Institut Riset dan Publikasi Indonesia (IRPI)
MALCOM: Indonesian Journal of Machine Learning and Computer Science
Journal Homepage: https://journal.irpi.or.id/index.php/malcom
Vol. 4 Iss. 2 April 2024, pp: 498-506
P-ISSN: 2797-2313 | ISSN(E): 2775-8575

Information Security Management System Assessment Model by Integrating ISO 27002 and 27004

Khafidh Sunny Al Fajri[1], Ruki Harwahyu[2]*

[1,2]Department of Electrical Engineering, Faculty of Engineering,
Universitas Indonesia, Indonesia

E-Mail: [1]khafidh.sunny@ui.ac.id, [2]ruki.h@ui.ac.id

Received Nov 8th 2023; Revised Dec 25th 2023; Accepted Feb 20th 2024
Corresponding Author: Ruki Harwahyu

Abstract

The rapid development of information and communication technology has also led to a significant increase in cybercrime activities. According to the Annual Cybersecurity Monitoring Report by the National Cyber and Cryptography Agency, there were 495 million instances of traffic anomalies or attempted attacks in 2020, which rose to 1.6 billion in 2021 in Indonesia. Implementing the ISO 27001 standard for information security management system (ISMS) can help mitigate these cyber-attack attempts. However, with various levels of resources and organizational commitment, different levels of ISMS maturity can be achieved. Therefore, there is a need for an ISMS assessment model. This is crucial, considering cyber incidents such as data breaches in organizations that have implemented or are certified with ISO 27001. This research proposed a concept of ISMS assessment model by integrating ISO 27002 and 27004 to a case study (Directorate XYZ), where the guidance function of ISO 27002 is transformed into assessment parameters and ISO 27004 for measuring performance. Using this model, the score of the case study's ISMS was found to be 53.925, which is still below the established standard of 80.

Keyword: Assessment Model, Information Security Management System, ISO 27001, ISO 27002, ISO 27004

1. INTRODUCTION

Information and communication technology development continues to grow, as well as cybercrimes, which are also increasing. In Indonesia, in 2020, based on the Annual Cybersecurity Monitoring Report by the National Cyber and Crypto Agency, traffic anomalies or suspicious attempts to attack cybersecurity have occurred 495 million times (495,337,202) and increased to 1.6 billion times (1,637,973,022) in 2021, whereas in 2022 it decreased to 976 million times (976,429,996) due to decreased traffic on sensors installed at ISPs and a decrease in the number of detected indicators of compromise. The traffic anomalies above include attacks such as malware, botnets, information leakage, mining pools, denial of services, exploitation, information gathering, trojan activity, web application attacks, advanced persistent threats, and others. Apart from traffic anomalies, there is also a trend of Data Breach cases where there have been 79,439 cases in 2020 and increased to 83,991 cases in 2021 in Indonesia [2]-[4].

One of the efforts in mitigating cyberattacks is to apply the ISO 27001 standard regarding information security management systems or ISMS. By implementing the ISO 27001 standard, agencies or organizations can obtain several benefits, such as ensuring information security in all forms (physical and digital), increasing resilience against cyberattacks, providing a centrally managed framework for securing organizational information security, and ensuring protection against risks. Technology-based or other threats can reduce the cost of spending on ineffective security technologies and maintain the integrity, confidentiality, and availability of organizational information [9].

However, with various levels of resources and organizational commitment, different levels of ISMS maturity can be achieved. Therefore, there is a need for an ISMS assessment model. This is crucial, considering cyber incidents such as data breaches in organizations that have implemented or are certified with ISO 27001, as seen in cases like Tokopedia (2020), Indihome (2022), Indonesia Syariah Bank (2023), Social Security Agency on Health (2023), General Elections Commission (2023), Civil Registry Service Office (2023), and so on [27]-[29].

In this research, a case study was conducted at one of the government agencies in Indonesia, namely the XYZ Directorate, which is engaged in state revenue through the customs and excise sector. Based on the results of an interview with one of the ISMS practitioners belonging to the XYZ Directorate, information was

obtained that the agency had implemented ISMS by the Decree of the Minister of Finance number 942/KMK.01/2019 concerning the Management of Information Security within the Ministry of Finance, which follows ISO 27001:2013 standard. In addition, another unit has carried out an internal audit, but only limited to the fulfilment of supporting documents [14].

