	5	1.98
A.7	Human resource security	3.38	5	1.62
A.8.	Asset management	3.33	5	1.67
A.9.	Access control	3.36	5	1.64
A.10	Cryptography	2.43	5	2.57
A.11.	Physical and environmental security	3.02	5	1.98
A.12	Operation security	3.08	5	1.92
A.13	Communications security	3.20	5	1.80
A.14	System acquisition, development, and maintenance	2.94	5	2.06
A.15	Supplier relationships	2.88	5	2.12
A.16	Information security incident management	2.87	5	2.13
A.17	Information security aspects of business continuity management	3.06	5	1.94
A.18	Compliance	2.66	5	2.34
Average		3.05	**5**	1.95

From Table 5, it is known that Annex A.10 has the highest score of gap (2.57), followed by Annex A.18 (2.34) and Annex A.16 (2.13). Annex 5 has the lowest score of gap (1.58), followed by Annex A.7 & A.9.

This assessment also shows the weaknesses of some policies which have already been put in place. By following this initial check and implementing the suggestions, it is expected to improve current controls and reduce known intrusion events.

Evaluation & Recommendation

Based on research results related to the implementation of information security at the Ministry of XYZ, it can be concluded as follows: Information security maturity readiness is at Level 3 (Defined). It means that the processes have been implemented In a structured and methodical approach to work (carefully planned, tracked, and adjusted), and its resulting outputs are accurately specified, managed, and maintained. It also shows that the processes are well-understood by all Pusdatin staff since standards and procedures

are existing to provide guidance. However, we found several problems based on the highest gap level:

1. The policies on cryptography management, system procurement, development and maintenance, incident management in information security, as well as adherence to regulations, have been implemented. All the policies have been communicated and socialized to all Pusdatin workers.

However, there is no post-test on the training mechanism to ensure that all the staff understand the policies and procedures. From the findings on this matter, some recommendations were made to improve the state of information security within the Ministry of XYZ as follows:

Develop a more comprehensive training program for all Pusdatin staff and make sure the post-test is mandatory.

Future work

The initial audit of information security at Pusdatin within the XYZ Ministry adopting ISO 27001:2013 assessed its maturity using the SSE-CMM evaluation scale adjusted to ISO 15504-6:2013 capability levels. For future research purposes, other maturity models such as ISO 27017/8:2013, COBIT5 for Information Security, or NIST could be employed to compare the effectiveness of these models alongside different information security standards. This would contribute to a more comprehensive integration of not just the ISMS, but also IT governance.

Conclusion

This article summarizes the progress made in applying the Information Security Framework to the public sector. The paper explores the advantages of employing ISO 27001:2013 for the assessment and quantification of information security implementation. It also addresses the determination of information security capability (level of maturity) within the XYZ Ministry. Though ISO 27001 is required to show customers, suppliers, and stakeholders that the organization can keep information data safe and secure, there is still a need for further evaluation against the standard and ongoing surveillance audits to ensure ongoing compliance. The analysis benefits provided by this article are as follows: Firstly, exploiting maturity levels and gaps can give insight into the weak points of both information security. Second, it could open up further discussion and assessment on how to improve the management of information security within organizations in the future.

Bibliography

Aedah, Abd Rahman, & Hoga, Saragih. (2020). Maturity framework analysis ISO 27001: 2013 on indonesian higher education. *International Journal of Engineering & Technology*, *9*(2), 429–436.

Bawono, Marastika Wicaksono Aji, Soetomo, Mohammad Amin, & Apriatin, Thata. (2020). Analysis correlation of the Implementation Framework COBIT 5, ITIL V3 and ISO 27001 for ISO 10002 Customer satisfaction. *ACMIT Proceedings*, *7*(1), 31–46. https://doi.org/10.33555/acmit.v7i1.105

Butzer, Steffen, Schötz, Sebastian, & Steinhilper, Rolf. (2017). Remanufacturing process capability maturity model. *Procedia Manufacturing*, *8*, 715–722. https://doi.org/10.1016/j.promfg.2017.02.092

COMPUTING, CYBERSECURITY O. N. PRIVATE CLOUD. (2019). Measuring information security and cybersecurity on private cloud computing. *Journal of Theoretical and Applied Information Technology*, *96*(1).

Disterer, Georg. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(2).

Ella, Raches, Reddy, Siddarth, Blackwelder, William, Potdar, Varsha, Yadav, Pragya, Sarangi, Vamshi, Aileni, Vinay K., Kanungo, Suman, Rai, Sanjay, & Reddy, Prabhakar. (2021). Efficacy, safety, and lot-to-lot immunogenicity of an inactivated SARS-CoV-2 vaccine (BBV152): interim results of a randomised, double-blind, controlled, phase 3 trial. *The Lancet*, *398*(10317), 2173–2184.

Fathurohman, Adrian, & Witjaksono, R. Wahjoe. (2020). Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City). *Bulletin of Computer Science and Electrical Engineering*, *1*(1), 1–11. https://doi.org/10.25008/bcsee.v1i1.2

Kitsios, Fotis, Chatzidimitriou, Elpiniki, & Kamariotou, Maria. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability*, *15*(7), 5828.

Monev, Veselin. (2020). Organisational information security maturity assessment based on ISO 27001 and ISO 27002. *2020 International Conference on Information Technologies (InfoTech)*, 1–5. IEEE.

Shammugam, Inthrani, Samy, Ganthan Narayana, Magalingam, Pritheega, Maarop, Nurazean, Perumal, Sundresan, & Shanmugam, Bharanidharan. (2021). Information security threats encountered by Malaysian public sector data centers. *Indonesian Journal of Electrical Engineering and Computer Science*, *21*(3), 1820–1829.

Somepalli, Sri Harsha, Tangella, Sai Kishore Reddy, & Yalamanchili, Santosh. (2020). Information Security Management. *HOLISTICA–Journal of Business and Public Administration*, *11*(2), 1–16.

Walker, Alastair, McBride, Tom, Basson, Gerhard, & Oakley, Robert. (2012). ISO/IEC 15504 measurement applied to COBIT process maturity. *Benchmarking: An International Journal*, *19*(2), 159–176.

Yasin, Muhammad, Arman, Arry Akhmad, Edward, Ian Joseph M., & Shalannanda, Wervyan. (2020). Designing information security governance recommendations and roadmap using COBIT 2019 Framework and ISO 27001: 2013 (Case Study Ditreskrimsus Polda XYZ). *2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA*, 1–5. IEEE.

Zammani, Mazlina, & Razali, Rozilawati. (2016). Information security management success factors. *Advanced Science Letters*, *22*(8), 1924–1929. https://doi.org/10.1166/asl.2016.7746