So, it is required to model an assessment or audit of the ISMS that is more in-depth, not only for the completeness of the documents but also for conformity with the ISO 27001 standard. A paper review has been conducted on research papers focusing on the audit or assessment of information security management systems (ISMS). The results indicate that several other researchers have utilized existing frameworks such as COBIT5 [6],[18],[23],[24], System Security Engineering – Capability Maturity Model (SSE-CMM) [5],[20], ISO 27002:2013 [21],[22], Information Technology Infrastructure Library (ITIL) [15], and customized frameworks [1],[16],[25],[26].

Therefore, to diversify the methods for assessing ISMS and considering the issues encountered in the previous case study, modelling ISMS assessment is required by leveraging the integration of ISO 27002 and ISO 27004 standards. Unlike previous research, the proposed method employs the integration of two standards in assessing ISMS, using the reverse function of the implementation guidance from ISO 27002 as testing parameters and measuring the performance of information security controls using ISO 27004 standards. The advantage of this method is that every ISMS document that is tested will be verified as conforming to the ISO 27001 and ISO 27002 standards, both in terms of the document and how the ISMS document is implemented. Apart from that, by utilizing the ISO 27004 standard, the performance of each information security control can be obtained according to the ISO standard.

It is crucial as it allows referencing how each security control is implemented. ISO 27004 serves as a standard for measuring the performance or effectiveness of information security controls as per ISO 27001 [8].

2. MATERIALS AND METHOD

The research utilized a qualitative method approach during the phase of research scope identification and data collection, while a quantitative method approach was employed during the phase of design, measurement, and analysis of the information security management system assessment results. The research framework employed the PDCA (Plan, Do, Check, and Act) framework, a management method used to continuously enhance the performance and effectiveness of a process or system sustainably [19].

2.1. Plan Phase

In this phase, several steps were taken, including the identification and scope of the research, which aimed to determine which information security management systems would be the subject of the study. In the case study, an interview was conducted with one of the practitioners of the ISMS. The research was limited only to Annex A of ISO 27001, as it contains technical aspects related to information security. Next, the data collection was conducted by observing the elements of the ISMS case study, including the ISMS case study worksheets, which aligned with the ISO 27001:2022 standard, and determining which information security controls would be tested. Finally, a new set of worksheets was prepared by adopting the previous ISMS case study worksheets. This was done to facilitate the process of assessing the ISMS case study.

2.2. Do Phase

The assessment workflow of the ISMS case study was initiated, and a research proposal was made to utilize the integration of ISO 27002 and ISO 27004 standards for the assessment method. The ISMS assessment was performed using the newly prepared worksheets from the previous phase and was conducted in collaboration with the ISMS case study practitioner. Each tested information security control was ensured to comply with the ISO 27001 standard, and then it was further evaluated using the ISO 27002 standard (a guideline for ISO 27001 implementation). The reverse function of the ISO 27002 guidelines was used as one of the parameters for the ISMS assessment. A score of 0 was given if the tested control did not comply, and a score was assigned according to the ISO 27004 standard if it was compliant. Below is an example of the assessment of information security controls in the case study:

The case study involved Document A, which, upon closer examination, was found to follow ISO 27001:2022 standard's information security control A.5.1 Policies for information security. Previously, in ISO 27001:2013, this control was divided into A.5.1.1 and A.5.1.2. It was also noted that this control had sample calculations according to Annex B.3 Policy Review in ISO 27004 standard for control A.5.1.2.

Subsequently, in collaboration with the ISMS case study practitioner, Document A was observed and analyzed to determine if its content aligned with the implementation guidelines of the ISO 27002 standard. For control A.5.1.1 Policies for information security, Document A was found to comply with ISO 27002 standard, as it included information such as information security definitions, role determination, responsibilities, etc. The ISMS case study practitioner was also asked whether Document A underwent periodic reviews.

Due to the absence of sample calculations for control A.5.1.1 in Annex B of ISO 27004, a predetermined calculation method was used (Annex C of ISO 27004). According to this method, if the control is not fulfilled or is empty, it is given a score of 0. If the supporting data for the control is available but not implemented, it is given a score of 50. When the supporting data for the control is available and implemented, it is assigned a score of 80. Finally, if the supporting data for the control is implemented and reviewed periodically, it is given a score of 100. Based on this calculation, a score of 80 was obtained for security control A.5.1.1. As for security control A.5.1.2, review of the policies for information security, ISO 27002 standard states that each policy requires an owner responsible for its development, review, and evaluation. According to Annex B of ISO 27004, specifically B.3 Policy review, the scoring formula for this control is (Number of information security policies reviewed in previous years/number of information security policies in place) x 100. The target achievements are Green >80%, Orange >=40%, and Red < 40%.

The case study practitioner stated that periodic reviews related to Document A had never been conducted, resulting in security control A.5.1.2 being assigned a score of 0 as it did not comply with ISO 27002 standard and could not proceed to the following assessment stage using ISO 27004. Since ISO 27004:2016 still references ISO 27001:2013, the assessment followed each information security control in ISO 27001:2013. The scores were then combined and averaged to obtain the final score. Thus, it becomes (80 + 0)/2 = 40 for the final score of security control A.5.1 Policies for information security. The assessment process flow for the ISMS can be seen in Figure 1 and Figure 2.

2.3. Check Phase

The analysis of the previous ISMS assessment results is initiated. The calculated scores of information security controls will be grouped according to the ISO 27001:2022 standard's categories: Organizational, People, Physical, and Technology. The maturity level of the ISMS is then determined based on the ISO 27004 standard, where Annex B specifies the minimum targets for each information security control. A minimum standard of 80 (from averaging all minimum target: (80 + 90 + 80 + 70 + 95 + 60 + 100 + 90 + 60 + 75 + 100 + 20) / 12=76.67 round up to 80) is set for each information security control to facilitate the ISMS assessment based on the target data from Annex B of ISO 27004:2016, as shown in Table 1.

Table 1. The Targets of Annex B ISO 27004

Annex A ISO 27001:2013	Annex B ISO 27004:2016	Target	Minimum Target
A5.1.2	B.3 Policy Review	Green > 80, Orange >= 40 & Red < 40	80
A7.2.1	B.13 Information Security Awareness Compliance	Minimal >90%	90
A.9.3.1	B.17 Password Quality - Automated	Target 90%, Minimal 80%	80
A.9.2.5	B.18 Review of user access rights	Target 90%, Minimal 70%	70
A16.1.1	B.33 Security Incident Management Effectiveness	Indicator 1 > 0.9 & Indicator 2 (Trend) is Stable or Upward	NA
A16.1.4-5-7	B.34 Security incidents trend	Green < 1.0 (Comparison of incident Trends in different timeframe)	NA
A16.1.6	B.9 Learning from information security incidents	Target > Organization Threshold	NA
A18.2.1	B.6 Audit Programme	Target > 95%	95
	B.36 ISMS review process	Target 0.8, Minimum 0.6	60
A18.2.3	B.37 Vulnerability coverage	Target 100%	100
A.7.2.2	B.12 Information security training	Target 90%	90
A16.1.3	B.35 Security event reporting	At least one security event per security role per year	NA
A11.1.2	B.19 Physical entry controls system evaluation	Value 3 from 5 (60%)	60
A11.1.6	B.20 Physical entry controls effectiveness	Target < 1 (Comparison of physical incident compare with previous year)	NA
A12.2.1	B.23 Protection against malicious code	Downward Trend or 0	NA
	B.24 Anti-malware	Target 0	NA
A12.6.1	B.29 Pentest and vulnerability assessment	Target > 75%	75
A18.2.3	B.37 Vulnerability coverage	Target 100%	100
A17.2.1	B.25 Total Availability	Organization's SLA	NA
A12.4.1	B.27 Log files review	Target > 20%	20
A13.1.3	B.26 Firewall Rules	Target 0	NA
A12.1.2	B.22 Change Management	Refers to Change Management Guidelines	NA

2.4 Act Phase

The results of the ISMS assessment will be communicated to the management of the case study, along with recommendations to address the information security controls that still need to be fulfilled. In addition, the following steps regarding the ISMS assessment results will determine whether it requires revision for retesting or awaits the decision of the case study management.

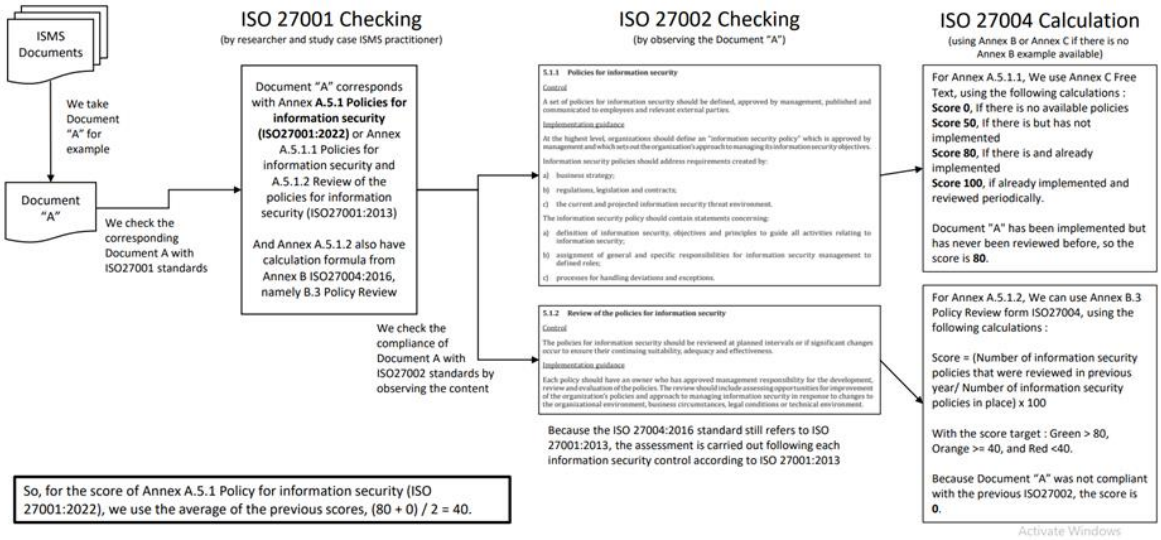


Figure. 1. Example of Assessment of Document A from ISMS Case Study.

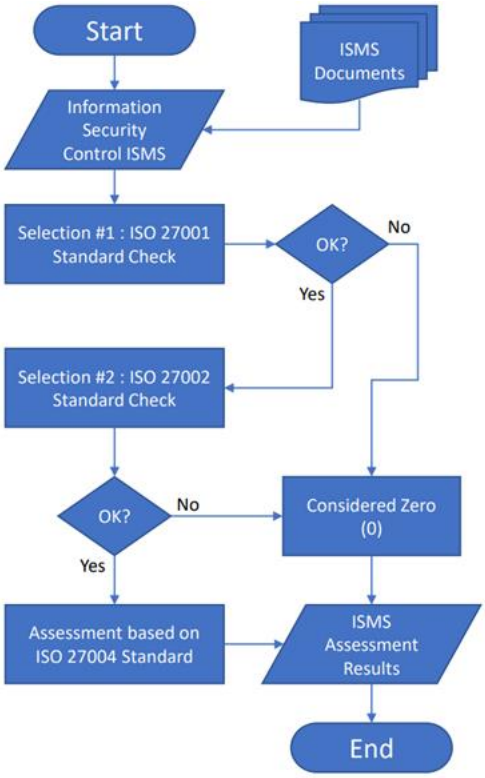


Figure. 2. Overall ISMS Assessment Workflow

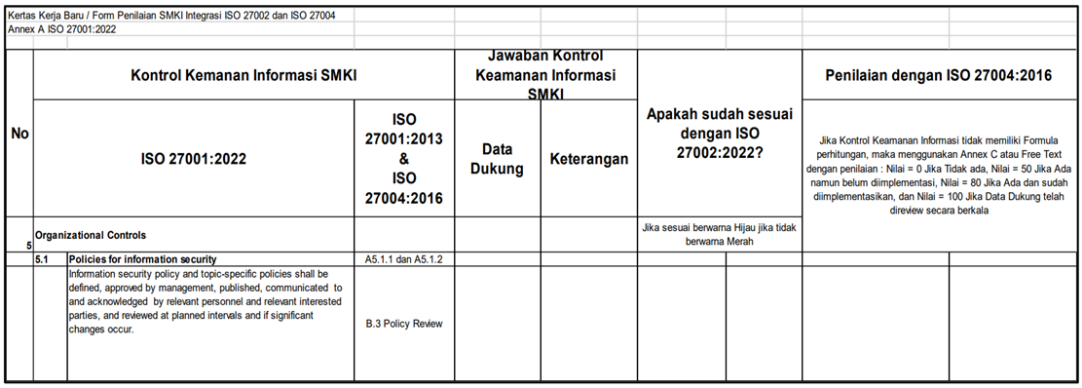
3. RESULTS AND DISCUSSION

3.1 Plan Phase

An interview was conducted with one of the ISMS practitioners from the case study. The practitioner mentioned that the ISMS being assessed is the Customs and Excise Information System ISMS owned by the case study. Additionally, several controls were not included in the testing process because another party had

already handled them. Furthermore, new information security controls based on the ISO 27001:2022 standard have not been implemented, so they were neither included in the assessment.

By adopting the ISMS case study's previous worksheets, a corresponding column between ISO 27001:2013 and ISO 27002:2022 was added, along with the addition of columns for ISO 27002 and ISO 27004 testing parameters, resulting in a new set of worksheets as shown in Figure 3.



Kertas Kerja Baru / Form Penilaian SMKI Integrasi ISO 27002 dan ISO 27004
Annex A ISO 27001:2022

No	Kontrol Kemanan Informasi SMKI		Jawaban Kontrol Keamanan Informasi SMKI		Apakah sudah sesuai dengan ISO 27002:2022?		Penilaian dengan ISO 27004:2016	
	ISO 27001:2022	ISO 27001:2013 & ISO 27004:2016	Data Dukung	Keterangan			Jika Kontrol Keamanan Informasi tidak memiliki Formula perhitungan, maka menggunakan Annex C atau Free Text dengan penilaian : Nilai = 0 Jika Tidak ada, Nilai = 50 Jika Ada namun belum diimplementasi, Nilai = 80 Jika Ada dan sudah diimplementasikan, dan Nilai = 100 Jika Data Dukung telah direview secara berkala	
5	Organizational Controls				Jika sesuai berwarna Hijau jika tidak berwarna Merah			
5.1	Policies for information security	A5.1.1 dan A5.1.2						
	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	B.3 Policy Review						

Figure. 3. The New ISMS Assessment Worksheet with ISO 27002 and ISO 27004 Integration.

In the figure, the matching of columns between ISO 27001:2013 and ISO 27002:2022 is used to compare the correlation between information security controls. ISO 27004:2016 shows that these controls have sample calculations according to Annex B. Annex C or free text is used for controls without sample calculations, following the assessment rules mentioned earlier

3.2 Do Phase

The ISMS assessment was conducted through interviews and observations, accompanied by the ISMS case study practitioner. The assessment began with explanations of each information security control based on ISO 27001:2022. Additionally, an explanation of the usage and purpose of each column in the new assessment worksheets was provided. Subsequently, adjustments were made for each information security control owned by the case study that still adhered to the ISO 27001:2013 standard. After the adjustments were made, each control was checked for supporting data, including regulations, procedures, manuals, agreements, etc., to determine whether their contents aligned with the implementation guidelines from the ISO 27002 standard. Controls that did not comply were assigned a score of 0, while those that complied were evaluated according to the ISO 27004 standard.

Lastly, to determine the final score for each control, the average score of each control was calculated, and then these averages were averaged again to obtain the category score for the group of information security controls. Below is a summary of the ISMS case study assessment results, which can be seen in Table 2.

3.3 Check Phase

Observing the results, it is evident that the case study has the weakest score in the Organizational Control group, indicating that implementing information security controls within the organizational aspect needs to be better executed. Furthermore, the case study's ISMS practitioner also mentioned similar concerns, considering that the organization comprises individuals with different competencies, high work intensity, and information security is yet to be a primary concern. Therefore, building information security awareness or establishing an ISMS that aligns with the standards takes time and effort. On the other hand, the Physical Control group achieved the highest score of 82.9. This is due to some aspects of physical security controls being assisted by other units or departments. Meanwhile, the ISMS maturity level can be determined by averaging all the scores of the information security control groups, resulting in a score of 53.925, which is still below the established standard of 80.

3.4 Act Phase

The results of the assessment analysis and the ISMS maturity score have been communicated to the management of the case study. Additionally, several suggestions or recommendations have been provided to the case study if they intend to improve their ISMS for re-evaluation. However, the decision regarding improving the ISMS primarily rests with the top management of the case study.

4. CONCLUSION

In this research, the assessment of the ISMS based on ISO 27001:2022 with the integration of ISO 27002 and ISO 27004, especially in the Annex A section of the case study, was successfully carried out. By

using this method, more in-depth results are obtained, not only focusing on the completeness of the supporting data documents but also the contents of the supporting data documents which are also in accordance with the ISO 27002 standard. The results of the assessment showed that the scores for the Organizational Control group were 32.6, the People Control group were 58.8, the Physical Control group was 82.9, the Technological Control group were 41.4, and the overall ISMS maturity score was 53.925, which is below the established standard of 80. Despite these findings, several suggestions or recommendations have been conveyed to the top management of the case study regarding the controls that do not comply with the requirements. These recommendations are intended to be addressed to improve the ISMS in the future.

Table 2. Summary of Case Study ISMS Assessment Results

ISO 27001:2022		ISO 27001:2013	ISO 27002:2022			ISO 27004:2016			Mark (Average)	Final
Organizational Controls										
5.1	Policies for information security	A5.1.1 and A5.1.2	√	×		80	0		40,0	32,6
5.2	Information security roles and responsibilities	A6.1.1	√			80			80,0	
5.3	Segregation of duties	A6.1.2	√			80			80,0	
5.4	Management responsibilities	A7.2.1	√			100			100,0	
5.5	Contact with authorities	A6.1.3	×			0			0,0	
5.6	Contact with special interest groups	A6.1.4	√			80			80,0	
5.8	Information security in project management	A6.1.5 and A14.1.1	×	×		0	0		0,0	
5.9	Inventory of information and other associated assets	A8.1.1 and A8.1.2	×	×		0	0		0,0	
5.10	Acceptable use of information and other associated assets	A8.1.3 and A8.2.3	√	×		80	0		40,0	
5.11	Return of assets	A8.1.4	√			80			80,0	
5.12	Classification of information	A.8.2.1	×			0			0,0	
5.13	Labelling of information	A8.2.2	×			0			0,0	
5.14	Information transfer	A13.2.1, A13.2.2 and A13.2.3	×	√	×	0	80	0	26,7	
5.15	Access control	A9.1.1 and A9.1.2	×	√		0	80		40,0	
5.16	Identity management	A9.2.1	×			0			0,0	
5.17	Authentication information	A9.2.4, A9.3.1 and A9.4.3	×	×	×	0	0	0	0,0	
5.18	Access rights	A9.2.2, A9.2.5 and A9.2.6	×	×	×	0	0	0	0,0	
5.24	Information security incident management planning and preparation	A16.1.1	×			0			0,0	
5.25	Assessment and decision on information security events	A16.1.4	×			0			0,0	
5.26	Response to information security incidents	A16.1.5	×			0			0,0	
5.27	Learning from information security incidents	A16.1.6	√			100			100,0	
5.28	Collection of evidence	A16.1.7	×			0			0,0	
5.29	Information security during disruption	A17.1.1, A17.1.2 and A17.1.3	√	√	√	80	80	80	80,0	
5.31	Legal, statutory, regulatory, and contractual requirements	A18.1.1 and A18.1.5	×	×		0	0		0,0	
5.32	Intellectual property rights	A18.1.2	×			0			0,0	

	ISO 27001:2022	ISO 27001:2013	ISO 27002:2022			ISO 27004:2016			Mark (Average)	Final
5.33	Protection of records	A18.1.3	×			0			0,0	
5.34	Privacy and protection of personal identifiable information (PII)	A18.1.4	×			0			0,0	
5.35	Independent review of information security	A18.2.1	√			100			100,0	
5.36	Compliance with policies, rules and standards for information security	A18.2.2 and A18.2.3	×	√		0	100		50,0	
5.37	Documented operating procedures	A12.1.1	√			80			80,0	
			People Controls							
6.1	Screening	A7.1.1	×			0			0,0	
6.2	Terms and conditions of employment	A7.1.2	√			80			80,0	
6.3	Information security awareness, education, and training	A7.2.2	√			100			100,0	
6.4	Disciplinary process	A7.2.3	√			80			80,0	
6.5	Responsibilities after termination or change of employment	A7.3.1	×			0			0,0	58,8
6.6	Confidentiality or non-disclosure agreements	A13.2.4	√			80			80,0	
6.7	Remote working	A6.2.2	√			80			80,0	
6.8	Information security event reporting	A16.1.2 and A16.1.3	×	√		0	100		50,0	
			Physical Controls							
7.1	Physical security perimeters	A11.1.1	√			100			100,0	
7.2	Physical entry	A11.1.2 and A11.1.6	√			100			100,0	
7.3	Securing offices, rooms and facilities	A11.1.3	√			100			100,0	
7.5	Protecting against physical and environmental threats	A11.1.4	√			100			100,0	
7.7	Clear desk and clear screen	A11.2.9	√			80			80,0	82,9
7.8	Equipment siting and protection	A11.2.1	√			100			100,0	
7.10	Storage media	A8.3.1, A8.3.2, A8.3.3 and A11.2.5	×	×	×	0	0	0	0,0	
			Technological controls							
8.1	User end point devices	A6.2.1 and A11.2.8	×	×		0	0		0,0	
8.2	Privileged access rights	A9.2.3	√			80			80,0	
8.3	Information access restriction	A9.4.1	√			80			80,0	
8.4	Access to source code	A9.4.5	×			0			0,0	
8.5	Secure authentication	A9.4.2	×			0			0,0	
8.6	Capacity management	A12.1.3	√			80			80,0	
8.7	Protection against malware	A12.2.1	√			100			100,0	
8.8	Management of technical vulnerabilities	A12.6.1 and A18.2.3	√	√		100	100		100,0	41,1
8.13	Information backup	A12.3.1	√			80			80,0	
8.14	Redundancy of information processing facilities	A17.2.1	√			100			100,0	
8.15	Logging	A12.4.1, A12.4.2 and A12.4.3	×	×	×	0	0	0	0,0	

ISO 27001:2022		ISO 27001:2013	ISO 27002:2022								ISO 27004:2016				Mark (Average)	Final
8.17	Clock synchronization	A12.4.4	√								80				80,0	
8.18	Use of privileged utility programs	A9.4.4	×								0				0,0	
8.19	Installation of software on operational systems	A12.5.1 and A12.6.2	×	×							0	0			0,0	
8.20	Networks security	A13.1.1	×								0				0,0	
8.21	Security of network services	A13.1.2	√								100				100,0	
8.22	Segregation of networks	A13.1.3	×								0				0,0	
8.24	Use of cryptography	A10.1.1 and A10.1.2	×	×							0	0			0,0	
8.25	Secure development life cycle	A14.2.1	√								80				80,0	
8.26	Application security requirements	A14.1.2 and A14.1.3	×	×							0	0			0,0	
8.27	Secure system architecture and engineering principles	A14.2.5	×								0				0,0	
8.29	Security testing in development and acceptance	A14.2.8 and A14.2.9	√	√							100	80			90,0	
8.30	Outsourced development	A14.2.7	×								0				0,0	
8.31	Separation of development, test and production environments	A12.1.4 and A14.2.6	√	×							80	0			40,0	
8.32	Change management	A12.1.2, A14.2.2, A14.2.3 and A14.2.4	×	×	×	×					0	0	0	0	0,0	
8.33	Test information	A14.3.1	×								0				0,0	
8.34	Protection of information systems during audit testing	A12.7.1	√								100				100,0	

ACKNOWLEDGMENTS

This work was fully funded by the Ministry of Communication and Information Technology, Indonesia – Domestic Masters Scholarship Program. Thanks to the XYZ Directorate for their cooperation during this research.

REFERENCES

[1] Achmadi, D., Suryanto, Y. and Ramli, K. "On Developing Information Security Management System (ISMS) framework for ISO 27001-based data center", 2018 International Workshop on Big Data and Information Security (IWBIS) [Preprint]. doi:10.1109/iwbis.2018.8471700, 2018.

[2] BSSN, 2020 Cyber Security Monitoring Results Report, BSSN Cloud. Available at: https://cloud.bssn.go.id/s/ZSdfebRTKW7p8nW, 2021. (Accessed: 19 December 2022).

[3] BSSN, 2021 Cyber Security Monitoring Annual Report, BSSN Cloud. Available at: https://cloud.bssn.go.id/s/Lyw8E4LxwNiJoNw, 2022. (Accessed: 20 December 2022).

[4] BSSN, Indonesia's Cybersecurity Landscape in 2022, BSSN Cloud. Available at: https://cloud.bssn.go.id/s/3S5B2ToddAFsiXs, 2023. (Accessed: 27 February 2023).

[5] Eskaluspita, AY, "ISO 27001:2013 for Laboratory Management Information System at School of Applied Science Telkom University", IOP Conference Series: Materials Science and Engineering, 879(1), p. 012074.doi:10.1088/1757-899x/879/1/012074, 2020.

[6] Fathoni, Simbolon, N. and Yunika Hardiyanti, D., "Security audit on loan Debit Network Corporation system using COBIT 5 and ISO 27001: 2013", Journal of Physics: Conference Series, 1196, p. 012033.doi:10.1088/1742-6596/1196/1/012033, 2019.

[7] ISO, ISO/IEC 27002:2013 Information security, cybersecurity and privacy protection — Information security control, ISO. Available at: https://www.iso.org/standard/54533.html, 2022. (Accessed: 28 November 2022).

[8] ISO, ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation, ISO. Available at: https://www.iso.org/standard/64120.html, 2022. (Accessed: 29 November 2022).

[9] ISO, ISO/IEC 27001 and related standards Information security management, ISO. Available at: https://www.iso.org/isoiec-27001-information-security.html, 2022. (Accessed: 11 November 2022).
[10] ISO, ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, ISO. Available at: https://www.iso.org/standard/54534.html, 2022. (Accessed: 12 November 2022).
[11] ISO, ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, ISO. Available at: https://www.iso.org/standard/82875.html, 2022. (Accessed: 20 November 2022).
[12] ISO, ISO/IEC 27002:2022 - Information technology - Security techniques - Code of practice for information security controls, ISO. Available at: https://www.iso.org/standard/78342.html, 2022. (Accessed: 20 November 2022).
[13] Indonesia Ministry of Finance, Decree of the Minister of Finance Number 942/KMK.01/2019 concerning Management of Information Security within the Ministry of Finance, Jakarta, 2019.
[14] Indonesia Ministry of Finance, Regulation of the Minister of Finance Number 118/010/2021 concerning the Organization and Work Procedure of the Ministry of Finance, Jakarta, 2021.
[15] Kholis Gunawan, N., Budiarto Hadiprakoso, R. and Kabetta, H, "Comparative study between the integration of ITIL and ISO / IEC 27001 with the integration of COBIT and ISO / IEC 27001", IOP Conference Series: Materials Science and Engineering, 852(1), p. 012128.doi:10.1088/1757-899x/852/1/012128, 2020.
[16] Monev, V, "Organizational Information Security Maturity Assessment based on ISO 27001 and ISO 27002", 2020 International Conference on Information Technologies (InfoTech) [Preprint]. doi:10.1109/infotech49733.2020.9211066, 2020.
[17] Nasir A, Arshah R.A, Ab Hamid M.R, and Fahmy S, "An analysis on the dimensions of information security culture concept: A Review", Journal of Information Security and Applications, 44, pp. 12–22. doi:10.1016/j.jisa.2018.11.003, 2019.
[18] Prapenan, GG and Pamuji, GC, "Information System Security Analysis of XYZ Company using COBIT 5 framework and ISO 27001:2013", IOP Conference Series: Materials Science and Engineering, 879(1), p. 012047.doi:10.1088/1757-899x/879/1/012047, 2020.
[19] R. Basu, The Green Six Sigma Handbook: A Complete Guide for Lean Six Sigma Practitioners and Managers. New York: Productivity Press, 2022.
[20] Nurbojatmiko, A. Susanto, and E. Shobariah, "Assessment of ISMS based on standard ISO/IEC 27001:2013 at DISKOMINFO depok city," 2016 4th International Conference on Cyber and IT Service Management, 2016. doi:10.1109/citsm.2016.7577471
[21] N. Al-shaibany, "A model for enhancing the information security management systems in Yemen banks," Sana'a University Journal of Applied Sciences and Technology, vol. 1, no. 1, 2023. doi:10.59628/jast.v1i1.14
[22] R. Santi, A. I. Alfresi, and B. Octariana, "Information system security audit using ISO/IEC 27002:2013 at University of XXX," Jurnal Teknik Informatika (Jutif), vol. 4, no. 4, pp. 733–750, 2023. doi:10.52436/1.jutif.2023.4.4.689
[23] W. Adi Nugroho and R. Sutomo, "Evaluation of Information System Governance Capability Level of engineering construction services firm using COBIT framework 5," International Journal of Science, Technology & Management, vol. 4, no. 4, pp. 1015–1022, 2023. doi:10.46729/ijstm.v4i4.879
[24] L. Sikman, T. Latinovic, N. Sarajlic, and G. Sikanjic, "A model of sustainable information security management system in Higher Education Institutions," Journal of Physics: Conference Series, vol. 2540, no. 1, p. 012003, 2023. doi:10.1088/1742-6596/2540/1/012003
[25] A. Fathurohman and R. W. Witjaksono, "Analysis and design of information security management system based on ISO 27001: 2013 using Annex Control (Case Study: District of Government of Bandung City)," Bulletin of Computer Science and Electrical Engineering, vol. 1, no. 1, pp. 1–11, 2020. doi:10.25008/bcsee.v1i1.2
[26] Fonseca-Herrera OA, Rojas AE, Florez H, "A model of an information security management system based on NTC-ISO/IEC 27001 standard," IAENG Int. J. Comput. Sci, 2021.
[27] CNN Indonesia, "10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-Ramai Bantah," teknologi, https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah (accessed Dec. 10, 2023).
[28] CNN Indonesia, "4 Kasus Kebocoran data di semester I 2023, Mayoritas Dibantah," teknologi, https://www.cnnindonesia.com/teknologi/20230720060802-192-975421/4-kasus-kebocoran-data-di-semester-i-2023-mayoritas-dibantah (accessed Dec. 10, 2023).
[29] CNN Indonesia, "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor Dan Dijual," teknologi, https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual (accessed Dec. 10, 2023).